



L3 Switch Series

OS6256, OS7156, OS8132

CLI Reference Guide

Preface

Manual Instruction

This manual describes the commands for configuring various functions of the switch, covering the function, format, parameters, default value, view, usage guidelines, and usage example of each command. This manual helps you quickly find and understand information about configuration commands.

Intended Readers

This manual is intended for

- Project designers
- Product provisioning engineers
- Product maintenance engineers

Content Introduction

Chapter	Summary
Chapter 1 Introduction to Command Configuration Views	Introduces the command configuration views in the system.
Chapter 2 Basic Commands	Introduces the commands for configuring basic functions of the system, including basic configuration, user terminal configuration, file system configuration, system configuration files, file uploading and downloading configuration, and Telnet or SSH login.
Chapter 3 Ethernet Commands	Introduces commands for configuring the following functions: Ethernet interface, MAC table, ARP, link aggregation, VLAN, VLAN mapping, VLAN STACKING, QinQ, ARP agent, MAM, port security, port isolation, and storm control.
Chapter 4 IP Commands	Introduces commands for configuring IPv4/IPv6 addresses and DHCP functions.
Chapter 5 Routing Commands	Introduces commands for routing configuration.
Chapter 6 QoS Commands	Introduces the commands for configuring QoS functions, including traffic policing, traffic shaping, queue scheduling, and congestion control.
Chapter 7 Multicast Commands	Introduces the commands for configuring multicast services, including IGMP Snooping, IGMP, and MLD Snooping.
Chapter 8 Service Security	Introduces the commands for configuring security functions on the

Chapter	Summary
Commands	Switch, including Time-range, ACL, Anti-attack, AAA/Radius, 802.1x, and defense.
Chapter 9 Reliability Commands	Introduces the commands for configuring reliability functions, including MSTP and BFD.
Chapter 10 Device Management Commands	Introduces the commands used for device management.
Chapter 11 O&M Commands	Introduces configuration commands related to O&M and network management.
Chapter 12 VPN Commands	Introduces the VPN configuration commands on the Switch.
Chapter 13 Data Center Feature Commands	Introduces scenarios such as using the VXLAN technology for virtualization and serving the data center.
Chapter 14 Virtualization Configuration Commands	Introduces the Virtualization configuration commands on the Switch.

Version Updates

Document Version	Update Description
A/02	First release

Conventions

The following introduces the general format, symbol conventions, keyboard / mouse operations and signs.

1. General format

Typeface	Description
Times New Roman	Standard font for manual text including Arabic numerals.
Bold	Chapter / section names, menus, menu options, radio button names, check boxes, drop-down lists, dialog box names and window names.

2. Symbol conventions

Typeface	Description
Bold	Keywords (fixed contents) in command lines.
<i>Italic</i>	Parameters (variables) in command lines.
[]	Optional part in command configuration.
{ x y ... }	Select only one from multiple options.
[x y ...]	Select one or none from multiple options.
{ x y ... }*	Select at least one from multiple options.
[x y ...]*	Select one, multiple or none from multiple options.
#	The following is note.

3. Keyboard operation convention

Typeface	Description
Characters with angle brackets	Means keyboard typing names or button names, e.g., <Enter>, <Tab>, <Backspace>, <a> respectively mean keyboard enter, tab, backspace and lowercase character "a".
<Key 1+ Key 2>	Means pressing two or more keys at the same time, e.g., <Ctrl + Alt+ A> means pressing "Ctrl", "Alt" and "A" at the same time.
< Key 1, Key 2>	Means pressing key 1 first, release it and then press key 2, e.g., <Alt, F> means pressing "Alt" first, then release it and then press "F".

4. Mouse operation conventions

Typeface	Description
Click	Means clicking the primary mouse button (left button) once.
Double-click	Means quickly clicking the primary mouse button (left button) twice.
Right-click	Means clicking the secondary mouse button (right button) once.
Drag	Means pressing and holding the primary mouse button (left button) and moving the mouse.

5. Signs

This manual uses the following three signs to emphasize what needs attention during operation, installation or maintenance.



Note,



Caution,



Warning

Contents

Chapter 1 Introduction to Command Configuration Views	1
1.1 Command Line Interface.....	1
1.2 Features of Command Configuration Views	1
Chapter 2 Basic Commands.....	7
2.1 Basic Configuration Commands	7
2.1.1 auth-degenerate {enable disable}	7
2.1.2 case-sensitive.....	8
2.1.3 clear configuration.....	8
2.1.4 cls	9
2.1.5 configure.....	10
2.1.6 command-privilege level view	10
2.1.7 debug cli	12
2.1.8 debug clock	12
2.1.9 disable	13
2.1.10 enable	14
2.1.11 enable password.....	14
2.1.12 end	15
2.1.13 exit.....	16
2.1.14 header login	17
2.1.15 help	18
2.1.16 hostname.....	19
2.1.17 list.....	20
2.1.18 ping ping6.....	21
2.1.19 ping vxlan vni.....	23
2.1.20 quit.....	24
2.1.21 reset recycle.....	25
2.1.22 reboot.....	25
2.1.23 reboot {at in}	26
2.1.24 reboot cancel	27

2.1.25 show history	28
2.1.26 show module version.....	29
2.1.27 show privilege	30
2.1.28 show reboot	30
2.1.29 show system	31
2.1.30 show version.....	32
2.1.31 show	33
2.1.32 write file	34
2.1.33 password.....	35
2.1.34 show login-type count	36
2.1.35 show user config.....	36
2.1.36 show user glob-info	37
2.1.37 show user verbose	38
2.1.38 username group	39
2.1.39 username group password	40
2.1.40 username domain.....	42
2.1.41 user pwd-complex	43
2.1.42 user pwd-length	44
2.1.43 user fail-count.....	44
2.1.44 user same-name-pwd	45
2.1.45 username fail-count	46
2.1.46 username reauth-interval	46
2.1.47 username ftp-directory	47
2.1.48 who.....	48
2.1.49 temporary-password	49
2.1.50 show management acl	49
2.1.51 show counter	50
2.1.52 show command-privilege	51
2.1.53 send message.....	52
2.1.54 management acl management acl6	52
2.1.55 check temporary-password.....	54
2.1.56 clock set.....	55

2.1.57 clock summer-time	56
2.1.58 clock timezone.....	58
2.1.59 command authorization aaa method.....	59
2.1.60 command authorization config-command.....	60
2.1.61 trace trace6.....	61
2.1.62 trace vxlan vni	62
2.1.63 debug soa.....	63
2.1.64 show soa subsys	64
2.1.65 show soa global	64
2.1.66 user pwd-live	65
2.1.67 user pwd-live-prompt	66
2.1.68 user {telnet ssh} max-count.....	67
2.1.69 debug command-privilege.....	67
2.2 User Terminal Configuration Commands.....	68
2.2.1 color.....	68
2.2.2 debug delay	69
2.2.3 enable authentication.....	70
2.2.4 terminal color	70
2.2.5 terminal length.....	71
2.2.6 terminal monitor	72
2.2.7 terminal timeout	73
2.2.8 terminal language	74
2.2.9 temporary-password.....	75
2.2.10 monitor	75
2.2.11 language.....	76
2.2.12 length.....	77
2.2.13 line console.....	78
2.2.14 line vty.....	78
2.2.15 kill vty	79
2.2.16 show lines.....	80
2.2.17 show line config	81
2.2.18 show vty	82

2.2.19 timeout.....	83
2.2.20 unlock-command vty	84
2.2.21 mmi-mode	85
2.3 File System Configuration Commands	86
2.3.1 boot password recovery	86
2.3.2 cd	86
2.3.3 copy	87
2.3.4 del	88
2.3.5 dir	89
2.3.6 ls tree	90
2.3.7 mkdir	92
2.3.8 move	92
2.3.9 pwd.....	93
2.3.10 remove.....	94
2.3.11 rename	94
2.3.12 rmdir	95
2.3.13 type.....	96
2.3.14 xcopy	99
2.3.15 zero	100
2.3.16 find	101
2.4 System Configuration File Commands	102
2.4.1 copy startup-config running-config.....	102
2.4.2 compare configuration.....	103
2.4.3 erase startup-config	104
2.4.4 upgrade {os config fpga} system.....	105
2.4.5 show running-config.....	106
2.4.6 show startup-config	107
2.4.7 del os-file.....	109
2.4.8 show os-file	110
2.4.9 remote upgrade {enable disable}	110
2.5 File Uploading and Downloading Configuration Commands	111
2.5.1 tftp get	111

2.5.2 tftp put	112
2.5.3 tftpd	114
2.5.4 debug tftp.....	115
2.5.5 debug l2tftpd	115
2.5.6 debug ftpd.....	116
2.5.7 ftp put	117
2.5.8 ftp get	119
2.5.9 ftp delete.....	120
2.5.10 ftpd	122
2.5.11 ftp6 get.....	122
2.5.12 ftp6 put	124
2.5.13 ftp6 delete.....	126
2.5.14 tftpd6	127
2.5.15 tftp6 get	128
2.5.16 tftp6 put	130
2.5.17 debug ftpd6.....	131
2.5.18 ftpd6	132
2.5.19 file export tftp.....	133
2.6 Telnet and SSH Configuration Commands	134
2.6.1 debug ssh.....	134
2.6.2 debug sftp	134
2.6.3 key.....	135
2.6.4 sshd.....	136
2.6.5 sshd auth.....	136
2.6.6 ssh keygen	137
2.6.7 ssh user key begin	138
2.6.8 sftp-server {enable disable}	139
2.6.9 sshd login-grace-time	140
2.6.10 telnet crlf	140
2.6.11 telnetd	141
2.6.12 telnet6d.....	142
2.6.13 telnet telnet6	143

2.6.14 show ssh config	144
Chapter 3 Ethernet Commands.....	146
3.1 Interface Configuration Commands	146
3.1.1 switch	146
3.1.2 debug {rx tx rxpkt txpkt config event stats none}	147
3.1.3 debug ifm.....	147
3.1.4 alias	149
3.1.5 shutdown	150
3.1.6 reset counter	151
3.1.7 interface loopback	152
3.1.8 interface null.....	152
3.1.9 show interface null config.....	153
3.1.10 error-down auto-recovery cause link-flap interval	154
3.1.11 port link-flap interval.....	155
3.1.12 crc-error protection interval.....	155
3.1.13 port crc-error threshold.....	156
3.1.14 port crc-error error-down {enable disable}	157
3.1.15 error-down auto-recovery cause crc-error interval	158
3.1.16 error-down auto-recovery cause port-security interval.....	159
3.1.17 error-down auto-recovery cause storm-suppression interval.....	160
3.1.18 port link-flap protection {enable disable}	161
3.1.19 port link-flap threshold.....	161
3.1.20 flow-stat interval	162
3.1.21 show linkflap config.....	163
3.1.22 port flow-stat interval	164
3.1.23 debug linkflap.....	164
3.1.24 error-down auto-recovery cause mac-address-flapping interval	165
3.1.25 flow-control.....	166
3.1.26 flow-statistic include-interframe	167
3.1.27 interface mgt-eth	168
3.1.28 mtu.....	168
3.1.29 port-down holdoff-time	169

3.1.30 port-up delay-time	170
3.1.31 shutdown	171
3.1.32 show interface unit-number	172
3.1.33 show interface	173
3.1.34 show interface statistic	176
3.1.35 work-mode	178
3.1.36 interface	179
3.1.37 rate-limit	180
3.1.38 rate-limit out threshold	181
3.1.39 show interface ethernet brief	182
3.1.40 link-flap protection {start stop}	183
3.1.41 port mode	184
3.1.42 fec mode	185
3.1.43 reset counter interface	185
3.1.44 show interface error-down	187
3.1.45 show crc-error config	187
3.1.46 show l3int bridge-domain	188
3.1.47 show l3int ethernet	189
3.1.48 show l3int eth-trunk	189
3.1.49 show l3int vlan	190
3.2 MAC Address Table Configuration Commands	191
3.2.1 mac-address flapping action {quit-vlan error-down}	191
3.2.2 mac-address flapping action priority	192
3.2.3 mac-address notification {add remove all}	192
3.2.4 mac-learning {enable disable}	193
3.2.5 mac-learning disable action {forward drop}	194
3.2.6 no mac-address flapping action	195
3.2.7 show mac-address	195
3.2.8 show mac-address dynamic	197
3.2.9 show mac-address config	198
3.2.10 show mac-address flapping record	199
3.2.11 show mac-address notification history	200

3.2.12 show mac-address total-number	201
3.2.14 mac-address blackhole	203
3.2.15 mac aging-time	204
3.2.16 no mac-address	205
3.2.17 no mac-address dynamic	206
3.2.18 mac-limit	207
3.2.19 reset mac-address flapping record	208
3.2.20 reset mac-address notification history	209
3.2.21 mac-address flapping detection {enable disable}	209
3.2.22 mac-address flapping aging-time	210
3.2.23 mac-address flapping detection exclude-vlan.....	211
3.2.24 mac-address flapping detection vlan security-level.....	212
3.2.25 mac-address notification interval	212
3.2.26 mac-address notification history-size	213
3.2.27 mac-address flapping quit-vlan recover-time	214
3.2.28 mac-address static	215
3.2.29 show mac-address l3	216
3.2.30 show mac-address bridge-domain	217
3.3 ARP Configuration Commands	217
3.3.1 arp detect-mode unicast.....	217
3.3.2 arp-limit maxnum	218
3.3.3 arp-limit vlan maxnum	219
3.3.4 arp direct-route {enable disable}	220
3.3.5 show ip arp	221
3.3.6 show arp-limit maxnum.....	222
3.3.7 show arp-probe config.....	223
3.3.8 show arp-probe database	224
3.3.9 show arp-probe global	225
3.3.10 debug arp {in out error all}	226
3.3.11 debug arp dst-addr	227
3.3.12 debug arp src-addr	228
3.3.13 debug arp-probe.....	229

3.3.14 ip arp.....	230
3.3.15 ip arp vni source-ip peer-ip.....	232
3.3.16 ip arp detect {enable disable}	233
3.3.17 ip arp detect-times	234
3.3.18 ip arp aging-time	234
3.3.19 debug arp l2-proxy	235
3.3.20 show arp l2-proxy.....	236
3.3.21 arp l2-proxy timeout.....	237
3.3.22 flush arp l2-proxy all	237
3.3.23 arp broadcast-suppress {enable disable}	238
3.3.24 arp collect-host {enable disable}	239
3.3.25 arp l2-proxy {enable disable}	240
3.3.26 arp l2-proxy gateway-mac {enable disable}.....	240
3.3.27 show arp-limit config	241
3.3.28 show ip arp bridge-domain.....	242
3.4 Link Aggregation Configuration Commands	242
3.4.1 add.....	242
3.4.2 active-linknumber.....	244
3.4.3 interface eth-trunk	246
3.4.4 mode.....	247
3.4.5 join eth-trunk	247
3.4.6 remove	249
3.4.7 show interface eth-trunk verbose.....	250
3.4.8 show interface statistic	251
3.4.9 debug schedule-profile	253
3.4.10 load-balance	254
3.4.11 ip field.....	256
3.4.12 ipv6 field	257
3.4.13 l2 field	259
3.4.14 mpls field.....	260
3.4.15 schedule-profile	261
3.4.16 show schedule-profile.....	262

3.4.17 lacp timeout	263
3.4.18 debug lacp	264
3.4.19 lacp system-priority	265
3.4.20 lacp port-id extension {enable disable}	265
3.4.21 lacp system-id.....	266
3.4.22 reset lacp statistic	267
3.4.23 reset lacp statistic interface.....	267
3.4.24 reset lacp statistic interface eth-trunk	268
3.4.25 show lacp config.....	269
3.4.26 show lacp eth-trunk	269
3.4.27 show lacp statistic interface eth-trunk	270
3.4.28 show lacp system.....	271
3.4.29 show interface eth-trunk	272
3.4.30 unknown-unicast load-balance	275
3.4.31 show unknown-unicast load-balance.....	276
3.5 VLAN Configuration Commands	276
3.5.1 port default vlan	276
3.5.2 port hybrid vlan	278
3.5.3 port hybrid pvid.....	279
3.5.4 port link-type	279
3.5.5 port trunk allow-pass vlan	281
3.5.6 port trunk pvid.....	281
3.5.7 show vlan.....	282
3.5.8 show port vlan	285
3.5.9 unknown-multicast {forward drop}.....	286
3.5.10 unknown-unicast {forward drop}	287
3.5.11 no vlan	287
3.5.12 vlan.....	288
3.5.13 protocol up-delay-time	289
3.5.14 protocol-vlan	290
3.5.15 protocol-vlan vid	291
3.5.16 debug protocol-vlan.....	292

3.5.17 show protocol-vlan	293
3.5.18 debug mac-vlan	294
3.5.19 mac-vlan {enable disable}	295
3.5.20 mac-vlan priority	296
3.5.21 show mac-vlan.....	297
3.5.22 vlan precedence	298
3.5.23 debug ip-subnet-vlan	299
3.5.24 vlan-mode {normal super}	300
3.6 VLAN Mapping Configuration Commands	300
3.6.1 debug vlan-mapping.....	300
3.6.2 vlan-mapping {enable disable}	301
3.6.3 vlan-mapping vlan map-vlan.....	302
3.6.4 show vlan-mapping	305
3.7 VLAN STACKING Configuration Commands.....	306
3.7.1 debug vlan-stacking.....	306
3.8 QinQ Configuration Commands	307
3.8.1 vlan-stacking {enable disable}	307
3.8.2 vlan-stacking vlan stack-vlan	308
3.8.3 show vlan-stacking	310
3.9 ARP Proxy Configuration Commands	311
3.9.1 show arp-proxy config.....	311
3.9.2 show arp-proxy interface.....	312
3.9.3 show arp-proxy vlan.....	313
3.9.4 debug arp-proxy	314
3.9.5 arp-proxy {enable disable}	315
3.9.6 arp-proxy inner-sub-vlan-proxy {enable disable}	316
3.9.7 arp-proxy inter-sub-vlan-proxy {enable disable}	316
3.10 MAM Configuration Commands	317
3.10.1 debug mam	317
3.11 Port Security Configuration Commands.....	318
3.11.1 port-security {enable disable}	318
3.11.2 port-security mac-address sticky {enable disable}	319

3.11.3 port-security maximum	320
3.11.4 port-security mac-address sticky vlan	320
3.11.5 port-security protect-action.....	321
3.12 Port Isolation Configuration Commands.....	322
3.12.1 debug port-isolate	322
3.12.2 port-isolate mode.....	323
3.12.3 port-isolate group	324
3.12.4 port-uniisolate.....	324
3.12.5 join port-isolate group	325
3.12.6 add interface	326
3.12.7 show port-isolate group	327
3.12.8 show port-isolate information	328
3.12.9 show port-uniisolate interface	329
3.12.10 show port-isolate config	330
3.13 Storm Control Configuration Commands	331
3.13.1 storm-control	331
3.13.2 debug storm-control	332
3.13.3 show storm-control.....	333
3.14 MLAG Configuration Commands.....	334
3.14.1 debug mlag	334
3.14.2 lacp mlag priority	335
3.14.3 lacp mlag system-id.....	336
3.14.4 mlag exclude interface.....	337
3.14.5 mlag-group	337
3.14.6 mlag interface eth-trunk	338
3.14.7 peerlink exclude vlan.....	339
3.14.8 peerlink interface eth-trunk	340
3.14.9 priority	341
3.14.10 reset counter	341
3.14.11 security-key	342
3.14.12 show mlag	343
3.14.13 show mlag config	344

3.14.14 show mlag consistency	345
3.14.15 show mlag exclude interface	346
3.14.16 show mlag-group	346
3.14.17 source-address	348
3.14.18 timer hello	349
3.14.19 timer hold-on-failure multiplier	350
3.14.20 up-delay	350
3.14.21 dad enhance {enable disable}	351
3.14.22 mlag ip address	352
3.14.23 mlag ipv6 address	353
3.14.24 mlag ipv6 address link-local	354
Chapter 4 IP Commands	356
4.1 IPv4 Address Configuration Commands	356
4.1.1 ip address	356
4.1.2 ip tcp max-connect	357
4.1.3 debug ip	358
4.1.4 debug ip dst-addr	359
4.1.5 debug ip src-addr	359
4.1.6 show ip config	360
4.1.7 show ip connect-table	361
4.1.8 show ip interface	364
4.1.9 show ip statistic	365
4.2 IPv6 Address Configuration Commands	367
4.2.1 debug ipv6	367
4.2.2 ipv6 {enable disable}	367
4.2.3 ipv6 nd direct-route {enable disable}	368
4.2.4 ipv6 address	369
4.2.5 ipv6 address eui	370
4.2.6 ipv6 address link-local	371
4.2.7 ipv6 address auto link-local	372
4.2.8 ipv6 hop-limit	373
4.2.9 ipv6 neighbor	373

4.2.10	ipv6 mtu.....	375
4.2.11	ipv6 nd lifetime.....	375
4.2.12	show ipv6 interface loopback.....	376
4.2.13	show ipv6 interface vlan.....	377
4.2.14	show ipv6 neighbor	378
4.2.15	show ipv6 neighbor summary	378
4.2.16	show ipv6 route summary	379
4.2.17	show ipv6 statistic	380
4.2.18	show ipv6 route	381
4.3	DHCP Configuration Commands	383
4.3.1	debug dhcp relay	383
4.3.2	debug dhcp server.....	384
4.3.3	dhcp {start stop}	385
4.3.4	dhcp relay server-ip	385
4.3.5	dhcp relay user refresh-interval	386
4.3.6	ip dhcp.....	387
4.3.7	reset dhcp relay statistic	388
4.3.8	show dhcp.....	388
4.3.9	show dhcp config	389
4.3.10	show dhcp relay statistic.....	390
4.3.11	show dhcp relay.....	391
4.3.12	show dhcp vlan config.....	392
4.4	DHCP Client Configuration Commands	393
4.4.1	ip address dhcp {enable disable}	393
4.4.2	ip address dhcp release	394
4.4.3	ip address dhcp renew	394
4.4.4	reset dhcp client statistic.....	395
4.4.5	show dhcp client.....	396
4.4.6	show dhcp client statistic.....	397
4.4.7	show dhcpv6 relay.....	397
4.4.8	show dhcpv6 statistic.....	398
4.4.9	show dhcpv6 interface.....	399

Chapter 5 Routing Commands	401
5.1 Basic IP Routing Commands	401
5.1.1 show ecmp-profile	401
5.1.2 show ecmp load-balance	402
5.1.3 ecmp-profile	402
5.1.4 ecmp hash-mode	403
5.1.5 ecmp load-balance profile	404
5.1.6 ecmp load-balance {src-ip default}	405
5.2 DID Configuration Commands	405
5.2.1 debug did	405
5.2.2 show did resource	406
5.2.3 show did peer	407
5.3 Static Route Configuration Commands	407
5.3.1 ip route-static	407
5.3.2 ipv6 route-static	410
5.3.3 ipv6 route-static interface vlan link-local	413
5.3.4 show ip route	414
5.3.5 show ip route {static local}	415
5.3.6 show {ip ipv6} route statistic	416
5.3.7 show ip route summary	417
5.3.8 show ipv6 route	418
5.3.9 show ip hwrout summary	420
5.3.10 show ipv6 hwrout summary	420
5.4 OSPFv2 Configuration Commands	421
5.4.1 debug ospf	421
5.4.2 maxage-lsa route-calculate-delay	422
5.4.3 preference	423
5.4.4 filter route-policy	424
5.4.5 valid-ttl-hops	425
5.4.6 area authentication	426
5.4.7 area nssa default-cost	427
5.4.8 area nssa translator	428

5.4.9 area nssa	429
5.4.10 area nssa range	430
5.4.11 area range	432
5.4.12 area stub.....	433
5.4.13 area stub no-summary	435
5.4.14 area nssa no-summary	435
5.4.15 area virtual-link	436
5.4.16 area virtual-link authentication.....	438
5.4.17 bandwidth-reference.....	439
5.4.18 default-route-advertise always	440
5.4.19 graceful-restart begin.....	441
5.4.20 graceful-restart helper.....	442
5.4.21 graceful-restart	442
5.4.22 ip ospf dead-interval.....	443
5.4.23 ip ospf hello-interval	444
5.4.24 ip ospf if-type	445
5.4.25 ip ospf authentication	446
5.4.26 ip ospf bfd {enable disable}	447
5.4.27 ip ospf cost	448
5.4.28 ip ospf fast-change.....	448
5.4.29 ip ospf flooding-group.....	449
5.4.30 ip ospf mtu.....	450
5.4.31 ip ospf mtu-ignore {enable disable}	451
5.4.32 ip ospf passive-interface	452
5.4.33 ip ospf poll-interval	452
5.4.34 ip ospf priority.....	453
5.4.35 ip ospf retransmit-interval	454
5.4.36 ip ospf transmit-delay	455
5.4.37 loop-prevent {enable disable}	456
5.4.38 maximum load-balancing	457
5.4.39 network area	457
5.4.40 peer priority	458

5.4.41 redistribute.....	459
5.4.42 redistribute {rip isis ospf}.....	460
5.4.43 redistribute range.....	461
5.4.44 redistribute route-policy	462
5.4.45 redistribute metric	463
5.4.46 redistribute not-advertise advertise.....	465
5.4.47 redistribute translate no-translate.....	466
5.4.48 router-id	467
5.4.49 router ospf	468
5.4.50 reset ospf	469
5.4.51 reset ospf counters.....	469
5.4.52 rfc1583 compatible.....	470
5.4.53 route-tag	471
5.4.54 show ip ospf area.....	472
5.4.55 show ip ospf bfd session.....	472
5.4.56 show ip ospf brief.....	473
5.4.57 show ip ospf config	475
5.4.58 show ip ospf database.....	476
5.4.59 show ip ospf graceful-restart	478
5.4.60 show ip ospf import-route	479
5.4.61 show ip ospf interface.....	479
5.4.62 show ip ospf log	480
5.4.63 show ip ospf neighbor	481
5.4.64 show ip ospf route	482
5.4.65 show ip ospf route count	483
5.4.66 show ip ospf trap	484
5.4.67 show ip ospf virtual interface	485
5.4.68 show ip ospf virtual neighbor.....	486
5.4.69 show ip ospf statistic bfd.....	487
5.4.70 show ip ospf statistic global	488
5.4.71 show ip ospf statistic interface	489
5.4.72 show ip ospf statistic lsa.....	491

5.4.73 show ip ospf statistic memory	492
5.4.74 show ip ospf statistic neighbor	493
5.4.75 show ip ospf statistic route process	494
5.4.76 show ip ospf statistic route	495
5.4.77 show ip ospf statistic spf	496
5.4.78 snmp-trap	497
5.4.79 spf-running-interval	498
5.4.80 opaque	499
5.4.81 ip ospf source sub-address	500
5.4.82 stub-router on-startup	501
5.5 OSPFv3 Configuration Commands	502
5.5.1 area nssa	502
5.5.2 area nssa range	503
5.5.3 area range	504
5.5.4 area virtual-link	505
5.5.5 area stub	507
5.5.6 area stub no-summary	508
5.5.7 area nssa no-summary	509
5.5.8 area default-cost	510
5.5.9 bandwidth-reference	511
5.5.10 debug ospf6	511
5.5.11 graceful-restart (OSPFv3)	512
5.5.12 graceful-restart begin (OSPFv3)	513
5.5.13 graceful-restart helper (OSPFv3)	514
5.5.14 ipv6 ospf if-type	514
5.5.15 ipv6 ospf hello-interval	515
5.5.16 ipv6 ospf dead-interval	516
5.5.17 ipv6 ospf transmit-delay	517
5.5.18 ipv6 ospf area	518
5.5.19 ipv6 ospf bfd {enable disable}	519
5.5.20 ipv6 ospf cost	520
5.5.21 ipv6 ospf peer	521

5.5.22 ipv6 ospf priority	522
5.5.23 ipv6 ospf retransmit-interval	523
5.5.24 ipv6 ospf mtu.....	524
5.5.25 ipv6 ospf mtu-ignore	525
5.5.26 maximum load-balancing	526
5.5.27 router ipv6 ospf	526
5.5.28 router ipv6 ospf vpn-instance	527
5.5.29 reset ipv6 ospf	528
5.5.30 reset ipv6 ospf counters.....	529
5.5.31 redistribute.....	530
5.5.32 redistribute route-policy	530
5.5.33 router-id	531
5.5.34 show ipv6 ospf graceful-restart	532
5.5.35 show ipv6 ospf brief.....	533
5.5.36 show ipv6 ospf area.....	534
5.5.37 show ipv6 ospf bfd session.....	535
5.5.38 show ipv6 ospf config	536
5.5.39 show ipv6 ospf database.....	537
5.5.40 show ipv6 ospf database count.....	539
5.5.41 show ipv6 ospf import-route	541
5.5.42 show ipv6 ospf interface.....	541
5.5.43 show ipv6 ospf log	543
5.5.44 show ipv6 ospf neighbor	544
5.5.45 show ipv6 ospf route	545
5.5.46 show ipv6 ospf route count	546
5.5.47 show ipv6 ospf statistic global	547
5.5.48 show ipv6 ospf statistic memory	548
5.5.49 show ipv6 ospf trap	549
5.5.50 show ipv6 ospf virtual interface	550
5.5.51 show ipv6 ospf virtual neighbor.....	551
5.5.52 filter route-policy.....	552
5.5.53 spf-running-interval.....	552

5.5.54 area nssa translator	553
5.5.55 snmp-trap	554
5.5.56 ipv6 ospf passive-interface	555
5.5.57 preference	556
5.5.58 redistribute range	557
5.5.59 stub-router on-startup	558
5.6 BGP Configuration Commands	559
5.6.1 aggregate	559
5.6.2 aggregate adminstatus	561
5.6.3 show ip bgp error-statistics	562
5.6.4 debug bgp neighbor	564
5.6.5 filter-policy {export import} route-policy	565
5.6.6 filter-policy export	566
5.6.7 neighbor advertisement-interval	567
5.6.8 neighbor as-origin-interval	568
5.6.9 neighbor connect-retry-interval	569
5.6.10 neighbor ebgp-multihop	570
5.6.11 neighbor keepalive-timer hold-timer	571
5.6.12 neighbor next-hop-local	572
5.6.13 neighbor password	573
5.6.14 neighbor remote-as	574
5.6.15 neighbor route-reflector-client	575
5.6.16 neighbor route-refresh	576
5.6.17 neighbor send-community	577
5.6.18 neighbor send route-refresh	578
5.6.19 neighbor shutdown	579
5.6.20 neighbor update-source	580
5.6.21 neighbor valid-ttl-hops	581
5.6.22 neighbor connect-interface	582
5.6.23 neighbor allow-as-loop	583
5.6.24 neighbor bfd	584
5.6.25 neighbor public-as-only	585

5.6.26 preference	586
5.6.27 neighbor upe	587
5.6.28 redistribute	588
5.6.29 redistribute route-policy	589
5.6.30 show ip bgp route label	590
5.6.31 show ip bgp aggregate	591
5.6.32 show ip bgp config	592
5.6.33 show ip bgp damping-route	593
5.6.34 show ip bgp log	594
5.6.35 show ip bgp log period-statistic	595
5.6.36 show ip bgp neighbor	597
5.6.37 show ip bgp orf	598
5.6.38 show ip bgp resource	599
5.6.39 show ip bgp route	601
5.6.40 show ip bgp summary	603
5.6.41 show ip bgp vpn-instance neighbor	604
5.6.42 show ipv6 bgp route	605
5.6.43 neighbor tcp	606
5.6.44 cluster-id	607
5.6.45 community	607
5.6.46 confederation identifier	609
5.6.47 confederation peer-as	609
5.6.48 dampening	610
5.6.49 dampening {enable disable}	611
5.6.50 debug bgp	612
5.6.51 default local-med	613
5.6.52 default local-preference	614
5.6.53 graceful-restart {enable disable}	614
5.6.54 graceful-restart timer restart	615
5.6.55 graceful-restart timer selection-deferral	616
5.6.56 ipv4[ipv6]-family	616
5.6.57 advertise l2vpn evpn	617

5.6.58 maximum load-balancing	618
5.6.59 neighbor next-hop-invariable	619
5.6.60 neighbor.....	620
5.6.61 neighbor substitute-as.....	621
5.6.62 neighbor route-policy {export import}	622
5.6.63 network.....	623
5.6.64 router bgp	624
5.6.65 router-id	625
5.6.66 reset bgp	626
5.6.67 snmp-trap {enable disable}	627
5.6.68 synchronization {enable disable}	628
5.6.69 update-size.....	628
5.6.70 auto-summary {enable disable}.....	629
5.6.71 neighbor preference.....	630
5.6.72 neighbor next-hop-local	631
5.6.73 default local-preference.....	631
5.6.74 evpn-family	632
5.6.75 show ip bgp evpn route	633
5.7 ISIS Configuration Commands	635
5.7.1 area-authentication-mode	635
5.7.2 area-password.....	636
5.7.3 cost-style.....	637
5.7.4 debug isis.....	638
5.7.5 default-route-originate.....	640
5.7.6 domain-authentication-mode.....	640
5.7.7 domain-password	641
5.7.8 filter-policy import route-policy.....	642
5.7.9 fr {enable disable}.....	643
5.7.10 fr noloop.....	643
5.7.11 graceful-restart {enable disable}	644
5.7.12 hostname.....	645
5.7.13 ignore-lsp-errors	646

5.7.14 ip router isis	646
5.7.15 ipv6 preference	647
5.7.16 ipv6 router isis	648
5.7.17 isis bfd {enable disable}	649
5.7.18 isis circuit-ext-domain	650
5.7.19 isis circuit-level	650
5.7.20 isis circuit-type	651
5.7.21 isis csnp-interval	652
5.7.22 isis default-metric	653
5.7.23 isis fast-sense neighbor	654
5.7.24 isis graceful-restart	654
5.7.25 isis hello padding	655
5.7.26 isis hello-interval	656
5.7.27 isis hello-multiplier	657
5.7.28 isis ipv6 bfd {enable disable}	658
5.7.29 isis mesh-group	658
5.7.30 isis passive-interface	659
5.7.31 isis password	660
5.7.32 isis priority	661
5.7.33 isis psnp-interval	662
5.7.34 isis three-way-handshake	662
5.7.35 isis wide-metric	663
5.7.36 is-type	664
5.7.37 lsp-generation max-interval	665
5.7.38 lsp-refresh-interval	666
5.7.39 maximum load-balancing	667
5.7.40 max-lsp-lifetime	667
5.7.41 net	668
5.7.42 redistribute	669
5.7.43 redistribute level-2 to level-1	672
5.7.44 router isis	673
5.7.45 router-id	674

5.7.46 set-overload-bit.....	675
5.7.47 preference.....	676
5.7.48 reset isis	677
5.7.49 show ip isis	677
5.7.50 show {ip ipv6} isis bfd session.....	679
5.7.51 show ip isis config.....	680
5.7.52 show ip isis database	681
5.7.53 show ip isis database count	687
5.7.54 show ip isis database verbose	688
5.7.55 show ip isis event-log.....	705
5.7.56 show {ip ipv6} isis fr route	706
5.7.57 show ip isis hostname.....	707
5.7.58 show ip isis import-route.....	708
5.7.59 show ip isis interface	708
5.7.60 show ip isis lsp-log.....	710
5.7.61 show ip isis lsp-option.....	711
5.7.62 show ip isis neighbor.....	715
5.7.63 show {ip ipv6} isis route	716
5.7.64 show ip isis spf-log.....	718
5.7.65 show ip isis spf-tree	720
5.7.66 show ip isis statistic.....	721
5.7.67 show ip isis virtual-system	723
5.7.68 snmp-trap.....	724
5.7.69 summary-address.....	725
5.7.70 summary-prefix	726
5.7.71 timer spf max-interval init-interval incr-interval.....	727
5.7.72 traffic-engineer	728
5.7.73 virtual-system	728
5.8 Routing Policy Configuration Commands	729
5.8.1 apply as-path	729
5.8.2 apply cost.....	731
5.8.3 apply cost-type	732

5.8.4 apply local-preference	733
5.8.5 apply isis.....	733
5.8.6 apply origin	734
5.8.7 apply ospf	735
5.8.8 apply preferred-value	736
5.8.9 apply tag	737
5.8.10 debug route-policy.....	738
5.8.11 match aspath	738
5.8.12 match community-filter	739
5.8.13 match extcommunity-filter rt.....	740
5.8.14 match process	741
5.8.15 match cost.....	742
5.8.16 match ip filter-list	742
5.8.17 match ip-prefix	744
5.8.18 match ip {next-hop route-source} ip-prefix	745
5.8.19 match ipv6 filter-list	746
5.8.20 match ipv6 {address next-hop route-source} prefix-list	747
5.8.21 match route-type.....	748
5.8.22 match tag	749
5.8.23 route-policy	750
5.8.24 show route-policy config.....	751
5.8.25 show route-policy information	752
5.8.26 show route-policy	753
5.8.27 as-path-filter	754
5.8.28 show as-path-filter	755
5.8.29 debug as-path-filter.....	756
5.9 Policy-based Route Configuration Commands	757
5.9.1 apply ip-address next-hop	757
5.9.2 apply ipv6-address next-hop	758
5.9.3 apply ip-precedence.....	759
5.9.4 apply output-interface.....	760
5.9.5 if-match acl.....	760

5.9.6 policy-based-route	761
5.9.7 ip policy-based-route	763
5.9.8 show ip policy-based-route	763
5.9.9 apply load-balance next-hop	764
5.9.10 show ip policy-based-route config	765
5.9.11 debug policy-based-route	766
5.10 Hwroute Configuration Commands	767
5.10.1 debug hwroute	767
5.10.2 show hwroute ecmp-group	768
5.10.3 show hwroute statistic	769
5.10.4 show hwroute hardware.....	772
5.10.5 show hwroute nexthop.....	773
Chapter 6 QoS Commands	775
6.1 Diffserv Configuration Commands	775
6.1.1 debug diffserv.....	775
6.1.2 diffserv domain.....	776
6.1.3 8021p-inbound	776
6.1.4 8021p-outbound	778
6.1.5 ip-dscp-inbound.....	781
6.1.6 ip-dscp-outbound.....	783
6.1.7 show diffserv domain	784
6.1.8 trust 8021p.....	785
6.1.9 trust dscp	786
6.1.10 trust none	786
6.1.11 qos phb marking 8021p	787
6.1.12 qos phb marking dscp.....	788
6.1.13 trust diffserv	788
6.2 Traffic Policing and Traffic Shaping Configuration Commands	789
6.2.1 counter.....	789
6.2.2 debug cos.....	790
6.2.3 meter.....	791
6.2.4 reset counter filter-list filter.....	793

6.2.5 show counter	794
6.2.6 show meter	795
6.2.7 show meter config	796
6.2.8 traffic-car include-interframe	796
6.3 Queue Scheduling and Congestion Control Configuration Commands	797
6.3.1 cos queue weight	797
6.3.2 cos queue priority	798
6.3.3 cos scheduling	799
6.3.4 cos queue {min-bandwidth max-bandwidth}	800
6.3.5 show cos interface	801
6.3.6 show cos config	803
6.3.7 show drop-profile	803
6.3.8 show wred config	804
6.3.9 debug wred	805
6.3.10 drop-profile	806
6.3.11 qos ecn	807
6.3.12 qos wred	807
6.3.13 qos queue wred	808
6.3.14 qos queue ecn	809
6.3.15 ecn low-limit low-limit high-limit discard-percent	810
6.3.16 qos ecn {enable disable}	811
6.3.17 reset cos statistics	812
6.3.18 show cos statistics	812
Chapter 7 Multicast Commands	815
7.1 IGMP Snooping Configuration Commands	815
7.1.1 debug igmpsnoop	815
7.1.2 hwmc mac-ip-check {enable disable}	816
7.1.3 igmp-snooping {enable disable}	816
7.1.4 igmp-snooping ctrlmode {enable disable}	817
7.1.5 igmp-snooping fast-leave	818
7.1.6 igmp-snooping fast-switch	819
7.1.7 igmp-snooping fast-switch query {enable disable}	820

7.1.8 igmp-snooping group-address mvlan	821
7.1.9 igmp-snooping max-response-time	821
7.1.10 igmp-snooping multicast user-vlan	823
7.1.11 igmp-snooping multicast-vlan	823
7.1.12 igmp-snooping mvlan.....	824
7.1.13 igmp-snooping mvlan uplink-port.....	825
7.1.14 igmp-snooping forwarding-mode {ip mac}.....	826
7.1.15 igmp-snooping group-policy filter-list	826
7.1.16 igmp-snooping querier {enable disable}	827
7.1.17 igmp-snooping proxy-ip	828
7.1.18 igmp-snooping proxy-uplink-port	829
7.1.19 igmp-snooping query-interval	830
7.1.20 igmp-snooping report-suppress	831
7.1.21 igmp-snooping require-router-alert	831
7.1.22 igmp-snooping query-duplicate-suppress {enable disable}	832
7.1.23 igmp-snooping robust-count.....	833
7.1.24 igmp-snooping router-aging-time.....	834
7.1.25 igmp-snooping send-query source-address	835
7.1.26 igmp-snooping lastmember-querynumber.....	836
7.1.27 igmp-snooping lastmember-queryinterval.....	837
7.1.28 igmp-snooping {start stop}.....	838
7.1.29 igmp-snooping 8021p priority	838
7.1.30 igmp-snooping group-limit.....	839
7.1.31 igmp-snooping static-group group-address mvlan	840
7.1.32 igmp-snooping static-group group-address mvlan user-vlan.....	841
7.1.33 igmp-snooping uplink-port.....	842
7.1.34 igmp-snooping uplink-port drop-report.....	843
7.1.35 igmp-snooping uplink-port-limit	844
7.1.36 igmp-snooping version	845
7.1.37 igmp-snooping workmode.....	845
7.1.38 igmp-snooping drop	846
7.1.39 reset igmp-snooping group.....	847

7.1.40 reset igmp-snooping statistic	848
7.1.41 show igmp-snooping	848
7.1.42 show igmp-snooping config	849
7.1.43 show igmp-snooping egress-port.....	850
7.1.44 show igmp-snooping egress-port interface.....	850
7.1.45 show igmp-snooping egress-port mvlan.....	851
7.1.46 show igmp-snooping group	852
7.1.47 show igmp-snooping interface	853
7.1.48 show igmp-snooping mvlan	854
7.1.49 show igmp-snooping source-address.....	855
7.1.50 show igmp-snooping uplinkport.....	855
7.1.51 show igmp-snooping statistic	856
7.2 IGMP Configuration Commands	857
7.2.1 clear igmp-control config	857
7.2.2 debug igmp.....	858
7.2.3 general-query.....	859
7.2.4 igmp {enable disable}	860
7.2.5 igmp {start stop}	861
7.2.6 igmp fast-leave	862
7.2.7 igmp general-query	863
7.2.8 igmp group-policy filter-list	863
7.2.9 igmp lastmember-queryinterval.....	865
7.2.10 igmp limit	866
7.2.11 igmp max-response-time	867
7.2.12 igmp require-router-alert	868
7.2.13 igmp robust-count	869
7.2.14 igmp send-router-alert	870
7.2.15 igmp static-group egress-port.....	871
7.2.16 igmp static-group source egress-port.....	872
7.2.17 igmp static-group source	873
7.2.18 igmp static-group.....	874
7.2.19 igmp timer other-querier-present.....	875

7.2.20 igmp timer query	876
7.2.21 igmp version	877
7.2.22 igmp	878
7.2.23 lastmember-queryinterval	879
7.2.24 igmp max-response-time	880
7.2.25 limit	881
7.2.26 max-response-time	882
7.2.27 no igmp group	882
7.2.28 require-router-alert	884
7.2.29 send-router-alert	885
7.2.30 robust-count	886
7.2.31 show igmp config	887
7.2.32 show igmp egress-port	888
7.2.33 show igmp group	890
7.2.34 show igmp interface	891
7.2.35 show igmp source	892
7.2.36 show igmp vpn-instance	894
7.2.37 show igmp	895
7.2.38 timer other-querier-present	895
7.2.39 timer query	897
7.3 MLD Snooping Configuration Commands	897
7.3.1 debug mldsnoop	897
7.3.2 mld-snooping {enable disable}	898
7.3.3 mld-snooping {start stop}	899
7.3.4 mld-snooping fast-leave {enable disable}	900
7.3.5 mld-snooping fast-switch {enable disable}	900
7.3.6 mld-snooping fast-switch query {enable disable}	901
7.3.7 mld-snooping forwarding-mode	902
7.3.8 mld-snooping lastmember-queryinterval	903
7.3.9 mld-snooping leave-suppress {enable disable}	903
7.3.10 mld-snooping max-response-time	904
7.3.11 mld-snooping static-group group-address mvlan	905

7.3.12 mld-snooping uplink-port.....	906
7.3.13 mld-snooping multicast user-vlan	907
7.3.14 mld-snooping multicast-vlan.....	908
7.3.15 mld-snooping mvlan.....	909
7.3.16 mld-snooping mvlan uplink-port.....	910
7.3.17 mld-snooping proxy-ip	910
7.3.18 mld-snooping group-policy	911
7.3.19 mld-snooping querier {enable disable}	912
7.3.20 mld-snooping query-interval	913
7.3.21 mld-snooping report-suppress {enable disable}	914
7.3.22 mld-snooping require-router-alert	914
7.3.23 mld-snooping robust-count.....	915
7.3.24 mld-snooping router-aging-time.....	916
7.3.25 reset mld-snooping group	916
7.3.26 mld-snooping uplink-port drop-report {enable disable}	917
7.3.27 mld-snooping uplink-port-limit	918
7.3.28 mld-snooping version	918
7.3.29 mld-snooping workmode.....	919
7.3.30 mld-snooping group-address mvlan	920
7.3.31 mld-snooping send-query source-address	921
7.3.32 show mld-snooping config	921
7.3.33 show mld-snooping egress-port.....	922
7.3.34 show mld-snooping group	923
7.3.35 show mld-snooping interface	923
7.3.36 show mld-snooping mvlan	924
7.3.37 show mld-snooping source-address.....	925
7.3.38 show mld-snooping uplinkport.....	926
7.3.39 show mld-snooping	926
7.4 PIM Configuration Commands	927
7.4.1 ip multicast-routing	927
7.4.2 pim.....	928
7.4.3 anycast-rp	929

7.4.4 c-bsr admin-scope	930
7.4.5 c-bsr send-interval	931
7.4.6 c-rp hold-time	932
7.4.7 c-rp send-interval.....	932
7.4.8 rp-address	933
7.4.9 receive-check-neighbor	934
7.4.10 send-check-neighbor	935
7.4.11 source-lifetime	936
7.4.12 state-refresh-interval.....	937
7.4.13 state-refresh-rate-limit	938
7.4.14 state-refresh-ttl	939
7.4.15 register probe-interval	939
7.4.16 register suppression-timeout.....	940
7.4.17 ip pim-sm.....	941
7.4.18 ip pim-dm.....	942
7.4.19 ip pim bsr-boundary group	943
7.4.20 ip pim c-bsr group	944
7.4.21 ip pim c-rp group.....	945
7.4.22 ip pim dr-priority	946
7.4.23 ip pim silent	947
7.4.24 ip pim hello-interval	948
7.4.25 ip pim hello-option holdtime	949
7.4.26 ip pim hello-option override-interval	950
7.4.27 ip pim hello-option prune-delay	951
7.4.28 ip pim join-prune holdtime	952
7.4.29 ip pim join-prune interval	953
7.4.30 ip pim graft retry-time	954
7.4.31 ip pim state-refresh-capable	955
7.4.32 reset pim routing-table.....	955
7.4.33 debug pim.....	956
7.4.34 show ip pim config.....	957
7.4.35 show ip pim anycast-rp.....	958

7.4.36 show ip pim bsr	959
7.4.37 show ip pim c-rp	959
7.4.38 show ip pim interface	960
7.4.39 show ip pim neighbor	961
7.4.40 show ip pim route	962
7.4.41 show ip pim rp	963
7.4.42 show ip pim statistic	964
7.4.43 show ip pim vpn-instance	965
Chapter 8 Service Security Commands	967
8.1 Time-range Configuration Commands	967
8.1.1 debug time-range	967
8.1.2 name	967
8.1.3 time-range list	968
8.1.4 no time-range	969
8.1.5 time-range absolute	970
8.1.6 time-range everyday	970
8.1.7 time-range everyhour	971
8.1.8 time-range everymonth	972
8.1.9 time-range everyweek	973
8.1.10 time-range everyweekday	973
8.1.11 time-range everyweekend	974
8.1.12 time-range everyyear	975
8.1.13 show time-range config	976
8.1.14 show time-range list	976
8.2 IP Address Prefix Filter List Configuration Commands	977
8.2.1 debug prefix-list {config match error all}	977
8.2.2 ip prefix-list	978
8.2.3 ipv6 prefix-list	979
8.2.4 show {ip ipv6} prefix-list	981
8.2.5 show ip prefix-list information	982
8.3 ACL Configuration Commands	983
8.3.1 filter action {permit deny}	983

Switch Command Reference Manual
xxxvii

8.3.33 filter ip fragment.....	1014
8.3.34 filter ip precedence	1015
8.3.35 filter ip precedence fragment.....	1016
8.3.36 filter ip proto-type	1017
8.3.37 filter ip tos	1018
8.3.38 filter ip ttl.....	1020
8.3.39 filter mac	1021
8.3.40 filter tcp	1023
8.3.41 filter udp	1025
8.3.42 filter-list.....	1027
8.3.43 filter-list-hybrid {in out}	1028
8.3.44 filter-list-ipv4 {in out}	1029
8.3.45 filter-list-ipv6 {in out}	1030
8.3.46 filter-list-l2 {in out}	1031
8.3.47 filter action {outer-tag-priority inner-tag-priority}.....	1032
8.3.48 filter-list-hybrid global {in out}	1032
8.3.49 filter-list-ipv4 global {in out}	1033
8.3.50 filter-list-ipv6 global {in out}	1034
8.3.51 filter-list-l2 global {in out}	1035
8.4 ACL6 Configuration Commands.....	1036
8.4.1 filter icmp6	1036
8.4.2 filter igmp6.....	1037
8.4.3 filter ip6	1038
8.4.4 filter ip6 hop-limit	1039
8.4.5 filter ip6 next-header	1040
8.4.6 filter ip6 traffic-class	1041
8.4.7 filter tcp6	1042
8.4.8 filter udp6.....	1043
8.5 CPU Defense Configuration Commands.....	1045
8.5.1 debug cpu-defend	1045
8.5.2 cpu-defend policy	1045
8.5.3 car packet-type	1046

8.5.4 description	1047
8.5.5 show cpu-defend config	1048
8.5.6 packet-type queue	1048
8.5.7 cpu-defend bind-policy	1049
8.5.8 show cpu-defend policy	1050
8.5.9 cpu-defend application-apperceive	1051
8.6 Anti-attack Configuration Commands	1052
8.6.1 show antiattack config	1052
8.6.2 debug antiattack	1052
8.6.3 antiattack pkt-limit {enable disable}	1053
8.6.4 antiattack pkt-limit	1054
8.6.5 arp-antiattack {src-ip src-mac arp-cheat gratuitous-arp}	1055
8.6.6 arp-antiattack check user-bind {enable disable}	1056
8.6.7 arp-antiattack check user-bind alarm	1057
8.6.8 arp-antiattack check user-bind alarm threshold	1058
8.6.9 arp-antiattack check user-bind check-item	1059
8.6.10 arp-antiattack gratuitous-arp {enable disable}	1060
8.6.11 debug arp-antiattack	1061
8.6.12 arp-antiattack gateway-cheat {enable disable}	1061
8.6.13 reset arp-antiattack statistic check user-bind	1062
8.6.14 reset arp-antiattack statistic gateway-cheat	1063
8.6.15 show arp-antiattack check user-bind	1063
8.6.16 show arp-antiattack config	1064
8.6.17 show arp-antiattack statistic	1065
8.6.18 show auto-defend attack-source packet-type	1066
8.6.19 show cpu-defend statistic	1066
8.6.20 debug cpudefend	1067
8.6.21 error-down auto-recovery cause auto-defend interval	1068
8.6.22 reset cpu-defend statistics	1069
8.6.23 auto-defend {enable disable}	1069
8.6.24 auto-defend action {deny error-down}	1070
8.6.25 auto-defend action deny timeout	1071

8.6.26 auto-defend alarm {enable disable}	1071
8.6.27 auto-defend alarm threshold	1072
8.6.28 auto-defend attack-packet sample	1073
8.6.29 auto-defend protocol {enable disable}	1074
8.6.30 auto-defend threshold	1074
8.6.31 auto-defend trace-type	1075
8.6.32 auto-port-defend aging-time	1076
8.6.33 auto-port-defend protocol {enable disable}	1076
8.6.34 reset auto-defend packet-type	1077
8.6.35 reset cpu-defend statistics packet-type	1078
8.6.36 reset antiattack dos-limit statistics	1079
8.6.37 show antiattack dos-limit config	1079
8.6.38 show antiattack dos-limit statistics	1080
8.6.39 debug dos-antiattack	1081
8.6.40 antiattack dos-limit {enable disable}	1081
8.6.41 dosantiattack dos-limit car cir	1082
8.7 IP Source Guard Configuration Commands	1083
8.7.1 debug ip source check	1083
8.7.2 ip source check user-bind {enable disable}	1084
8.7.3 ip source check user-bind alarm {enable disable}	1085
8.7.4 ip source check user-bind alarm threshold	1086
8.7.5 ip source check user-bind check-item	1086
8.7.6 reset ip source statistic check user-bind	1088
8.7.7 show ip source check user-bind	1088
8.7.8 show user-bind	1089
8.7.9 show user-bind config	1090
8.7.10 user-bind alarm untrust-user	1090
8.7.11 user-bind black-list	1091
8.7.12 user-bind static ip ip6 mac	1092
8.8 AAA /RADIUS Configuration Commands	1094
8.8.1 aaa	1094
8.8.2 aaa {authentication accounting}	1095

8.8.3 aaa authentication enable method.....	1096
8.8.4 aaa authorization method.....	1097
8.8.5 aaa none-author privilege	1098
8.8.6 accounting realtime	1099
8.8.7 debug aaa.....	1100
8.8.8 no aaa method.....	1101
8.8.9 no radius-server	1102
8.8.10 no server-group.....	1102
8.8.11 no tacacs-server	1103
8.8.12 radius-server acct-port.....	1104
8.8.13 radius-server auth-port	1105
8.8.14 radius-server deadtime	1105
8.8.15 radius-server {ip-address ip6-address} key	1106
8.8.16 radius-server {ip-address ip6-address} key auth-port acct-port	1107
8.8.17 radius-server max-retransmit.....	1109
8.8.18 radius-server retransmit-interval	1109
8.8.19 radius-server {src-ip src-ip6}	1110
8.8.20 reset server statistic	1111
8.8.21 sever-group {radius-server tacacs-server}	1112
8.8.22 show aaa	1113
8.8.23 show aaa config.....	1113
8.8.24 show aaa method	1114
8.8.25 show aaa server	1115
8.8.26 show aaa server-group.....	1116
8.8.27 show aaa tacacs-server statistic	1117
8.8.28 show radius client.....	1118
8.8.29 tacacs-server deadtime	1118
8.8.30 tacacs-server {ip-address ip6-address} key	1119
8.8.31 tacacs-server {ip-address ip6-address} key port single-connection {enable disable}	1120
8.8.32 tacacs-server port.....	1121
8.8.33 tacacs-server single-connection {enable disable}	1122
8.8.34 tacacs-server {src-ip src-ip6}	1123

8.8.35 tacacs-server timeout.....	1124
8.8.36 aaa authorization console	1124
8.8.37 login accounting aaa method.....	1125
8.8.38 login authentication	1126
8.8.39 login authorization aaa method	1127
8.9 802.1x Configuration Commands	1128
8.9.1 debug dot1x {config out in timer fsm all}	1128
8.9.2 dot1x {enable disable}	1128
8.9.3 dot1x {start stop}.....	1129
8.9.4 dot1x aaa-accounting.....	1130
8.9.5 dot1x aaa-authentication.....	1131
8.9.6 dot1x authentication auth-method	1132
8.9.7 dot1x authentication client-timeout.....	1133
8.9.8 dot1x authentication logical-port.....	1134
8.9.9 dot1x authentication max-request.....	1135
8.9.10 dot1x authentication max-user	1136
8.9.11 dot1x authentication quiet-period.....	1136
8.9.12 dot1x authentication reauthenticate-period	1137
8.9.13 dot1x authentication server-timeout	1138
8.9.14 dot1x authentication tx-period.....	1139
8.9.15 dot1x default aaa-accounting.....	1140
8.9.16 dot1x default aaa-authentication.....	1141
8.9.17 dot1x default supplicant-support	1142
8.9.18 dot1x default vlan-assginment-mode	1142
8.9.19 dot1x authentication retry.....	1143
8.9.20 dot1x guest vlan	1144
8.9.21 dot1x link-mode	1145
8.9.22 dot1x mac-delete-notify	1146
8.9.23 dot1x reauthenticate	1147
8.9.24 dot1x reauthenticate user-mac	1147
8.9.25 dot1x supplicant-support	1148
8.9.26 dot1x unicast-trigger.....	1149

Switch Command Reference Manual

xliii

9.1.12 stp reset statistic	1173
9.1.13 stp process	1174
9.1.14 stp priority (STP configuration view).....	1175
9.1.15 stp priority (interface configuration view)	1175
9.1.16 stp point-to-point	1176
9.1.17 Stp pathcost-standard	1177
9.1.18 stp path-cost.....	1178
9.1.19 stp mode	1179
9.1.20 stp migration-time	1180
9.1.21 stp mcheck.....	1180
9.1.22 stp max-hops	1181
9.1.23 stp max-age	1182
9.1.24 stp loop-guard.....	1183
9.1.25 stp link-share binding process	1184
9.1.26 stp link-detection	1184
9.1.27 stp instance path-cost.....	1185
9.1.28 stp instance priority (STP configuration view).....	1186
9.1.29 stp instance priority (interface configuration view)	1187
9.1.30 stp instance vlan	1188
9.1.31 stp hello-time.....	1189
9.1.32 stp forward-delay.....	1190
9.1.33 stp flush	1190
9.1.34 stp edge-port.....	1191
9.1.35 stp edge-default	1192
9.1.36 stp config-name	1193
9.1.37 stp bridge-address.....	1194
9.1.38 stp bpdu-guard.....	1194
9.1.39 stp bpdu-filter	1195
9.1.40 stp binding process	1196
9.1.41 stp {enable disable}	1197
9.1.42 stp enhance-mode {enable disable}.....	1198
9.1.43 debug stp	1198

9.1.44 no stp instance	1201
9.1.45 show stp.....	1201
9.1.46 show stp brief	1202
9.1.47 show stp config.....	1203
9.1.48 show stp information	1204
9.1.49 show stp instance interface.....	1205
9.1.50 show stp interface.....	1207
9.1.51 show stp interface {ethernet xgigaethernet 10gigaethernet 25gigaethernet 40gigaethernet 100gigaethernet}	1208
9.1.52 show stp process brief	1210
9.1.53 show stp process interface.....	1210
9.1.54 show stp tc-bpdu statistic	1212
9.1.55 show stp topology-change.....	1213
9.2 BFD Configuration Commands.....	1214
9.2.1 show bfd config.....	1214
9.2.2 show bfd interface	1215
9.2.3 show bfd track.....	1216
9.2.4 show bfd session.....	1217
9.2.5 show bfd link-bundle session	1219
9.2.6 bfd {enable disable}	1220
9.2.7 bfd {start stop}	1220
9.2.8 bfd min-echo	1221
9.2.9 bfd min-tx min-rx multiplier	1222
9.2.10 bfd track.....	1223
9.2.11 bfd track link-bundle remote-ip.....	1225
9.2.12 bfd track bind vxlan peer-ip source-ip peer-mac.....	1227
9.2.13 bfd track min-tx min-rx multiplier	1228
9.2.14 bfd trap	1229
9.2.15 debug bfd.....	1229
9.2.16 bfd bind ingress (global configuration view)	1230
9.2.17 bfd bind ingress (interface configuration view)	1231
9.2.18 bfd bind egress (interface configuration view).....	1232

9.2.19 process-interface-status {enable disable}	1233
9.3 VRRP Configuration Commands	1234
9.3.1 show ip vrrp associate interface	1234
9.3.2 show ip vrrp binding admin-vrrp interface.....	1235
9.3.3 show ip vrrp interface.....	1237
9.3.4 show ip vrrpv3 interface.....	1238
9.3.5 show ip vrrp verbose	1240
9.3.6 show ipv6 vrrp interface.....	1240
9.3.7 show ipv6 vrrp binding admin-vrrp interface.....	1241
9.3.8 show ipv6 vrrp verbose	1243
9.4 EFM Configuration Commands	1243
9.4.1 debug efm.....	1243
9.4.2 efm {enable disable}	1244
9.4.3 efm fault-logs clear all.....	1245
9.4.4 efm fault-logs clear.....	1246
9.4.5 efm link-monitor {supported unsupported}	1247
9.4.6 efm link-monitor frame threshold window.....	1247
9.4.7 efm link-monitor frame-period threshold window	1248
9.4.8 efm link-monitor frame-seconds threshold window.....	1249
9.4.9 efm link-monitor high-threshold action.....	1250
9.4.10 efm link-monitor recover-period	1251
9.4.11 efm link-monitor never recover.....	1252
9.4.12 efm critical-event.....	1252
9.4.13 efm max-rate	1253
9.4.14 efm min-rate	1254
9.4.15 efm mode.....	1255
9.4.16 efm remote-loopback {supported unsupported}.....	1255
9.4.17 efm remote-loopback start.....	1257
9.4.18 efm remote-loopback start holdtime.....	1257
9.4.19 efm remote-loopback stop	1258
9.4.20 efm remote-loopback timeout.....	1259
9.4.21 efm timeout	1260

9.4.22 show efm fault-logs	1261
9.4.23 show efm session.....	1262
9.4.24 show efm statistic	1264
9.4.25 show efm status	1265
9.4.26 show efm summary	1267
9.5 CFM Configuration Commands	1267
9.5.1 ccm {enable disable}	1267
9.5.2 ccm-interval.....	1268
9.5.3 ccm loss-threshold.....	1269
9.5.4 cfm.....	1270
9.5.5 cfm mep vlan level mepid	1270
9.5.6 cfm mep vlan level mepid ccm.....	1272
9.5.7 cfm mep vlan level mepid mac.....	1273
9.5.8 cfm mep vlan level mepid reset counter.....	1273
9.5.9 cfm mip vlan level.....	1274
9.5.10 cfm mip vlan level mac	1275
9.5.11 cfm ping.....	1276
9.5.12 cfm reset counter	1278
9.5.13 cfm trace.....	1279
9.5.14 cross-check {enable disable}	1282
9.5.15 cross-check start-delay	1283
9.5.16 debug cfm.....	1284
9.5.17 ma name vlan	1285
9.5.18 md name level	1287
9.5.19 mip auto-config vlan	1288
9.5.20 mip-ccdb aging-time.....	1289
9.5.21 no mep all.....	1289
9.5.22 no mip all.....	1290
9.5.23 remote-mep aging-time	1291
9.5.24 remote-mep mep-id	1292
9.5.25 reset counter	1293
9.5.26 senderid-tlv-type.....	1294

9.5.27 show cfm	1294
9.5.28 show cfm config	1295
9.5.29 show cfm error ccdb	1296
9.5.30 show cfm ma	1297
9.5.31 show cfm md	1299
9.5.32 show cfm mep	1301
9.5.33 show cfm mep ccdb	1302
9.5.34 show cfm mip	1303
9.5.35 show cfm mip ccdb	1304
9.5.36 show cfm pdu-statistic	1305
9.5.37 show cfm remote-mep	1306
9.5.38 show cfm trace-result mep vlan level mepid	1307
9.5.39 snmp-trap	1308
9.5.40 trace-replay aging-time	1309
9.6 Y.1731 Configuration Commands	1309
9.6.1 debug y1731 packet	1309
9.6.2 debug y1731 module	1312
9.6.3 show y1731	1314
9.6.4 show y1731 ccdb	1314
9.6.5 show y1731 config	1316
9.6.6 show y1731 error ccdb	1317
9.6.7 show y1731 meg	1317
9.6.8 show y1731 mep	1318
9.6.9 show y1731 mip	1319
9.6.10 show y1731 pdu-statistic	1320
9.6.11 show y1731 remote-mep	1321
9.6.12 show y1731 trace-result	1323
9.6.13 y1731 ping	1323
9.6.14 y1731 trace	1325
9.6.15 y1731	1327
9.6.16 meg vlan level	1328
9.6.17 no meg all	1329

9.6.18 mip auto-config vlan	1330
9.6.19 snmp-trap	1331
9.6.20 y1731 mep vlan level mepid	1331
9.6.21 y1731 mep vlan level mepid ais	1332
9.6.22 y1731 mep vlan level mepid ccm	1334
9.6.23 y1731 mep vlan level mepid mac	1335
9.6.24 y1731 mep vlan level mepid reset counter	1336
9.6.25 y1731 mep vlan level mepid service-type	1337
9.6.26 y1731 mip vlan level	1337
9.6.27 y1731 mip vlan level mac	1338
9.6.28 y1731 reset counter	1339
9.6.29 ais {enable disable}	1340
9.6.30 ais loss-threshold	1341
9.6.31 ais-interval	1341
9.6.32 ccm {enable disable}	1342
9.6.33 ccm loss-threshold	1343
9.6.34 ccm-interval	1343
9.6.35 cross-check {enable disable}	1344
9.6.36 cross-check start-delay	1345
9.6.37 lock {enable disable}	1345
9.6.38 lock loss-threshold	1346
9.6.39 lock-interval	1347
9.6.40 no remote-mep all	1347
9.6.41 no y1731 mep all	1348
9.6.42 no y1731 mip all	1349
9.6.43 remote-mep aging-time	1349
9.6.44 remote-mep mep-id mac	1350
9.6.45 remote-mep mep-id	1351
9.6.46 reset counter	1352
9.6.47 senderid-tlv-type	1352
9.6.48 service-type	1353
9.6.49 trace-reply aging-time	1354

9.7 G.8032 Configuration Commands.....	1355
9.7.1 debug g8032	1355
9.7.2 g8032.....	1356
9.7.3 g8032 instance mip-port.....	1357
9.7.4 g8032 instance {port1 port2}[Interface Configuration View].....	1357
9.7.5 g8032 instance {add remove} mip-port.....	1358
9.7.6 g8032 instance {port1 port2}[G8032 Configuration View]	1359
9.7.7 g8032 instance {port1 port2} fs.....	1360
9.7.8 g8032 instance {port1 port2} ms.....	1361
9.7.9 g8032 instance channel	1361
9.7.10 g8032 instance clear	1362
9.7.11 g8032 instance mel.....	1363
9.7.12 g8032 instance mode	1364
9.7.13 g8032 instance role.....	1364
9.7.14 g8032 instance rpl	1365
9.7.15 g8032 instance vc-holdoff-timer	1366
9.7.16 g8032 instance vc-mel.....	1367
9.7.17 g8032 instance vc-mep {port1 port2 none}	1367
9.7.18 g8032 instance version	1368
9.7.19 g8032 instance virtual-channel.....	1369
9.7.20 g8032 instance vlan.....	1369
9.7.21 g8032 instance wtr-timer.....	1370
9.7.22 g8032 instance guard-timer	1371
9.7.23 g8032 instance hold-off-timer	1372
9.7.24 g8032 trap {enable disable}	1372
9.7.25 g8032 vs-switch {enable disable}	1373
9.7.26 no g8032 instance.....	1374
9.7.27 show g8032	1374
9.7.28 show g8032 instance	1375
9.7.29 show g8032 instance interface	1376
9.7.30 show g8032 interface.....	1377
9.8 UDLD Configuration Commands	1377

9.8.1 debug udd	1377
9.8.2 udd work-mode	1378
9.8.3 udd uni-shutdown	1379
9.8.4 udd advertise-interval	1379
9.8.5 udd {enable disable}	1380
9.8.6 udd aggressive {enable disable}	1381
9.8.7 udd cisco-checksum {enable disable}	1382
9.8.8 show udd local	1382
9.8.9 show udd interface	1383
9.8.10 show udd peer	1384
9.8.11 show udd config	1384
Chapter 10 Device Management Commands	1386
10.1 Hardware Configuration Commands	1386
10.1.1 debug fan	1386
10.1.2 cpu low-threshold high-threshold	1387
10.1.3 cpu trap	1388
10.1.4 cpu monitor	1388
10.1.5 fanctrl level	1389
10.1.6 fanctrl low-threshold high-threshold	1390
10.1.7 fanctrl mode	1391
10.1.8 fanctrl trap	1391
10.1.9 fanctrl monitor	1392
10.1.10 power trap	1393
10.1.11 power monitor	1394
10.1.12 memory low-threshold high-threshold	1394
10.1.13 memory trap	1395
10.1.14 memory monitor	1396
10.1.15 show cpu configure	1397
10.1.16 show cpu statistic	1397
10.1.17 show fan	1398
10.1.18 show memory pool	1399
10.1.19 show temperature	1402

10.1.20 show temperature config	1403
10.1.21 temperature low-threshold high-threshold	1404
10.1.22 temperature trap.....	1405
10.1.23 temperature monitor	1406
10.1.24 show cpu.....	1406
10.1.25 show fanctrl config.....	1407
10.1.26 show power	1408
10.1.27 show system chassis	1409
10.1.28 show hwmc l2 forwarding-table.....	1409
10.1.29 show hwmc l3 forwarding-table.....	1410
10.2 Mirror Configuration Commands.....	1411
10.2.1 debug mirror	1411
10.2.2 mirror group (Local Mirror).....	1412
10.2.3 mirror group (Remote Mirror).....	1413
10.2.4 mirror {ingress egress both} group.....	1414
10.2.5 show mirror config.....	1415
10.2.6 show mirror group	1416
10.2.7 show mirror interface	1417
10.3 Log Management Commands	1418
10.3.1 show syslog	1418
10.3.2 syslog facility	1418
10.3.3 syslog server.....	1420
10.3.4 clear abnormal-log.....	1421
10.3.5 clear logging {logbuffer trapbuffer}	1422
10.3.6 clear logging logfile.....	1422
10.3.7 clear logging source.....	1423
10.3.8 logging import {log trap debug}.....	1424
10.3.9 logging logfile path	1425
10.3.10 logging logfile max-number	1425
10.3.11 logging logfile size	1426
10.3.12 logging source action.....	1427
10.3.13 logging source logfile size kbytes	1430

10.4.11 laser bias-current-threshold auto	1462
10.4.12 laser rx-power-threshold.....	1463
10.4.13 laser rx-power-threshold auto.....	1463
10.4.14 laser temperature-threshold	1464
10.4.15 laser temperature-threshold auto	1465
10.4.16 laser trap {enable disable}	1466
10.4.17 laser tx-power-threshold.....	1466
10.4.18 laser tx-power-threshold auto	1467
10.4.19 laser voltage-threshold	1468
10.4.20 laser voltage-threshold auto.....	1469
10.4.21 transceiver power low trigger error-down {enable disable}	1469
10.4.22 ddm report interval	1470
10.5 Patch Configuration Commands	1471
10.5.1 debug patch	1471
10.5.2 patch load	1472
10.5.3 patch active.....	1473
10.5.4 patch deactivate	1473
10.5.5 patch delete.....	1474
10.5.6 show patch information	1475
10.6 STG Configuration Commands.....	1476
10.6.1 debug stg	1476
10.6.2 reset stg error.....	1476
10.6.3 show stg.....	1477
10.6.4 show stg instance.....	1478
10.6.5 show stg interface.....	1478
10.6.6 show stg protocol	1479
Chapter 11 O&M Commands.....	1481
11.1 NTP Configuration Commands	1481
11.1.1 debug ntp	1481
11.1.2 ntp.....	1482
11.1.3 ntp broadcast-client	1482
11.1.4 ntp multicast-client	1483

11.1.5 ntp broadcast-server.....	1484
11.1.6 ntp multicast-server	1485
11.1.7 show ntp	1487
11.1.8 show ntp service	1487
11.1.9 show ntp service verbose.....	1488
11.1.10 show ntp config	1491
11.1.11 authentication {enable disable}	1492
11.1.12 authentication-keyid	1492
11.1.13 client update-interval	1493
11.1.14 master	1494
11.1.15 ntp unicast-peer	1495
11.1.16 ntp unicast-server.....	1498
11.1.17 oncesync	1501
11.1.18 server broadcast-interval.....	1502
11.1.19 stratum	1503
11.1.20 trusted-keyid {enable disable}	1504
11.1.21 ntp6 multicast-client	1504
11.1.22 ntp6 multicast-server	1505
11.1.23 ntp6 unicast-peer	1507
11.1.24 ntp6 unicast-server.....	1510
11.1.25 timestamp precision-time	1513
11.1.26 icmp timestamp to-cpu	1514
11.2 RMON Configuration Commands.....	1514
11.2.1 rmon history	1514
11.2.2 rmon statistics.....	1515
11.2.3 show rmon alarm	1516
11.2.4 show rmon config.....	1517
11.2.5 show rmon event.....	1518
11.2.6 show rmon history	1519
11.2.7 show rmon history statistics	1520
11.2.8 show rmon log.....	1521
11.2.9 show rmon statistics	1522

11.2.10 rmon event	1524
11.2.11 rmon alarm	1525
11.3 SNMP Configuration Commands	1526
11.3.1 snmp trap-history {enable disable}	1526
11.3.2 snmp trap-history	1527
11.3.3 snmp rich-trap {enable disable}	1528
11.3.4 show snmp trap-history	1528
11.3.5 show snmp trap-description	1529
11.3.6 snmp snmp6 trap-server	1530
11.3.7 snmp view	1531
11.3.8 snmp version	1532
11.3.9 snmp user	1533
11.3.10 snmp trap-source	1534
11.3.11 snmp rw-community	1535
11.3.12 snmp reply-source-ip {enable disable}	1536
11.3.13 snmp contact	1537
11.3.14 snmp fail-count	1538
11.3.15 snmp group	1538
11.3.16 snmp location	1539
11.3.17 snmp reauth-interval	1540
11.3.18 snmp reply-auth-fail {enable disable}	1541
11.3.19 snmp community	1542
11.3.20 snmp auth-trap	1543
11.3.21 snmp bulk max-varbind	1544
11.3.22 show snmp agent	1545
11.3.23 show snmp community	1546
11.3.24 show snmp config	1546
11.3.25 show snmp group	1547
11.3.26 show snmp statistic	1548
11.3.27 show snmp trap-server	1549
11.3.28 show snmp trap state	1550
11.3.29 show snmp user	1551

11.3.30 show snmp view	1552
11.3.31 debug snmp.....	1553
11.3.32 snmp snmp6 port	1553
11.4 LLDP Configuration Commands.....	1554
11.4.1 debug lldp.....	1554
11.4.2 lldp faststart-count	1555
11.4.3 lldp admin-status	1556
11.4.4 lldp basic-tlv-tx.....	1556
11.4.5 lldp dot1-tlv-tx port-vid.....	1557
11.4.6 lldp dot1-tlv-tx protocol-vid protocol-id.....	1558
11.4.7 lldp dot1-tlv-tx vlan-name.....	1559
11.4.8 lldp dot3-tlv-tx.....	1560
11.4.9 lldp location-id civic-address elin-address	1560
11.4.10 lldp management-address	1562
11.4.11 lldp med-notification	1563
11.4.12 lldp med-tlv-tx	1564
11.4.13 lldp trap {enable disable}	1565
11.4.14 lldp notification-interval	1566
11.4.15 lldp reinit-delay	1566
11.4.16 lldp tx-delay.....	1567
11.4.17 lldp tx-hold	1568
11.4.18 lldp tx-interval	1568
11.4.19 show lldp config interface	1569
11.4.20 show lldp config	1570
11.4.21 show lldp interface	1571
11.4.22 show lldp local.....	1572
11.4.23 show lldp local interface.....	1574
11.4.24 show lldp remote interface	1575
11.4.25 show lldp remote	1576
11.4.26 show lldp statistic	1577
11.5 Packet Capturing Configuration Commands.....	1578
11.5.1 capture cpupkt interface	1578

11.5.2 debug cpupkt interface	1580
11.5.3 show cpupkt interface statistic.....	1581
11.5.4 reset cpupkt interface statistic.....	1582
11.6 Telemetry Configuration Commands	1584
11.6.1 ip address port ipv6 address port	1584
11.6.2 sensor-path.....	1585
11.6.3 destination-group.....	1586
11.6.4 sensor-group	1586
11.6.5 telemetry {enable disable}.....	1587
11.6.6 telemetry destination-group.....	1588
11.6.7 telemetry sensor-group	1589
11.6.8 telemetry subscription	1590
11.6.9 show telemetry.....	1590
11.7 NQA Configuration Commands	1591
11.7.1 nqa {start stop}	1591
11.7.2 nqa test-instance	1592
11.7.3 type	1593
11.7.4 description	1593
11.7.5 frequency	1594
11.7.6 probe count	1595
11.7.7 probe timeout.....	1596
11.7.8 ttl.....	1596
11.7.9 tos	1597
11.7.10 destination ip	1598
11.7.11 data-fill	1598
11.7.12 data-size.....	1599
11.7.13 source ip	1600
11.7.14 history-record {enable disable}	1600
11.7.15 history-record keep-time.....	1601
11.7.16 history-record number	1602
11.7.17 nqa schedule	1602
11.7.18 show nqa result.....	1603

11.7.19 show nqa history.....	1604
11.7.20 show nqa agent	1605
11.7.21 show nqa config.....	1607
Chapter 12 VPN Commands	1608
12.1 L3VPN Configuration Commands	1615
12.1.1 debug l3vpn.....	1615
12.1.2 description	1615
12.1.3 ip binding vpn-instance	1616
12.1.4 ip ipv6 import-rib vpn-instance protocol static.....	1617
12.1.5 import-rib public protocol static.....	1618
12.1.6 ip vpn-instance snmp-trap	1619
12.1.7 ipv4-family ipv6-family	1620
12.1.8 vxlan vni.....	1621
12.1.9 vpn-target	1621
12.1.10 route-distinguisher.....	1623
12.1.11 show ip vpn-instance	1624
12.1.12 show ip vpn-instance verbose.....	1625
12.1.13 show ip vpn-instance config.....	1627
12.1.14 show ip vpn-instance import-vt	1628
12.1.15 show import-route	1629
12.1.16 route-distinguisher.....	1630
12.1.17 routing-table limit.....	1631
Chapter 13 Data Center Feature Commands.....	1633
13.1 VXLAN Configuration Commands	1633
13.1.1 bridge-domain	1633
13.1.2 interface nve	1634
13.1.3 interface bridge-domain	1634
13.1.4 vni ucast-peer	1635
13.1.5 tunnel source	1636
13.1.6 debug vxlan	1637
13.1.7 show bridge-domain.....	1638
13.1.8 show vxlan resource	1639

13.1.9 show nve peer.....	1639
13.1.10 show interface nve.....	1640
13.1.11 show ip arp vxlan.....	1641
13.1.12 show vxlan vni	1642
13.1.13 vxlan vni.....	1642
13.1.14 unknown-ucast {forward drop}	1643
13.1.15 vxlan anycast-gateway {enable disable}	1644
13.1.16 show ip bgp evpn route	1645
13.1.17 debug ipv6 nd l2-proxy	1646
13.1.18 show ipv6 nd l2-proxy.....	1647
13.1.19 reset vxlan statistics peer-ip.....	1648
13.1.20 debug trace vxlan.....	1648
13.1.21 ping vxlan vni source peer.....	1649
13.1.22 trace vxlan vni source peer.....	1650
13.1.23 rewrite egress vid.....	1651
13.1.24 rewrite no-action	1652
13.1.25 rewrite pop double.....	1653
13.1.26 debug hwvrf.....	1654
13.1.27 debug grpc	1654
13.1.28 grpc debug-level	1656
13.1.29 show mac-limit bridge-domain.....	1657
13.1.30 arp l2-proxy active-active gateway {enable disable}	1658
13.1.31 ipv6 nd l2-proxy active-active gateway {enable disable}	1659
13.2 EVPN Configuration Commands.....	1660
13.2.1 debug evpn	1660
13.2.2 evpn	1661
13.2.3 evpn-family	1661
13.2.4 evpn route-distinguisher	1662
13.2.5 evpn vpn-target.....	1663
13.2.6 neighbor enable	1665
13.2.7 vni replication-protocol	1666
13.2.8 vxlan vni.....	1667

13.2.9 show evpn.....	1667
13.2.10 show evpn vpn-target	1668
13.3 NETCONF Configuration Commands	1669
13.3.1 netconf {enable disable}	1669
13.3.2 netconf log {none terminal file}	1670
13.3.3 netconf debug-level {none off error warn info debug debug2 debug3 debug4}	1670
13.3.4 netconf log-per-size	1671
13.3.5 clear netconf candidate database	1672
13.3.6 show netconf candidate database.....	1673
13.3.7 show netconf	1673
13.3.8 show netconf sessions	1674
13.3.9 show netconf session statistics	1675
Chapter 14 Virtualization Configuration Commands.....	1677
14.1 Stack Command Configuration	1677
14.1.1 iss mode.....	1677
14.1.2 iss domain.....	1678
14.1.3 iss member.....	1678
14.1.4 iss priority.....	1679
14.1.5 iss master	1680
14.1.6 iss hello-interval	1681
14.1.7 interface stack-port.....	1681
14.1.8 join stack-port.....	1682
14.1.9 erase iss-config	1683
14.1.10 show iss-config.....	1683
14.1.11 show iss interface	1684
14.1.12 show iss topo	1685
14.1.13 show iss topo stack-port	1686
14.1.14 show iss topo stack-port hops.....	1686
14.1.15 show iss member	1687
14.1.16 show iss	1688
14.1.17 debug iss/no debug iss.....	1689
14.1.18 mad detect	1690

14.1.19 mad restore	1690
14.1.20 mad detect mode direct.....	1691
14.1.21 no mad detect	1692
14.1.22 mad exclude { enable disable}	1692
14.1.23 mad backup ip address	1693
14.1.24 debug mad	1694
14.1.25 show mad.....	1695
14.1.26 show mad config	1696

Chapter 1 Introduction to Command Configuration Views

1.1 Command Line Interface

The Switch provides a command line interface (CLI) with a series of configuration commands, using which you can configure and manage the switch. The CLI has the following features:

Local configuration is performed through the console interface.

Configuration commands are assigned different levels and can be used only by privileged users. This prevents unauthorized access to the switch by unauthorized users.

You can type in a question mark (?) to obtain online help information.

Network testing tools, such as ping, can help you quickly determine the reachability of a network.

A variety of detailed debugging information is available to help in network fault diagnosis.

To facilitate management, commands are divided into different groups. Each group has a specific command mode. You can switch between different command modes. Generally, a command mode supports only certain commands. Some commonly used commands (such as **help**, **list**, **exit**, and **end**) can be used in all modes.

1.2 Features of Command Configuration Views

The following table describes the command modes (views) on the Switch and their functions.

Command View	Function	Prompt	Entry Command	Exit Command
Privileged user view	Checks all running status and statistical information on the switch, and manages files and the system.	Switch#	You will enter this view as soon as a connection is set up with the switch.	Run exit to log out. You need to enter the user name and password again upon the next login.
Global configuration view	Configures global parameters of the switch.	Switch (config)#	Run config in the privileged user view.	Run exit to return to the privileged user view.
Common user view	Debugs some functions of the switch, upgrades the system software, and checks the running status and statistics of	Switch>	Run disable in the privileged user view.	Run enable to return to the privileged user view.

Command View	Function	Prompt	Entry Command	Exit Command
	the switch.			
Terminal configuration view	Configures a terminal.	Switch (config-line)#	Run line vty <1-32> in the global configuration view.	Run exit to return to the global configuration view.
Interface configuration view	Configures interface parameters on the switch. (N: interface number) You can configure individual Ethernet interfaces or trunk interfaces.	Switch(config- xe1/0/1)# Switch(config-e th-trunkN)#	Run interface xgigaethernet 1/0/1 or interface eth-trunk- N in the global configuration view.	Run exit to return to the global configuration view.
Interface group configuration view	Configures interface parameters on the switch.	Switch(config- xe1/0/1->xe1 /0/12)# Switch(config-i f-group)#	Run Switch(config)#i nterface xgigaethernet 1/0/1 to xgigaethernet 1/0/12 or Switch(config)#i nterface group 1/0/1,1/0/12-1/0/20 in the global configuration view.	Run exit to return to the global configuration view.
VLAN configuration view	Configures Layer 2 VLANs on the switch.	Switch(vlan-N1)#	Run vlan N1 in the global configuration view.	Run exit to return to the global configuration view.
VLANIF configuration view	Configures Layer 3 VLAN interfaces on the switch. (N: VLAN ID)	Switch (config-vlanif- N)#	Run interface vlan N in the global configuration view.	Run exit to return to the global configuration view.
STP configuration view	Configures the Spanning Tree Protocol (STP) on the switch.	Switch (config-stp)#	Run stp in the global configuration view.	Run exit to return to the global configuration view.
AAA configuration view	Configures the Remote	Switch(config-a aa)#	Run aaa in the global	Run exit to return to the global

Command View	Function	Prompt	Entry Command	Exit Command
	Authentication Dial In User Service (RADIUS) on the switch.		configuration view.	configuration view.
OSPFv2 configuration view	Configures the Open Shortest Path First (OSPF) on the switch.	Switch(config-ospf-1)#	Run router ospf in the global configuration view.	Run exit to return to the global configuration view.
Line configuration view	Line view configuration for user terminals, including the console terminal and virtual terminal	Switch (config-line)#	Run line console/vty in the global configuration view.	Run exit to return to the global configuration view.
Schedule-profile configuration view	Configures schedule-profile parameters.	Switch(config-schedule-profile-#)#	Run schedule-profile # in the global configuration view.	Run exit to return to the global configuration view.
Time-range configuration view	Configures the time-range on the switch.	Switch(config-timerange1)#	Run time-range list number in the global configuration view.	Run exit to return to the global configuration view.
MPLS remote-peer configuration view	Configures the remote-peer on the switch.	Switch(config-mplsldp-remote1)#	Run mpls ldp remote-peer index in the global configuration view.	Run exit to return to the global configuration view.
BGP configuration view	Configures the BGP on the switch.	Switch(config-bgp)#	Run router bgp AS -number in the global configuration view.	Run exit to return to the global configuration view.
Route-policy configuration view	Configure the route policy on the switch.	Switch(config-route-policy)#	Run route-policy name permit/deny node Index in the global configuration view.	Run exit to return to the global configuration view.
Rlink configuration	Configures the Rlink	Switch(config-r	Run rlink group	Run exit to return to

Command View	Function	Prompt	Entry Command	Exit Command
view	function on the switch.	link1)#	rlink-group-number in the global configuration view.	the global configuration view.
Mlink configuration view	Configures mlink on the switch.	Switch(config-mlink1)#	Run mlink group mlink-group number in the global configuration view.	Run exit to return to the global configuration view.
NTP configuration view	Configures the Network Time Protocol (NTP) on the switch.	Switch(config-ntp)#	Run ntp in the global configuration view.	Run exit to return to the global configuration view.
Filter configuration view	Configures filters on the switch.	Switch(configure-filter-filter type- filter list number)#	Run filter filter list number in the global configuration view. List numbers 1001-2000 specify IPv4 ACLs.	Run exit to return to the global configuration view.
Filter configuration view (IPv6)	Configures the Filterv6r on the switch.	Switch(configure-filter-filter type- filter list number)#	Run filter filter list number in the global configuration view. List numbers <3001-4000> specify IPv6 ACLs.	Run exit to return to the global configuration view.
Filter-hybrid configuration view	Configures hybrid filters on the switch.	Switch(configure-filter-filter type- filter list number)#	Run filter filter list number in the global configuration view. List numbers 2001-3000 specify hybrid	Run exit to return to the global configuration view.

Command View	Function	Prompt	Entry Command	Exit Command
			ACLs.	
Layer-2 filter configuration view	Configures Layer-2 filters on the switch.	Switch(configure-filter-filter type- filter list number)#	Run filter filter list number in the global configuration view. List numbers 1-1000 specify Layer-2 ACLs.	Run exit to return to the global configuration view.
DHCP pool configuration view	Configures the DHCP address pool on the switch.	Switch(config-dhcp-pool-N1)#	Run dhcp pool N1 in the global configuration view.	Run exit to return to the global configuration view.
VPN configuration view	Configures the L3VPNP on the switch.	Switch(config-vpn-instance-name)#	Run ip vpn-instance name in the global configuration view.	Run exit to return to the global configuration view.
Y1731 configuration view	Configures the Y1731 on the switch.	Switch(config-y1731)#	Run y1731 in the global configuration view.	Run exit to return to the global configuration view.
Address family configuration view	Configures the address family on the switch.	Switch(config-bgp-af-ipv4)#	Run ipv4-family unicast in the BGP view.	Run exit to return to the global configuration view.
MA configuration view	Configures the MA on the switch.	Switch(config-md-mdname-ma-maname)#	Run ma name ma-name vlan vlan-id in the MD view.	Run exit to return to the global configuration view.
Meg configuration view	Configures the meg on the switch.	Switch(config-meg-icc string-umc string)#	Run meg vlan vlan-id level level icc icc-string umc umc-string in the Y1731 configuration view.	Run exit to return to the global configuration view.
Loopback interface configuration view	Configures the loopback interface on the switch.	Switch(config-loopback-loopbacknumber)#	Run interface loopback number in the global	Run exit to return to the global configuration view.

Command View	Function	Prompt	Entry Command	Exit Command
			configuration view.	
Tunnel interface configuration view	Configures the tunnel interface on the switch.	Switch(config-tunnel- Tunnel interface number)#	Run interface tunnel Tunnel interface number in the global configuration view.	Run exit to return to the global configuration view.
MVLAN configuration view	Configures IGMP snooping on the switch.	Switch(config-igmpsnoop-mvlan4000)#	Run igmp-snooping mvlan vlan-id in the global configuration view.	Run exit to return to the global configuration view.
MPLS LDP configuration view	Configures the MPLS VPN on the switch.	Switch(config-mpls-ldp-1)	Run mpls ldp vpn-instance name in the global configuration view.	Run exit to return to the global configuration view.
BD view	Configures bridge domains on the switch.	Switch(config)#bridge-domain 1	Run bridge-domain bd-id in the global configuration view.	Run exit to return to the global configuration view.

Chapter 2 Basic Commands

This chapter introduces the commands for configuring basic functions of the system, including basic configuration, user terminal configuration, file system configuration, configuration file operations, file uploading and downloading configuration, and Telnet or SSH login.

2.1 Basic Configuration Commands

This section introduces basic configuration commands of this device.

2.1.1 auth-degenerate {enable|disable}

Function

The **auth-degenerate {enable|disable}** command enables or disables switching from the user authentication mode to the local authentication mode.

Format

auth-degenerate { enable | disable }

Parameter

Parameter	Description	Value
enable	Enables switching from the user authentication mode to the local authentication mode.	-
disable	Disables switching from the user authentication mode to the local authentication mode.	-

Default Value

NA

View

Global configuration view

Usage Guidelines

NA

Example

Enable switching from the user authentication mode to the local authentication mode.

```
Switch(config)#auth-degenerate
```

```
Switch(config)#
```

2.1.2 case-sensitive

Function

The **case-sensitive** command configures the CLI terminal to be case sensitive or case insensitive.

Format

case-sensitive { enable | disable }

Parameter

Parameter	Description	Value
enable	Configures the terminal to be case sensitive.	-
disable	Configures the terminal to be case insensitive.	-

Default Value

enable

View

Global configuration view

Usage Guidelines

NA

Example

Enable the terminal to be case sensitive.

```
Switch(config)#case-sensitive enable
Switch(config)#
```

2.1.3 clear configuration

Function

The **clear configuration** clears configurations of an interface.

Format

clear configuration

Parameter

NA

Default Value

NA

View

Out-of-band interface configuration view, Loopback interface configuration view, Tunnel interface configuration view, BD interface configuration view, NVE interface configuration view, Ethernet bridge interface configuration view, Ethernet routing interface configuration view, Trunk interface configuration view, and interface configuration view (trunk)

Usage Guidelines

NA

Example

Switch from the privileged user view to the global configuration view.

```
Switch(config-10ge1/0/1)#clear configuration
WARNING:All configurations of the interface will be cleared, and its state will be shutdown.Continue?(y/n) [y]y
Switch(config-10ge1/0/1)#
```

2.1.4 cls

Function

The **cls** command clears information displayed on the current CLI.

Format

cls

Parameter

NA

Default Value

NA

View

All configuration views except the common user view

Usage Guidelines

If too much information is displayed on CLI and affects operations on the system or you no longer need the displayed information, run this command to clear the information.

Example

Clear information displayed on the CLI.

```
Switch#cls
Switch#
```

2.1.5 configure

Function

The **configure** command switches from the privileged user view to the global configuration view.

Format

configure

Parameter

NA

Default Value

NA

View

Privileged user view

Usage Guidelines

In the privileged user view, you can check all running status and statistical information on the switch, and manages files and the system.

In the global configuration view, you can configure global parameters of the switch in addition to configuration privilege in the privileged user view.

Example

Switch from the privileged user view to the global configuration view.

```
Switch#configure
Switch(config)#
```

2.1.6 command-privilege level view

Function

The **command-privilege level view** command sets the command level in the specified view.

The **no command-privilege level view** command restores the command level to the default value.

Format

- **command-privilege level** *level-value* **view** { **configure** | **bgp**|**bgp-af-ipv4** | **bgp-af-ipv4-mcast** | **bgp-af-ipv4-vpn** | **bgp-af-ipv4-vpn-mcast** | **bgp-af-ipv6** | **bgp-af-ipv6-vpn** | **bgp-af-vpnv4** | **bgp-af-vpnv6** | **bgp-af-l2vpn** | **bgp-af-ipv4-label** | **bgp-af-vpls** | **aaa** | **cpu-defend-policy** | **dhcp-pool** | **dhcpv6-pool** | **filter-lay2** | **filter-ipv4** | **filter-ipv6** | **filter-hybrid** | **g8032** | **igmpsnoop-mvlan** | **igmp** | **igmp-vpn** | **isis** | **mld** | **mldsnoop-mvlan** | **mlink** | **ip-vpn** | **ntp** | **ospf** | **ospfv3** | **pim** | **pim6** | **policy-route** | **isolate-group** | **ripng** | **rip** | **rlink** | **route-policy** | **stp** | **time-range** | **schedule-profile** | **view** | **enable** | **if-fe** | **if-ge** | **if-10ge** | **vlanif** | **eth-trunk** | **line** | **view** | **vlan** } [*.COMMAND*]
- **no command-privilege level** *level-value* **view** { **configure** | **bgp**|**bgp-af-ipv4** | **bgp-af-ipv4-mcast** | **bgp-af-ipv4-vpn** | **bgp-af-ipv4-vpn-mcast** | **bgp-af-ipv6** | **bgp-af-ipv6-vpn** | **bgp-af-vpnv4** | **bgp-af-vpnv6** | **bgp-af-l2vpn** | **bgp-af-ipv4-label** | **bgp-af-vpls** | **aaa** | **cpu-defend-policy** | **dhcp-pool** | **dhcpv6-pool** | **filter-lay2** | **filter-ipv4** | **filter-ipv6** | **filter-hybrid** | **g8032** | **igmpsnoop-mvlan** | **igmp** | **igmp-vpn** | **isis** | **mld** | **mldsnoop-mvlan** | **mlink** | **ip-vpn** | **ntp** | **ospf** | **ospfv3** | **pim** | **pim6** | **policy-route** | **isolate-group** | **ripng** | **rip** | **rlink** | **route-policy** | **stp** | **time-range** | **schedule-profile** | **view** | **enable** | **if-fe** | **if-ge** | **if-10ge** | **vlanif** | **eth-trunk** | **line** | **view** | **vlan** } [*.COMMAND*]

Parameter

Parameter	Description	Value
level-value	Specifies the command level.	The value is an integer ranging from 0 to 15.
COMMAND	Specifies the set command.	The value is a command string.

Default Value

NA

View

Global configuration view

Usage Guidelines

The system assigns a level for each command in each view. The device administrator can reset the command level so some low-level users can use some high-level commands or increase the command level to increase the device security.

Non-professionals are not recommended to change the command default level; otherwise, operation or maintenance inconvenience or even device security hazard may occur.

Example

Set the **cd** command level to 5.

```
Switch(config)#command-privilege level 5 view configure cd
Switch(config)#
```

2.1.7 debug cli

Function

The **debug cli** command enables the CLI debugging function.

The **no debug cli** command disables the CLI debugging function.

Format

- **debug cli** { cmd | pty | auth | exec-config | show-config | sync | telnetd }
- **no debug cli** { cmd | pty | auth | exec-config | show-config | sync | telnetd | all }

Parameter

NA

Default Value

NA

View

Privileged user view

Usage Guidelines

NA

Example

Enable the CLI debugging function.

```
Switch#debug cli cmd
Switch#
```

2.1.8 debug clock

Function

The **debug clock** command enables the clock debugging function.

The **no debug clock** command disables the clock debugging function.

Format

- **debug clock**

- **no debug clock**

Parameter

NA

Default Value

NA

View

Privileged user view

Usage Guidelines

NA

Example

Enable the clock debugging function.

```
Switch#debug clock
Switch#
```

2.1.9 disable

Function

The **disable** command returns to the global configuration view from the privileged user view.

The **disable *privilege-value*** command decreases the current user privilege level to 0-15.

Format

- **disable**
- **disable *privilege-value***

Parameter

Parameter	Description	Value
privilege-value	Specifies a user privilege level.	The value is an integer ranging from 0 to 15.

Default Value

NA

View

Privileged user view, common user view

Usage Guidelines

NA

Example

Return to the global configuration view from the privileged user view.

```
Switch#disable
Switch>
```

2.1.10 enable**Function**

The **enable** command switches from the common user view to the privileged user view.

The **enable *privilege-value*** command increases the current user privilege level to 0-15. The default is 15.

Format

enable *privilege-value*

Parameter

Parameter	Description	Value
privilege-value	Specifies a user privilege level.	The value is an integer ranging from 0 to 15.

Default Value

NA

View

Common user view, privileged user view

Usage Guidelines

NA

Example

Increase the current user privilege level to 11.

```
Switch#enable 11
Switch#
```

2.1.11 enable password**Function**

The **enable password** command sets the global local secondary authentication password for users of level 0-15.

The **no enable password** command deletes the global local secondary authentication password for users of level 0-15.

Format

- **enable password level** *level-value* { **cipher** | **plain** } *password*
- **enable password** { **cipher** | **plain** } *password*
- **no enable password level** *level-value*
- **no enable password**

Parameter

Parameter	Description	Value
level-value	Specifies a privilege level.	The value is an integer ranging from 0 to 15.
{ cipher plain }	Displays the password in cipher text or plain text.	-
password	Specifies a password.	The value is a character string.

Default Value

NA

View

Global configuration view

Usage Guidelines

If you do not specify a privilege level in the command, the command configures or deletes the local secondary authentication password for users of level 15.

Example

Configure the local secondary authentication password globally.

```
Switch(config)#enable password cipher password testkey
Switch(config)#
```

2.1.12 end

Function

The **end** command returns to the privileged user view from the current configuration view.

Format

end

Parameter

NA

Default Value

NA

View

All configuration views

Usage Guidelines

You can use this command to return to the privileged user view directly from any configuration view.

Example

Return to the privileged user view.

```
Switch(config)#end
Switch#
```

2.1.13 exit

Function

The **exit** command returns to the previous configuration view from the current configuration view. If you run this command in the common user view or privileged user view, the login interface is displayed or the connection with the switch is terminated.

Format

exit

Parameter

NA

Default Value

NA

View

All configuration views

Usage Guidelines

You can use this command to exit from the current configuration view and return to the previous lower-level configuration view.

The **end** and **exit** commands differ in that the **end** command returns to the privileged user view regardless of the current view, whereas the **exit** command returns to the previous configuration view.

The **exit** command returns from a high-level command view to a low-level command view. You can also switch between command modes of the same level. You can also enter the **CTRL+Z** or **end** command to return from a high-level command view directly to the privileged user view.

Example

Return to the previous lower-level configuration view.

```
Switch(config-vlanif-10)#exit
Switch(config)#
```

2.1.14 header login

Function

The **header login** command configures the login title.

The **no header login** command restores the default login title.

Format

- **header login**
- **header login localfile** *file-name*
- **no header login**

Parameter

Parameter	Description	Value
file-name	Specifies the local file name.	The value is a character string of up to 128 bytes. The path and name of the directory or file are case insensitive and cannot contain the following characters: space, ~, *, /, \, :, and '.

Default Value

NA

View

Global configuration view

Usage Guidelines

When you log in to the switch from a terminal, the switch displays the login title.

The login title is a character string and can contain up to 500 bytes. If you enter more than 500 bytes, the first 500 bytes takes effect. Press **CTRL+Z** to end the input and press **CTRL+C** to exit the input.

Example

Set the login title to "Hello! Welcome to use Switch!".

```
Switch(config)#header login
Enter message, end with CTRL+Z ; abort with CTRL+C

Input header login:Hello!Welcome to use Switch!

Switch(config)#quit
Switch#quit

User Access Verification

Username: admin
Password: *****
Hello!Welcome to use Switch!
Switch#
```

2.1.15 help**Function**

The **help** command displays system help information.

Format

help

Parameter

NA

Default Value

NA

View

All configuration views

Usage Guidelines

The Switch provides convenient online help. The **help** command displays information about the entire online help system. You can type in a question mark (?) anytime, anywhere to obtain all or part of help information.

If online help is unavailable, the help information is blank. You must return to the previous status until online help information is displayed after you type in a question mark (?).

Example

Display online help information.

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

2.1.16 hostname

Function

The **hostname** command sets the host name of the switch.

The **no hostname** command restores the default host name of the switch.

Format

- **hostname** *host-name*
- **no hostname**

Parameter

Parameter	Description	Value
host-name	Specifies a host name for the switch.	The value is a string of 1-128 bytes.

Default Value

NA

View

Global configuration view

Usage Guidelines

Changing the host name of the switch will change the prompt displayed on the CLI. For example, if the host name of the switch is set to Switch, the prompt in the user view will be Switch.

Example

Set the host name of the switch to S1.

```
Switch(config)#hostname S1
S1(config)#
```

2.1.17 list

Function

The **list** command displays all the commands that can be used in the current configuration view.

Format

list [*keyword*]

Parameter

Parameter	Description	Value
keyword	Specifies the command keyword.	The value is a character string.

Default Value

NA

View

All configuration views

Usage Guidelines

This command has many advantages and functions like **dir** of MS-DOS and **ls** of UNIX. The advantage of this command is that it releases you from remembering all commands. If you forget a command, use this command to find the desired command.

Example

View all commands available in the global configuration view.

```
Switch(config)#list
  attrib NAME (+r|+s|+h|-r|-s|-h)
  attrib NAME (+r|+s|+h|-r|-s|-h) subtree
  cd
  cd DIR
```

```

clear ip pim resource
clock set <0-23>:<0-59>:<0-59> <1-31> <1-12> <2001-2100>
clock set <0-23>:<0-59>:<0-59> <2001-2100>/<1-12>/<1-31>
clock summer-time NAME date <0-23>:<0-59> <1-31> <1-12> <2001-2100> <0-23>:<0-59> <1-31>
<1-12> <2001-2100>
clock summer-time NAME date <0-23>:<0-59> <2001-2100>/<1-12>/<1-31> <0-23>:<0-59>
<2001-2100>/<1-12>/<1-31>
clock summer-time NAME recurring (first|second|third|fourth|fifth|last)
(monday|tuesday|wednesday|thursday|friday|saturday|sunday)
(january|february|march|april|may|june|july|august|september|october|november|december) <0-23>:<0-59>
(first|second|third|fourth|fifth|last) (monday|wednesday|tuesday|thursday|friday|saturday|sunday)
(january|february|march|april|may|june|july|august|september|october|november|december) <0-23>:<0-59>
clock timezone NAME (add|minus) <0-23>:<0-59>
cls
configure
copy SRCFILE DESTFILE
cpu spy-window <5-900>
Switch(config)#

```

2.1.18 ping|ping6

Function

The **ping** command tests the connectivity of the IPv4 network.

The **ping6** command tests the connectivity of the IPv6 network.

Format

- **ping** *mac-address*
- **ping** *mac-address* { **-n** | **-l** | **-w** | **-v** } *VALUE1*
- **ping** *mac-address* { **-n** | **-l** | **-w** | **-v** } *VALUE1* { **-n** | **-l** | **-w** | **-v** } *VALUE1*
- **ping** *mac-address* { **-n** | **-l** | **-w** | **-v** } *VALUE1* { **-n** | **-l** | **-w** | **-v** } *VALUE1* { **-n** | **-l** | **-w** | **-v** } *VALUE1*
- **ping** *mac-address* { **-n** | **-l** | **-w** | **-v** } *VALUE1* { **-n** | **-l** | **-w** | **-v** } *VALUE1* **-t**
- **ping** *mac-address* { **-n** | **-l** | **-w** | **-v** } *VALUE1* **-t**
- **ping** *mac-address* **-t**
- **ping** *ipv4-address string1*
- **ping** *ipv6-address string2*

Parameter

Parameter	Description	Value
-t	Sends the ICMP ECHO packet repeatedly.	-
-n	Indicates the number of ICMP ECHO packets sent.	The value ranges from 1 to 4294967295. The default value is 5.
-l	Indicates the length of ICMP ECHO packets sent.	The value ranges from 12 to 65500. The default value is 64.
-w	Specifies a timeout duration for each response.	The value ranges from 1 to 10000, in ms. The default value is 5000.
mac-address	Specifies the MAC address of a host.	The format is AA:BB:CC:DD:EE:FF, where A to F are hexadecimal digits.
ipv6-address	Specifies an IPv6 address.	In this format, a 128-digit IP address is divided into 8 segments. Each segment consists of 16 digits and is represented by 4 hexadecimal characters (0-9 and A-F). Segments are separated by colons (:). Every "X" represents a group of hexadecimal digits.
ipv4-address	Specifies an IPv4 address.	The value is in dotted decimal notation.
string1	Selects the parameter based on the switch prompt message.	(-n system-time t q f <1-4294967295> h <1-255> l <12-65500> w <1-10000> tos <0-255> m <1-65500> dscp <0-63> -8021p <0-7> s A.B.C.D -vpn-instance VPNNAME -i xgigae thernet 10gigaethernet 25gigaethernet 40gigaethernet 100giga ethernet vlan loopback eth-trunk mgt-eth <1-32> <0-2> <1-48 > <1-4094> <0-127> <1-128> <0-0> <0-0> <0-0> NAMECR)
string2	Selects the parameter based on the switch prompt message.	(-n t <1-4294967295> h <1-255> l <12-65500> w <1-10000> m <1-65500> tc <0-255> -8021p <0-7> s X:X::X:X -vp n-instance VPNNAME -i xgigaethernet 10gigaethernet 25gig aethernet 40gigaethernet 100gigaethernet vlan loopback eth-tr unk mgt-eth <1-32> <0-2> <1-48> <1-4094> <0-127> <1-128> <0-0> <0-0> <0-0> NAMECR)

Default Value

NA

View

Privileged user view

Usage Guidelines

If an IP network fails, you can use this command to locate the failure point.

In a ping test, the switch sends ICMP Echo Request packets to the destination host. If the network connection with the destination is normal,

the destination responds with ICMP Echo Reply packets after receiving the ICMP Echo Request packets.

The **ping** command can be used to determine whether a network connection failure occurs or to evaluate the quality of network lines. The command output information includes the following:

Response of destination host to each Echo Request packet. If the switch does not receive an Echo Reply packet, it displays “Request time out.” If the switch receives an Echo Reply packet, it displays the number of bytes, response time, Time-to-Live (TTL) value, and sequence number of the packet.

Final statistics, including the number of packets sent, number of reply packets received, percentage of packets for which no reply is received, as well as the minimum, maximum, and average of response time.

Example

Test whether the IP address 10.18.10.8 is reachable.

```
Switch#ping 10.18.10.8 -t
PING 10.18.10.8: 56 data bytes
Reply from 10.18.10.8: bytes=64 time=0ms TTL=128 icmp_seq=0
Reply from 10.18.10.8: bytes=64 time=0ms TTL=128 icmp_seq=1
Reply from 10.18.10.8: bytes=64 time=0ms TTL=128 icmp_seq=2
Reply from 10.18.10.8: bytes=64 time=0ms TTL=128 icmp_seq=3
Reply from 10.18.10.8: bytes=64 time=0ms TTL=128 icmp_seq=4
PING Statistic for 10.18.10.8
5 packets transmitted, 5 packets received, 0% packet loss
round-trip (ms)  min/avg/max = 0/0/0
Switch#
```

2.1.19 ping vxlan vni

Function

The **ping vxlan vni** command tests the connectivity of the VXLAN tunnel.

Format

ping vxlan vni *vni-id*

Parameter

Parameter	Description	Value
vni-id	Specifies a VNI ID.	The value is an integer ranging from 1 to 16777215.

Default Value

NA

View

Privileged user view

Usage Guidelines

NA

Example

Test the connectivity of the VXLAN tunnel.

```
Switch#ping vxlan vni 1
Switch#
```

2.1.20 quit**Function**

The **quit** command returns to the previous configuration view from the current configuration view. If you run this command in the common user view or privileged user view, the login interface is displayed or the connection with the switch is terminated.

Format**quit****Parameter**

NA

Default Value

NA

View

All configuration views

Usage Guidelines

The **quit** command returns from a high-level command view to a low-level command view. You can also switch between command modes of the same level. You can enter CTRL+Z or end command to return from a high-level command view directly to the privileged user view. This command provides the same function as the **exit** command.

Example

Return to the previous lower-level configuration view.

```
Switch(config-vlanif-10)#quit
Switch(config)#
```

2.1.21 reset recycle**Function**

The **reset recycle** command resets the recycle bin.

Format

reset recycle

Parameter

NA

Default Value

NA

View

Privileged user view

Usage Guidelines

NA

Example

Display information about users who have logged in and are configuring the switch.

```
Switch(config)#reset recycle
Switch(config)#
```

2.1.22 reboot**Function**

The **reboot** command reboots the switch.

Format

reboot

Parameter

NA

Default Value

NA

View

Privileged user view

Usage Guidelines

This command provides the same function as a cold restart. Using this command, you can reboot the switch remotely, without the need to go to the equipment room.



Warning:

Do not use this command unless necessary, because it will cause a temporary interruption of the network. In addition, it is recommended that you determine whether to save the configuration file before the reboot.

Example

Reboot Switch.

```
Switch#reboot
  WARNING:System will reboot! Continue?(y/n) [y]y
  System now is rebooting,please wait.
Switch
```

2.1.23 reboot {at|in}

Function

The **reboot at** command reboots the switch at specified time.

The **reboot in** command reboots the switch after a specified delay.

Format

- **reboot at** *time1*
- **reboot at** *time2*
- **reboot in** *time*

Parameter

Parameter	Description	Value
time1	Specifies the reboot time accurate to specific hours and minutes.	The value is an integer in the format of <0-23>:<0-59>.
time2	Specifies the reboot time accurate to specific hours, minutes, days, and months.	The value is an integer in the format of <0-23>:<0-59> <1-31> <1-12>.
time	Specifies the delayed reboot time accurate to specific hours and minutes.	The value is an integer in the format of <0-23>:<0-59>.
at	Reboots the switch at the specified time.	-
in	Reboots the switch after a specified delay.	-

Default Value

NA

View

Privileged user view

Usage Guidelines



Warning:

Do not use this command unless necessary, because it will cause a temporary interruption of the network. In addition, it is recommended that you determine whether to save the configuration file before the reboot.

Example

Reboot the switch at the specified time.

```
Switch#reboot at 23:23
WARNING:System will reboot after a specified delay! Continue?(y/n) [y]y
System will rebooting at 8/17/2017 14:45:57 (after 23 hours 23 minutes),please wait.
Switch#
```

2.1.24 reboot cancel

Function

The **reboot cancel** command cancels scheduled reboot of the switch.

Format

reboot cancel

Parameter

NA

Default Value

NA

View

Privileged user view

Usage Guidelines

NA

Example

Cancel scheduled reboot of the switch.

```
Switch#reboot in 23:23
  WARNING: System will reboot after a specified delay! Continue?(y/n) [y]y
  System will rebooting at 8/17/2017 14:45:57 (after 23 hours 23 minutes), please wait.

Switch(config)#reboot cancel
  WARNING: System will cancel reboot! Continue?(y/n) [y]y
  System now canceled reboot.

Switch#
```

2.1.25 show history**Function**

The **show history** command displays the historical commands used by the user.

Format

show history

Parameter

NA

Default Value

NA

View

Common user view

Usage Guidelines

You can use this command to view the recently used commands.

Example

Display historical commands that have been used recently.

```
Switch>show history
      disable
Switch>
```

2.1.26 show module version

Function

The **show module version** command displays the version of the module software.

Format

show module version

Parameter

NA

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

Display current version of each module.

```
Switch>show module version
Module                : Version
cli                   : CLI_VB3.00.00.00
snmp                  : SNMP_VB3.00.00.00
stp                   : MSTP_VB3.70.00.00
rlink                 : RLINK_VB3.00.02.00
mlink                 : MLINK_VB3.00.01.00
rip                   : RIP_VB3.00.07.00
vlan-mapping          : VLANMAPPING_VB3.00.02.00
```



```

qinq                : QINQ_VB3.00.02.00
port-isolate        : PORTISOLATE_VB3.00.08.00
ospf                 : OSPFV2_VB3.00.07.27
ospfv3               : OSPFV3_VX3.00.07.25
bfd                  : BFD_VX2.10.00.00
udld                 : UDLD_VB3.00.05.00
lldp                 : LLDP_VB3.00.04.00
aaa                  : AAA_VB3.00.00.00
mvrp                 : MVRP_VX2.10.00.00
vtp                  : VTP_VB3.00.00.00
Switch>

```

2.1.27 show privilege

Function

The **show privilege** command displays the privilege of the current user.

Format

show privilege

Parameter

NA

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

Display the privilege of the current user..

```

Switch>show privilege
    %Current privilege level is 15.
Switch>

```

2.1.28 show reboot

Function

The **show reboot** command displays the reboot management configuration.

Format

show reboot

Parameter

NA

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

Display the reboot management configuration.

```
Switch>show reboot
    System will reboot at 2020-09-0218:00:23
Switch>
```

2.1.29 show system

Function

The **show system** command displays the default MAC address and the current MAC address of Switch.

Format

show system

Parameter

NA

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

View the MAC address of Switch.

```
Switch>show system
  System device code   : G7FE200T00B200923
  Default mac-address : 04:f8:f8:e5:b8:ba
  Current mac-address : 04:f8:f8:e5:b8:ba
Switch>
```

2.1.30 show version**Function**

The **show version** command displays the current software and hardware version, compilation time, and memory size of the system.

Format**show version****Parameter**

NA

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

Display the current version information on the system.

```
Switch>show version
  Universal Software Platform
  Copyright (c) 2016-2020.
  USP (R) Software Version V410R240
  Compiled Sep 23 2020 12:15:24
```

```

Routing Switch
System Uptime is 0 days 3 hours 48 minutes 19 seconds

```

```

Hardware Version : N/A
BIOS Version      : N/A
FPGA Version      : N/A
Serial Number     : 583554X2023005

```

```

System Memory      : 16396408K

```

```

Switch>

```

2.1.31 show

Function

The **show** command outputs all configuration of the module node under the current protocol.

Format

show

Parameter

NA

Default Value

NA

View

Common user view, global configuration view, VLANIF configuration view, and STP process view

Usage Guidelines

You can use this command to get the configuration of the current node.

Example

Output all configuration of the current node.

```

Switch>show
!Device running configuration:
!version V410R240
!2008/04/21 22:35:17
!
hostname Switch
enable password level 15 plain 123

```

```

!
logging source default action monitor log state enable
logging source default action monitor debug state enable
!
username DUT2 group operators password $1$kiyv$blP5gEaeX6wG6eQLeT3Di0
username admin group administrators password $1$kiyv$blP5gEaeX6wG6eQLeT3Di0
username admin online-count 64
username zcd group guests password $1$kiyv$FrLivsk/A2cnj4wGdatKo.
username zcd fail-count 10
username zcd2 group operators password $1$kiyv$3Dd122971F4H3Ejh.GwaL0
username zcd2 fail-count 10
user fail-count 10
!
no snmp version v1
no snmp version v3
snmp community $9$kiyv$10ca10aa5145c2d9 rw cipher view internet
Switch(config)#

```

2.1.32 write file

Function

The **write file** command saves the current system configuration in the startup configuration file.

Format

write file

Parameter

NA

Default Value

NA

View

Privileged user view, global configuration view

Usage Guidelines

You do not need to specify the path of the startup configuration file because the path has been written in the system.

If you want to permanently use a series of configuration you complete, run this command to save the configuration in the current startup configuration file.

Example

Save the current system configuration in the startup configuration file.

```
Switch#write file
  This will save the configuration in the flash memory.
  Are you sure?(y/n) [y]y
  Building configuration,please wait for a moment.....
  Begin to write.
  Finishing writing the configuration file.

  [OK]
Switch#
```

2.1.33 password**Function**

The **password** command changes the password of the current user.

Format

- **password** *pass-word*
- **password** *pass-word* **simple**

Parameter

Parameter	Description	Value
pass-word	Modifies the password of the current user.	The value is a string of 8 to 64 characters.
simple	Indicates that the new password is encrypted using a reversible algorithm. If this keyword is not specified, the new password is encrypted using the MD5 algorithm.	-

Default Value

The system has a default user with the administrator privilege, of which the user name is **admin** and password is **12345**.

View

Common user view, privileged user view, global configuration view

Usage Guidelines

The switch supports both reversible and irreversible encryption algorithms for the user password because some authentication methods (such as dot1x) requires plaintext passwords of users. Irreversible encryption cannot be used in this scenario.

Example

Change the password of the current user to **fhn0001**.

```
Switch(config)#password fhn0001
Switch(config)#
```

2.1.34 show login-type count

Function

The **show login-type count** command displays the number of terminals using different login modes.

Format

show login-type count

Parameter

NA

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

Display the numbers of terminals using different login modes.

```
Switch>show login-type count
  LoginType      Count
  Console        1
  Telnet         3
Switch>
```

2.1.35 show user config

Function

The **show user config** command displays the configuration of the created local user.

Format

show user config

Parameter

NA

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

Display the configuration of the local user.

```
Switch>show user config
!
username DUT2 group operators password $1$kijv$b1P5gEaeX6wG6eQLeT3Di0
username admin group administrators password $1$kijv$b1P5gEaeX6wG6eQLeT3Di0
username admin online-count 64
username zcd group guests password $1$kijv$FrLivsk/A2cnj4wGdatKo.
username zcd fail-count 10
username zcd2 group operators password $1$kijv$3Dd12297IF4H3Ejh.GwaL0
username zcd2 fail-count 10
user fail-count 10
Switch>
```

2.1.36 show user glob-info

Function

The **show user glob-info** command displays the global configuration of the created local user.

Format

show user glob-info

Parameter

NA

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

Display the global configuration of the local user.

```
Switch>show user glob-info
Password length           : 1
Password complexity       : 1
Same name password        : deny
User reauthentication interval : 0(minutes)
Authntication max fail count : 10
Switch>
```

2.1.37 show user verbose**Function**The **show user verbose** command displays the details of the created local user.**Format**

- **show user verbose**
- **show user verbose** *name*

Parameter

Parameter	Description	Value
name	Specifies a user name.	The value is a character string.

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

Display the details of the local user.

```

Switch>show user verbose
User name                : DUT2
User group                : operators
Password type             : cipher
Password complexity       : 0
Authntication max fail count : 3
User reauthntication interval : 0(minutes)
User online count         : 5

User name                : admin
User group                : administrators
Password type             : cipher
Password complexity       : 0
Authntication max fail count : 3
User reauthntication interval : 0(minutes)
User online count         : 64

User name                : zcd
User group                : guests
Password type             : cipher
Password complexity       : 0
Authntication max fail count : 10
User reauthntication interval : 0(minutes)
Switch>

```

2.1.38 username group**Function**

The **username group** command changes the privilege group of a specified user.

The **no username** command deletes a specified user.

Format

- **username** *user-name* **group** { **administrators** | **operators** | **users** | **guests** }
- **no username** *user-name*

Parameter

Parameter	Description	Value
user-name	Specifies the name of the user for which you want to change the privilege group.	The value is a character string.
administrators	Specifies the privilege of the administrators level.	-
operators	Specifies the privilege of the operators level.	-
users	Specifies the privilege of the users level.	-
guests	Specifies the privilege of the guests level.	-

Default Value

NA

View

Global configuration view

Usage Guidelines

You can use this command to change the privilege group of the user. Ensure that the specified user exists in the system. To run this command, you must have the administrator privilege.

The switch divides the user privilege into the following four groups in descending order

- The administrators group has the highest level and can run any commands. Key operations greatly affecting the switch must have the administrators privilege, such as commands for user management, FTP operations, history record clearing, terminal number reduction, image and configuration file upgrading, and FTP/Telnet enabling/disabling.
- The operators group has a lower level than the administrators group, and can run all commands except those related to key operations requiring the administrators privilege.
- The users group has a lower level than the operators group, and can run all commands except **upgrade**, **tftp**, **sntp**, **snmp**, and **sgm**.
- The guests group has the lowest level and can only be used to view some configurations.

Example

Change the privilege group of the user "test" from "administrators" to "users".

```
Switch(config)#username test group users
Switch(config)#
```

2.1.39 username group password**Function**

The **username group password** command creates a user account for switch login.

Format

- **username** *user-name* **password** *pass-word*
- **username** *user-name* **password** *pass-word* **simple**
- **username** *user-name* **group** { **administrators** | **operators** | **users** | **guests** } **password** *pass-word*
- **username** *user-name* **group** { **administrators** | **operators** | **users** | **guests** } **password** *pass-word* **simple**

Parameter

Parameter	Description	Value
user-name	Specifies the user name of the account.	The value is a character string.
administrators	Specifies the privilege of the administrators level.	-
operators	Specifies the privilege of the operators level.	-
users	Specifies the privilege of the users level.	-
guests	Specifies the privilege of the guests level.	-
simple	Indicates the user password can use the reversible encryption algorithm.	-
pass-word	Specifies the password of the user to be created.	The value is a string consisting of 1 to 64 characters.

Default Value

NA

View

Global configuration view

Usage Guidelines

If you do not specify a privilege group when using this command to create a user, the user is added to the default privilege group operators. When creating a dot1x user, you can only set a password by specifying the **simple** keyword. If want to delete a user but specify a nonexistent user, an operation failure message will be displayed.

To run this command, you must have the administrator privilege.

The switch divides the user privilege into the following four groups in descending order

- The administrators group has the highest level and can run any commands. Key operations greatly affecting the switch must have the administrators privilege, such as commands for user

management, FTP operations, history record clearing, terminal number reduction, image and configuration file upgrading, and FTP/Telnet enabling/disabling.

- The operators group has a lower level than the administrators group, and can run all commands except those related to key operations requiring the administrators privilege.
- The users group has a lower level than the operators group, and can run all commands except **upgrade**, **tftp**, **sntp**, **snmp**, and **sgm**.
- The guests group has the lowest level and can only be used to view some configurations.

Example

Add a user account of which the name is "test", the privilege is "users", and the password is "test" to the switch.

```
Switch(config)#username test group users password test
Switch(config)#
```

2.1.40 username domain

Function

The **username domain** command configures different domains to manage user login privilege and specifies a user to add or exit a certain domain or all domains.

Format

- **username** *user-name* **domain** { **telnet** | **ssh** | **jsonrpc** | **console** }
- **username** *user-name* **domain** **all**
- **no username** *user-name* **domain** **all**
- **no username** *user-name* **domain** { **telnet** | **ssh** | **jsonrpc** | **console** }

Parameter

Parameter	Description	Value
user-name	Specifies the name of the user that you want to add to or remove from the domain.	The value is a character string.
telnet	Supports Telnet login.	-
ssh	Supports SSH login.	-
console	Supports serial port login.	-
jsonrpc	Supports JSONRPC login.	-
all	Supports all login modes.	-

Default Value

NA

View

Global configuration view

Usage Guidelines

New users only have the serial port login privilege. The administrator has all the four privileges: Telnet, FTP, SSH, and serial port.

Example

Add the user "test" to the Telnet domain.

```
Switch(config)#username test domain telnet
Switch(config)#
```

2.1.41 user pwd-complex

Function

The **user pwd-complex** command sets the password complexity of a user.

Format

user pwd-complex { *password-complex* | **default** }

Parameter

Parameter	Description	Value
password-complex	Specifies the password complexity.	The value is an integer ranging from 1 to 4.
default	Specifies the default password complexity.	3

Default Value

3

View

Global configuration view

Usage Guidelines

The **user pwd-complex** command sets the password complexity of all users.

Example

Set the password complexity of all users to 1.

```
Switch(config)#user pwd-complex 1
Switch(config)#
```

2.1.42 user pwd-length

Function

The **user pwd-length** command sets the password length of a certain user or all users.

Format

user pwd-length { *password-length* | **default** }

Parameter

Parameter	Description	Value
password-length	Specifies a password length.	The value is an integer ranging from 1 to 64.
default	Specifies the default password length.	8

Default Value

8

View

Global configuration view

Usage Guidelines

If you do not set the *word* parameter (user name), the command sets the password length for all users in the system.

Example

Set the password length to 32 characters for all users.

```
Switch(config)#user pwd-length 32
Switch(config)#
```

2.1.43 user fail-count

Function

The **user fail-count** command sets the maximum number of login failures for all users.

Format

user fail-count *fail-count-time*

Parameter

Parameter	Description	Value
fail-count-time	Specifies the maximum number of login failures.	The value is an integer ranging from 1 to 10, in times.

Default Value

By default, a maximum of 3 login failures are allowed for a user.

View

Global configuration view

Usage Guidelines

NA

Example

Set the maximum number of login failures to 5 for all users.

```
Switch(config)#user fail-count 5
Switch(config)#
```

2.1.44 user same-name-pwd**Function**

The **user same-name-pwd** command configures whether to permit or deny access from a login user with identical user name and password.

Format

user same-name-pwd { permit | deny }

Parameter

Parameter	Description	Value
permit	Permits access from a login user with identical user name and password.	-
deny	Denies access from a login user with identical user name and password.	-

Default Value

Deny

View

Global configuration view

Usage Guidelines

NA

Example

Permit access from a login user with identical user name and password.


```
Switch(config)#user same-name-pwd permit
Switch(config)#
```

2.1.45 username fail-count

Function

The **username fail-count** command sets the maximum number of login failures for a specified user.

Format

username *user-name* **fail-count** { *fail-count-time* | **default** }

Parameter

Parameter	Description	Value
user-name	Specifies a user name. The specified user must have been created.	The value is a character string.
fail-count-time	Specifies the maximum number of login failures.	The value is an integer ranging from 1 to 10, in times.
default	Specifies the default number of login failures.	3

Default Value

By default, a maximum of 3 login failures are allowed for a user.

View

Global configuration view

Usage Guidelines

Before running this command, you must run **username** command to create the specified user.

Example

Set the maximum number of login failures to 5 for the user **fhn**.

```
Switch(config)#username fhn fail-count 5
Switch(config)#
```

2.1.46 username reauth-interval

Function

The **username reauth-interval** command sets the reauthentication interval when the number of continuous authentication failures reaches the upper limit.

Format

- **user reauth-interval** *reauth-interval-time*
- **username** *user-name* **reauth-interval** { *reauth-interval-time* | **default** }

Parameter

Parameter	Description	Value
user-name	Specifies a user name. The specified user must have been created.	The value is a character string.
reauth-interval-time	Specifies a reauthentication interval.	The value is an integer ranging from 0 to 65535, in minutes.
default	Specifies the default reauthentication interval.	0

Default Value

The default value is 0.

View

Global configuration view

Usage Guidelines

When the number of continuous authentication failures reaches the upper limit, you need to wait for reauthentication after the reauthentication interval ends.

Example

Set the reauthentication interval of the user **fhn** to 20 minutes.

```
Switch(config)#username fhn reauth-interval 20
Switch(config)#
```

2.1.47 username ftp-directory

Function

The **username ftp-directory** command sets the user FTP path.

Format

username *user-name* **ftp-directory** { *dir* | **default** }

Parameter

Parameter	Description	Value
user-name	Specifies a user name.	The value is a character string.
dir	Specifies an FTP path.	The value is a character string.
default	Specifies the default value.	/temp/ram/.user/admin/admin/admin

Default Value

The default value is /temp/ram/.user/admin/admin/admin.

View

Global configuration view

Usage Guidelines

NA

Example

Set the user FTP path.

```
Switch(config)#username fiber ftp-directory /ram
Switch(config)#
```

2.1.48 who**Function**

The **who** command displays information about the users who have logged in and are configuring the switch.

Format

who

Parameter

NA

Default Value

NA

View

Common user view

Usage Guidelines

You can use this command to check which users are configuring the switch. The user name with an asterisk (*) is the one you are using.

Example

Display information about users who have logged in and are configuring the switch.

```
Switch(config)#who
```

Line	Location	Idle	Pri	User
* 1 con 1	Console	00:00:00	admin	admin
Switch(config)#				

2.1.49 temporary-password

Function

The **temporary-password** command enables or disables the temporary password function.

Format

temporary-password { enable | disable }

Parameter

Parameter	Description	Value
enable	Enables the temporary password function.	-
disable	Disables the temporary password function.	-

Default Value

This function is enabled.

View

Global configuration view

Usage Guidelines

NA

Example

Disable the temporary password function.

Switch(config)#temporary-password disable
Switch(config)#

2.1.50 show management acl

Function

The **show management acl** command displays the ACL configuration.

Format

- **show management acl**
- **show management acl { ipv4 | ipv6 }**

Parameter

NA

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

View the ACL configuration.

```
Switch>show management acl
T=telnet,S=snmp,W=web,H=ssh,F=ftp
No.  Owner      Address/Mask
1    F          192.168.1.0/24
2    T+S+W+H+F 192.167.2.1/32
Switch>
```

2.1.51 show counter**Function**

The **show counter** command displays counter information and configuration information.

Format**show counter** *counter-id***Parameter**

Parameter	Description	Value
counter-id	Indicates the counter ID.	The value is an integer ranging from 1 to 1024.

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

Display counter information.

```
Switch> show counter
  P=Packets
  B=Bytes
  CounterId Type(P|B) Sort
  1   All   Green
Switch>
```

2.1.52 show command-privilege**Function**

The **show command-privilege config** command displays the command privilege configuration.

The **show command-privilege verbose** command displays the details of the command privilege.

Format

- **show command-privilege config**
- **show command-privilege verbose**

Parameter

NA

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

Display the command privilege configuration.

```
Switch>show command-privilege config
Switch>
```

2.1.53 send message

Function

The **send message** command sends messages from one operation terminal to another operation terminal.

Format

- **send message** *data*
- **send message**

Parameter

Parameter	Description	Value
data	Specifies the content of the message to be sent.	The value is a character string.

Default Value

NA

View

Privileged user view

Usage Guidelines

You can use this command to send a message from the current operation terminal to all the other operation terminals that have logged in to the system. When you run **send message data**, a message will be send immediately after you press **Enter**. If you run **send message**, press **Enter**, and then enter the message, you must press **Ctrl+Z** as required to send the message.

Example

Send a message "Hello" from the current operation terminal to all the other operation terminals that have logged in to the system.

```
Switch#send message Hello
Switch#
```

2.1.54 management acl|management acl6

Function

The **management acl|management acl6** command enables or configures the ACL.

The **no management acl|no management acl6** command cancels the configuration.

Format

- **management acl { enable | disable }**
- **management acl ipv4-address**
- **management acl ipv4-address1 ipv4-address2**
- **management acl ipv4-address1 ipv4-address2 { telnet | snmp | ssh | tftp | ftp | all }**
- **management acl ipv4-address/M**
- **management acl ipv4-address/M { telnet | snmp | ssh | tftp | ftp | all }**
- **management acl6 ipv6-address/M**
- **management acl6 ipv6-address/M { telnet | snmp | ssh | tftp | ftp | all }**
- **no management acl ipv4-address/M**
- **no management acl6 ipv6-address/M**
- **no management acl6 ipv6-address/M { telnet | snmp | ssh | tftp | ftp | all }**
- **no management acl6 ipv6-address/M**
- **no management acl ipv6**
- **no management acl ipv4-address/M { telnet | snmp | ssh | tftp | ftp | all }**
- **no management acl { ipv4 | all }**
- **no management acl ipv4-address1 ipv4-address2**
- **no management acl ipv4-address1 ipv4-address2 { telnet | snmp | ssh | tftp | ftp | all }**

Parameter

Parameter	Description	Value
enable	Enables the ACL function.	-
disable	Disables the ACL function.	-
Ipv4-address, ipv4-address1, ipv4-address2	Specifies an IPv4 address or a network segment address visited by a user.	The value is in dotted decimal notation. For example, an IPv4 address is in the A.B.C.D. IPv6:X:X::X:X
ipv6-address	Specifies an IPv6 address or a network segment address visited by a user.	The value is in dotted decimal notation. For example, an IPv4 address is in the A.B.C.D. IPv6:X:X::X:X
M	Specifies the number of mask digits.	The value is an integer ranging from 1 to 32 for IPv4 address and 128 for IPv6 address.
telnet snmp ssh tftp ftp all	Configures ACL for any or all of telnet, snmp, ssh, tftp, and ftp.	-

Default Value

NA

View

Global configuration view

Usage Guidelines

NA

Example

Enable the ACL function.

```
Switch(config)#management acl enable
Switch(config)#
```

Enable the user with IP address 10.2.3.1 and mask 255.255.255.255 to log in to the switch using Telnet.

```
Switch(config)#management acl 10.2.3.1 255.255.255.255 telnet
Switch(config)#
```

2.1.55 check temporary-password**Function**The **check temporary-password** command checks a temporary password.**Format****check temporary-password** *pwd***Parameter**

Parameter	Description	Value
pwd	Specifies a temporary password.	The value is a character string.

Default Value

NA

View

Key configuration view

Usage Guidelines

You can enter **control+p** in the password field without entering the user name to directly go to the key configuration view.

After obtaining a temporary password SN using the command, you can obtain the temporary password UXBek0y0 using the password recovery tool. In the key configuration view, run the **check temporary-password command** to verify the password. If the password is valid, you can log in to the switch.

Example

Check a temporary password.

```
Switch(key)#check temporary-password UXBek0y0
    %The temporary password is invalid now,please change user 'admin' password and save it.
Switch(config)#
```

2.1.56 clock set

Function

The **clock set** command sets the current date and time on the switch.

Format

- **clock set** *HH:MM:SS DD MM YYYY*
- **clock set** *HH:MM:SS YYYY/MM/DD*

Parameter

Parameter	Description	Value
HH:MM:SS	Specifies the current time on the switch. HH specifies hours. MM specifies minutes. SS specifies seconds.	The HH value is an integer ranging from 0 to 23. The MM value is an integer ranging from 0 to 59. The SS value is an integer ranging from 0 to 59.
DD	Specifies the current date on the switch.	The value is an integer ranging from 1 to 31.
MM	Specifies the current month on the switch.	The value is an integer ranging from 1 to 12.
YYYY	Specifies the current year on the switch.	The value is an integer ranging from 2001 to 2036.

Default Value

NA

View

Privileged user view

Usage Guidelines

In an environment that requires the absolute time, you must set the current date and time on the switch.

The time must be in the 24-hour format. If you do not specify MM:SS, the value is 00:00. You must set the value of HH (at least one digit). For example, if you enter 0, the time is 00:00:00.

The year in the date must be four digits.

Example

Set the current date and time to 2016-3-31 16:10:19.

```
Switch#clock set 16:10:19 31 3 2016
Switch#
```

2.1.57 clock summer-time

Function

The **clock summer-time** command sets the name, start time, and end time of daylight saving time.

The **no clock summer-time** command cancels the configuration of daylight saving time.

Format

- **clock summer-time** *summer-time-name* **date** *start-hour:start-minutes start-day start-month start-year end-hour:end-minutes end-day end-month end-year*
- **clock** **summer-time** *summer-time-name* **date** *start-hour:start-minutes start-year/start-month/start-day end-hour:end-minutes end-year/end-month/ end-day*
- **clock summer-time** *summer-time-name* **recurring** { **first** | **second** | **third** | **fourth** | **fifth** | **last** } { **monday** | **tuesday** | **wednesday** | **thursday** | **friday** | **saturday** | **sunday** } { **january** | **february** | **march** | **april** | **may** | **june** | **july** | **august** | **september** | **october** | **november** | **december** } *start-hour:start-minutes* { **first** | **second** | **third** | **fourth** | **fifth** | **last** } { **monday** | **tuesday** | **wednesday** | **thursday** | **friday** | **saturday** | **sunday** } { **january** | **february** | **march** | **april** | **may** | **june** | **july** | **august** | **september** | **october** | **november** | **december** } *end-hour:end-minutes*
- **no clock summer-time**

Parameter

Parameter	Description	Value
summer-time-name	Specifies the name of the daylight	The value is an integer ranging from 1 to 32,

Parameter	Description	Value
	saving time zone.	in character string format.
date	Specifies the absolute daylight saving time.	-
recurring	Specifies the periodic daylight saving time.	-
start-hour	Specifies the start hour.	The value is an integer ranging from 0 to 23.
start-minutes	Specifies the start minute.	The value is an integer ranging from 0 to 59.
start-day	Specifies the start day.	The value is an integer ranging from 1 to 31.
start-month	Specifies the start month.	The value is an integer ranging from 1 to 12.
start-year	Specifies the start year.	The value is an integer ranging from 2001 to 2099.
end-hour	Specifies the end hour.	The value is an integer ranging from 0 to 23.
end-minutes	Specifies the end minute.	The value is an integer ranging from 0 to 59.
end-day	Specifies the end day.	The value is an integer ranging from 1 to 31.
end-month	Specifies the end month.	The value is an integer ranging from 1 to 12.
end-year	Specifies the end year.	The value is an integer ranging from 2001 to 2099.
first second third fourth fifth last	Specifies the first, second, third, fourth, fifth, or last workday in a month when the daylight saving time starts or ends.	-

Default Value

By default, the daylight saving time is not set.

View

Global configuration view

Usage Guidelines

You can use this command to set the daylight saving time rule in the local time zone. The valid year range is 2001 to 2099. After the rule is set, the switch automatically takes effect within the specified period of time according to the rule.

Example

Configure the daylight saving time to start at 1:0 on 7/15/2019 and end at 23:59 on 8/31/2019.

```
Switch#clock summer-time BJ date 1:0 2019/7/15 23:59 2019/8/31
Switch#
Switch>show clock
  System Running Time : 0 hours,30 minutes,46 seconds
  Clock                : 2000-04-06 10:16:42
```

```

Time Zone      : UTC +00:00
Summer Time    :
    Name       : BJ
    Repeat mode : date
    Start year  : 2014
    End year    : 2014
    Start time  : 7/15/2014 01:00
    End time    : 8/31/2014 23:59

```

```
Switch#
```

Cancel the configuration of daylight saving time.

```

Switch#no clock summer-time
Switch>show clock
    System Running Time : 0 hours,31 minutes,10 seconds
    Clock               : 2000-04-06 10:17:06
    Time Zone           : UTC +00:00

```

```
Switch#
```

2.1.58 clock timezone

Function

The **clock timezone** command sets the local time zone.

The **no clock timezone** command restores the local time zone to Universal Time Coordinated (UTC).

Format

- **clock timezone** *time-zone-name* { **add** | **minus** } *offset*
- **no clock timezone**

Parameter

Parameter	Description	Value
time-zone-name	Specifies the time zone name.	The value is a string consisting of 1 to 10 characters.
add	Indicates the offset added to <i>time-zone-name</i> relative to UTC. That is, the time of the default UTC time zone of the system plus the <i>offset</i> equals the time of the time zone identified by <i>time-zone-name</i> .	-
minus	Indicates the offset subtracted from <i>time-zone-name</i> relative to UTC. That is, the time of the default UTC time zone of the	-

Parameter	Description	Value
	system minus the <i>offset</i> equals the time of the time zone identified by <i>time-zone-name</i> .	
offset	Specifies the time lag with the UTC.	The value is in the HH:MM format, where HH indicates hours and ranges from 0 to 12, whereas MM indicates minutes and ranges from 0 to 59.

Default Value

UTC +00:00

View

Privileged user view

Usage Guidelines

NA

Example

Set the local time zone to Wuhan.

```

Switch#clock timezone WuHan add 8:0
    Finishing writing the configuration file.

Switch>show clock
    clock : 1/3/2100 7:36:44 AM
    Time Zone:WuHan +08:00
    System running time : 1 hours,0 minutes,46 seconds
Switch#

```

2.1.59 command authorization aaa method**Function**

The **command authorization aaa method** command sets the AAA authentication method used for password check at a specified privilege level.

Format

- **command authorization** *privilege-level* **aaa method** *name*
- **no command authorization** *privilege-level* **aaa method**

Parameter

Parameter	Description	Value

Parameter	Description	Value
privilege-level	Specifies a privilege level.	The value is an integer ranging from 0 to 15.
name	Specifies an AAA authorization method name.	The value is a string containing up to 32 bytes.

Default Value

NA

View

Line configuration view

Usage Guidelines

NA

Example

Set the AAA authentication method used for password check at a specified privilege level.

```
Switch(config-line)#command authorization 1 aaa method auth1
Switch (config-line)#
```

2.1.60 command authorization config-command**Function**

The **command authorization config-command** command configures authorization for commands in the global configuration view.

Format

- **command authorization config-command**
- **no command authorization config-command**

Parameter

NA

Default Value

NA

View

Line configuration view

Usage Guidelines

NA

Example

Configure authorization for commands in the global configuration view.

```
Switch(config-line)#command authorization config-command
Switch (config-line)#
```

2.1.61 trace|trace6**Function**

The **trace** command tests the connectivity of the IPv4 network.

The **trace6** command tests the connectivity of the IPv6 network.

Format

- **trace** *ipv4-address* [*string1*]
- **trace6** *ipv6-address* [*string2*]

Parameter

Parameter	Description	Value
ipv6-address	Specifies an IPv6 address.	In this format, a 128-digit IP address is divided into 8 segments. Each segment consists of 16 digits and is represented by 4 hexadecimal characters (0-9 and A-F). Segments are separated by colons (:). Every "X" represents a group of hexadecimal digits.
ipv4-address	Specifies an IPv4 address.	The value is in dotted decimal notation.
string1	Selects the parameter based on the switch prompt message.	-n r q f <1-4294967295> l <12-65500> w <1-10000> m <1-65500> fh <1-255> h <1-255> tos <0-255> dscp <0-63> 8021p <0-7> s A.B.C.D -vpn-instance VPNNAME NAMECR
string2	Selects the parameter based on the switch prompt message.	-n r q f <1-4294967295> l <12-65500> w <1-10000> m <1-65500> fh <1-255> h <1-255> tos <0-255> tc <0-255> 8021p <0-7> nexthop s X:X::X:X -vpn-instance VPNNAME NAMECR

Default Value

NA

View

Privileged user view

Usage Guidelines

NA

Example

Test whether the IPv4 address **192.168.1.118** is reachable.

```
Switch#trace 192.168.1.118
```

Tracing route to 192.168.1.118 over a maximum of 16 hops.

1	*	*	*	Request timed out
2	*	*	*	Request timed out
3	*	*	*	Request timed out
4	*	*	*	Request timed out
5	*	*	*	Request timed out
6	*	*	*	Request timed out
7	*	*	*	Request timed out
8	*	*	*	Request timed out
9	*	*	*	Request timed out
10	*	*	*	Request timed out
11	*	*	*	Request timed out
12	*	*	*	Request timed out
13	*	*	*	Request timed out
14	*	*	*	Request timed out
15	*	*	*	Request timed out
16	*	*	*	Request timed out

Trace complete.

```
Switch#
```

2.1.62 trace vxlan vni

Function

The **trace vxlan vni** command traces the connectivity of the VXLAN tunnel.

Format

trace vxlan vni *vni-id*

Parameter

Parameter	Description	Value
vni-id	Specifies a VNI ID.	The value is an integer ranging from 1 to 16777215.

Default Value

NA

View

Privileged user view

Usage Guidelines

NA

Example

Trace the connectivity of the VXLAN tunnel.

```
Switch#trace vxlan vni 1
Switch#
```

2.1.63 debug soa**Function**The **debug soa** command enables the SOA debugging function.The **no debug soa** command disables the SOA debugging function.**Format**

- **debug soa { rx | tx | rxpkt | txpkt | config | event | transfer | upgrade | all }**
- **no debug soa { rx | tx | rxpkt | txpkt | config | event | transfer | upgrade | all }**

Parameter

NA

Default Value

NA

View

Privileged user view

Usage Guidelines

NA

Example

Enable the SOA debugging function.

```
Switch#debug soa all
Switch#
```

2.1.64 show soa subsys

Function

The **show soa subsys** command displays the SOA subsystem information.

Format

- **show soa subsys** *system-number*
- **show soa subsys operator**
- **show soa subsys** *system-number* **operator**

Parameter

Parameter	Description	Value
system-number	Specifies the system number.	The value is an integer ranging from 1 to 4.

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

View the SOA subsystem information.

```
Switch>show soa subsys operator
Switch>
```

2.1.65 show soa global

Function

The **show soa global** command displays the SOA global information.

Format

show soa global

Parameter

NA

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

View the SOA global information.

```

Switch>show soa global
Version:                SOA_VX2.10.00.00
  Max operation count:   30
  Max subsys count:     1
  Max slot count:       2
  Max card count:       0
  Self sys index:       1
  Self slot index:      1
  Self card index:      0
  Max query times:      3
  Query interval:       2000
  Wait ack interval:    2000
Switch>

```

2.1.66 user pwd-live**Function**The **user pwd-live** command configures the live time of the user password.**Format**

- **user pwd-live** { *live-value* | **default** }
- **username** *name* **password-live** { *live-value* | **default** }

Parameter

Parameter	Description	Value
live-value	Specifies the live time of the user password.	The value is an integer ranging from 0 to 90, in days.

Parameter	Description	Value
default	Specifies the default live time of the user password.	30 days
name	Specifies a user name.	The value is a character string.

Default Value

0 days

View

Global configuration view

Usage Guidelines

NA

Example

Configure the live time of the user password.

```
Switch(config)#user pwd-live 30
Switch(config)#
```

2.1.67 user pwd-live-prompt**Function**

The **user pwd-live-prompt** command configures the live prompt time of the user password.

Format

user pwd-live-prompt { *live-value* | **default** }

Parameter

Parameter	Description	Value
live-value	Specifies the live prompt time of the user password.	The value is an integer ranging from 1 to 90, in days.
default	Specifies the default live prompt time of the user password.	10 days

Default Value

60 days

View

Global configuration view

Usage Guidelines

NA

Example

Configure the live prompt time of the user password.

```
Switch(config)#user pwd-live-prompt 30
Switch(config)#
```

2.1.68 user {telnet|ssh} max-count**Function**

The **user {telnet|ssh} max-count** command configures the maximum number of users that support Telnet or SSH login.

Format

user { telnet | ssh } max-count { count-number | default }

Parameter

Parameter	Description	Value
count-number	Specifies the maximum number of login users.	The value is an integer ranging from 1 to 30.
default	Specifies the default maximum number of login users.	10

Default Value

10

View

Global configuration view

Usage Guidelines

NA

Example

Configure the maximum number of users that support Telnet login.

```
Switch(config)#user telnet max-count 15
Switch(config)#
```

2.1.69 debug command-privilege**Function**

The **debug command-privilege** command enables the command privilege debugging function.

The **no debug command-privilege** command disables the command privilege debugging function.

Format

- **debug command-privilege**
- **no debug command-privilege**

Parameter

NA

Default Value

NA

View

Privileged user view

Usage Guidelines

NA

Example

Enable the command privilege debugging function.

```
Switch#debug command-privilege
Switch#
```

2.2 User Terminal Configuration Commands

2.2.1 color

Function

The **color** command sets the background color of the terminal. The system supports the following colors: gray, red, green, yellow, blue, purple, water, and white.

The **no color** command cancels the background color setting of a terminal.

Format

- **color { gray | red | green | yellow | blue | purple | water | white }**
- **no color**

Parameter

NA

Default Value

NA

View

Line configuration view

Usage Guidelines

NA

Example

Set the background color of a terminal to blue.

```
Switch(config)#line vty 1
Switch(config-line)#color blue
```

2.2.2 debug delay

Function

The **debug delay** command configures a delay before debugging information output.

Format

debug delay { *value* | **default** }

Parameter

Parameter	Description	Value
value	Specifies a delay before debugging information output	The value is an integer ranging from 0 to 10, in seconds.
default	Specifies the default delay time before debugging information output	3 seconds

Default Value

The default value is 3 seconds.

View

Line configuration view, privileged user view

Usage Guidelines

NA

Example

Set a delay before debugging information output to 5 seconds.

```
Switch(config-line)#debug delay 5
Switch (config-line)#
```

2.2.3 enable authentication**Function**

The **enable authentication** command configures secondary authentication for user terminals.

Format

- **enable authentication { local | none }**
- **enable authentication aaa method *name***

Parameter

Parameter	Description	Value
name	Specifies an AAA secondary authentication method name.	The value is a character string.
local	Enables local secondary authentication.	-
none	Disables secondary authentication.	-

Default Value

NA

View

Line configuration view

Usage Guidelines

NA

Example

Configure the secondary authentication mode for a terminal.

```
Switch(config-line)#enable authentication local
Switch (config-line)#
```

2.2.4 terminal color**Function**

The **terminal color** command sets the background color of a virtual terminal. The system supports the following colors: gray, red, green, yellow, blue, purple, water, and white.

The **no terminal color** command cancels the background color setting of a virtual terminal.

Format

- **terminal color** { gray | red | green | yellow | blue | purple | water | white }
- **no terminal color**

Parameter

NA

Default Value

NA

View

Privileged user view

Usage Guidelines

NA

Example

Set the background color of a virtual terminal to blue.

```
Switch#terminal color blue
Switch#
```

2.2.5 terminal length

Function

The **terminal length** command sets the number of the lines that can be displayed on the terminal.

The **terminal length temporary** command configures the number of the lines that can be displayed on the terminal temporarily.

The **no terminal length** command restores the default configuration.

The **no terminal length temporary** command cancels the number of the lines that can be displayed on the terminal.

Format

- **terminal length** { 0 | *terminal-length* | default }
- **terminal length** { 0 | *terminal-length* } **temporary**
- **no terminal length**

- **no terminal length temporary**

Parameter

Parameter	Description	Value
terminal-length	Specifies the number of lines displayed on the screen.	The value is 0 or an integer ranging from 5 to 512.
default	Specifies the default number of lines displayed on the screen.	24

Default Value

By default, 24 lines can be displayed on a screen.

View

Privileged user view

Usage Guidelines

You can use this command to set the number of lines displayed on a screen when using the CLI. If the length is set to 0, the multi-screen display function is disabled.

Example

Set the number of lines displayed on a screen to 30.

```
Switch#terminal length 30
Switch#
```

2.2.6 terminal monitor

Function

The **terminal monitor** command enables debugging information display on the screen.

Format

- **terminal monitor**
- **no terminal monitor**

Parameter

NA

Default Value

By default, terminals that log in through the serial port can receive debugging information, and those that log in through Telnet cannot receive debugging information.

View

Privileged user view

Usage Guidelines

You can run this command after running the **debug** command to output the debugging information to the terminal. Before running this command, run the **logging history** command to set the privilege to **debug**.

Example

Enable debugging information display on the screen.

```
Switch#terminal monitor
Switch#
```

2.2.7 terminal timeout**Function**

The **terminal timeout** command sets the timeout duration of a virtual terminal with no operation performed.

The **no terminal timeout** command restores the timeout duration of a virtual terminal with no operation performed to the default value.

Format

- **terminal timeout** *time1*
- **terminal timeout** *time1 time2*
- **no terminal timeout**

Parameter

Parameter	Description	Value
time1	Specifies the timeout duration in minutes.	The value is an integer ranging from 0 to 35791, in minutes.
time2	Specifies the timeout duration in seconds.	The value is an integer ranging from 0 to 59.

Default Value

By default, the timeout duration of a virtual terminal with no operation performed is 600 seconds.

View

Privileged user view

Usage Guidelines

This command functions like the screen saver program of a PC. Once a console terminal does not perform any operation within the timeout duration, the system will return to the authentication interface. For a Telnet terminal, its connection with the switch will be terminated in this case.

Example

Set the timeout duration of a virtual terminal to 5 seconds. That is, the system will return to the authentication interface if there is no input on the terminal within 5 seconds.

```
Switch#terminal timeout 5
Switch#
```

2.2.8 terminal language**Function**

The **terminal language** command configures the language of help information displayed on the user terminal.

Format

terminal language { chinese | english }

Parameter

Parameter	Description	Value
chinese	Displays help information in Chinese.	-
english	Displays help information in English.	-

Default Value

NA

View

Privileged user view

Usage Guidelines

NA

Example

Set the user terminal to display help information in Chinese.

```
Switch#terminal language chinese
Switch#
```

2.2.9 temporary-password

Function

The **temporary-password** command enables or disables the temporary password function.

Format

temporary-password { enable | disable }

Parameter

Parameter	Description	Value
enable	Enables the temporary password function.	-
disable	Disables the temporary password function.	-

Default Value

Enables the synchronization function.

View

Global configuration view

Usage Guidelines

NA

Example

Disable the temporary password function.

```
Switch(config)#temporary-password disable
Switch(config)#
```

2.2.10 monitor

Function

The **monitor** command enables the CLI terminal to receive debugging information.

The **no monitor** command disables the CLI terminal from receiving debugging information.

Format

- **monitor**
- **no monitor**

Parameter

NA

Default Value

By default, terminals that log in through the serial port can receive debugging information, and those that log in through Telnet cannot receive debugging information.

View

Line configuration view

Usage Guidelines

You can run this command to configure whether the virtual terminal can receive the debugging information. **monitor** means yes and **no monitor** means no. This command can be used in the terminal configuration view.

Example

Configure the function of receiving debugging information on the CLI terminal

```
Switch(config)#line vty 1
Switch(config-line)#monitor
```

2.2.11 language**Function**

The **language** command configures the language of help information displayed on the user terminal.

Format

language { chinese | english }

Parameter

Parameter	Description	Value
chinese	Displays help information in Chinese.	-
english	Displays help information in English.	-

Default Value

NA

View

Line configuration view

Usage Guidelines

NA

Example

Set the language of help information displayed on the switch to Chinese.

```
Switch(config-line)#language Chinese
Switch (config-line)#
```

2.2.12 length**Function**

The **length** command sets the number of lines that can be displayed on the CLI terminal.

The **no length** command restores the number of lines that can be displayed on the CLI terminal to the default value.

Format

- **length** *length*
- **no length**

Parameter

Parameter	Description	Value
length	Specifies the number of lines that can be displayed on the CLI terminal.	The value is an integer ranging from 0 to 512.

Default Value

By default, 25 lines of information can be displayed on the CLI terminal.

View

Line configuration view

Usage Guidelines

You can use this command to set the number of lines displayed on a screen when using the CLI. If the length is set to 0, the multi-screen display function is disabled.

Example

Set the number of lines that can be displayed on the CLI terminal to 30.

```
Switch(config-line)#length 30
Switch (config-line)#
```


2.2.13 line console

Function

The **line console** command displays the console terminal configuration view.

Format

- **line console**
- **line console** *number*

Parameter

Parameter	Description	Value
number	Specifies the number of the console terminal to be configured.	The value is an integer ranging from 1 to 1.

Default Value

NA

View

Global configuration view, line configuration view

Usage Guidelines

Using this command, you can enter the console terminal configuration view to set attributes of the terminal.

Example

Enter the console terminal configuration view.

```
Switch(config-line)#line console 1
Switch (config-line)#
```

2.2.14 line vty

Function

The **line vty** command displays the virtual terminal (Telnet connection) view.

Format

Global configuration view, line configuration view:

- **line vty** *vty-number*
- **line vty** *vty-number1 vty-number2*

Global configuration view:

no line vty *vti-number*

Parameter

Parameter	Description	Value
vti-number	Specifies the number of a virtual terminal.	The value is an integer ranging from 1 to 32.
vti-number1	Specifies the start virtual terminal number for batch configuration.	The value is an integer ranging from 1 to 32.
vti-number2	Specifies the end virtual terminal number for batch configuration.	The value is an integer ranging from 1 to 32.

Default Value

NA

View

Global configuration view, line configuration view

Usage Guidelines

After logging in to the switch through Telnet, you can use this command to enter the Telnet terminal configuration view, and then set other attributes of the terminal.

The switch has five virtual terminals by default. That is, five users can log in to the switch through Telnet concurrently.

Example

Configure virtual terminals line vty 1 to 5.

```
Switch(config-line)#line vty 1 5
Switch (config-line)#
```

2.2.15 kill vty

Function

The **kill vty** command terminates the connection with a virtual terminal (Telnet or SSH terminal) and resets the terminal.

Format

kill vty *vti-number*

Parameter

Parameter	Description	Value
vtty-number	Specifies the number of a virtual terminal.	The value is an integer ranging from 1 to 32.

Default Value

NA

View

Global configuration view

Usage Guidelines

Virtual terminals are those connecting to the switch through Telnet or SSH.

The switch has five virtual terminals by default. That is, five users can log in to the switch through Telnet concurrently.

Example

Terminate the connection with virtual terminal line vty 1.

```
Switch(config)#kill vty 1
Switch(config)#
```

2.2.16 show lines**Function**

The **show lines** command displays the terminal information.

Format

show lines

Parameter

NA

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

Display the terminal information.

```
Switch>show lines
      Line      Location      Idle      User
    * 2 Tel 1 150.1.1.254 00:00:00 admin
      3 vty 2
      4 vty 3
      5 vty 4
      6 vty 5
      7 vty 6
      8 vty 7
      9 vty 8
     10 vty 9
     11 vty 10
     12 vty 11
     13 vty 12
     14 vty 13
     15 vty 14
     16 vty 15
     17 vty 16
     18 vty 17
     19 vty 18
     20 vty 19
     21 vty 20
Switch>
```

2.2.17 show line config**Function**

The **show line config** command displays the terminal configuration.

Format

show line config

Parameter

NA

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

Display the terminal configuration.

```
Switch>show line config
!
line console 1
  length 24
  monitor
  timeout 1000 0
  login authentication local
  enable authentication none
  language english
line vty 1 30
  length 24
  no monitor
  timeout 0 0
  login authentication local
  enable authentication aaa method m4
  language chinese
line vty 31 32
  length 24
  no monitor
  timeout 0 0
  login authentication local
  enable authentication none
  language english
Switch>
```

2.2.18 show vty**Function**

The **show vty** command displays the virtual terminal information.

Format

show vty { *vty-number* | **console** }

Parameter

Parameter	Description	Value
vtty-number	Specifies the number of a virtual terminal.	The value is an integer ranging from 1 to 32.

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

View the virtual terminal information.

```

Switch>show vty 1
  vty 0 info:
  fd                      :215
  privilege                :15
  orig_privilege          :15
  used                     :1
  address                  :150.1.1.254
  auth user                :admin
  login user               :admin
  cmd length               :0
  width                    :132
  height                   :43
  cmd max length           :512
  current cli is NULL
  last cli                 :show ip ospf route
  cwd                      :/ram
  input bakupbuf           :
  node_histnum             :2
  i = 0 prev_node :view(2)  cmd : view
  i = 1 prev_node :enable(3) cmd : conf
Switch>

```

2.2.19 timeout**Function**

The **timeout** command sets the timeout duration of a virtual terminal with no operation performed.

The **no timeout** command restores the timeout duration of a virtual terminal with no operation performed to the default value.

Format

- **timeout** *time1*
- **timeout** *time1 time2*
- **no timeout**

Parameter

Parameter	Description	Value
time1	Specifies the timeout duration in minutes.	The value is an integer ranging from 0 to 35791, in minutes.
time2	Specifies the timeout duration in seconds.	The value is an integer ranging from 0 to 59.

Default Value

By default, the timeout duration of a virtual terminal with no operation performed is 600 seconds.

View

Line configuration view

Usage Guidelines

This command functions like the screen saver program of a PC. Once a console terminal does not perform any operation within the timeout duration, the system will return to the authentication interface. For a Telnet terminal, its connection with the switch will be terminated in this case.

Example

Set the timeout duration of a virtual terminal to 5seconds. That is, the system will return to the authentication interface if there is no input on the terminal within 5 seconds.

```
Switch(config-line)#terminal timeout 5
Switch (config-line)#
```

2.2.20 unlock-command vty

Function

The **unlock-command vty** command unlocks the VTY user command.

Format

unlock-command vty vty-number**Parameter**

Parameter	Description	Value
vtty-number	Specifies the number of a virtual terminal.	The value is an integer ranging from 1 to 32.

Default Value

NA

View

Global configuration view

Usage Guidelines

NA

Example

Unlock the VTY user command.

```
Switch(config)#unlock-command vty 1
Switch(config)#
```

2.2.21 mmi-mode**Function**The **mmi-mode** command enables or disables the MMI mode.**Format****mmi-mode { enable | disable }****Parameter**

Parameter	Description	Value
enable	Enters the MMI mode.	-
disable	Enters the human-machine mode.	-

Default Value

Human-machine mode

View

Line configuration view

Usage Guidelines

NA

Example

Enter the MMI mode.

```
Switch(config-line)#mmi-mode enable
Switch (config-line)#
```

2.3 File System Configuration Commands

2.3.1 boot password recovery

Function

The **boot password recovery** command restores the default login password of the switch.

Format**boot password recovery****Parameter**

NA

Default Value

NA

View

Global configuration view

Usage Guidelines

NA

Example

Restore the default login password of the switch.

```
Switch(config)#boot password recovery
Switch(config)#
```

2.3.2 cd

Function

The **cd** command changes the working directory of the current user, enabling the user to switch between different directories.

Format

- **cd**
- **cd** *directory*

Parameter

Parameter	Description	Value
directory	Specifies a file directory.	The value is a character string. The directory name is case insensitive and cannot contain any of the following characters: space, wave line (~), asterisk (*), slash (/), back slash (\), colon (:), and apostrophe (').

Default Value

NA

View

Privileged user view

Usage Guidelines

You can run this command to switch between directories. If you run this command without specifying directory parameter, you will return to the root directory of the file system.

The directory specified in the command must exist; otherwise, the Switch displays the following error message:

```
Switch#cd abc
%"Ram:/flash/abc" isn't a directory
```

Example

Change the working directory of the current user from **Ram:/flash** to **Ram:/flash/user**.

```
Switch#cd
%Current Directory is "Ram:/flash".
Switch#cd user
%Current Directory is "Ram:/flash/user".
Switch#
```

2.3.3 copy

Function

The **copy** command copies the content of one file to another file.

Format

copy *srcfile destfile*

Parameter

Parameter	Description	Value
srcfile	Specifies the path and name of the source file to be copied.	The value is a character string.
destfile	Specifies the path and name of the destination file.	The value is a character string.

Default Value

NA

View

Privileged user view

Usage Guidelines

The path and name of the source and target files are case insensitive and cannot contain the following characters: space, ~, *, /, \, and .:

If you do not specify a file name when setting the *destfile* parameter, the destination file will have the same file name as the source file. However, if the source and destination files are in the same directory, the destination file name must be specified; otherwise, the file copy will fail.

Example

Copy the file **clock.sys** from the root directory of the flash (assuming that this directory is the current working directory) to flash: /user/, and set the destination file name to **clock1.sys**.

```
Switch#copy clock.sys /user/clock1.sys
    %Copying file Ram:/flash/clock.sys -> Ram:/flash/user/clock1.sys
Switch#
```

2.3.4 del

Function

The **del** command deletes a specified file from the flash.

Format

del *file-name*

Parameter

Parameter	Description	Value
file-name	Specifies a file name.	The value is a character string.

Default Value

NA

View

Privileged user view

Usage Guidelines

NA

Example# Delete the file **123** from the flash.

```
Switch(config)#del 123
Switch(config)#
```

2.3.5 dir**Function**The **dir** command displays the directory and file information in the storage device.**Format**

- **dir**
- **dir all**
- **dir tree dir**
- **dir tree dir subtree**
- **dir tree dir all**
- **dir tree dir subtree all**

Parameter

Parameter	Description	Value
dir	Specifies a directory.	The value is a character string.
[subtree]	It is an optional parameter, indicating to view the directory or subdirectory information.	-

Default Value

NA

View

Common user view

Usage Guidelines

This command supports fuzzy match with a wildcard *. If the value is not set, the output of this command displays directory and file information on the current path.

The following table describes the Attr values in the **dir** command output.

Item	Description
d	Indicates a directory. A value without this item indicates a file. For example:
r	Indicates a readable directory or file.
w	Indicates a writable directory or file.
X	Indicates a writable directory or file.

Example

Display information about all files and directories in the current path.

```
Switch#dir
Listing Directory Ram:/flash:
  attr   link   uid    gid    size    date    time    name
-----
-rwxrwxrwx 1    0    0          0 2100-01-01 07:18:14 bootparam.sys
-rwxrwxrSx 1    0    0          0 2100-01-01 07:18:14 clock.sys
drwxrwxrwx 1    0    0        4096 2100-01-01 07:18:14 user/
drwxrwxrwx 1    0    0        4096 2100-01-01 07:33:14 ssh/
-rwxrwxrwx 1    0    0          0 2100-01-01 07:18:22 swapfile
-rwxrwxrwx 1    0    0          0 2100-01-01 07:18:14 cfgresultfile
drwxrwxrwx 1    0    0        4096 2100-01-01 07:18:14 ifcfg/
-rwxrwxrSx 1    0    0          0 2100-01-01 07:18:18 startcfg
-rwxrwxrwx 1    0    0          0 2100-01-01 07:18:22 execfile

        6 files,3 directorys,total space:0 bytes
        available space: 16302080 bytes.

Switch#
```

2.3.6 ls tree**Function**

The **ls tree** command lists the content in a directory or its sub-directories.

Format

- **ls tree** *directory*
- **ls tree** *directory* **all**
- **ls tree** *directory* **subtree**
- **ls tree** *directory* **subtree** **all**

Parameter

Parameter	Description	Value
directory	Specifies a directory name.	The value is a character string. The path and name of the directory or file are case insensitive and cannot contain the following characters: space, ~, *, /, \, :, and '.

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

List the content in the directory **user**.

```
Switch>ls tree user
Listing Directory Ram:/flash/user:
  attr   link   uid     gid     size     date       time     name
-----
drwxrwxrwx 1    0      0         4096 2100-01-01 00:00:56 ./
drwxrwxrwx 1    0      0         4096 2100-01-01 00:00:56 ../
drwxrwxrwx 1    0      0         4096 2100-01-01 00:00:52 admin/
drwxrwxrwx 1    0      0         4096 2100-01-01 00:00:52 root/
drwxrwxrwx 1    0      0         4096 2100-01-01 00:00:56 123/

      0 files,5 directories,total space:0 bytes

      available space: 16285696 bytes.

Switch>
```

2.3.7 mkdir

Function

The **mkdir** command creates a new directory.

Format

mkdir *directory*

Parameter

Parameter	Description	Value
directory	Specifies a name of the new directory.	The value is a character string. The path and name of the directory or file are case insensitive and cannot contain the following characters: space, ~, *, /, \, :, and '.

Default Value

NA

View

Privileged user view

Usage Guidelines

NA

Example

Create a new directory **fhn** under %"Ram:/flash/.

```
Switch#mkdir fhn
Switch#
```

2.3.8 move

Function

The **move** command moves a source file or wildcard to the target file or directory.

Format

move *srcfile destfile*

Parameter

Parameter	Description	Value
srcfile	Specifies the source file.	The length is up to 255 characters.

Parameter	Description	Value
destfile	Specifies the target file.	The length is up to 255 characters.

Default Value

NA

View

Privileged user view

Usage Guidelines

NA

Example

Move source file **fhn** to the **dmp** directory.

```
Switch#move fhn dmp
Switch#
```

2.3.9 pwd**Function**

The **pwd** command displays the current directory.

Format**pwd****Parameter**

NA

Default Value

NA

View

Privileged user view

Usage Guidelines

NA

Example

Display the current directory.


```
Switch#pwd
    %Current Directory is "Ram:/flash".
Switch#
```

2.3.10 remove

Function

The **remove** command deletes a specified file from the storage device of the switch.

The **remove unreserved** command permanently deletes a specified file in the Switch storage to the recycle bin.

Format

remove *file-name*

remove *filename* **unreserved**

Parameter

Parameter	Description	Value
file-name	Specifies the path and name of the file to be deleted.	The value is a character string. The path and name of the directory or file are case insensitive and cannot contain the following characters: space, ~, *, /, \, :, and '.

Default Value

NA

View

Privileged user view

Usage Guidelines

This command supports fuzzy match with a wildcard *.

Example

Delete files in the directory **TEMP** on the core switch card.

```
Switch#remove TEMP
Switch#
```

2.3.11 rename

Function

The **rename** command renames a file.

Format

rename *src-filename new-filename*

Parameter

Parameter	Description	Value
src-filename	Specifies original file name.	The value is a character string. The path and name of the directory or file are case insensitive and cannot contain the following characters: space, ~, *, /, \, :, and '.
new-filename	Specifies a new file name.	

Default Value

NA

View

Privileged user view

Usage Guidelines

If the new file name is the same as an existing directory name or file name, the system will display an error message.

If the values of *src-filename* and *new-filename* do not contain the directory of the file to be renamed, ensure that the file is saved in the working directory of the current user.

Example

Change the name of the file **sample.txt** to **sample.bak**.

```
Switch#rename STARTCFG aaa
Switch#
```

2.3.12 rmdir**Function**

The **rmdir** command deletes a directory or its sub-directories.

Format

- **rmdir** *directory*
- **rmdir** *directory subtree*

Parameter

Parameter	Description	Value

Parameter	Description	Value
directory	Specifies the name of the directory to be deleted.	The value is a character string. The path and name of the directory or file are case insensitive and cannot contain the following characters: space, ~, *, /, \, :, and '.

Default Value

NA

View

Privileged user view

Usage Guidelines

NA

Example

Delete the directory **123**.

Switch#rmdir 123							
Switch#ls							
Listing Directory Ram:/flash:							
attr	link	uid	gid	size	date	time	name

-rwxrwxrwx	1	0	0		0	2100-01-01 00:43:08	bootparam.sys
-rwxrwxrSx	1	0	0		0	2100-01-01 00:43:08	clock.sys
drwxrwxrwx	1	0	0	4096	2100-01-01 00:43:08		user/
-rwxrwxrwx	1	0	0		0	2100-01-01 00:43:26	execfile
-rwxrwxrwx	1	0	0		0	2100-01-01 00:43:26	swapfile
-rwxrwxrwx	1	0	0		0	2100-01-01 00:43:08	cfgresultfile
drwxrwxrwx	1	0	0	4096	2100-01-01 00:43:08		ifcfg/
-rwxrwxrSx	1	0	0		0	2100-01-01 00:43:10	startcfg
6 files,2 directories,total space:0 bytes							
available space: 16318464 bytes.							
Switch#							

2.3.13 type

Function

The **type** command displays the content of a specified binary or text file. The file system displays the file content in a text file.

Format

- **type** *file-name*
- **type** *file-name* { **binary** | **text** }

Parameter

Parameter	Description	Value
file-name	Specifies the specific file name.	The value is a character string.
binary	Specifies a binary file name.	The value is a character string. The path and name of the directory or file are case insensitive and cannot contain the following characters: space, ~, *, /, \, :, and '.
text	Specifies a text file name.	The value is a character string. The path and name of the directory or file are case insensitive and cannot contain the following characters: space, ~, *, /, \, :, and '.

Default Value

NA

View

Privileged user view

Usage Guidelines

The file system of the Switch displays files in the text format. If you do not specify the file directory in the command, the system defaults the directory as the current directory.

You can use the **dir** or **ls** command in the current view to obtain the name of the file you want to check.

Example

Display the content of the text file **startcfg**.

```
Switch#type startcfg
!System startup configuration
!version V310R230
!2019/01/09 00:18:18
!
  hostname Switch
  no auth-degenerate
!
  logging history 7
!
```

```
username admin group administrators password 827ccb0eea8a706c4c34a16891f84e7b
user reauth-interval 10
user fail-count 10
user privilege level administrators password 306b6341993337d4
user privilege level operators password 306b6341993337d4
user privilege level users password 306b6341993337d4
user privilege level guests password 306b6341993337d4
!
snmp trap-history 1024
snmp rich-trap enable
!
vlan 1
!
interface ethernet 0/0/0
!
line console 1
length 24
timeout 0 0
login local
language english
no color
line vty 1 5
length 24
no monitor
timeout 10 0
login local
language english
no color
!
!
interface xgigaethernet 1/0/1
!
interface xgigaethernet 1/0/2
!
interface xgigaethernet 1/0/3
!
interface xgigaethernet 1/0/4
!
interface xgigaethernet 1/0/5
!
interface xgigaethernet 1/0/6
!
interface xgigaethernet 1/0/7
```

```
!  
interface xgigaethernet 1/0/8  
!  
interface xgigaethernet 1/0/9  
!  
interface xgigaethernet 1/0/10  
!  
interface xgigaethernet 1/0/11  
!  
interface xgigaethernet 1/0/12  
!  
interface xgigaethernet 1/0/13  
!  
interface xgigaethernet 1/0/14  
!  
interface xgigaethernet 1/0/15  
!  
interface xgigaethernet 1/0/16  
!  
interface xgigaethernet 1/0/17  
!  
interface xgigaethernet 1/0/18  
!  
interface xgigaethernet 1/0/19  
!  
interface xgigaethernet 1/0/20  
!  
interface xgigaethernet 1/0/21  
!  
interface xgigaethernet 1/0/22  
!  
interface xgigaethernet 1/0/23  
!  
interface xgigaethernet 1/0/24  
!  
!end  
  
Switch#
```

2.3.14 xcopy

Function

The **xcopy** command copies one folder to another folder.

Format

xcopy *srcfile destfile*

Parameter

Parameter	Description	Value
srcfile	Specifies the path and name of the source folder to be copied.	The value is a character string.
destfile	Specifies the path and name of the destination folder.	The value is a character string.

Default Value

NA

View

Privileged user view

Usage Guidelines

The path and name of the source and target files are case insensitive and cannot contain the following characters: space, ~, *, /, \, and .:

Example

Copy the folder **clock** from the root directory of the flash (assuming that this directory is the current working directory) to flash: /user/.

```
Switch#xcopy clock /user/clock1.sys
    %Copying file Ram:/flash/clock -> Ram:/flash/user/clock
Switch#
```

2.3.15 zero**Function**

The **zero** command deletes all content of a specified file.

Format

zero *filename*

Parameter

Parameter	Description	Value
filename	Specifies the path and name of the file of which the content will be deleted.	The value is a character string. The path and name of the directory or file are case insensitive and cannot contain the following characters: space, ~, *, /, \, :, and '.

Default Value

NA

View

Privileged user view

Usage Guidelines

NA

Example

Deletes all the content of the file **temp**.

```
Switch#zero temp
Switch#
```

2.3.16 find**Function**

The **find** command searches for a file with the specified name.

The **find string** command searches for a file with the specified character string in the file name.

Format

- **find file-name**
- **find file-name string**

Parameter

Parameter	Description	Value
file-name	Specifies the name of the file to be found.	The value is a character string. The path and name of the directory or file are case insensitive and cannot contain the following characters: space, ~, *, /, \, :, and '.
string	Specifies a string of characters.	The value is a character string.

Default Value

NA

View

Privileged user view

Usage Guidelines

After you run this command, the system will list the path of the specified file.

Example

Find the file named **user**.

```
Switch(config)#find user
    find dir Ram:/flash/user

Switch(config)#
```

2.4 System Configuration File Commands

2.4.1 copy startup-config running-config

Function

The **copy startup-config running-config** command copies the configuration file to the current system configuration.

Format

copy startup-config running-config

Parameter

NA

Default Value

NA

View

Global configuration view

Usage Guidelines

After configuring the switch, you can run this command to copy the current configuration to the system running configuration to make the new configuration take effect.

After running this command, you must run **write file** to save the current configuration; otherwise, the new configuration becomes invalid.

Example

After creating a VLAN, copy the current configuration to the running configuration.

```
Switch(config)#copy startup-config running-config
This will update current device configuration.
Are you sure?[y/n]
```

```
It will take a few minutes,please waiting.....
```

```
[OK]
```

```
Switch(config)#
```

2.4.2 compare configuration

Function

The **compare configuration** command compares whether the current configuration and the configuration file for next startup are consistent.

Format

- **compare configuration** *skip-lines1* *skip-lines2*
- **compare configuration** **startup-config**

Parameter

Parameter	Description	Value
skip-lines1	Indicates starting from the current running configuration of this line number.	The value is an integer ranging from 1 to 65535.
skip-lines2	Indicates starting from the saved configuration file of this line number.	The value is an integer ranging from 1 to 65535.

Default Value

NA

View

Common user view

Usage Guidelines

If **startup-config Skip lines** is not specified, the system compares whether the current configuration and the configuration file for next startup are consistent.

If **startup-config Skip lines** is specified, the system compares whether the current configuration and the specified startup configuration file are consistent.

Example

Start from the lines 1 to 3 of the current running configuration.

```
Switch>compare configuration 1 3
```

```
Warning:The current configuration is not the same as the saved configuration!.
```

```
===== Running configuration line 2 =====.
```

```
hostname Switch
```

```

no auth-degenerate
!
!logging configuration.
!
!
!User configuration.
  username admin group operators password 827ccb0eea8a706c4c34a16891f84e7b
  username 123 group operators password e10adc3949ba59abbe56e057f20f883e
  user privilege level administrators password 306b6341993337d4
  ===== Saved configuration line 4 =====.
!
hostname Switch
no auth-degenerate
!
!logging configuration.
!
!
!User configuration.
  username admin group administrators password 827ccb0eea8a706c4c34a16891f84e7b
  username 123 group operators password e10adc3949ba59abbe56e057f20f883e
Switch>

```

2.4.3 erase startup-config

Function

The **erase startup-config** command clears the startup configuration file in the switch storage.

Format

erase startup-config

Parameter

NA

Default Value

NA

View

Global configuration view, privileged user view

Usage Guidelines

This command is usually used in either of the following conditions:

- After the system software of the switch is upgraded, the configuration file saved in the storage does not match the new software version. In this case, run this command to delete the old startup configuration file.
- When the switch is used in a new environment, the original configuration file does not meet requirements of the new application. In this case, you need to delete the old startup configuration file and re-configure the switch.



Warning:

It is recommended that you use this command under instruction of technical support personnel.

Example

Delete the startup configuration file in the storage device.

```
Switch(config)#erase startup-config
This will erase the configuration in the flash memory.
Are you sure?(y/n) [y] y
Switch(config)#
```

2.4.4 upgrade {os|config|fpga} system

Function

The **upgrade {os|config|fpga} system** command upgrades the active core switch card or updates the configuration file.

Format

- **upgrade { os | config | fpga } system { all | self }**
- **upgrade { os | config | fpga } system { all | self } file** *local-filename*
- **upgrade { os | config | fpga } system** *system-id*
- **upgrade { os | config | fpga } system** *system-id* **file** *local-filename*

Parameter

Parameter	Description	Value
local-filename	Specifies the local file name.	The value is a character string.
system-id	Specifies the system ID	The value is an integer ranging from 1 to 4.

Default Value

NA

View

Global configuration view

Usage Guidelines

If upgrading fails, the system prompts "file error".

Example

Update the configuration file of the active core switch card.

```
Switch(config)#ftp get 192.168.0.152 123 123 e:\Switchconfig.txt
Local path is "Ram:/flash/download".
Getting data...
16105 bytes downloaded.

If you want to update system,use "upgrade" command!
Switch(config)#upgrade config system all
WARNING:System will upgrade! Continue?[y/n]y
System now is upgrading,please wait.
%Local path is "Ram:/flash/download".
OK
Switch(config)#
```

2.4.5 show running-config

Function

The **show running-config** command displays the running system configuration.

The **show running-config include-default** command displays the system configuration parameters that are effective currently, including the default values.

Format

show running-config

show running-config include-default

Parameter

NA

Default Value

NA

View

Common user view

Usage Guidelines

After completing a series of configuration, you can run this command to check whether the running system configurations and their default values are correct.

Example

Display the running system configuration.

```
Switch>show running-config
!Device running configuration:
!version V410R240
!2008/04/21 22:19:24
!
hostname DUT2
enable password level 15 plain 123
!
logging source default action monitor log state enable
logging source default action monitor debug state enable
!
username DUT2 group operators password $1$kiyv$b1P5gEaeX6wG6eQLeT3Di0
username admin group administrators password $1$kiyv$b1P5gEaeX6wG6eQLeT3Di0
username admin online-count 64
username zcd group guests password $1$kiyv$FrLivsk/A2cnj4wGdatKo.
username zcd fail-count 10
username zcd2 group operators password $1$kiyv$3Dd12297IF4H3Ejh.GwaL0
username zcd2 fail-count 10
user fail-count 10
!
no snmp version v1
no snmp version v3
snmp community $9$kiyv$10ca10aa5145c2d9 rw cipher view internet
Switch>
```

2.4.6 show startup-config**Function**

The **show startup-config** command displays the configuration file used upon the last startup of the switch.

Format

- **show startup-config**
- **show startup-config { include | exclude| begin | end } substring *string***

Parameter

Parameter	Description	Value
string	Specifies a character string used for filtering the configuration information to be displayed.	The value is a character string.

Default Value

NA

View

Common user view

Usage Guidelines

The startup configuration file is the configuration file that the switch uses when it is powered on or reboots.

If the switch is powered on successfully but does not work normally after entering CLI, you can use this command to check the startup configuration file.

If no configuration file is saved in the system, this command cannot display any information.

Example

Display the configuration file used upon the last startup of the switch.

```
Switch>show startup-config
!System startup configuration
!2008/04/18 18:08:34
!
hostname DUT2
enable password level 15 plain 123
!
logging source default action monitor log state enable
logging source default action monitor debug state enable
!
username DUT2 group operators password $1$kijv$b1P5gEaeX6wG6eQLeT3Di0
username admin group administrators password $1$kijv$b1P5gEaeX6wG6eQLeT3Di0
username admin online-count 64
username zcd group guests password $1$kijv$FrLivsk/A2cnj4wGdatKo.
username zcd fail-count 10
username zcd2 group operators password $1$kijv$3Dd12297IF4H3Ejh.GwaL0
```

```

username zcd2 fail-count 10
user fail-count 10
!
 ftpd
!
 tftpd
!
 sshd
!
 mirror group 1 10gigaethernet 1/0/48
Switch>

```

2.4.7 del os-file

Function

The **del os-file** command deletes all OS files or OS files with the specified name stored in the switch memory.

Format

- **del os-file**
- **del os-file** *name*

Parameter

Parameter	Description	Value
name	Specifies the OS file name.	The value is a character string.

Default Value

NA

View

Global configuration view

Usage Guidelines

NA

Example

Delete OS files with the specified name stored in the switch memory.

```

Switch(config)#del os-file Switch_OS.bin
Switch(config)#

```


2.4.8 show os-file

Function

The **show os-file** command displays the OS files stored in the switch memory.

Format

show os-file

Parameter

NA

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

View the OS files stored in the switch memory.

```
Switch>show os-file
attr          link          uid      gid      size          date      time      name
-----
total:321048
-rw-r--r--    1      root    root    328744984    Jun 18    11:43    Switch_OS.bin

Switch>
```

2.4.9 remote upgrade {enable|disable}

Function

The **remote upgrade {enable|disable}** command enables or disables the remote upgrading function.

Format

remote upgrade { enable | disable }

Parameter

Parameter	Description	Value
enable	Enables the remote upgrading function.	-

Parameter	Description	Value
disable	Disables the remote upgrading function.	-

Default Value

NA

View

Global configuration view

Usage Guidelines

NA

Example

Enable the remote upgrading function.

```
Switch(config)#remote upgrade enable
Switch(config)#
```

2.5 File Uploading and Downloading Configuration Commands

2.5.1 tftp get

Function

The **tftp get** command downloads a remote file using the TFTP protocol and saves it on the local device. (This command applies to IPv4 networks.)

Format

- **tftp get** *ipv4-address remotefile* [*port-id*]
- **tftp get** *ipv4-address remotefile localfile filename* [*port-id*]
- **tftp get** *ipv4-address vpn-instance name remotefile* [*port-id*]
- **tftp get** *ipv4-address vpn-instance name remotefile localfile filename* [*port-id*]

Parameter

Parameter	Description	Value
ipv4-address	Specifies a host IPv4 address.	The value is in dotted decimal notation.
remotefile	Specifies the name of the file to be downloaded from the host.	The value is a character string consisting of 1 to 63 characters.
filename	Specifies the local file name.	The value is a character string consisting of 1 to 63 characters.

Parameter	Description	Value
port-id	Specifies the port number, which is optional.	The value is an integer ranging from 1 to 65535.
name	Specifies a VPN instance name.	The value is a character string.

Default Value

NA

View

Global configuration view

Usage Guidelines

During switch running maintenance, you need to download the configuration file or operating system file from the host to the switch to configure or upgrade the operating system. This command is used download such files to the switch.

If you do not specify *filename* in the command, the downloaded file will have the same name as the file on the TFTP server.

Before running this command, ensure that the switch can communicate with the TFTP server, and the user name and password have been configured on the TFTP server.



Caution

It is recommended that you use this command under instruction of technical support personnel.

Example

Download the file **Switch_OS.bin** to the switch from the TFTP server, and save the file on the switch as **v2.4.bin**.

```
Switch(config)#tftp get 10.18.21.141 Switch_OS.bin localfile v2.4.bin
Getting File " Switch_OS.bin " from 192.168.1.200...
1528618 bytes downloaded.
If you want to upgrade system,use "upgrade" command!
Switch(config)#
```

2.5.2 tftp put

Function

The **tftp put** command uploads a local file to a remote TFTP server. (This command applies to IPv4 networks.)

Format

- **tftp put** *ipv4-address* *remotefile* **running-config**
- **tftp put** *ipv4-address* *remotefile* **config**
- **tftp put** *ipv4-address* *remotefile* **localfile** *filename* [*port-id*]
- **tftp put** *ipv4-address* **vpn-instance** *name* *remotefile* **config**
- **tftp put** *ipv4-address* **vpn-instance** *name* *remotefile* **localfile** *filename* [*port-id*]

Parameter

Parameter	Description	Value
ipv4-address	Specifies a host IPv4 address.	The value is in dotted decimal notation.
remotefile	Specifies the name of the file to be uploaded from the host to the server.	The value is a character string consisting of 1 to 63 characters.
filename	Specifies the name of the local file to be uploaded.	The value is a character string consisting of 1 to 63 characters.
port-id	Specifies the port number, which is optional.	The value is an integer ranging from 1 to 65535.
config	Uploads the configuration file of the switch.	-
name	Specifies a VPN instance name.	The value is a character string.

Default Value

NA

View

Global configuration view

Usage Guidelines

During device operation and maintenance, you can use this command to upload files of the switch (including the configuration file) to a remote TFTP server for backup.

Before running this command, ensure that the switch can communicate with the TFTP server, and the user name and password have been configured on the TFTP server. In addition, the user account must have the read and write permissions on the TFTP server. Otherwise, the host will not respond for a long time or the upload task will be suspended.

**Caution**

It is recommended that you use this command under instruction of technical support personnel.

Example

Upload the configuration file of the switch to the TFTP server, and save the file as **config.ini** on the server.

```
Switch(config)#tftp put 10.18.33.127 d:/config.ini config
1136 bytes uploaded
Switch(config)#
```

2.5.3 tftpd**Function**

The **tftpd** command enables the TFTP server function on the switch.

The **no tftpd** command disables the TFTP server function on the switch.

Format

- **tftpd**
- **no tftpd**

Parameter

NA

Default Value

By default, the TFTP server function is disabled.

View

Global configuration view

Usage Guidelines

After the TFTP server function is enabled on the switch, the switch acts as a TFTP server. You can log in to the switch using a TFTP client and upload files to or download files from the switch. The TFTP server uses the local user name and password for login authentication.

Example

Enable the TFTP server function on the switch.

```
Switch(config)#tftpd
    %TFTP server successfully start!
Switch(config)#
```

2.5.4 debug tftp

Function

The **debug tftp** command enables the TFTP debugging function. (This command applies to IPv4 networks.)

The **no debug tftp** command disables this debugging function.

Format

- **debug tftp**
- **no debug tftp**

Parameter

NA

Default Value

By default, debugging of the FTP server is disabled.

View

Privileged user view

Usage Guidelines

NA

Example

Enable the TFTP debugging function.

```
Switch#debug tftp
Switch#
```

Disable debugging of the FTP server.

```
Switch#no debug tftp
Switch#
```

2.5.5 debug l2tftpd

Function

The **debug l2tftpd** command enables debugging of the TFTP server.

The **no debug l2tftpd** command disables debugging of the TFTP server.

Format

- **debug l2tftpd**
- **no debug l2tftpd**

Parameter

NA

Default Value

NA

View

Global configuration view

Usage Guidelines

NA

Example

Enable debugging of the TFTP server.

```
Switch(config)#debug l2tftpd
Switch(config)#
```

2.5.6 debug ftpd

Function

The **debug ftpd** command enables debugging of the FTP server on the switch. (This command applies to IPv4 networks.)

The **no debug ftpd** command disables debugging of the FTP server on the switch.

Format

- **debug ftpd**
- **no debug ftpd**

Parameter

NA

Default Value

By default, debugging of the FTP server is disabled.

View

Privileged user view

Usage Guidelines

If the switch acts as an FTP server and experiences a failure or problem, you can use this command to enable FTP server debugging. This function helps to locate the problem.

Example

Enable debugging of the FTP server on the switch.

```
Switch#debug ftpd
Switch#
```

Disable debugging of the FTP server.

```
Switch#no debug ftpd
Switch#
```

2.5.7 ftp put**Function**

The **ftp put** command uploads a local file to a remote FTP server. (This command applies to IPv4 networks.)

Format

- **ftp put** *ipv4-address user password remotefile config*
- **ftp put** *ipv4-address user password remotefile localfile filename [port-id]*
- **ftp put** *ipv4-address src-ip src-ipv4-address vpn-instance name user password remotefile config*
- **ftp put** *ipv4-address user password remotefile running-config*
- **ftp put** *ipv4-address src-ip src-ipv4-address vpn-instance name user password remotefile localfile filename port-id*
- **ftp put** *ipv4-address src-ip src-ipv4-address vpn-instance name user password remotefile localfile filename*

Parameter

Parameter	Description	Value
ipv4-address	Specifies a host IPv4 address.	The value is in dotted decimal notation.
user	Specifies the user name used for logging to the FTP server.	The value is a character string consisting of 1 to 63 characters.
password	Specifies the password used for logging to the FTP server.	The value is a character string consisting of 1 to 63 characters.
remotefile	Specifies the name of the file to be downloaded from the host.	The value is a character string consisting of 1 to 63 characters.
filename	Specifies the local file name.	The value is a character string consisting of 1 to 63 characters.
port-id	Specifies the port number, which is optional.	The value is an integer ranging from 1 to 65535.
config	Uploads the configuration file of the switch.	-
name	Specifies a VPN instance name.	The value is a character string containing a maximum of 64 characters.

Default Value

NA

View

Global configuration view

Usage Guidelines

During device operation and maintenance, you can use this command to upload files of the switch (including the configuration file) to a remote FTP server for backup.

Before running this command, ensure that the switch can communicate with the FTP server, and the user name and password have been configured on the FTP server. In addition, the user account must have the read and write permissions on the TFTP server. Otherwise, the host will not respond for a long time or the upload task will be suspended.



Caution

It is recommended that you use this command under instruction of technical support personnel.

Example

Use the user name **123** and password **123** to log in to the FTP server with IP address 192.168.1.200, upload the configuration file of the switch to the FTP server, and save the file as **config.ini** on the server.

```
Switch(config)#ftp put 192.168.1.200 123 123 d:/config.ini config
1136 bytes uploaded
Switch(config)#
```

2.5.8 ftp get

Function

The **ftp get** command downloads a remote file and saves it on the local device. (This command applies to IPv4 networks.)

Format

Common user view, global configuration view:

- **ftp get** *ipv4-address user password remotefile [port-id]*
- **ftp get** *ipv4-address user password remotefile localfile filename [port-id]*

Global configuration view:

- **ftp get** *ipv4-address src-ip src-ipv4-address vpn-instance name user password remotefile*
- **ftp get** *ipv4-address src-ip src-ipv4-address vpn-instance name user password remotefile port-id*
- **ftp get** *ipv4-address src-ip src-ipv4-address vpn-instance name user password remotefile localfile filename*
- **ftp get** *ipv4-address src-ip src-ipv4-address vpn-instance name user password remotefile localfile filename port-id*

Parameter

Parameter	Description	Value
ipv4-address	Specifies a host IPv4 address.	The value is in dotted decimal notation.
user	Specifies the user name used for logging to the FTP server.	The value is a character string consisting of 1 to 63 characters.
password	Specifies the password used for logging to the FTP server.	The value is a character string consisting of 1 to 63 characters.
remotefile	Specifies the name of the file to be downloaded from the host.	The value is a character string consisting of 1 to 63 characters.
filename	Specifies the local file name.	The value is a character string consisting of 1 to 63 characters.
port-id	Specifies the port number, which is optional.	The value is an integer ranging from 1 to 65535.
name	Specifies the VPN instance name of the	The value is a character string consisting of 1 to

Parameter	Description	Value
	remote FTP server.	64 characters.

Default Value

NA

View

Common user view, global configuration view

Usage Guidelines

During switch running maintenance, you need to download the configuration file or operating system file from the host to the switch to configure or upgrade the operating system. This command is used download such files to the switch.

If you do not specify *filename* in the command, the downloaded file will have the same name as the file on the FTP server.

Before running this command, ensure that the switch can communicate with the FTP server, and the user name and password have been configured on the FTP server.



Caution

It is recommended that you use this command under instruction of technical support personnel.

Example

Use the user name **123** and password **123** to log in to the FTP server with IP address 192.168.1.200, download the file **Switch.bin** to the switch from the FTP server, and save the file on the switch as **v2.4.bin**.

```
Switch(config)#ftp get 192.168.1.200 123 123 Switch.bin v2.4.bin
Getting File "Switch.bin" from 192.168.1.200...
1528618 bytes downloaded.
If you want to upgrade system,use "upgrade" command!
Switch(config)#
```

2.5.9 ftp delete

Function

The **ftp delete** command deletes a file from a specified FTP server. (This command applies to IPv4 networks.)

Format

- **ftp delete** *ipv4-address user password remotefile*
- **ftp delete** *ipv4-address user password remotefile port-id*
- **ftp delete** *ipv4-address src-ip src-ipv4-address vpn-instance name user password remotefile*
- **ftp delete** *ipv4-address src-ip src-ipv4-address vpn-instance name user password remotefile port-id*

Parameter

Parameter	Description	Value
ipv4-address	Specifies a host IPv4 address.	The value is in dotted decimal notation.
user	Specifies the user name used for logging to the FTP server.	The value is a character string consisting of 1 to 63 characters.
password	Specifies the password used for logging to the FTP server.	The value is a character string consisting of 1 to 63 characters.
remotefile	Specifies the name of the file to be downloaded from the host.	The value is a character string consisting of 1 to 63 characters.
port-id	Specifies the port number, which is optional.	The value is an integer ranging from 1 to 65535.
name	Specifies a VPN instance name.	The value is a character string.
src-ipv4-address	Specifies a source IPv4 address.	The value is in dotted decimal notation.

Default Value

NA

View

Global configuration view

Usage Guidelines



Caution

It is recommended that you use this command under instruction of technical support personnel.

Example

Delete the files on the specified FTP server

```
Switch(config)#ftp delete 10.18.2.16 aaa 111 rem 11
Switch(config)#
```

2.5.10 ftpd

Function

The **ftpd** command enables the FTP server function on the switch. (This command applies to IPv4 networks.)

The **no ftpd** command disables the FTP server function on the switch.

Format

- **ftpd**
- **no ftpd**

Parameter

NA

Default Value

By default, the FTP server function is disabled.

View

Global configuration view

Usage Guidelines

After the FTP server function is enabled on the switch, the switch acts as an FTP server. You can log in to the switch using an FTP client and upload files to or download files from the switch. The FTP server uses the local user name and password for login authentication.

Example

Enable the FTP server function on the switch.

```
Switch(config)#ftpd
Switch(config)#
```

2.5.11 ftp6 get

Function

The **ftp6 get** command downloads a remote file and saves it on the local device. (This command applies to IPv6 networks.)

Format

Common user view, global configuration view:

- **ftp6 get** *ipv6-address user password remotefile [port-id]*
- **ftp6 get** *ipv6-address user password remotefile localfile filename [port-id]*

Global configuration view:

- **ftp6 get** *ipv6-address src-ipv6 src-ipv6-address vpn-instance name user password remotefile*
- **ftp6 get** *ipv6-address src-ipv6 src-ipv6-address vpn-instance name user password remotefile port-id*
- **ftp6 get** *ipv6-address src-ipv6 src-ipv6-address vpn-instance name user password remotefile localfile filename*
- **ftp6 get** *ipv6-address src-ipv6 src-ipv6-address vpn-instance name user password remotefile localfile filename port-id*

Parameter

Parameter	Description	Value
ipv6-address	Specifies a host IPv6 address.	In this format, a 128-digit IP address is divided into 8 segments. Each segment consists of 16 digits and is represented by 4 hexadecimal characters (0-9 and A-F). Segments are separated by colons (:). Every "X" represents a group of hexadecimal digits.
user	Specifies the user name used for logging to the FTP server.	The value is a character string consisting of 1 to 63 characters.
password	Specifies the password used for logging to the FTP server.	The value is a character string consisting of 1 to 63 characters.
remotefile	Specifies the name of the file to be downloaded from the host.	The value is a character string consisting of 1 to 63 characters.
filename	Specifies the local file name.	The value is a character string consisting of 1 to 63 characters.
port-id	Specifies the port number, which is optional.	The value is an integer ranging from 1 to 65535.
config	Downloads the configuration file of the device.	-
name	Specifies a VPN instance name.	The value is a character string.

Default Value

NA

View

Common user view, global configuration view

Usage Guidelines

During switch running maintenance, you need to download the configuration file or operating system file from the host to the switch to configure or upgrade the operating system. This command is used download such files to the switch.

If you do not specify *filename* in the command, the downloaded file will have the same name as the file on the FTP server.

Before running this command, ensure that the switch can communicate with the FTP server, and the user name and password have been configured on the FTP server.



Caution

It is recommended that you use this command under instruction of technical support personnel.

Example

Use the user name **123** and password **123** to log in to the server **2001::1**, download the file **Switch.bin** from the FTP server to a local device, and rename the file as **v2.3.bin**.

```
Switch(config)#ftp6 get 2001::1 123 123 Switch.bin v2.3.bin
Getting File "Switch.bin" from 2001::1...
1528618 bytes downloaded.
If you want to upgrade system,use "upgrade" command!
Switch(config)#
```

2.5.12 ftp6 put**Function**

The **ftp6 put** command uploads a local file to a remote FTP server. (This command applies to IPv6 networks.)

Format

- **ftp6 put** *ipv6-address user password remotefile config*

- **ftp6 put** *ipv6-address user password remotefile localfile filename [port-id]*
- **ftp6 put** *ipv6-address src-ipv6 src-ipv6-address vpn-instance name user password remotefile config*
- **ftp6 put** *ipv6-address src-ipv6 src-ipv6-address vpn-instance name user password remotefile localfile filename*
- **ftp6 put** *ipv6-address src-ipv6 src-ipv6-address vpn-instance name user password remotefile localfile filename port-id*
- **ftp6 put** *ipv6-address user password remotefile running-config*

Parameter

Parameter	Description	Value
ipv6-address	Specifies a host IPv6 address.	The value is in dotted decimal notation.
user	Specifies the user name used for logging to the FTP server.	The value is a character string consisting of 1 to 63 characters.
password	Specifies the password used for logging to the FTP server.	The value is a character string consisting of 1 to 63 characters.
remotefile	Specifies the name of the file to be downloaded from the host.	The value is a character string consisting of 1 to 63 characters.
filename	Specifies the local file name.	The value is a character string consisting of 1 to 63 characters.
port-id	Specifies the port number, which is optional.	The value is an integer ranging from 1 to 65535.
config	Uploads the configuration file of the switch.	-
name	Specifies a VPN instance name.	The value is a character string.

Default Value

NA

View

Global configuration view

Usage Guidelines

During device operation and maintenance, you can use this command to upload files of the switch (including the configuration file) to a remote FTP server for backup.

Before running this command, ensure that the switch can communicate with the FTP server, and the user name and password have been configured on the FTP server. In addition, the user account must

have the read and write permissions on the TFTP server. Otherwise, the host will not respond for a long time or the upload task will be suspended.



Caution

It is recommended that you use this command under instruction of technical support personnel.

Example

Use the user name **123** and password **123** to log in to the server **2001::1**, upload a local configuration file from the switch to the FTP server, and save and rename the file as **config.ini**.

```
Switch(config)#ftp6 put 2001::1 123 123 d:/config.ini config
1136 bytes uploaded
Switch(config)#
```

2.5.13 ftp6 delete

Function

The **ftp6 delete** command deletes a file from a specified FTP server. (This command applies to IPV6 networks.)

Format

- **ftp6 delete** *ipv6-address user password remotefile*
- **ftp6 delete** *ipv6-address user password remotefile port-id*
- **ftp6 delete** *ipv6-address src-ipv6 src-ipv6-address vpn-instance name user password remotefile*
- **ftp6 delete** *ipv6-address src-ipv6 src-ipv6-address vpn-instance name user password remotefile port-id*

Parameter

Parameter	Description	Value
ipv6-address	Specifies a host IPv6 address.	In this format, a 128-digit IP address is divided into 8 segments. Each segment consists of 16 digits and is represented by 4 hexadecimal characters (0-9 and A-F). Segments are separated by colons (:). Every "X" represents a group of hexadecimal digits.

Parameter	Description	Value
user	Specifies the user name used for logging to the FTP server.	The value is a character string consisting of 1 to 63 characters.
password	Specifies the password used for logging to the FTP server.	The value is a character string consisting of 1 to 63 characters.
remotefile	Specifies the name of the file to be downloaded from the host.	The value is a character string consisting of 1 to 63 characters.
[port-id]	Specifies the port number, which is optional.	The value is an integer ranging from 1 to 65535.
name	Specifies a VPN instance name.	The value is a character string.

Default Value

NA

View

Global configuration view

Usage Guidelines



Caution

It is recommended that you use this command under instruction of technical support personnel.

Example

Delete the files on the specified FTP server

```
Switch(config)#ftp6 delete 22:11 aaa 111 rem 11
Switch(config)#
```

2.5.14 tftpd6

Function

The **tftpd6** command enables TFTP6 Server function for the switch.

The **no tftpd6** command disables TFTP6 Server function for the switch.

Format

- **tftpd6**
- **no tftpd6**

Parameter

NA

Default Value

By default, the switch TFTP6 Server function is disabled.

View

Global configuration view

Usage Guidelines

After TFTP6 Server is enabled for the switch, the switch can serve as a TFTP6 server and you can log in to the switch from TFTP6 Client to upload and download files. TFTP6 Server uses the switch local user for authentication.

Example

Enable the TFTP6 Server function on the switch.

```
Switch(config)#tftpd6
    %TFTP6 server successfully start!
Switch(config)#
```

2.5.15 tftp6 get**Function**

The **tftp6 get** command downloads a file from a remote TFTP server and saves it in a local device. (This command applies to IPv6 networks.)

Format

- **tftp6 get** *ipv6-address remotefile* [*port-id*]
- **tftp6 get** *ipv6-address remotefile localfile filename* [*port-id*]
- **tftp6 get** *ipv6-address vpn-instance name remotefile* [*port-id*]
- **tftp6 get** *ipv6-address vpn-instance name remotefile localfile filename* [*port-id*]

Parameter

Parameter	Description	Value
ipv6-address	Specifies a host IPv6 address.	In this format, a 128-digit IP address is divided into 8 segments. Each segment consists of 16 digits and is represented by 4 hexadecimal characters (0-9 and A-F). Segments are

Parameter	Description	Value
		separated by colons (:). Every "X" represents a group of hexadecimal digits.
remote file	Specifies the name of the file to be downloaded from the host.	The value is a character string consisting of 1 to 63 characters.
filename	Specifies the local file name.	The value is a character string consisting of 1 to 63 characters.
[port-id]	Specifies the port number, which is optional.	The value is an integer ranging from 1 to 65535.
name	Specifies a VPN instance name.	The value is a character string.

Default Value

NA

View

Global configuration view

Usage Guidelines

During switch running maintenance, you need to download the configuration file or operating system file from the host to the switch to configure or upgrade the operating system. This command is used download such files to the switch.

If you do not specify *filename* in the command, the downloaded file will have the same name as the file on the TFTP server.

Before running this command, ensure that the switch can communicate with the TFTP server, and the user name and password have been configured on the TFTP server.



Caution

It is recommended that you use this command under instruction of technical support personnel.

Example

Download the file **Switch_OS.bin** from the server **TFTP6 2001::1** to a local device and rename the file as **v1.1.bin**.

```
Switch(config)#tftp6 get 2001::1 Switch_OS.bin localfile v1.1.bin
Getting File " Switch_OS_v3.00M_build20110727-2.bin " from 2001::1...
1528618 bytes downloaded.
If you want to upgrade system,use "upgrade" command!
```

```
Switch(config)#
```

2.5.16 tftp6 put

Function

The **tftp6 put** command uploads a local file to a remote TFTP server. (This command applies to IPv6 networks.)

Format

- **tftp6 put** *ipv6-address remotefile config*
- **tftp6 put** *ipv6-address remotefile localfile filename* [*port-id*]
- **tftp6 put** *ipv6-address remotefile running-config*
- **tftp6 put** *ipv6-address vpn-instance name remotefile config*
- **tftp6 put** *ipv6-address vpn-instance name remotefile localfile filename*

Parameter

Parameter	Description	Value
ipv6-address	Specifies a host IPv4 address.	In this format, a 128-digit IP address is divided into 8 segments. Each segment consists of 16 digits and is represented by 4 hexadecimal characters (0-9 and A-F). Segments are separated by colons (:). Every "X" represents a group of hexadecimal digits.
remotefile	Specifies the name of the file to be uploaded from the host to the server.	The value is a character string consisting of 1 to 63 characters.
filename	Specifies the name of the local file to be uploaded.	The value is a character string consisting of 1 to 63 characters.
[port-id]	Specifies the port number, which is optional.	The value is an integer ranging from 1 to 65535.
config	Uploads the configuration file of the switch.	-
name	Specifies a VPN instance name.	The value is a character string.

Default Value

NA

View

Global configuration view

Usage Guidelines

During device operation and maintenance, you can use this command to upload files of the switch (including the configuration file) to a remote TFTP server for backup.

Before running this command, ensure that the switch can communicate with the TFTP server, and the user name and password have been configured on the TFTP server. In addition, the user account must have the read and write permissions on the TFTP server. Otherwise, the host will not respond for a long time or the upload task will be suspended.



Caution

It is recommended that you use this command under instruction of technical support personnel.

Example

Upload the configuration file of the switch to the TFTP server, and save the file as **config.ini** on the server.

```
Switch(config)#ftp6 put 2001::1 d:/config.ini config
1136 bytes uploaded
Switch(config)#
```

2.5.17 debug ftpd6

Function

The **debug ftpd6** command enables debugging of the FTP server on the switch. (This command applies to IPv6 networks.)

The **no debug ftpd6** command disables this debugging function.

Format

- **debug ftpd6**
- **no debug ftpd6**

Parameter

NA

Default Value

By default, debugging of the FTP server is disabled.

View

Privileged user view

Usage Guidelines

If the switch acts as an FTP server and experiences a failure or problem, you can use this command to enable FTP server debugging. This function helps to locate the problem.

Example

Enable debugging of the FTP server on the switch.

```
Switch#debug ftpd6
Switch#
```

Disable debugging of the FTP server.

```
Switch#no debug ftpd6
Switch#
```

2.5.18 ftpd6

Function

The **ftpd6** command enables FTP Server for the switch. (This command applies to IPv6 networks.)

The **no ftpd6** command disables FTP Server for the switch.

Format

- **ftpd6**
- **no ftpd6**

Parameter

NA

Default Value

By default, the FTP server function is disabled.

View

Global configuration view

Usage Guidelines

After the FTP server function is enabled on the switch, the switch acts as an FTP server. You can log in to the switch using an FTP client and upload files to or download files from the switch. The FTP server uses the local user name and password for login authentication.

Example

Enable the FTP server function on the switch.

```
Switch(config)#ftpd6
Switch(config)#
```

2.5.19 file export tftp**Function**

The **file export tftp** command enables one-click export of files based on the TFTP protocol.

Format

file export tftp *ipv4-address remotedir localdir*

Parameter

Parameter	Description	Value
ipv4-address	Specifies the IP address of the TFTP server.	The value is in dotted decimal notation, such as A.B.C.D, where each of A to D is a decimal number ranging from 0 to 255.
remotedir	Specifies the relative path on the host (the file must exist).	-
localdir	Specifies the local folder path.	-

Default Value

NA

View

Global configuration view

Usage Guidelines

NA

Example

Use TFTP to export files in one click.

```
Switch(config)#file export tftp 172.17.1.177 /1 log
Putting data...
3165 bytes uploaded  $Transmission success.
Putting data...
692 bytes uploaded  %Transmission success.
```


2.6 Telnet and SSH Configuration Commands

2.6.1 debug ssh

Function

The **debug ssh** command enables SSH debugging.

The **no debug ssh** command disables SSH debugging.

Format

- **debug ssh**
- **no debug ssh**

Parameter

NA

Default Value

By default, SSH debugging is disabled.

View

Privileged user view

Usage Guidelines

NA

Example

Enable SSH debugging.

```
Switch#debug ssh
Switch#
```

2.6.2 debug sftp

Function

The **debug sftp** command enables SSH file transmission protocol debugging.

The **no debug sftp** command disables SSH file transmission protocol debugging.

Format

- **debug sftp**
- **no debug sftp**

Parameter

NA

Default Value

NA

View

Privileged user view

Usage Guidelines

NA

Example

Enable SSH file transmission protocol debugging.

Switch#debug sftp

Switch#

2.6.3 key**Function**The **key** command configures the key string.**Format**

- **key** { **ssh-dss** | **ssh-rsa** } *key-string*
- **key** *key-string*

Parameter

Parameter	Description	Value
key-string	Specifies the key string.	The value is a character string.

Default Value

NA

View

Global configuration view

Usage Guidelines

NA

Example

Configure the key string.

```
Switch(config)#key dabiadalieng
Switch(config)
```

2.6.4 sshd**Function**

The **sshd** command enables the SSH function on the switch.

The **no sshd** command cancels the configuration.

Format

- **sshd**
- **no sshd**

Parameter

NA

Default Value

By default, the SSH function is disabled.

View

Global configuration view

Usage Guidelines

After the switch is powered on for the time, you must log in to the switch through the console interface, enable the SSH function, and complete related SSH configuration, so that users can log in to the switch using SSH later. Generally, SSH login is used when there are relatively high security requirements for user login.

Example

Enable the SSH function on the switch.

```
Switch(config)#sshd
Switch(config)#
```

2.6.5 sshd auth**Function**

The **sshd auth** command configures the SSHD authentication mode, including password authentication and public key authentication.

Format

- **sshd auth { password | pubkey }**
- **no sshd auth { password | pubkey }**

Parameter

NA

Default Value

By default, the system supports both password authentication and public key authentication.

View

Global configuration view

Usage Guidelines

This command sets the SSH authentication mode. Password authentication and public key authentication can coexist. Configuring public authentication will not disable password authentication, and configuring password authentication will not disable public key authentication.

Example

Set the SSHD authentication mode to password authentication.

```
Switch(config)#sshd auth password
Switch(config)#
```

2.6.6 ssh keygen

Function

The **ssh keygen** command creates an SSH public key.

Format

- **ssh keygen dsa**
- **ssh keygen rsa bits { 1024 | 2048 | 3072 }**

Parameter

NA

Default Value

NA

View

Global configuration view

Usage Guidelines

Most of servers support Digital Signature Algorithm (DSA) keys, whereas most of servers may not support Rivest-Shamir-Adleman (RSA) keys.

Shorter keys provide lower security but take less time in key generation and verification. Longer keys provide higher security but take more than in key generation and verification. The recommended key length is 1024.

Example

Create an SSH public key and set the key length to 1024.

```
Switch(config)#ssh keygen rsa bits 1024
Generating public/private DSA key pair.
Enter passphrase (empty for no passphrase): *****
Enter same passphrase again: *****
Your identification has been saved in Ram:/flash/id_dsa_512.
Your public key has been saved in Ram:/flash/id_dsa_512.
The key fingerprint is:
e4:2e:c0:de:5c:a4:7a:39:76:06:aa:59:f0:84:0f:60 admin@fengine

Switch(config)#
```

2.6.7 ssh user key begin**Function**

The **ssh user key begin** command configures the SSH user key.

Format

ssh user *user-name* **key begin**

Parameter

Parameter	Description	Value
user-name	Specifies an SSH user name.	The value is a character string.

Default Value

NA

View

Global configuration view

Usage Guidelines

NA

Example

Configure the SSH user key.

```
Switch(config)#ssh user user1 key begin
Switch(config)
```

2.6.8 sftp-server {enable|disable}**Function**

The **sftp-server {enable|disable}** command enables or disables the SSH file transmission protocol service.

Format

sftp-server { enable | disable }

Parameter

Parameter	Description	Value
enable	Enables the SSH file transmission protocol service.	-
disable	Disables the SSH file transmission protocol service.	-

Default Value

Disable

View

Global configuration view

Usage Guidelines

NA

Example

Enables the SSH file transmission protocol service.

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

2.6.9 sshd login-grace-time

Function

The **sshd login-grace-time** command configures the SSHD login grace time.

Format

sshd login-grace-time { *login-grace-timer* | **default** }

Parameter

Parameter	Description	Value
login-grace-time	Specifies the valid time range.	The value is an integer ranging from 60 to 600, in seconds.
default	Specifies the default valid time range.	The value is 300 seconds.

Default Value

300

View

Global configuration view

Usage Guidelines

After you connect to the switch through SSH, the system displays the validity period to enter the user name and password. If you do not enter the user name and password within this period, the login authentication fails.

Example

Set the SSHd login grace time to 400 seconds.

```
Switch(config)#sshd login-grace-time 400
Switch(config)#
```

2.6.10 telnet crlf

Function

The **telnet crlf** command sends the CR and LF remote connection mode.

The **no telnet crlf** command deletes this configuration mode.

Format

- **telnet crlf**
- **no telnet crlf**

Parameter

NA

Default Value

NA

View

Global configuration view

Usage Guidelines

NA

Example

Configure to send the CR and LF remote connection mode.

```
Switch(config)#telnet crlf
```

```
Switch(config)#
```

2.6.11 telnetd**Function**

The **telnetd** command enables the IPv4 Telnet server function for the switch.

The **no telnetd** command disables the IPv4 Telnet server function for the switch.

Format

- **telnetd**
- **no telnetd**

Parameter

NA

Default Value

The IPv4 Telnet server function is enabled.

View

Global configuration view

Usage Guidelines

After the IPv4 Telnet server function is enabled for the switch, you can configure and manage the switch remotely. To ensure switch security, set the IPv4 address to the Telnet server ACL to ensure authorized switch configuration and management and protect the Telnet server of the IPv4 address from remote attack.

Example

Disable the IPv4 Telnet server function for the switch.

```
Switch(config)#no telnetd
Switch(config)#
```

2.6.12 telnet6d

Function

The **telnet6d** command enables the IPv6 Telnet server function for the switch.

The **no telnet6d** command disables the IPv6 Telnet server function for the switch.

Format

- **telnet6d**
- **no telnet6d**

Parameter

NA

Default Value

The IPv6 Telnet server function is enabled.

View

Global configuration view

Usage Guidelines

After the IPv6 Telnet server function is enabled for the switch, you can configure and manage the switch remotely. To ensure switch security, set the IPv6 address to the Telnet server ACL to ensure authorized switch configuration and management and protect the Telnet server of the IPv6 address from remote attack.

Example

Disable the IPv6 Telnet server function for the switch.

```
Switch(config)#no telnet6d
```

```
Switch(config)#
```

2.6.13 telnet|telnet6

Function

The **telnet|telnet6** command enables you to log in to a remote device.

Format

- **telnet** *ipv4-address* [*port-id*]
- **telnet** *ipv4-address* -s *src-ipv4-address* [*port-id*]
- **telnet** *ipv4-address* **vpn-instance** *name* [*port-id*]
- **telnet** *ipv4-address* **vpn-instance** *name* -s *src-ipv4-address* [*port-id*]
- **telnet** *mac-address* [*port-id*]
- **telnet6** *ipv6-address* [*port-id*]
- **telnet6** *ipv6-address* -s *src-ipv6-address* [*port-id*]
- **telnet6** *ipv6-address* **vpn-instance** *name* [*port-id*]
- **telnet6** *ipv6-address* **vpn-instance** *name* -s *src-ipv6-address* [*port-id*]

Parameter

Parameter	Description	Value
ipv4-address	Specifies the IPv4 address of the device you want to log in.	The value is in dotted decimal notation.
ipv6-address	Specifies the IPv6 address of the device you want to log in.	In this format, a 128-digit IP address is divided into 8 segments. Each segment consists of 16 digits and is represented by 4 hexadecimal characters (0-9 and A-F). Segments are separated by colons (:). Every "X" represents a group of hexadecimal digits.
src-ipv4-address	Specifies a source IPv4 address.	The value is in dotted decimal notation.
src-ipv6-address	Specifies a source IPv6 address.	In this format, a 128-digit IP address is divided into 8 segments. Each segment consists of 16 digits and is represented by 4 hexadecimal characters (0-9 and A-F). Segments are separated by colons (:). Every "X" represents a group of hexadecimal digits.
port-id	Specifies a Telnet port number. This parameter is optional.	The value is an integer ranging from 1 to 65535.

Parameter	Description	Value
name	Specifies a VPN instance name.	The value is a character string.

Default Value

NA

View

Privileged user view

Usage Guidelines

NA

Example

Remotely log in to the switch with IP address 10.18.14.249.

```
Switch#telnet 10.18.16.249
Login authentication
Username:
Switch#
```

2.6.14 show ssh config**Function**The **show ssh config** command displays the SSH configuration on the switch.**Format****show ssh config****Parameter**

NA

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

Display the SSH configuration.

```
Switch>show ssh config
sshd
Switch(config)#
```

Chapter 3 Ethernet Commands

This chapter introduces commands for configuring the following functions: Ethernet interface, MAC table, ARP, link aggregation, VLAN, VLAN mapping, VLAN STACKING, QinQ, ARP agent, MAM, port security, port isolation, and storm control.

3.1 Interface Configuration Commands

3.1.1 switch

Function

The **switch** command switches between Ethernet interfaces and accesses the interface configuration node.

Format

switch { **ethernet** | **xgigaehternet** | **10gigaehternet** | **25gigaehternet** | **40gigaehternet** | **100gigaehternet** } *interface-number*

Parameter

Parameter	Description	Value
interface-number	Specifies an Ethernet interface number.	The value is an integer in the range of <1-1>/<0-1>/<1-48>.

Default Value

NA

View

Ethernet bridge interface configuration view, Ethernet routing interface configuration view

Usage Guidelines

NA

Example

Access **gigaehternet1/0/12** from the interface **gigaehternet1/0/1**.

```
Switch(config-10ge1/0/1)#switch gigaehternet 1/0/12
Switch(config-10ge1/0/12)#
```

3.1.2 debug {rx|tx|rxpkt|txpkt|config|event|stats|none}

Function

The **debug {rx|tx|rxpkt|txpkt|config|event|stats|none}** command configures the interface debugging function.

Format

debug { rx | tx | rxpkt | txpkt | config | event | stats | none }

Parameter

NA

Default Value

NA

View

Interface configuration view (Ethernt/Trunk), VLANIF configuration view, Peerlink configuration view

Usage Guidelines

NA

Example

Configure the interface debugging function.

```
Switch(config)#interface xgigaethernet 1/0/1
Switch(config-10ge1/0/1)#debug rx
Switch(config-10ge1/0/1)#
```

3.1.3 debug ifm

Function

The **debug ifm** command enables the interface management debugging function.

The **no debug ifm** command disables the interface management debugging function.

Format

- **debug ifm { rx | tx | load | ioctl | rx-pkt | tx-pkt | event | error | stats | cmd | all }**
- **debug ifm { rx | tx | load | ioctl | rx-pkt | tx-pkt | event | error | stats | cmd | all } { ethernet | xgigaethernet | 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet } interface-number**

- **debug ifm { rx | tx | load | ioctl | rx-pkt | tx-pkt | event | error | stats | cmd | all } eth-trunk *trunk-number***
- **debug ifm { rx | tx | load | ioctl | rx-pkt | tx-pkt | event | error | stats | cmd | all } vlan *vlan-id***
- **debug ifm { rx | tx | load | ioctl | rx-pkt | tx-pkt | event | error | stats | cmd | all } stack port *stack-port number***
- **no debug ifm { rx | tx | load | ioctl | rx-pkt | tx-pkt | event | error | stats | cmd | all }**
- **no debug ifm { rx | tx | load | ioctl | rx-pkt | tx-pkt | event | error | stats | cmd | all } { ethernet | xgigaethernet | 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet } *interface-number***
- **no debug ifm { rx | tx | load | ioctl | rx-pkt | tx-pkt | event | error | stats | cmd | all } eth-trunk *trunk-number***
- **no debug ifm { rx | tx | load | ioctl | rx-pkt | tx-pkt | event | error | stats | cmd | all } vlan *vlan-id***

Parameter

Parameter	Description	Value
interface-number	Specifies an Ethernet interface number.	The value is an integer in the range of <1-1>/<0-1>/<1-48>
trunk-number	Specifies the number of a Trunk interface.	The value is an integer ranging from 1 to 128.
vlan-id	Specifies a VLAN ID.	The value is an integer ranging from 1 to 4094.
stack-port number	Specifies a stack port ID.	The value is an integer ranging from 1 to 2.

Default Value

Disable

View

Privileged user view

Usage Guidelines

NA

Example

Enable the interface management debugging function.

```
Switch#debug ifm all
Switch#
```

3.1.4 alias

Function

The **alias** command sets an alias (description) for an interface.

The **no alias** command cancels the alias configuration of an interface.

Format

- **alias** *alias-name*
- **no alias**

Parameter

Parameter	Description	Value
alias-name	Specifies the alias of an interface.	The value is a string of 1 to 64 characters without spaces.

Default Value

NA

View

Out-of-band interface configuration view, Loopback interface configuration view, Tunnel interface configuration view, BD interface configuration view, NVE interface configuration view, Ethernet bridge interface configuration view, Ethernet routing interface configuration view, Trunk interface configuration view, Ethernet stack interface configuration view, interface configuration view (Trunk), VLANIF configuration view, and Peerlink configuration view

Usage Guidelines

NA

Example

Set an alias for an interface.

```
Switch(config)#interface xgigaethernet 1/0/1
Switch(config-10ge1/0/1)#alias wuhan
Switch(config-10ge1/0/1)#quit
Switch>show interface xgigaethernet 1/0/1
Interface xgigaethernet-1/0/1
  Alias:wuhan
  Admin state is up,operation state is down
  Negotiation auto enable
  flow-control negotiation disable
```



```
Duplex is half
Speed is 1000M(bps)
Mtu is 1522
...
```

3.1.5 shutdown

Function

The **shutdown** command shuts down the current Ethernet interface.

The **no shutdown** command starts the current Ethernet interface.

Format

- **shutdown**
- **no shutdown**

Parameter

NA

Default Value

By default, an Ethernet interface is in working state.

View

Out-of-band interface configuration view, Tunnel interface configuration view, BD interface configuration view, NVE interface configuration view, Ethernet bridge interface configuration view, Ethernet routing interface configuration view, Trunk interface configuration view, Ethernet stack interface configuration view, interface configuration view (Trunk), and Peerlink configuration view

Usage Guidelines

If you modify the attributes of an interface but the new configuration does not take effect immediately, run the **shutdown** and **no shutdown** commands to shut down and then start the interface. The new configuration can then take effect.

If an interface is idle (with no cable connected), run the **shutdown** command to shut down the interface. This prevents exceptions caused by interference.

If you run the **shutdown** command in the trunk interface view, all member interfaces of the trunk interface are shut down.

**Caution**

An interface must be started before configuration can be performed on it.

If an interface is shut down during data transmission, data will be lost. Exercise caution when using this command.

Example

Shut down Ethernet interface xgigaethernet 1/0/1.

```
Switch(config-10ge1/0/1)#shutdown
Switch(config-10ge1/0/1)#
```

3.1.6 reset counter**Function**

The **reset counter** command resets packet counters on an interface.

Format

reset counter

Parameter

NA

Default Value

NA

View

Out-of-band interface configuration view, Loopback interface configuration view, Tunnel interface configuration view, Trunk sub-interface configuration view, BD interface configuration view, NVE interface configuration view, GRP bridge interface configuration view, GRP routing interface configuration view, Ethernet sub-interface configuration view, Ethernet bridge interface configuration view, Ethernet routing interface configuration view, routing interface configuration view, Trunk interface configuration view, Ethernet stack interface configuration view, interface configuration view (Trunk), and stack interface configuration view

Usage Guidelines

NA

Example

Reset packet counters on interface xgigaethernet 1/0/1.

```
Switch(config-10ge1/0/1)#reset counter
Switch(config-10ge1/0/1)#
```

3.1.7 interface loopback

Function

The **interface loopback** command enters the loopback interface view.

The **no interface loopback** command deletes a loopback interface view.

Format

- **interface loopback** *loopback-number*
- **no interface loopback** *loopback-number*

Parameter

Parameter	Description	Value
loopback-number	Specifies a loopback interface number.	The value is an integer ranging from 1 to 127.

Default Value

NA

View

Global configuration view

Usage Guidelines

NA

Example

Enter the loopback1 configuration view.

```
Switch(config)#interface loopback 1
Switch(config-loopback-1)#
```

3.1.8 interface null

Function

The **interface null** command enters the NULL interface view.

Format

interface null *null-number*

Parameter

Parameter	Description	Value
null-number	Specifies a NULL interface number.	The value is 0.

Default Value

NA

View

Global configuration view

Usage Guidelines

NA

Example

Enter the null1 interface view.

```
Switch(config)#interface null 0
Switch(config-null-0)#
```

3.1.9 show interface null config**Function**The **show interface null config** command displays the NULL interface configuration.**Format****show interface null *null-number* config****Parameter**

Parameter	Description	Value
null-number	Specifies a NULL interface ID.	The value is an integer ranging from 0 to 0.

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

Display the NULL interface configuration. 1

```
Switch> show interface null 0 config
!
interface null 0
Switch>
```

3.1.10 error-down auto-recovery cause link-flap interval

Function

The **error-down auto-recovery cause link-flap interval** command enables automatically restoring a port going **down** due to link flapping to **up** state and sets a delay for such automatic restoration.

The **no error-down auto-recovery cause link-flap interval** command disables the above function.

Format

- **error-down auto-recovery cause link-flap interval** *interval*
- **no error-down auto-recovery cause link-flap**

Parameter

Parameter	Description	Value
interval	Specifies a delay for automatically restoring a port to up state.	The value is an integer ranging from 30 to 86400, in seconds. A smaller value indicates a shorter delay and more frequent port Up/Down oscillation. A larger value indicates a longer delay and longer port traffic interruption.

Default Value

Enables the synchronization function.

View

Global configuration view

Usage Guidelines

NA

Example

Enable automatically restoring a port going **down** due to link flapping to **up** state and set a delay for such automatic restoration to 50s.

```
Switch(config)#error-down auto-recovery cause link-flap interval 50
Switch(config)#
```

3.1.11 port link-flap interval

Function

The **port link-flap interval** command configures the link flapping interval for a port.

Format

port link-flap interval { *interval-value* | **default** }

Parameter

Parameter	Description	Value
interval-value	Specifies the link flapping interval for a port.	The value is an integer ranging from 5 to 60, in seconds.
default	Specifies the default link flapping interval for a port.	10 seconds

Default Value

10 seconds

View

Ethernet bridge interface configuration view, Trunk interface configuration view

Usage Guidelines

If a physical port on a local device changes between **Up** and **Down** frequently due to network jitter or link fault, its link flaps and the network topology changes frequently, affecting the user communication. If the link flapping count reaches the threshold within the link flapping interval, the port is closed.

Before running this command, run **port link-flap protection enable** to enable link flapping protection on a port.

Example

Set the link flapping interval to 10s.

```
Switch(config-10ge1/0/1)#port link-flap interval 10
Switch(config-10ge1/0/1)#
```

3.1.12 crc-error protection interval

Function

The **crc-error protection interval** command configures the alarm interval for CRC error packets.

The **no crc-error protection interval** command deletes the alarm interval for CRC error packets.

Format

- **crc-error protection interval** *interval*
- **no crc-error protection interval**

Parameter

Parameter	Description	Value
interval	Specifies the alarm interval for CRC error packets.	The value is an integer ranging from 10 to 65535, in seconds.

Default Value

By default, CRC error packet alarm is disabled.

View

Global configuration view

Usage Guidelines

This command is valid for all ports and should be used together with the CRC error packet threshold configured for ports.

Example

Configure the alarm interval for CRC error packets to 30s.

```
Switch(config)#crc-error protection interval 30
Switch(config)#
```

3.1.13 port crc-error threshold**Function**

The **port crc-error threshold** command configures the CRC error packet alarm threshold of a port.

The **no port crc-error threshold** command deletes the CRC error packet alarm threshold of a port.

Format

- **port crc-error threshold** *threshold*
- **no port crc-error threshold**

Parameter

Parameter	Description	Value

threshold	Specifies a CRC error packet alarm threshold.	The value is an integer ranging from 1 to 65535.

Default Value

By default, CRC error packet alarm is disabled for ports.

View

Ethernet bridge interface configuration view, Ethernet routing interface configuration view, GRP bridge interface configuration view, and GRP routing interface configuration view

Usage Guidelines

An alarm is triggered when the number of CRC error packets received by a port within the global **crc-error detection time** specified by the **crc-error protection interval** command exceeds the threshold.

Example

Configure the CRC error packet alarm threshold of a port to 10.

```
Switch(config-ge1/0/1)#port crc-error threshold 10
Switch(config-ge1/0/1)#
```

3.1.14 port crc-error error-down {enable|disable}

Function

The **port crc-error error-down {enable | disable}** command enables a port to enter error down state when the number of received CRC error packets exceeds the threshold, or disables a port from going down in this case.

Format

port crc-error error-down { enable | disable }

Parameter

NA

Default Value

By default, this function is not enabled.

View

Ethernet bridge interface configuration view, Ethernet routing interface configuration view, GRP bridge interface configuration view, and GRP routing interface configuration view

Usage Guidelines

When the number of CRC error packets received by a port in the unit time exceeds the threshold and the error down function is enabled, the port enters error down state automatically. You can run the **error-down auto-recovery cause crc-error interval** command to configure the automatic recovery interval in the global configuration view.

Example

Enable a port to enter error down state when the number of received CRC error packets exceeds the threshold.

```
Switch(config-10ge1/0/1)#port crc-error error-down enable
Switch(config-10ge1/0/1)#
```

3.1.15 error-down auto-recovery cause crc-error interval

Function

The **error-down auto-recovery cause crc-error interval** command configures the automatic recovery interval for ports going down when the number of CRC error packets exceeds the threshold.

The **no error-down auto-recovery cause crc-error** command disables a port in error down state from going up automatically..

Format

- **error-down auto-recovery cause crc-error interval** *interval*
- **no error-down auto-recovery cause crc-error**

Parameter

Parameter	Description	Value
interval	Specifies the automatic recovery interval.	The value is an integer ranging from 30 to 86400, in seconds.

Default Value

Ports are not automatically recovered by default.

View

Global configuration view

Usage Guidelines

This global command is valid only for ports going down due to CRC errors after auto-recovery is configured. It is invalid for ports going down before auto-recovery is configured. It must be used together with the **port crc-error error-down enable** command.

Example

Configure the recovery interval to 30s for ports going down when the number of CRC error packets exceeds the threshold.

```
Switch(config)#error-down auto-recovery cause crc-error interval 30
Switch(config)#
```

3.1.16 error-down auto-recovery cause port-security interval

Function

The **error-down auto-recovery cause port-security interval** command configures a delay for automatically restoring a port from **down** to **link up**. It applies to ports going down when the number of learned security MAC addresses exceeds the upper limit.

The **no error-down auto-recovery cause port-security** command disables this automatic recovery.

Format

- **error-down auto-recovery cause port-security interval** *interval*
- **no error-down auto-recovery cause port-security**

Parameter

Parameter	Description	Value
interval	Specifies a delay for automatically restoring a port to up state.	The value is an integer ranging from 30 to 86400, in seconds. A smaller value indicates a shorter delay and more frequent port Up/Down oscillation. A larger value indicates a longer delay and longer port traffic interruption.

Default Value

NA

View

Global configuration view

Usage Guidelines

NA

Example

Run this command to set the delay to 50s for automatically recovering a port from **down** to **link up** state.

```
Switch(config)#error-down auto-recovery cause port-security interval 50
Switch(config)#
```

3.1.17 error-down auto-recovery cause storm-suppression interval

Function

The **error-down auto-recovery cause storm-suppression interval** command configures a delay for automatically restoring a port going down due to storm suppression to **link up**.

The **no error-down auto-recovery cause storm-suppression** command disables this automatic recovery.

Format

- **error-down auto-recovery cause storm-suppression interval** *interval*
- **no error-down auto-recovery cause storm-suppression**

Parameter

Description	Description	Value
interval	Specifies a delay for automatically restoring a port to up state.	The value is an integer ranging from 30 to 86400, in seconds. A smaller value indicates a shorter delay and more frequent port Up/Down oscillation. A larger value indicates a longer delay and longer port traffic interruption.

Default Value

NA

View

Global configuration view

Usage Guidelines

When the storm suppression action of a port is set to **error-down** on the switch, if the average receiving rate of the broadcast, multicast, and unknown unicast packets of the port exceeds the upper limit, the port is shut down.

Example

Set the time for automatically restoring a port to **link up** state to 50s after the port is shut down due to storm suppression.

```
Switch(config)#error-down auto-recovery cause storm-suppression interval 50
Switch(config)#
```

3.1.18 port link-flap protection {enable|disable}

Function

The **port link-flap protection {enable|disable}** command enables or disables link flapping protection on a port.

Format

port link-flap protection { enable | disable }

Parameter

Parameter	Description	Value
enable	Enables link flapping protection on a port.	-
disable	Disables link flapping protection on a port.	-

Default Value

Disable

View

Ethernet bridge interface configuration view, Trunk interface configuration view

Usage Guidelines

Run this command to enable link flapping protection on a port before configuring other port link flapping commands.

Example

Enable link flapping protection on a port.

```
Switch(config-10ge1/0/1)#port link-flap protection enable
Switch(config-10ge1/0/1)#
```

3.1.19 port link-flap threshold

Function

The **port link-flap threshold** command configures the link flapping times for a port.

Format

port link-flap threshold { threshold-value | default }

Parameter

Parameter	Description	Value
threshold-value	Specifies the link flapping times for a port.	The value is an integer ranging from 5 to 10.
default	Specifies the default link flapping times for a port.	5

Default Value

5

View

Ethernet bridge interface configuration view, Trunk interface configuration view

Usage Guidelines

One link flapping means one **Up/Down** switchover.

Before running this command, run **port link-flap protection {enable|disable}** to enable link flapping protection on a port.

Example

Set the link flapping times to 10.

```
Switch(config-10ge1/0/1)#port link-flap threshold 10
Switch(config-10ge1/0/1)#
```

3.1.20 flow-stat interval**Function**

The **flow-stat interval** command configures count interval of global traffic.

Format

flow-stat interval { *interval* | **default** }

Parameter

Parameter	Description	Value
interval	Specifies the count interval of global traffic.	The value is an integer ranging from 30 to 300.
default	Specifies the default count interval of global traffic.	300

Default Value

NA

View

Global configuration view

Usage Guidelines

NA

Example

Set the count interval of global traffic to the default value.

```
Switch(config)#flow-stat interval default
Switch(config)#
```

3.1.21 show linkflap config**Function**

The **show linkflap config** command displays the link flapping configuration.

Format

show linkflap config

Parameter

NA

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

View the link flapping configuration.

```
Switch>show linkflap config
ge-1/0/1
port link-flap protection enable
port link-flap interval 50
Switch>
```

3.1.22 port flow-stat interval

Function

The **port flow-stat interval** command configures the traffic count interval for a port.

Format

port flow-stat interval { *interval* | **default** }

Parameter

Parameter	Description	Value
interval	Specifies the traffic count interval for a port.	The value is an integer ranging from 30 to 300, in seconds.
default	Specifies the default interval.	0s

Default Value

0

View

Ethernet bridge interface configuration view, Ethernet routing interface configuration view, interface configuration view (Trunk)

Usage Guidelines

NA

Example

Set the traffic count interval to 80s.

```
Switch(config-10ge1/0/1)#port flow-stat interval 80
Switch(config-10ge1/0/1)#
```

3.1.23 debug linkflap

Function

The **debug linkflap** command enables the link flapping debugging function for a port.

The **no debug linkflap** command disables the link flapping debugging function for a port.

Format

- **debug linkflap**
- **no debug linkflap**

Parameter

NA

Default Value

NA

View

Privileged user view

Usage Guidelines

NA

Example

Enable the link flapping debugging function for a port.

```
Switch#debug linkflap
Switch#
```

3.1.24 error-down auto-recovery cause mac-address-flapping interval**Function**

The **error-down auto-recovery cause mac-address-flapping interval** command enables automatically restoring a port going **down** due to MAC address flapping to up state and sets a delay for such automatic restoration.

The **no error-down auto-recovery cause mac-address-flapping** command disables this operation.

Format

- **error-down auto-recovery cause mac-address-flapping interval** *interval*
- **no error-down auto-recovery cause mac-address-flapping**

Parameter

Parameter	Description	Value
interval	Specifies a delay for automatically restoring a port to up state.	The value is an integer ranging from 30 to 86400, in seconds. A smaller value indicates a shorter delay and more frequent port Up/Down oscillation. A larger value indicates a longer delay and longer port traffic interruption.

Default Value

NA

View

Global configuration view

Usage Guidelines

NA

Example

Enable automatically restoring a port going **down** due to link flapping of the MAC address to **up** state and set a delay for such automatic restoration to 50s.

```
Switch(config)#error-down auto-recovery cause mac-address-flapping interval 50
Switch(config)#
```

3.1.25 flow-control**Function**

The **flow-control** command enables or disables the flow control function on a port.

Format

- **flow-control { enable | disable }**
- **flow-control negotiation { enable | disable }**

Parameter

Parameter	Description	Value
enable	Enables the traffic control function for a port.	-
disable	Disables the traffic control function for a port.	-

Default Value

By default, the flow control function is disabled on an Ethernet interface.

View

Ethernet bridge interface configuration view, Ethernet routing interface configuration view

Usage Guidelines

After the flow control function is enabled on an interface, this function takes effect in the following way if the rate of received traffic reaches the upper limit:

The local interface sends a special data frame to inform the remote device that the traffic rate has reached the upper limit of the local data processing capability.

After the remote device receives the data frame, it reduces the packet transmission rate to ensure that the local device can process the received packets normally.

This function prevents packet loss and ensures normal network operation.



Caution

Interfaces at both ends must have the flow control function enabled to ensure effective flow control.

Example

Enable the flow control function on Ethernet interface xgigaethernet 1/0/1.

```
Switch(config-10ge1/0/1)#flow-control enable
Switch(config-10ge1/0/1)#
```

3.1.26 flow-statistic include-interframe

Function

The **flow-statistic include-interframe** command enables or disables interframe traffic measurement.

Format

flow-statistic include-interframe { enable | disable }

Parameter

Parameter	Description	Value
enable	Enables the interframe gap.	-
disable	Disables the interframe gap.	-

Default Value

By default, interframe gap is not included in traffic measurement on an Ethernet interface.

View

Ethernet bridge interface configuration view, Ethernet routing interface configuration view

Usage Guidelines

NA

Example

Enable interframe traffic measurement on Ethernet interface xgigaethernet 1/0/1.

```
Switch(config-10ge1/0/1)#flow-statistic include-interframe enable
Switch(config-10ge1/0/1)#
```

3.1.27 interface mgt-eth

Function

The **interface mgt-eth** command enters the out-of-band interface configuration view.

Format

interface mgt-eth *eth-number*

Parameter

Parameter	Description	Value
eth-number	Specifies the number of an out-of-band interface.	The value is an integer in the range of <0-0>/<0-0>/<0-0>.

Default Value

NA

View

Global configuration view

Usage Guidelines

NA

Example

Configure **mgt-eth 0/0/0**.

```
Switch(config)#interface mgt-eth 0/0/0
Switch(config-mgt-eth-0/0/0)#
```

3.1.28 mtu

Function

The **mtu** command configures the MTU for an IPv4 port.

Format

mtu { *mtu-value* | **default** }

Parameter

Description	Description	Value

Description	Description	Value
mtu-value	Specifies an MTU size.	The value is an integer ranging from 128 to 9216. The default value is 1500 bytes.

Default Value

NA

View

VLANIF configuration view, out-of-band interface configuration view, Loopback interface configuration view, Tunnel interface configuration view, BD interface configuration view, Ethernet routing interface configuration view

Usage Guidelines

NA

Example

Set the MTU value to 1400.

```
Switch(config-vlanif-2)#mtu 1400
Switch(config-vlanif-2)#
```

3.1.29 port-down holdoff-time

Function

The **port-down holdoff-timer** command sets a delay before reporting a port down event.

Format

- **port-down holdoff-time** { *time-value* | **default** }
- **no port-down holdoff-time**

Parameter

Parameter	Description	Value
time-value	Specifies a delay before reporting a port down event.	The value is an integer ranging from 0 to 600000. The unit is milliseconds.
default	Specifies the default value.	0

Default Value

The default delay is 0 ms, which means reporting a port down event immediately.

View

Ethernet bridge interface configuration view, Ethernet routing interface configuration view

Usage Guidelines

When a device connected to the Switch is switched, the Switch port goes down. In this case, we need to set a delay before reporting a port down event to prevent service interruption.

Example

Set a delay before reporting a port down event to 150 ms.

```
Switch(config-10ge1/0/1)#port-down holdoff-timer 150
Switch(config-10ge1/0/1)#
```

3.1.30 port-up delay-time**Function**

The **port-up delay-time** command configures the delay for restoring port connection.

The **no port-up delay-time** command deletes this configuration.

Format

- **port-up delay-time** { *time* | **default** }
- **no port-up delay-time**

Parameter

Parameter	Description	Value
time	Specifies the delay for port link recovery.	The value is an integer ranging from 0 to 600000, in milliseconds.
default	Indicates the default value.	0

Default Value

NA

View

Ethernet bridge interface configuration view, Ethernet routing interface configuration view

Usage Guidelines

NA

Example

Configure the delay for port link recovery to 10 ms.

```
Switch(config-10ge1/0/1)#port-up delay-time 10
Switch(config-10ge1/0/1)#
```

3.1.31 shutdown

Function

The **shutdown** command shuts down the current Ethernet interface.

The **no shutdown** command starts the current Ethernet interface.

Format

- **shutdown**
- **no shutdown**

Parameter

NA

Default Value

By default, an Ethernet interface is in working state.

View

VLANIF configuration view, Ethernet bridge interface configuration view, Ethernet routing interface configuration view, out-of-band interface configuration view, Loopback interface configuration view, Tunnel interface configuration view, BD interface configuration view

Usage Guidelines

If you modify the attributes of an interface but the new configuration does not take effect immediately, run the **shutdown** and **no shutdown** commands to shut down and then start the interface. The new configuration can then take effect.

If an interface is idle (with no cable connected), run the **shutdown** command to shut down the interface. This prevents exceptions caused by interference.

If you run the **shutdown** command in the trunk interface view, all member interfaces of the trunk interface are shut down.

**Caution**

An interface must be started before configuration can be performed on it.

If an interface is shut down during data transmission, data will be lost. Exercise caution when using this command.

Example

Shut down Ethernet interface xgigaethernet 1/0/1.

```
Switch(config-10ge1/0/1)#shutdown
Switch(config-10ge1/0/1)#
```

3.1.32 show interface unit-number**Function**

The **show interface unit-number** command displays unit numbers of interfaces on the switch.

Format

show interface unit-number

Parameter

NA

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

Displays unit numbers of all interfaces on the switch.

```
Switch>show interface unit-number
  Interface      Unit Number
  xge-1/0/1      17410
  xge-1/0/2      17411
  xge-1/0/3      17412
```

```

xge-1/0/4      17413
xge-1/0/5      17414
xge-1/0/6      17415
xge-1/0/7      17416
xge-1/0/8      17417
xge-1/0/9      17418
xge-1/0/10     17419
xge-1/0/11     17420
xge-1/0/12     17421
xge-1/0/13     17422
xge-1/0/14     17423
xge-1/0/15     17424
xge-1/0/16     17425
xge-1/0/17     17426
xge-1/0/18     17427
xge-1/0/19     17428
xge-1/0/20     17429
xge-1/0/21     17430
xge-1/0/22     17431
xge-1/0/23     17432
xge-1/0/24     17433
eth-trunk-1    32769
vlan-1         49153
Switch>

```

3.1.33 show interface

Function

The **show interface** command displays attributes of an interface and related information.

Format

- **show interface**
- **show interface { ethernet | xgigaethernet | 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet } interface-number**
- **show interface { ethernet | xgigaethernet | 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet } interface-number config**
- **show interface eth-trunk trunk.subinterface config**
- **show interface verbose**

Parameter

Parameter	Description	Value
verbose	Displays information about all interfaces.	-
interface-number	Specifies an Ethernet interface number.	The value is an integer in the range of <1-1>/<0-1>/<1-48>.
trunk.subinterface	Specifies a Trunk sub-interface number.	The value is an integer ranging from 1 to 256 or 1 to 4094.

Default Value

NA

View

Common user view

Usage Guidelines

When checking interface attributes and related information:

If no interface type and interface number are specified in **show interface**, the number, state, filter table binding state, in-band IP address, and description of all Ethernet interfaces of the device are displayed. Otherwise, the basic information on the specified interface is displayed, including the duplex mode, broadcast storm control, and packet count. If **config** is specified, other function configurations of the specified interface are displayed.

If no interface number is specified in **show interface trunk**, the Trunk group, stream allocation algorithm and number of interfaces joined the Trunk group are displayed. If an interface number is specified, the basic statistics of the specified Trunk interface is displayed. If **config** is specified, other function configurations of the specified Trunk interface are displayed.

The **show interface verbose** command displays the basic information on all Ethernet and Trunk interfaces (if configured) of the current device.

Generally, commands described in this section are used to collect traffic statistics or diagnose faults on interfaces.

Example

Display the configuration of Ethernet interface xgigaethernet 1/0/1.

```
Switch>show interface xgigaethernet 1/0/1
Interface xgigaethernet-1/0/1
  Admin state is up,operation state is down
  Negotiation auto enable
  flow-control negotiation disable
```

```
Duplex is half
Speed is 1000M(bps)
Mtu is 1522
Connector is electronic
Priority is 0
In direction filter-group is disable
Out direction filter-group is disable
Bandwidth granularity is 64000(bps)
In direction bandwidth is disable
Out direction bandwidth is disable
Broadcast-storm packet-ctrl is disable
Multicast-storm packet-ctrl is disable
Dlf-storm packet-ctrl is disable
Broadcast-storm bps-ctrl is disable
Multicast-storm bps-ctrl is disable
Dlf-storm bps-ctrl is disable
Pvid is 1
Dot1q-tunnel disable
Port link-type is hybrid
Mdi is auto
Flow-control disable
Flow-statistic include-interframe disable
port-security disable
port-security mac-address sticky disable
Port-down holdoff-timer 0
Last 5 minutes input rate:0 Bps, 0 pps
Last 5 minutes output rate:0 Bps, 0 pps
Last 5 minutes input link utilization rate: 0.00%
Last 5 minutes output link utilization rate: 0.00%
Rx statistic:
    octets:0/0
    packets:0/0
    unicast:0/0
    multicast:0/0
    broadcast:0/0
Packets statistic:
    64 octets:0/0
    65-127 octets:0/0
    128-255 octets:0/0
    256-511 octets:0/0
    512-1023 octets:0/0
    1024-1518 octets:0/0
    >1518 octets:0/0
```

```

Tx statistic:
    octets:0/0
    packets:0/0
    unicast:0/0
    multicast:0/0
    broadcast:0/0
Packets statistic:
    64 octets:0/0
    65-127 octets:0/0
    128-255 octets:0/0
    256-511 octets:0/0
    512-1023 octets:0/0
    1024-1518 octets:0/0
    >1518 octets:0/0
Other statistic:
    fragments:0/0
    Jabbers:0/0
    CRC errors:0/0
    Collisions:0/0
    Undersize:0/0
    Oversize:0/0
Switch>

```

3.1.34 show interface statistic

Function

The **show interface statistic** command displays statistics on an interface.

Format

- **show interface statistic**
- **show interface statistic brief**

Parameter

NA

Default Value

NA

View

Common user view

Usage Guidelines

Generally, commands described in this section are used to collect traffic statistics or diagnose faults on interfaces.

If you do not specify a slot number when running this command, the command displays statistics about ingress and egress packets on all the working interfaces on the switch in the order of port numbers.

The command output information includes the following:

Port type and number

Total number of packets sent or received by a port

Total number of unicast packets sent or received by a port

Total number of multicast packets sent or received by a port

Total number of broadcast packets sent or received by a port

Total number of error packets sent or received by a port

Example

Display the statistics on Ethernet interface xgigaethernet 1/0/1.

Switch>show interface statistic					
Interface	In(pkts) :Total	UniCast	MultiCast	BroadCast	Err
	Out(pkts):Total	UniCast	MultiCast	BroadCast	Err
xge-1/0/1	0/0	0/0	0/0	0/0	0/0
	0/0	0/0	0/0	0/0	0/0
xge-1/0/2	0/0	0/0	0/0	0/0	0/0
	0/0	0/0	0/0	0/0	0/0
xge-1/0/3	0/0	0/0	0/0	0/0	0/0
	0/0	0/0	0/0	0/0	0/0
xge-1/0/4	0/0	0/0	0/0	0/0	0/0
	0/0	0/0	0/0	0/0	0/0
xge-1/0/5	0/0	0/0	0/0	0/0	0/0
	0/0	0/0	0/0	0/0	0/0
xge-1/0/6	0/0	0/0	0/0	0/0	0/0
	0/0	0/0	0/0	0/0	0/0
xge-1/0/7	0/0	0/0	0/0	0/0	0/0
	0/0	0/0	0/0	0/0	0/0
xge-1/0/8	0/0	0/0	0/0	0/0	0/0
	0/0	0/0	0/0	0/0	0/0
xge-1/0/9	0/0	0/0	0/0	0/0	0/0
	0/0	0/0	0/0	0/0	0/0
xge-1/0/10	0/0	0/0	0/0	0/0	0/0

	0/0	0/0	0/0	0/0	0/0
xge-1/0/11	0/0	0/0	0/0	0/0	0/0
	0/0	0/0	0/0	0/0	0/0
xge-1/0/12	0/0	0/0	0/0	0/0	0/0
	0/0	0/0	0/0	0/0	0/0
xge-1/0/13	0/0	0/0	0/0	0/0	0/0
	0/0	0/0	0/0	0/0	0/0
xge-1/0/14	0/0	0/0	0/0	0/0	0/0
	0/0	0/0	0/0	0/0	0/0
xge-1/0/15	0/0	0/0	0/0	0/0	0/0
	0/0	0/0	0/0	0/0	0/0
xge-1/0/16	0/0	0/0	0/0	0/0	0/0
	0/0	0/0	0/0	0/0	0/0
xge-1/0/17	0/0	0/0	0/0	0/0	0/0
	0/0	0/0	0/0	0/0	0/0
xge-1/0/18	0/0	0/0	0/0	0/0	0/0
	0/0	0/0	0/0	0/0	0/0
xge-1/0/19	0/0	0/0	0/0	0/0	0/0
	0/0	0/0	0/0	0/0	0/0
xge-1/0/20	0/0	0/0	0/0	0/0	0/0
	0/0	0/0	0/0	0/0	0/0
xge-1/0/21	0/0	0/0	0/0	0/0	0/0
	0/0	0/0	0/0	0/0	0/0
xge-1/0/22	0/0	0/0	0/0	0/0	0/0
	0/0	0/0	0/0	0/0	0/0
xge-1/0/23	0/0	0/0	0/0	0/0	0/0
	0/0	0/0	0/0	0/0	0/0
xge-1/0/24	0/0	0/0	0/0	0/0	0/0
	0/0	0/0	0/0	0/0	0/0
Switch>					

3.1.35 work-mode

Function

The **work-mode** command configures the work mode for a port.

Format

work-mode { bridge | router }

Parameter

Parameter	Description	Value
bridge	Sets the mode to bridge .	-

Parameter	Description	Value
router	Sets the mode to router .	-

Default Value

NA

View

Ethernet bridge interface configuration view, Ethernet routing interface configuration view

Usage Guidelines

NA

Example

Set the work mode for a port.

```
Switch(config-10ge1/0/1)#work-mode router
Switch(config-10ge1/0/1)#
```

3.1.36 interface

Function

The **interface** command enters the configuration view of a specified interface or its sub-interface. If an interface range is specified, the configuration view of the interface group is entered. The commands configured in the interface group are automatically executed on all the member interfaces in this group.

The **no interface** command deletes the configured sub-interface.

Format

- **interface** { **ethernet** | **xgigaethernet** | **10gigaethernet** | **25gigaethernet** | **40gigaethernet** | **100gigaethernet** } *interface-number*
- **interface** { **ethernet** | **xgigaethernet** | **10gigaethernet** | **25gigaethernet** | **40gigaethernet** | **100gigaethernet** } *interface-number* **to** { **ethernet** | **xgigaethernet** | **10gigaethernet** | **25gigaethernet** | **40gigaethernet** | **100gigaethernet** } *interface-number*
- **interface** { **ethernet** | **xgigaethernet** | **10gigaethernet** | **25gigaethernet** | **40gigaethernet** | **100gigaethernet** } *interface-number.subinterface-number*
- **interface group** *interface-number-list*

- **no interface { ethernet | xgigaethernet | 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet } interface-number.subinterface-number**

Parameter

Parameter	Description	Value
interface-number	Specifies an Ethernet interface number.	The value is an integer in the range of <1-1>/<0-1>/<1-48>.
subinterface-number	Specifies a sub-interface number.	The value is an integer ranging from 1 to 4094.
interface-number-list	Specifies the sequence of the Ethernet interface.	The value is an integer in the range of <1-1>/<0-1>/<1-48>.

Default Value

NA

View

Global configuration view

Usage Guidelines

To set parameters of an interface, you need to enter the interface configuration view using this command. If a trunk interface has no member interfaces, all commands are invalid on the trunk interface.

Example

Enter the configuration view of Ethernet interfaces xgigaethernet 1/0/1 to xgigaethernet 1/0/12.

```
Switch(config)#interface xgigaethernet 1/0/1 to xgigaethernet 1/0/12
Switch(config-10ge1/0/1->xge1/0/12)#
```

3.1.37 rate-limit

Function

The **rate-limit** command sets the bandwidth of an interface.

The **no rate-limit** command cancels the bandwidth setting on an interface.

Format

Ethernet bridge interface configuration view, Ethernet routing interface configuration view

- **rate-limit out { kbps | mbps | gbps } rate-limit**

Ethernet bridge interface configuration view, Ethernet routing interface configuration view, interface configuration view (Trunk)

- **no rate-limit out**

Parameter

Parameter	Description	Value
out	Sets the outbound bandwidth on the interface.	-
rate-limit	Specifies the control coefficient.	The value is an integer ranging from 0 to 100000000.
kbps	Specifies the bandwidth (Kbps).	The value is an integer ranging from 1 to 10000000.
mbps	Specifies the bandwidth (Mbps).	The value is an integer ranging from 1 to 10000.
gbps	Specifies the bandwidth (Gbps).	The value is an integer ranging from 1 to 10.

View

The view is specified in the command.

Usage Guidelines

Some application scenarios require control of interface rates so as to provide different bandwidth for different users. Compared with the traffic policing feature in QoS application, bandwidth limiting on an interface can control the rate of all packets passing through the interface. If you only need to control the packet transmission and receiving rates on an interface and do not require rate limiting based on packet types, setting a bandwidth limit on the interface is a more convenient and simple method.

Example

Set the inbound bandwidth of Ethernet interface **10gigaethernet 1/0/1** to two times of the granularity (2 x 1 kbit/s).

```
Switch(config-10ge1/0/1)#rate-limit out 128
Switch(config-10ge1/0/1)#
```

3.1.38 rate-limit out threshold**Function**

The **rate-limit out threshold** command configures the bandwidth alarm threshold and alarm recovery threshold.

Format

- **rate-limit out threshold** { *threshold-value* | **default** }
- **rate-limit out threshold** { **threshold-value** | **default** } **resume-threshold** { *resume-threshold-value* | **default** }

Parameter

Parameter	Description	Value
threshold-value	Specifies the bandwidth alarm threshold.	The value is an integer ranging from 1 to 100.
resume-threshold-value	Specifies the alarm recovery threshold.	The value is an integer ranging from 1 to 100.

Default Value

The default bandwidth alarm threshold is 0 and the default alarm recovery threshold is 90.

View

Ethernet bridge interface configuration view, Ethernet routing interface configuration view

Usage Guidelines

You can set appropriate bandwidth alarm threshold and alarm recovery threshold to monitor the real-time port bandwidth utilization.

Example

Set the outbound bandwidth alarm threshold to 95 and alarm recovery threshold to 85 for the Ethernet bridge interface 10gigaethernet 1/0/1.

```
Switch(config-10ge1/0/1)#rate-limit out threshold 95 resume-threshold 85
Switch(config-10ge1/0/1)#
```

3.1.39 show interface ethernet brief**Function**

The **show interface ethernet brief** command displays the running state, management state, and duplex rate of all physical ports.

Format

show interface ethernet brief

Parameter

NA

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

View the running state, management state, and duplex rate of all physical ports.

```
Switch>show interface ethernet brief
```

Interface	Link	Duplex/Speed	InUti	OutUti	Descr
ge1/0/1	Down	Half/1000M	0.00%	0.00%	-
ge1/0/2	Down	Half/1000M	0.00%	0.00%	-
ge1/0/3	Down	Half/1000M	0.00%	0.00%	-
ge1/0/4	Down	Half/1000M	0.00%	0.00%	-
ge1/0/5	Down	Half/1000M	0.00%	0.00%	-
ge1/0/6	Down	Half/1000M	0.00%	0.00%	-
ge1/0/7	Down	Half/1000M	0.00%	0.00%	-
ge1/0/8	Down	Half/1000M	0.00%	0.00%	-
ge1/0/9	Down	Half/1000M	0.00%	0.00%	-
ge1/0/10	Down	Half/10M	0.00%	0.00%	-
ge1/0/11	Down	Half/1000M	0.00%	0.00%	-
ge1/0/12	Down	Half/1000M	0.00%	0.00%	-
ge1/0/13	Down	Half/1000M	0.00%	0.00%	-
ge1/0/14	Down	Half/1000M	0.00%	0.00%	-
ge1/0/15	Down	Half/1000M	0.00%	0.00%	-
ge1/0/16	Down	Half/1000M	0.00%	0.00%	-
ge1/0/17	Down	Half/1000M	0.00%	0.00%	-
ge1/0/18	Down	Half/1000M	0.00%	0.00%	-
ge1/0/19	Down	Half/1000M	0.00%	0.00%	-
ge1/0/20	Down	Half/1000M	0.00%	0.00%	-
ge1/0/21	Down	Half/1000M	0.00%	0.00%	-

```
Switch>
```

3.1.40 link-flap protection {start|stop}

Function

The **link-flap protection {start|stop}** command enables or disables link flapping protection on all ports.

Format

link-flap protection { start | stop }

Parameter

Parameter	Description	Value
start	Enables link flapping protection on all ports.	-
stop	Disables link flapping protection on all ports.	-

Default Value

Disable

View

Global configuration view

Usage Guidelines

Run this command to enable link flapping protection on all ports before configuring other link flapping commands.

Example

Enable link flapping protection on all ports.

```
Switch(config)#link-flap protection start
Switch(config)#
```

3.1.41 port mode

Function

The **port mode** command configures the mode for all the specified interfaces.

Format

port mode { 10xgi | 25gi } **interface** { 10gigaethernet | 25gigaethernet } *interface-number*

Parameter

Parameter	Description	Value
interface-number	Specifies an Ethernet interface number.	The value is an integer in the range of <1-1>/<0-1>/<1-48>.

Default Value

NA

View

Global configuration view

Usage Guidelines

NA

Example

Set the mode for all the specified interfaces.

```
Switch(config)#port mode 10xge interface 25gigaethernet 1/0/1
Switch(config)#
```

3.1.42 fec mode**Function**

The **fec mode** command enables the RS-FEC or Base-R FEC function for a port.

Format

fec mode { rs | base-r | none }

Parameter

Parameter	Description	Value
rs	Enables the RS-FEC function.	-
base-r	Enables the Base-R FEC function.	-
none	Disables the RS-FEC or Base-R FEC function.	-

Default Value

NA

View

Ethernet routing configuration view

Usage Guidelines

This command is applicable only to 25G devices, and is not applicable to 10G devices.

Example

Enable the RS-FEC function.

```
Switch(config-10ge1/0/1)#fec mode rs
Switch(config-10ge1/0/1)#
```

3.1.43 reset counter interface**Function**

The **reset counter interface** command clears the statistics of the specified interface.

Format

- **reset counter interface eth-trunk** *trunk-number*

- **reset counter interface tunnel** *tunnel-number*
- **reset counter interface nve** *nve-id*
- **reset counter interface bridge-domain** *bd-id*
- **reset counter interface { ethernet | xgigaethernet | 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet }** *interface-number*
- **reset counter interface { ethernet | xgigaethernet | 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet }** *interface-number.subinterface*
- **reset counter interface eth-trunk** *trunk-number.subinterface*
- **reset counter interface mgt-eth** *outband-number*
- **reset counter interface all**

Parameter

Parameter	Description	Value
trunk-number	Specifies the number of a Trunk interface.	The value is an integer ranging from 1 to 128.
tunnel-number	Specifies the number of a Tunnel interface.	The value is an integer ranging from 1 to 1024.
nve-id	Specifies an NVE ID.	The value is an integer ranging from 1 to 1024.
bd-id	Specifies an L3 BD ID.	The value is an integer ranging from 1 to 16777215.
interface-number	Specifies an Ethernet interface number.	The value is an integer in the range of <1-1>/<0-1>/<1-48>.
subinterface	Specifies a sub-interface number.	The value is an integer ranging from 1 to 4094.
outband-number	Specifies the number of an out-of-band interface.	The value is an integer in the range of <0-0>/<0-0>/<0-0>.

Default Value

NA

View

Global configuration view

Usage Guidelines

NA

Example

Clear statistics of the specified interface.

```
Switch(config)#reset counter interface eth-trunk 1
Switch(config)#
```

3.1.44 show interface error-down

Function

The **show interface error-down** command displays information on the interface which is down due to an error.

Format

show interface error-down

Parameter

NA

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

Display information on the interface which is down due to an error.

```
Switch>show interface error-down
Switch>
```

3.1.45 show crc-error config

Function

The **show crc-error config** command displays the check error configuration.

Format

show crc-error config

Parameter

NA

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

View the check error configuration.

```
Switch>show crc-error config
Switch>
```

3.1.46 show l3int bridge-domain**Function**The **show l3int bridge-domain** command displays the reference count of a BD interface.**Format****show l3int bridge-domain** *domain-id***Parameter**

Parameter	Description	Value
domain-id	Specifies a domain ID.	The value is an integer ranging from 1 to 16777215.

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

View the reference count of a BD interface.

```
Switch>show l3int bridge-domain 1
Switch>
```

3.1.47 show l3int ethernet

Function

The **show l3int ethernet** command displays the reference count of an Ethernet interface and its sub-interfaces.

Format

- **show l3int ethernet** *interface-number*
- **show l3int ethernet** *interface-number.subinterface-number*

Parameter

Parameter	Description	Value
interface-number	Specifies an Ethernet interface number.	The value is an integer in the range of <1-128>/<0-2>/<1-256> (For reference only. The specific value range depends on the slot number and card type).
subinterface-number	Specifies a sub-interface number.	The value is an integer ranging from 1 to 4094.

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

View the reference count of Ethernet interface 1/0/1.

```
Switch>show l3int ethernet 1/0/1
Switch>
```

3.1.48 show l3int eth-trunk

Function

The **show l3int eth-trunk** command displays the reference count of a Trunk interface.

Format

show l3int eth-trunk *trunk-number*

Parameter

Parameter	Description	Value
trunk-number	Specifies the number of a Trunk interface.	The value is an integer ranging from 1 to 256.

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

View the reference count of interface trunk 1.

```
Switch>show l3int eth-trunk 1
Switch>
```

3.1.49 show l3int vlan**Function**The **show l3int vlan** command displays the reference count of a VLAN interface.**Format****show l3int vlan** *vlan-id***Parameter**

Parameter	Description	Value
vlan-id	Specifies a VLAN interface ID.	The value is an integer ranging from 1 to 4094.

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

View the reference count of interface vlan 1.

```
Switch>show l3int vlan 1
IFREF_FUNC_LLTABLE_NOTIFIER_PROCESS 2          will be deleted
IFREF_FUNC_LLTABLE_NOTIFIER_TIMER -2          will be deleted
IFREF_FUNC_M2IPIFGETAPI 1                    will be deleted
```

3.2 MAC Address Table Configuration Commands

3.2.1 mac-address flapping action {quit-vlan|error-down}

Function

The **mac-address flapping action {quit-vlan|error-down}** command configures the action taken by a port due to MAC address flapping.

Format

mac-address flapping action { quit-vlan | error-down }

Parameter

Parameter	Description	Value
quit-vlan	Indicates disconnecting a port from VLAN when its MAC address flaps.	-
error-down	Indicates shutting down a port when its MAC address flaps.	-

Default Value

NA

View

Ethernet bridge interface configuration view, interface configuration view (Trunk)

Usage Guidelines

NA

Example

Set a port to shut down when its MAC address flaps.

```
Switch(config-10ge1/0/1)#mac-address flapping action error-down
Switch(config-10ge1/0/1)#
```

3.2.2 mac-address flapping action priority

Function

The **mac-address flapping action priority** command configures the priority of the action taken by a port due to MAC address flapping.

Format

mac-address flapping action priority { *PRIORITY* | **default** }

Parameter

Parameter	Description	Value
PRIORITY	Sets the priority of the action taken by a port when its MAC address flaps.	The value is an integer ranging from 0 to 255.
default	Specifies the default priority of the action taken by a port.	The priority of the action is 127.

Default Value

127

View

Ethernet bridge interface configuration view, interface configuration view (Trunk)

Usage Guidelines

NA

Example

Set the priority of the action taken by a port when its MAC address flaps to 127.

```
Switch(config-10ge1/0/1)# mac-address flapping action priority 127
Switch(config-10ge1/0/1)#
```

3.2.3 mac-address notification {add|remove|all}

Function

The **mac-address notification {add|remove|all}** command enables the MAC address change notification function for a port and configures the notification policy.

The **no mac-address notification** command disables the MAC address change notification function for a port.

Format

- **mac-address notification { add | remove | all }**
- **no mac-address notification**

Parameter

Parameter	Description	Value
add	Adds the MAC address sending notification.	-
remove	Deletes the MAC address sending notification.	-
all	Adds or deletes the MAC address all sending notification.	-

Default Value

The MAC address change notification function is disabled by default.

View

Ethernet bridge interface configuration view, interface configuration view (Trunk)

Usage Guidelines

You can run this command to enable this function to monitor the MAC address change.

Example

Enable the MAC address change notification function for a port and set the notification policy.

```
Switch(config-10ge1/0/1)#mac-address notification add
Switch(config-10ge1/0/1)#
```

3.2.4 mac-learning {enable|disable}**Function**

The **mac-learning {enable|disable}** command enables or disables MAC address learning on an interface.

Format

mac-learning { enable | disable }

Parameter

Parameter	Description	Value
enable	Enables MAC address learning.	-
disable	Disables MAC address learning.	-

Default Value

By default, MAC address learning is enabled.

View

Ethernet bridge interface configuration view, interface configuration view (Trunk), BD configuration view

Usage Guidelines

NA

Example

Disable MAC address learning on trunk 1.

```
Switch(config-eth-trunk1)#mac-learning disable
Switch(config-eth-trunk1)#
```

3.2.5 mac-learning disable action {forward|drop}**Function**

The **mac-learning disable action {forward|drop}** command sets the action taken by a port after MAC address learning is disabled for the port.

Format

mac-learning disable action { forward | drop }

Parameter

Parameter	Description	Value
forward	Indicates that a port forwards the packet but does not add the packet to the MAC address table.	-
drop	Indicates that a port discards the packet and does not add the packet to the MAC address table.	-

Default Value

NA

View

Ethernet bridge interface configuration view, interface configuration view (Trunk), VLAN configuration view

Usage Guidelines

NA

Example

Set a port to discard the packet.

```
Switch(config-10ge1/0/1)#mac-learning disable action drop
Switch(config-10ge1/0/1)#
```

3.2.6 no mac-address flapping action

Function

The **no mac-address flapping action** command deletes the action triggered by MAC address flapping.

Format

no mac-address flapping action

Parameter

NA

Default Value

NA

View

Ethernet bridge interface configuration view, interface configuration view (Trunk)

Usage Guidelines

NA

Example

Delete the action triggered by MAC address flapping.

```
Switch(config-10ge1/0/1)#no mac-address flapping action
Switch(config-10ge1/0/1)#
```

3.2.7 show mac-address

Function

The **show mac-address** command displays MAC address entries with a specified destination MAC address or those with a specified destination MAC address and a specified VLAN ID.

Format

- **show mac-address**
- **show mac-address vlan** *vlan-id*

- **show mac-address vsi** *vsi-name*
- **show mac-address** *MAC-ADDRESS*
- **show mac-address** *MAC-ADDRESS* **vlan** *vlan-id*
- **show mac-address** { **ethernet** | **xgigaethernet** | **10gigaethernet** | **25gigaethernet** | **40gigaethernet** | **100gigaethernet** } *interface-number*
- **show mac-address eth-trunk** *trunk-number*
- **show mac-address eth-trunk** *trunk-number.subinterface-number*
- **show mac-address** { **static** | **security** | **sticky** }
- **show mac-address** { **static** | **security** | **sticky** } **vsi** *vsi-name*
- **show mac-address** { **static** | **security** | **sticky** } { **ethernet** | **xgigaethernet** | **10gigaethernet** | **25gigaethernet** | **40gigaethernet** | **100gigaethernet** } *interface-number*
- **show mac-address** { **static** | **security** | **sticky** } **eth-trunk** *trunk-number*
- **show mac-address** { **static** | **security** | **sticky** } **vlan** *vlan-id*
- **show mac-address** { **static** | **security** | **sticky** } **vlan** *vlan-id* { **ethernet** | **xgigaethernet** | **10gigaethernet** | **25gigaethernet** | **40gigaethernet** | **100gigaethernet** } *interface-number*
- **show mac-address** { **static** | **security** | **sticky** } **vlan** *vlan-id* **eth-trunk** *trunk-number*

Parameter

Parameter	Description	Value
MAC-ADDRESS	Specifies a MAC address.	The value is in the AA:BB:CC:DD:EE:FF format, where A to F are hexadecimal digits.
vlan-id	Specifies a VLAN ID.	The value is an integer ranging from 1 to 4094.
interface-number	Specifies an Ethernet interface number.	The value is an integer in the range of <1-1>/<0-1>/<1-48>
trunk-number	Specifies the number of a Trunk interface.	The value is an integer ranging from 1 to 128.
<i>subinterface-number</i>	Specifies a sub-interface number.	The value is an integer ranging from 1 to 4094.
vsi-name	Specifies a VSI instance name.	The value is a character string. No space can be contained.
security	Indicates secure dynamic MAC address entries.	which are learned on a port after port security is enabled.
sticky	Indicates sticky MAC address entries.	which are learned on a port after the sticky MAC address function is enabled.

Parameter	Description	Value
static	Indicates the static MAC address entries.	which are learned by a port after static MAC learning is enabled.

Default Value

NA

View

Common user view

Usage Guidelines

This command enables you to quickly find information about specific MAC address entries.

Example

View entries of the MAC address **00:00:00:00:00:01**.

Switch>show mac-address 00:00:00:00:00:01				
MAC Address	Vlan/Vsi	Interface	Oper-Type	Type
00:00:00:00:00:01	333	GE1/0/1	forward	static
	2	GE1/0/2	discard	black-hole
00:00:00:00:00:01	12	GE1/0/3	discard	black-hole
	3	GE1/0/2	forward	static
total number of mac-address is : 4				
Switch>				

3.2.8 show mac-address dynamic

Function

The **show mac-address dynamic** command displays the dynamic MAC address entries by interface, VLAN, or both interface and VLAN.

Format

- **show mac-address dynamic**
- **show mac-address dynamic { ethernet | xgigaethernet | 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet } interface-number**
- **show mac-address dynamic eth-trunk trunk-number**
- **show mac-address dynamic vlan vlan-id**
- **show mac-address dynamic vlan vlan-id { ethernet | xgigaethernet | 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet } interface-number**

- **show mac-address dynamic vlan** *vlan-id* **eth-trunk** *trunk-number*
- **show mac-address dynamic vsi** *vsi-name*

Parameter

Parameter	Description	Value
interface-number	Specifies an Ethernet interface number.	The value is an integer in the range of <1-1>/<0-1>/<1-48>
trunk-number	Specifies the number of a Trunk interface.	The value is an integer ranging from 1 to 128.
vlan-id	Specifies a VLAN ID.	The value is an integer ranging from 1 to 4094.
vsi-name	Specifies a VSI instance name.	The value is a character string. No space can be contained.

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

Display information about dynamic MAC address entries on an interface.

```

Switch>show mac-address dynamic
Dynamic          :1

MAC Address      Vlan/Vsi/BD   Learn-From      Oper-Type   Type
00:00:00:00:00:01  1/--/--      ge-1/0/7        forward    dynamic
Switch>

```

3.2.9 show mac-address config**Function**The **show mac-address config** command displays the configuration of the MAC address table.**Format****show mac-address config****Parameter**

NA

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

Display the configuration of the MAC address table.

```
Switch>show mac-address config
!
!Mac-address Configuration
Switch>
```

3.2.10 show mac-address flapping record**Function**The **show mac-address flapping record** command displays the MAC address flapping record.**Format****show mac-address flapping record****Parameter**

NA

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

View the flapping information on the MAC address learning priority.

```
Switch>show mac-address flapping record
```

PRIORITY	Flapping-status
0	enable
1	enable
2	enable
3	enable

```
Switch>
```

3.2.11 show mac-address notification history

Function

The **show mac-address notification history** command displays the MAC address adding and deletion record.

Format

show mac-address notification history

Parameter

NA

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

Display the MAC address adding and deletion record.

```
Switch>show mac-address notification history
```

```
History Index:1
```

```
Timestamp:2000-12-29 17:02:24
```

```
MAC Log Number:2
```

```
=====
```

Time Stamp	Operation	Vlan	MAC Address	Interface
2000-12-29 17:02:24	flush	1	00:04:67:47:20:04	ge-1/0/4
2000-12-29 17:02:27	add	1	00:04:67:47:20:04	ge-1/0/4

```
Switch>
```

3.2.12 show mac-address total-number

Function

The **show mac-address total-number** command displays the number of MAC addresses on an interface or VLAN.

Format

- **show mac-address total-number**
- **show mac-address total-number { ethernet | xgigaethernet | 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet } interface-number**
- **show mac-address total-number eth-trunk trunk-number**
- **show mac-address total-number vlan vlan-id**

Parameter

Parameter	Description	Value
interface-number	Specifies an Ethernet interface number.	The value is an integer in the range of <1-1>/<0-1>/<1-48>.
trunk-number	Specifies the number of a Trunk interface.	The value is an integer ranging from 1 to 128.
vlan-id	Specifies a VLAN interface ID.	The value is an integer ranging from 1 to 4094.

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

Display the number of MAC address entries in VLAN 10.

```
Switch>show mac-address total-number vlan 10
  Vlan  Total    Blackhole    Static    Dynamic
   2      9         0           4         5
Switch>
```

3.2.13 show mac-limit

Function

The **show mac-limit** command displays the MAC address learning limit configured on the switch.

Format

- **show mac-limit**
- **show mac-limit interface**
- **show mac-limit interface { ethernet | xgigaethernet | 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet } interface-number**
- **show mac-limit interface eth-trunk trunk-number**
- **show mac-limit config**

Parameter

Parameter	Description	Value
interface-number	Specifies an Ethernet interface number.	The value is an integer in the range of <1-1>/<0-1>/<1-48>.
trunk-number	Specifies the number of a Trunk interface.	The value is an integer ranging from 1 to 128.

Default Value

NA

View

Common user view

Usage Guidelines

You can use this command to check the MAC address learning limit configured globally, on a specified interface, or on a specified VLAN.

Example

View the MAC address learning limit of the interface **xgigaethernet 1/0/1**.

```
Switch>show mac-limit interface xgigaethernet 1/0/1
xge-1/0/1 MAC LIMIT:
Maximum MAC count:1435, used count :0;
Action:drop, Alarm:disable.

Switch>
```

3.2.14 mac-address blackhole

Function

The **mac-address blackhole** command creates a blackhole MAC address entry.

The **no mac-address blackhole** command deletes blackhole MAC address entries.

Format

- **mac-address blackhole** *vlan-id mac-address*
- **no mac-address blackhole**
- **no mac-address blackhole** *mac-address*
- **no mac-address blackhole vlan** *vlan-id*
- **no mac-address blackhole vlan** *vlan-id mac-address*

Parameter

Parameter	Description	Value
vlan-id	Specifies the ID of the VLAN to which the outbound interface belongs.	The value is an integer ranging from 1 to 4094.
mac-address	Specifies a destination MAC address.	The format is AA:BB:CC:DD:EE:FF, where A to F are hexadecimal digits.

Default Value

By default, no blackhole MAC address entries are configured in the system.

View

Global configuration view

Usage Guidelines

Blackhole MAC address entries can prevent theft of data using embezzled user identities, enhancing system security.

After you create a blackhole MAC address entry using this command, any data frames with the specified MAC address as the source or destination MAC address will be discarded.

Example

Create a blackhole MAC address entry, with the destination MAC address 00:00:00:01:02:03 and outbound VLAN 10.

```
Switch(config)#mac-address blackhole 10 00:00:00:01:02:03
Switch(config)#
```

3.2.15 mac aging-time

Function

The **mac aging-time** command sets the aging time of dynamic MAC address entries.

Format

mac aging-time { 0 | *aging-time* | **default**}

Parameter

Parameter	Description	Value
aging-time	Specifies the aging time of dynamic MAC address entries.	The value is an integer ranging from 0, and 60 to 1000000, in seconds.

Default Value

The default aging time of dynamic MAC address entries is 300 seconds.

View

Global configuration view

Usage Guidelines

If the aging time is set to 0, dynamic MAC address entries will not age out.

MAC address learning is a continuous dynamic process because the network topology keeps changing. To reduce the number of MAC address entries in the system, you can set an appropriate aging time for dynamic MAC address entries. This setting enables obsolete MAC address entries to be deleted in a timely manner.

The system starts an aging timer for each dynamic MAC address entry. A dynamic MAC address entry will be deleted if it is not updated within two times the aging time. If the MAC address entry is updated within this time period, the system resets its aging timer.



Note:

Once the system is reset or a line card is hot plugged or reset, dynamic entries are lost, but the stored static entries and blackhole entries are not aged or lost.

Example

Set the aging time of dynamic MAC address entries to 10000 seconds.

```
Switch(config)#mac aging-time 10000
```

```
Switch(config)#
```

3.2.16 no mac-address

Function

The **no mac-address** command deletes MAC address entries learned globally or on an interface.

Format

- **no mac-address**
- **no mac-address** *mac-address*
- **no mac-address** { **ethernet** | **xgigaethernet** | **10gigaethernet** | **25gigaethernet** | **40gigaethernet** | **100gigaethernet** } *interface-number*
- **no mac-address** **vlan** *vlan-id*
- **no mac-address** **vlan** *vlan-id* *mac-address*
- **no mac-address** **eth-trunk** *trunk-number*
- **no mac-address** { **static** | **security** | **sticky** }
- **no mac-address** { **static** | **security** | **sticky** } *mac-address*
- **no mac-address** { **static** | **security** | **sticky** } { **ethernet** | **xgigaethernet** | **10gigaethernet** | **25gigaethernet** | **40gigaethernet** | **100gigaethernet** } *interface-number*
- **no mac-address** { **static** | **security** | **sticky** } **eth-trunk** *trunk-number*
- **no mac-address** { **static** | **security** | **sticky** } **vlan** *vlan-id*
- **no mac-address** { **static** | **security** | **sticky** } **vlan** *vlan-id* *mac-address*

Parameter

Parameter	Description	Value
interface-number	Specifies an Ethernet interface number.	The value is an integer in the range of <1-1>/<0-1>/<1-48>.
trunk-number	Specifies the number of an aggregation interface.	The value is an integer ranging from 1 to 128.
mac-address	Specifies a MAC address.	The value is in AA:BB:CC:DD:EE:FF format, where A to F are hexadecimal digits.
vlan-id	Specifies a VLAN ID.	The value is an integer ranging from 1 to 4094.
static	Indicates the static MAC address entries.	which are learned by a port after static MAC learning is enabled.
security	Indicates secure dynamic MAC	which are learned on a port after port security is

Parameter	Description	Value
	address entries,	enabled.
sticky	Indicates sticky MAC address entries.	which are learned on a port after the sticky MAC address function is enabled.
vsi-name	Specifies the name of a VSI instance to be displayed.	The value is a case-sensitive character string without spaces.

Default Value

NA

View

Global configuration view

Usage Guidelines

You can use this command to delete all MAC address entries in the system.

Example

Delete all MAC address entries in the system.

```
Switch(config)#no mac-address
Switch(config)#
```

3.2.17 no mac-address dynamic

Function

The **no mac-address dynamic** command deletes all dynamic MAC address entries on the switch.

Format

- **no mac-address dynamic**
- **no mac-address dynamic** *mac-address*
- **no mac-address dynamic** { **ethernet** | **xgigaethernet** | **10gigaethernet** | **25gigaethernet** | **40gigaethernet** | **100gigaethernet** } *interface-number*
- **no mac-address dynamic** **vlan** *vlan-id*
- **no mac-address dynamic** **vlan** *vlan-id* *mac-address*
- **no mac-address dynamic** **eth-trunk** *trunk-number*

Parameter

Parameter	Description	Value

Parameter	Description	Value
vlan-id	Specifies a VLAN interface ID.	The value is an integer ranging from 1 to 4094.
mac-address	Specifies a dynamic MAC address.	The value is in AA:BB:CC:DD:EE:FF format, where A to F are hexadecimal digits.
interface-number	Specifies an Ethernet interface number.	The value is an integer in the range of <1-1>/<0-1>/<1-48>.
trunk-number	Specifies the number of a Trunk interface.	The value is an integer ranging from 1 to 128.

Default Value

NA

View

Global configuration view

Usage Guidelines

This command can delete global dynamic MAC address entries or specific dynamic MAC address entries according to the VLAN, VLAN+MAC address, MAC address, interface, or slot.

Example

Clear all dynamic MAC address entries.

```
Switch(config)#no mac-address dynamic
Switch(config)#
```

3.2.18 mac-limit

Function

The **mac-limit** command sets a MAC address learning limit.

The **mac-limit action** command sets a MAC address learning limit and action for handling packets beyond the limit.

Format

- **mac-limit** { *limit-value* | **default** }
- **mac-limit** { *limit-value* | **default** } **action** { **forward** | **drop** }

Parameter

Parameter	Description	Value
limit-value	Specifies the maximum number of MAC addresses that can be learned. The value 0	The value is an integer ranging from 0 to 98304.

Parameter	Description	Value
	indicates that the number of learned MAC addresses is not limited.	

Default Value

By default, the number of learned MAC addresses is not limited.

View

Interface configuration view (Trunk), Ethernet bridge interface configuration view, VLAN configuration view

Usage Guidelines

This command limits the number of MAC address entries learned in the system, thereby controlling the number of access users or preventing attacks to the MAC address table.

Example

Set the maximum number of MAC addresses that can be learned on interfaces in VLAN 1 to 1000. That is, packets carrying new MAC addresses will be dropped after 1000 MAC addresses are learned.

```
Switch(config-eth-trunk1)#mac-limit 1000 action drop
Switch(config-eth-trunk1)#
```

3.2.19 reset mac-address flapping record

Function

The **reset mac-address flapping record** command clears the MAC address flapping record.

Format

reset mac-address flapping record

Parameter

NA

Default Value

NA

View

Global configuration view

Usage Guidelines

NA

Example

Clear the MAC address flapping record.

```
Switch(config)# reset mac-address flapping record
Switch(config)#
```

3.2.20 reset mac-address notification history

Function

The **reset mac-address notification history** command clears the MAC address notification history.

Format

reset mac-address notification history

Parameter

NA

Default Value

NA

View

Global configuration view

Usage Guidelines

NA

Example

Clear the MAC address notification history.

```
Switch(config)# reset mac-address notification history
Switch(config)#
```

3.2.21 mac-address flapping detection {enable|disable}

Function

The **mac-address flapping detection {enable|disable}** command enables or disables global MAC address flapping detection.

Format

mac-address flapping detection { enable | disable }**Parameter**

Parameter	Description	Value
enable	Enables global MAC address flapping detection.	-
disable	Disables global MAC address flapping detection.	-

Default Value

Global MAC address flapping detection is enabled by default.

View

Global configuration view

Usage Guidelines

NA

Example

Enable global MAC address flapping detection.

```
Switch(config)#mac-address flapping detection enable
Switch(config)#
```

3.2.22 mac-address flapping aging-time**Function**

The **mac-address flapping aging-time** command sets the aging time for MAC address flapping entries.

Format

mac-address flapping aging-time { aging-time | default }

Parameter

Parameter	Description	Value
aging-time	Sets the aging time for MAC address flapping entries.	The value is an integer ranging from 60 to 900, in seconds.
default	Sets the default aging time for MAC address flapping entries.	300 seconds

Default Value

300 seconds

View

Global configuration view

Usage Guidelines

NA

Example

Set the aging time for MAC address flapping entries.

```
Switch(config)#mac-address flapping aging-time 100
Switch(config)#
```

3.2.23 mac-address flapping detection exclude-vlan**Function**

The **mac-address flapping detection exclude-vlan** command sets a VLAN whitelist for MAC address flapping detection.

Format

mac-address flapping detection exclude-vlan *vlan-id*

Parameter

Parameter	Description	Value
vlan-id	Sets a VLAN whitelist for MAC address flapping detection.	The value is an integer ranging from 1 to 4094.

Default Value

NA

View

Global configuration view

Usage Guidelines

NA

Example

Add VLAN100 to the VLAN whitelist for MAC address flapping detection.

```
Switch(config)#mac-address flapping detection exclude-vlan 100
Switch(config)#
```

3.2.24 mac-address flapping detection vlan security-level

Function

The **mac-address flapping detection vlan security-level** command sets the security level of MAC address flapping detection in VLAN.

Format

mac-address flapping detection vlan *vlan-id* **security-level** { **high** | **middle** | **low** }

Parameter

Parameter	Description	Value
vlan-id	Sets a VLAN whitelist for MAC address flapping detection.	The value is an integer ranging from 1 to 4094.
high	Sets the security level to high, which indicates that when the MAC address shifts for three times, the system regards that the MAC address has flapped.	-
middle	Sets the security level to middle, which indicates that when the MAC address shifts for 10 times, the system regards that the MAC address has flapped.	-
low	Sets the security level to low, which indicates that when the MAC address shifts for 50 times, the system regards that the MAC address has flapped.	-

Default Value

NA

View

Global configuration view

Usage Guidelines

NA

Example

Set the security level to low.

```
Switch(config)#mac-address flapping detection vlan security-level low
Switch(config)#
```

3.2.25 mac-address notification interval

Function

The **mac-address notification interval** command sets the interval for MAC address change notification.

Format

mac-address notification interval { *interval-value* | **default** }

Parameter

Parameter	Description	Value
interval-value	Specifies the interval for MAC address change notification.	The value is an integer ranging from 10 to 1000, in seconds.
default	Specifies the default value.	30 seconds

Default Value

30 seconds

View

Global configuration view

Usage Guidelines

When MAC address notification is enabled for the port, after the port learns a new MAC address or a MAC address is deleted, the change is recorded and notified to Trap Server after the notification interval.

Example

Set the interval to 60s.

```
Switch(config)#mac-address notification interval 60
Switch(config)#
```

3.2.26 mac-address notification history-size

Function

The **mac-address notification history-size** command sets the size of the MAC address adding or deletion record.

Format

mac-address notification history-size { *history-size* | **default** }

Parameter

Parameter	Description	Value

Parameter	Description	Value
history-size	Specifies the number of MAC address adding and deletion records.	The value is an integer ranging from 1 to 128.
default	Specifies the default value.	60 seconds

Default Value

30 seconds

View

Global configuration view

Usage Guidelines

NA

Example

Set the number of MAC address adding and deletion records to 50.

```
Switch(config)# mac-address notification history-size 50
Switch(config)#
```

3.2.27 mac-address flapping quit-vlan recover-time

Function

The **mac-address flapping quit-vlan recover-time** command sets the time for automatically reconnecting a port to the VLAN after it is disconnected from the VLAN due to MAC address flapping.

Format

mac-address flapping quit-vlan recover-time { *time* | **default** }

Parameter

Parameter	Description	Value
time	Specifies the automatic restoration time.	The value is an integer ranging from 0 to 1440.
default	Specifies the default priority of the automatic restoration time.	0 indicates no restoration. The default value is 10 minutes.

Default Value

10

View

Global configuration view

Usage Guidelines

NA

Example

Set the automatic restoration time to 10 minutes.

```
Switch(config)#mac-address flapping quit-vlan recover-time 10
Switch(config)#
```

3.2.28 mac-address static

Function

The **mac-address static** command creates a static MAC address entry.

Format

- **mac-address static** *vlan-id mac-address { ethernet | xgigaethernet | 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet } interface-number*
- **mac-address static** *vlan-id mac-address eth-trunk trunk-number*

Parameter

Parameter	Description	Value
vlan-id	Specifies a VLAN ID.	The value is an integer ranging from 1 to 4094.
mac-address	Specifies a unicast MAC address.	The format is H-H-H. "H" is a four-digit hexadecimal number. You can enter 1-4 digits for each H, for example, 00e0 and fc01. If you enter fewer than four digits, 0s will be appended before the digits. For example, if you enter e0, the final value will be 00e0. The MAC address cannot be set to FFFF-FFFF-FFFF.
interface-number	Specifies an Ethernet interface number.	The value is an integer in the range of <1-1>/<0-1>/<1-48>.
trunk-number	Specifies the number of an aggregation interface.	The value is an integer ranging from 1 to 128.

Default Value

By default, no static MAC address entries are configured in the system.

View

Global configuration view

Usage Guidelines

NA

Example

Create a static MAC address entry in VLAN 2, with destination MAC address 00:02:00:02:00:02, and outbound interface xgigaethernet 1/0/1. That is, frames with destination MAC address 00:02:00:02:00:02 and belonging to VLAN 2 will be forwarded through outbound interface xgigaethernet 1/0/1.

```
Switch(config)#mac-address static 2 00:02:00:02:00:02 xgigaethernet 1/0/1
Switch(config)#
```

3.2.29 show mac-address l3**Function**

The **show mac-address l3** command displays the MAC address of a Layer-3 interface.

Format

show mac-address l3

Parameter

NA

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

View the MAC addresses of a Layer-3 interface.

```
Switch>show mac-address l3

L3          :3

MAC Address      Vlan/Vsi/BD Interface  Oper-Type  Type
34:61:31:35:33:36  1/--/--  cpu        cpu-only      l3Mac
```

```

00:04:67:12:34:11  200/--/--  vlan200      cpu-only      l3Mac
34:61:31:35:33:36  --/--/1    cpu         cpu-only      l3Mac
Switch>

```

3.2.30 show mac-address bridge-domain

Function

The **show mac-address bridge-domain** command displays the MAC bridge domain range.

Format

show mac-address bridge-domain *domain-id*

Parameter

Parameter	Description	Value
domain-id	Specifies the bridge domain range.	The value is an integer ranging from 1 to 16777215.

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

View the MAC bridge domain range.

```

Switch>show mac-address bridge-domain 1
Switch>

```

3.3 ARP Configuration Commands

3.3.1 arp detect-mode unicast

Function

The **arp detect-mode unicast** command enables or disables unicast ARP aging detection.

Format

arp detect-mode unicast { **enable** | **disable** }

Parameter

Parameter	Description	Value
enable	Enables unicast ARP aging detection.	-
disable	Disables unicast ARP aging detection.	-

Default Value

By default, unicast ARP aging detection is disabled.

View

Global configuration view, VLANIF configuration view, Ethernet bridge interface configuration view, Ethernet routing interface configuration view, and interface configuration view (Trunk)

Usage Guidelines

NA

Example

Enable unicast ARP aging detection.

```
Switch(config-10ge1/0/1)#arp detect-mode unicast enable
```

```
Switch(config-10ge1/0/1)#
```

3.3.2 arp-limit maxnum**Function**

The **arp-limit maxnum** command sets the maximum number of dynamic ARP entries that can be learned on a VLAN interface.

The **no arp-limit** command cancels the limit on the number of dynamic ARP entries that can be learned on a VLAN interface.

Format

- **arp-limit maxnum** *max-num*
- **no arp-limit**

Parameter

Parameter	Description	Value
max-num	Specifies the maximum number of dynamic ARP mapping entries that can be learned by a port.	The value is an integer ranging from 1 to 49152.

Default Value

The number of dynamically learned ARP mapping entries is not limited by default.

View

VLANIF configuration view

Usage Guidelines

After this command is run for a port, if the number of ARP mapping entries learned by a port exceeds the value specified by this command, the system stops learning new ARP entries, retains the learned ARP mapping entries, and notifies the user that the learned number has exceeded the limit.

Example

Set the maximum number of dynamic ARP entries learned on VLAN interface 2 to 10.

```
Switch(config-vlanif-2)#arp-limit maxnum 10
Switch(config-vlanif-2)#
```

3.3.3 arp-limit vlan maxnum

Function

The **arp-limit vlan maxnum** command sets the maximum number of dynamic ARP entries that can be learned on an Ethernet interface.

The **no arp-limit vlan** command cancels the limit on the number of dynamic ARP entries that can be learned on an Ethernet interface.

Format

- **arp-limit vlan** *vlan-id* **maxnum** *maxnum*
- **no arp-limit vlan** *vlan-id*

Parameter

Parameter	Description	Value
vlan-id	Specifies the VLAN that limits the learning of dynamic ARP entries.	The value is an integer ranging from 1 to 4094.
maxnum	Specifies the maximum number of dynamic ARP mapping entries that can be learned by a port.	The value is an integer ranging from 1 to 49152.

Default Value

The number of dynamically learned ARP mapping entries is not limited by default.

View

Ethernet bridge interface configuration view, interface configuration view (Trunk)

Usage Guidelines

After this command is run for a port, if the number of ARP mapping entries learned by the port exceeds the value specified by this command, the system stops learning new ARP entries, retains the learned ARP mapping entries, and notifies the user that the learned number has exceeded the limit.

Example

Set the maximum dynamic ARP entries that can be learned by Ethernet interface **xgigaethernet 1/0/7** from **vlan 10** to 10.

```
Switch(config-10ge1/0/7)#arp-limit vlan 10 maxnum 10
Switch(config-10ge1/0/7)#
```

3.3.4 arp direct-route {enable|disable}**Function**

The **arp direct-route {enable | disable}** command enables the ARP module to forward host routes or disables such forwarding.

Format

arp direct-route { enable | disable }

Parameter

Parameter	Description	Value
enable	Enables the ARP module to forward host routes.	-
disable	Disables host route forwarding.	-

Default Value

The host route forwarding function is disabled by default.

View

VLANIF configuration view, BD interface configuration view

Usage Guidelines

NA

Example

Enable the ARP module to forward host routes.

```
Switch(config-vlanif-10)#arp direct-route enable
```

3.3.5 show ip arp

Function

The **show ip arp** command displays the ARP information, including the ARP dynamic address count and aging time of the ARP mapping entries. Configuration under multi-instance VPN is also supported.

Format

- **show ip arp**
- **show ip arp *ip-address***
- **show ip arp dynamic**
- **show ip arp static**
- **show ip arp { ethernet | xgigaethernet | 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet } *interface-number***
- **show ip arp eth-trunk *trunk-number***
- **show ip arp vpn-instance *name***
- **show ip arp vpn-instance**

Parameter

Parameter	Description	Value
vlan-id	Specifies a VLAN ID.	The value is an integer ranging from 1 to 4094.
interface-number	Specifies the Ethernet interface number in the static ARP entry.	The value is an integer in the range of <1-1>/<0-1>/<1-48>.
trunk-number	Specifies the trunk interface number in the static ARP entry.	The value is an integer ranging from 1 to 128.
name	Specifies a VPN instance name.	The value is a string of up to 64 characters.

View

Common user view

Usage Guidelines

You can use this command to check the numbers of ARP entries on different interfaces and specific ARP entries.

Example

Display ARP information on the switch.


```
Switch>show ip arp
```

```
Arp aging time: 1200(s)
```

Destination	Mac-addr	Type	Aging	Vlan	Interface	Vpn-instance
10.1.3.1	04f8:f8e5:b8ba	if	never	300	vlan300	N/A
10.1.3.2	0010:9400:0003	dynamic	965	300	10ge1/0/48	N/A
150.1.1.101	6821:5fdc:2300	dynamic	1194	N/A	mgt-eth0/0/0	N/A
150.1.1.102	04f8:f8e5:b8ba	if	never	1	mgt-eth0/0/0	N/A
150.1.1.103	803a:f440:a6b6	dynamic	1145	N/A	mgt-eth0/0/0	N/A
150.1.1.254	0050:5690:9dc3	dynamic	1177	N/A	mgt-eth0/0/0	N/A

```
Total: 6      Dynamic: 4      Static: 0      Other: 2
```

```
Switch>
```

3.3.6 show arp-limit maxnum

Function

The **show arp-limit maxnum** command sets the maximum number of dynamic ARP entries that can be learned on each interface.

Format

Common user view

- **show arp-limit maxnum vlan** *vlan-id*

Common user view, Ethernet routing interface configuration view

- **show arp-limit maxnum { ethernet | xgigaethernet | 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet } interface-number**
- **show arp-limit maxnum { ethernet | xgigaethernet | 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet } interface-number.channel-number**
- **show arp-limit maxnum eth-trunk** *trunk-number*
- **show arp-limit maxnum**

Parameter

Parameter	Description	Value
vlan-id	Specifies a VLAN ID.	The value is an integer ranging from 1 to 4094.
interface-number	Specifies an Ethernet interface number.	The value is an integer in the range of <1-1>/<0-1>/<1-48>.
trunk-number	Specifies the number of a Trunk interface.	The value is an integer ranging from 1 to 128.

Default Value

NA

View

Common user view, Ethernet routing interface configuration view

Usage Guidelines

You can use this command to check the numbers of ARP entries on different interfaces and specific ARP entries.

Example

Display ARP information on the switch.

```
Switch>show arp-limit maxnum
```

Interface	Vlan	Maxnum	LearnedNum
Vlanif100	0	1000	0
GigabitEthernet1/0/1	10	10	0
GigabitEthernet1/0/1	2	20	0

```
Switch>
```

3.3.7 show arp-probe config**Function**

The **show arp-probe config** command displays the ARP probing configuration.

Format

show arp-probe config

Parameter

NA

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

Clear all dynamic ARP mapping entries.

```
Switch>show arp-probe config
Switch>
```

3.3.8 show arp-probe database**Function**

The **show arp-probe database** command displays major content of all ARP entries reported by the kernel or obtained through active/standby synchronization.

Format

- **show arp-probe database**
- **show arp-probe { arp | nd } database**
- **show arp-probe database dst-ip** *dst-ip*
- **show arp-probe database dst-ip6** *dst-ip6*
- **show arp-probe database verbose**

Parameter

Parameter	Description	Value
dst-ip	Specifies a destination IP address.	The value is in dotted decimal notation.
dst-ip6	Specifies a destination IPv6 address.	In this format, a 128-digit IP address is divided into 8 segments. Each segment consists of 16 digits and is represented by 4 hexadecimal characters (0-9 and A-F). Segments are separated by colons (:).

Default Value

NA

View

Common user view

Usage Guidelines

You can use this command to view all ARP entry information notified by the kernel or obtained through active/standby synchronization.

Example

Display major content of all entries.

```
Switch>show arp-probe database
```

Dst-ip	Mac	Interface	Port	State
10.82.1.28	44:8A:5B:78:BF:A7	vlan-1	ge-1/0/29	reachable
10.82.1.86	C8:9C:DC:35:F2:43	vlan-1	ge-1/0/29	reachable
10.82.1.254	00:00:5E:00:01:52	vlan-1	ge-1/0/29	reachable
10.82.11.199	44:8A:5B:78:BF:BE	vlan-1	ge-1/0/29	reachable
10.82.20.62	1C:CD:E5:42:0E:DB	vlan-1	ge-1/0/29	reachable
10.82.20.76	44:8A:5B:78:B8:85	vlan-1	ge-1/0/29	reachable
10.82.20.95	C8:9C:DC:35:F1:83	vlan-1	ge-1/0/29	reachable
10.82.20.103	00:01:6C:46:F3:7D	vlan-1	ge-1/0/29	reachable
10.82.20.120	D4:3D:7E:A8:67:88	vlan-1	ge-1/0/29	reachable
10.82.20.138	D0:FC:CC:4F:30:F0	vlan-1	ge-1/0/29	reachable
10.82.20.147	44:8A:5B:0F:9D:71	vlan-1	ge-1/0/29	reachable
10.82.20.165	C8:9C:DC:35:F1:F8	vlan-1	ge-1/0/29	reachable
10.82.20.176	8C:89:A5:91:81:18	vlan-1	ge-1/0/29	reachable
10.82.20.182	44:8A:5B:78:BF:4C	vlan-1	ge-1/0/29	reachable
10.82.20.193	00:01:6C:47:2F:9C	vlan-1	ge-1/0/29	reachable
10.82.20.200	D4:3D:7E:68:3E:5E	vlan-1	ge-1/0/29	reachable
10.82.20.202	44:8A:5B:78:BE:FF	vlan-1	ge-1/0/29	reachable
10.82.22.56	D4:3D:7E:67:46:36	vlan-1	ge-1/0/29	reachable
10.82.90.251	00:23:24:87:01:D8	vlan-1	ge-1/0/29	reachable
10.82.93.251	90:FB:A6:0C:61:92	vlan-1	ge-1/0/29	reachable
10.82.251.248	44:87:FC:CC:74:A7	vlan-1	ge-1/0/29	reachable

```
Switch>
```

3.3.9 show arp-probe global**Function**

The **show arp-probe global** command displays global information and relevant statistics.

Format

show arp-probe global

Parameter

NA

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

Display global information and relevant statistics.

```
Switch>show arp-probe global
  Version                : ARPPROBE_VL3.00.03.00
  Max ARP Num             : 10240
  Current ARP Num         : 0
  Max Interface Num       : 512
  Current Interface Num   : 0
  Synchronous Add Num     : 0
  Synchronous Add Failed Num : 0
  Synchronous Del Num     : 0
  Synchronous Del Failed Num : 0
  Synchronous Recv Add Num : 0
  Synchronous Recv Add Failed Num : 0
  Synchronous Recv Del Num : 0
  Synchronous Recv Del Failed Num : 0
  Pkt Send Num            : 0
  Pkt Send Failed Num     : 0
  Sys Recv Add Num        : 0
  Sys Recv Add Failed Num : 0
  Sys Recv Del Num        : 0
  Sys Recv Del Failed Num : 0
  Sys Add Num             : 0
  Sys Add Failed Num      : 0
  Sys Del Num             : 0
Switch#
```

3.3.10 debug arp {in|out|error|all}**Function**

The **debug arp {in|out|error| all}** command enables debugging for received and sent ARP packets.

The **no debug arp {in|out|error| all}** command disables debugging for received and sent ARP packets.

Format

- **debug arp { in | out | error | all }**
- **no debug arp { in | out | error | all }**

Parameter

Parameter	Description	Value
in	Displays debugging information about received ARP packets.	-
out	Displays debugging information about sent ARP packets.	-
error	Displays debugging information about error ARP packets.	-
all	Displays debugging information about all ARP packets.	-

Default Value

By default, debugging for received and sent ARP packets is disabled.

View

Privileged user view

Usage Guidelines

NA

Example

Enable debugging for received and sent ARP packets.

```
Switch#debug arp in
[ARP];info=receive request 10.18.12.101 not target for me and no found arp proxy,discard packet
...
Switch#
```

3.3.11 debug arp dst-addr

Function

The **debug arp dst-addr** command enables the debugging for sent and received ARP packets with the specified destination IP address.

The **no debug arp dst-addr** command disables the debugging for sent and received ARP packets with the specified destination IP address.

Format

- **debug arp dst-addr *dst-addr***
- **no debug arp dst-addr**

Parameter

Parameter	Description	Value
dst-addr	Specifies a destination IP address.	The value is in dotted decimal notation.

Default Value

By default, debugging for received and sent ARP packets with the specified destination IP address is disabled.

View

Privileged user view

Usage Guidelines

NA

Example

Enable the debugging for sent and received ARP packets with the specified destination IP address.

```
Switch#debug arp dst-addr 10.12.3.23
Switch#
```

3.3.12 debug arp src-addr**Function**

The **debug arp src-addr** command enables the debugging for sent and received ARP packets with the specified source IP address.

The **no debug arp src-addr** command disables the debugging for sent and received ARP packets with the specified source IP address.

Format

- **debug arp src-addr** *source-address*
- **no debug arp src-addr**

Parameter

Parameter	Description	Value
source-address	Specifies a source IP address.	The value is in dotted decimal notation.

Default Value

By default, debugging for received and sent ARP packets with the specified source IP address is disabled.

View

Privileged user view

Usage Guidelines

NA

Example

Enable the debugging for sent and received ARP packets with the specified source IP address.

```
Switch#debug arp src-addr 10.12.3.23
Switch#
```

3.3.13 debug arp-probe

Function

The **debug arp-probe** command enables ARP detection and entry synchronous debugging.

The **no debug arp-probe** command disables ARP detection and entry synchronous debugging.

Format

- **debug arp-probe { rtm | sync | tx | error | all }**
- **no debug arp-probe { rtm | sync | tx | error | all }**

Parameter

Parameter	Description	Value
rtm	Displays debugging information about event notifications and processing of ARP entries sent to the kernel.	-
sync	Displays debugging information about ARP entry synchronization.	-
tx	Displays debugging information about probe packet sending.	-
error	Displays debugging information about errors.	-
all	Displays all debugging information about ARP probing and entry synchronization.	-

Default Value

ARP detection and entry synchronous debugging is disabled by default.

View

Privileged user view

Usage Guidelines

NA

Example

Disable ARP detection and entry synchronous debugging.

```
Switch#no debug arp-probe all
Switch#
```

3.3.14 ip arp

Function

The **ip arp** command creates a static ARP entry on an Ethernet interface or trunk interface. Configuration under multi-instance VPN is also supported.

The **no ip arp** command deletes a static ARP entry.

Format

- **ip arp** *ip-address mac-address* { **ethernet** | **xgigaethernet** | **10gigaethernet** | **25gigaethernet** | **40gigaethernet** | **100gigaethernet** } *interface-number*
- **ip arp** *ip-address mac-address* { **ethernet** | **xgigaethernet** | **10gigaethernet** | **25gigaethernet** | **40gigaethernet** | **100gigaethernet** } *interface-number* **vlan** *vlan-id* **inner-vlan** *inner-vid* **vpn-instance** *name*
- **ip arp** *ip-address mac-address* { **ethernet** | **xgigaethernet** | **10gigaethernet** | **25gigaethernet** | **40gigaethernet** | **100gigaethernet** } *interface-number.subinterface* **vlan** *vlan-id*
- **ip arp** *ip-address mac-address* { **ethernet** | **xgigaethernet** | **10gigaethernet** | **25gigaethernet** | **40gigaethernet** | **100gigaethernet** } *interface-number.subinterface* **vlan** *vlan-id* **vpn-instance** *name*
- **ip arp** *ip-address mac-address* { **ethernet** | **xgigaethernet** | **10gigaethernet** | **25gigaethernet** | **40gigaethernet** | **100gigaethernet** } *interface-number.subinterface* **vlan** *vlan-id* **inner-vlan** *inner-vid*
- **ip arp** *ip-address mac-address* { **ethernet** | **xgigaethernet** | **10gigaethernet** | **25gigaethernet** | **40gigaethernet** | **100gigaethernet** } *interface-number.subinterface* **vlan** *vlan-id* **inner-vlan** *inner-vid* **vpn-instance** *name*
- **ip arp** *ip-address mac-address* **eth-trunk** *trunk-number*

- **ip arp** *ip-address mac-address eth-trunk trunk-number vpn-instance name*
- **ip arp** *ip-address mac-address vlan vlan-id*
- **ip arp** *ip-address mac-address vlan vlan-id vpn-instance name*
- **ip arp** *ip-address mac-address vlan vlan-id inner-vlan inner-vid*
- **ip arp** *ip-address mac-address vlan vlan-id inner-vlan inner-vid vpn-instance name*
- **ip arp** *ip-address mac-address*
- **ip arp** *ip-address mac-address vpn-instance name*
- **no ip arp** *ip-address*
- **no ip arp** *ip-address vpn-instance name*

Parameter

Parameter	Description	Value
ip-address	Specifies an IP address in the static ARP entry.	The value is in dotted decimal notation.
mac-address	Specifies a MAC address in the static ARP entry.	The format is AA:BB:CC:DD:EE:FF, where A to F are hexadecimal digits.
interface-number	Specifies an Ethernet interface number in the static ARP entry.	The value is an integer in the range of <1-1>/<0-1>/<1-48>.
trunk-number	Specifies the trunk interface number in the static ARP entry.	The value is an integer ranging from 1 to 128.
name	Specifies a VPN instance name.	The value is a string of up to 64 characters.
vlan-id	Specifies an outer VLAN ID.	The value is an integer ranging from 1 to 4094.
inner-vid	Specifies an inner VLAN ID.	The value is an integer ranging from 1 to 4094.

Default Value

By default, the system has no ARP entries and learns MAC and IP address mappings through dynamic ARP.

View

Global configuration view

Usage Guidelines

Static ARP entries can only be deleted manually, and will not be aged out or updated dynamically. These static ARP entries are always effective during normal operation of the switch.

The IP address specified in a static ARP entry must be on the same network segment as the local IP address in the VLAN and cannot be the same as the local IP address.

The interface specified by *trunk-number* must be added to the VLAN on the same network segment as the IP address in the static ARP entry.



Note:

The *ip-address* specified in the command must be on the same network segment as the IP address of a port specified by *interface-number*.

ARP entries apply only to local area networks.

Currently, the switch does not support static ARP entry configuration on member interfaces off a trunk interface.

Example

Configure the VPN instance **fh** and bind it with an ARP entry, in which the IP address is 10.18.2.123, the MAC address is 00:04:67:00:00:01, and outbound interface is xgigaethernet 1/0/1.

```
Switch(config-vlanif-3)#ip address 10.18.2.1/24
Switch(config-vlanif-3)#quit
Switch(config)#ip arp 10.18.2.123 00:04:67:00:00:01 xgigaethernet 1/0/1 vpn-instance fh
Switch(config)#
```

3.3.15 ip arp vni source-ip peer-ip

Function

The **ip arp vni source-ip peer-ip** command creates a VXLAN static ARP entry.

Format

- **ip arp** *ip-address mac-address vni vni-number source-ip source-ip peer-ip destination-ip*
- **ip arp** *ip-address mac-address vni vni-number source-ip source-ip peer-ip destination-ip vpn-instance name*

Parameter

Parameter	Description	Value
ip-address	Specifies an IP address.	The value is in dotted decimal notation.
mac-address	Specifies a MAC address.	-
vni-number	Specifies a VXLAN network identifier (VNI).	The value ranges from 1 to 16777215.

Parameter	Description	Value
source-ip	Specifies the source IP address of a tunnel.	The value is in dotted decimal notation.
destination-ip	Specifies the destination IP address of a tunnel.	The value is in dotted decimal notation.
name	Specifies a VPN instance name.	The value is a character string.

Default Value

NA

View

Global configuration view

Usage Guidelines

NA

Example

Create a VXLAN static ARP entry.

```
Switch(config)#ip arp 1.1.1.1 00:00:00:00:00:01 vni 1 source-ip 10.18.1.12 10.18.1.13
Switch(config)#
```

3.3.16 ip arp detect {enable|disable}

Function

The **ip arp detect {enable|disable}** command enables or disables automatic ARP probing.

Format

ip arp detect {enable|disable}

Parameter

Parameter	Description	Value
enable	Enables automatic ARP probing.	-
disable	Disables automatic ARP probing.	-

Default Value

By default, automatic ARP probing is enabled.

View

Global configuration view

Usage Guidelines

NA

Example

Disable automatic ARP probing.

```
Switch(config)#ip arp detect disable
Switch(config)#
```

3.3.17 ip arp detect-times

Function

The **ip arp detect-times** command sets the number of aging probes for dynamic ARP entries.

Format

ip arp detect-times { *times-num* | **default** }

Parameter

Parameter	Description	Value
times-num	Specifies the number of aging probes for dynamic ARP entries.	The value is an integer ranging from 0 to 10.
default	Specifies the default number of aging detection times for dynamic ARP entries.	3

Default Value

By default, the number of aging probes for dynamic ARP entries is 3.

View

Global configuration view

Usage Guidelines

NA

Example

Set the number of aging probes for dynamic ARP entries to 5.

```
Switch(config)#ip arp detect-times 5
Switch(config)#
```

3.3.18 ip arp aging-time

Function

The **ip arp aging-time** command sets the aging time of dynamic ARP entries.

The **no ip arp aging-time** command restores the aging time of dynamic ARP entries to the default value.

Format

ip arp aging-time { *aging-time* | **default** }

Parameter

Parameter	Description	Value
aging-time	Specifies the aging time of dynamic ARP entries.	The value is an integer ranging from 60 to 86400, in seconds.
default	Default Value	1200 seconds

Default Value

The default aging time of dynamic ARP entries is 1200 seconds.

View

Global configuration view

Usage Guidelines

Setting an appropriate aging time of dynamic ARP entries can reduce the address resolution errors caused by slow updates of dynamic ARP entries.

Example

Set the aging time of dynamic ARP entries to 300 seconds.

```
Switch(config)#ip arp aging-time 300
Switch(config)#
```

3.3.19 debug arp l2-proxy

Function

The **debug arp l2-proxy** command enables ARP layer-2 proxy debugging.

The **no debug arp l2-proxy** command disables ARP layer-2 proxy debugging.

Format

- **debug arp l2-proxy**
- **no debug arp l2-proxy**

Parameter

NA

Default Value

Disable

View

Privileged user view

Usage Guidelines

NA

Example

Enable ARP layer-2 proxy debugging.

Switch#debug arp l2-proxy

Switch#

3.3.20 show arp l2-proxy**Function**The **show arp l2-proxy** command displays the ARP layer-2 proxy entries.The **show arp l2-proxy config** command displays the ARP layer-2 proxy configuration.**Format**

- **show arp l2-proxy**
- **show arp l2-proxy config**

Parameter

NA

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

View the ARP layer-2 proxy configuration.

```
Switch>show arp l2-proxy config
Switch>
```

3.3.21 arp l2-proxy timeout**Function**

The **arp l2-proxy timeout** command sets the aging time for ARP Snooping entries.

Format

arp l2-proxy timeout *timeout-value*

Parameter

Parameter	Description	Value
timeout-value	Specifies the aging time for ARP Snooping entries.	The value is an integer ranging from 0 to 10000.

Default Value

NA

View

Global configuration view

Usage Guidelines

NA

Example

Set the aging time for ARP Snooping entries.

```
Switch(config)#arp l2-proxy timeout 1000
Switch(config)#
```

3.3.22 flush arp l2-proxy all**Function**

The **flush arp l2-proxy all** command clears the ARP Snooping entries.

Format

flush arp l2-proxy all

Parameter

NA

Default Value

NA

View

Global configuration view

Usage Guidelines

NA

Example

Clear the ARP Snooping entries.

```
Switch(config)#flush arp l2-proxy all
Switch(config)#
```

3.3.23 arp broadcast-suppress {enable|disable}**Function**

The **arp broadcast-suppress {enable|disable}** command enables or disables the ARP broadcast suppression function.

Format**arp broadcast-suppress { enable | disable }****Parameter**

Parameter	Description	Value
enable	Enables the ARP broadcast suppression function.	-
disable	Disables the ARP broadcast suppression function.	-

Default Value

Disable

View

VLAN configuration view, BD configuration view

Usage Guidelines

After this function is enabled, when the device receives an ARP broadcast packet, the device converts the packet into a unicast packet and sends the packet, to reduce the number of broadcast packets in the BD domain and network congestion.

Example

Enable the ARP broadcast suppression function.

```
Switch(config-bridge-domain-1)#arp broadcast-suppress enable
Switch(config-bridge-domain-1)#
```

3.3.24 arp collect-host {enable|disable}

Function

The **arp collect-host {enable|disable}** command enables or disables collecting host information based on the BD granularity for BGP EVPN.

Format

arp collect-host { enable | disable }

Parameter

Parameter	Description	Value
enable	Enables collecting host information based on the BD granularity for BGP EVPN.	-
disable	Disables collecting host information based on the BD granularity for BGP EVPN.	-

Default Value

Disable

View

VLAN configuration view, BD configuration view

Usage Guidelines

Before running this command, run **arp l2-proxy enable** to enable the ARP layer-2 proxy function.

Example

Enable collecting host information based on the BD granularity for BGP EVPN.

```
Switch(config-bridge-domain-1)#arp collect-host enable
Switch(config-bridge-domain-1)#
```

3.3.25 arp l2-proxy {enable|disable}

Function

The **arp l2-proxy {enable|disable}** command enables or disables the ARP layer-2 proxy function.

Format

arp l2-proxy { enable | disable }

Parameter

Parameter	Description	Value
enable	Enables the ARP layer-2 proxy function.	-
disable	Disables the ARP layer-2 proxy function.	-

Default Value

Disable

View

VLAN configuration view, BD configuration view

Usage Guidelines

NA

Example

Enable the ARP layer-2 proxy function.

```
Switch(vlan-1)#arp l2-proxy enable
Switch(vlan-1)#
```

3.3.26 arp l2-proxy gateway-mac {enable|disable}

Function

The **arp l2-proxy gateway-mac {enable|disable}** command enables or disables using gateway as proxy for the ARP agent.

Format

arp l2-proxy gateway-mac { enable | disable }

Parameter

Parameter	Description	Value
enable	Enables using gateway as proxy for the ARP agent.	-
disable	Disables using gateway as proxy for the ARP agent.	-

Default Value

Disable

View

VLAN configuration view, BD configuration view

Usage Guidelines

Before running this command, you must run **arp broadcast-suppress enable** to enable ARP broadcast suppression.

Example

Enable using gateway as proxy for the ARP agent.

```
Switch(config-bridge-domain-1)#arp l2-proxy gateway-mac enable
Switch(config-bridge-domain-1)#
```

3.3.27 show arp-limit config**Function**

The **show arp-limit config** command displays the maximum number of dynamic ARP configurations that a port can learn.

Format

show arp-limit config

Parameter

NA

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

Display the maximum number of dynamic ARP configurations that a port can learn.

```
Switch>show arp-limit config
Switch>
```

3.3.28 show ip arp bridge-domain

Function

The **show ip arp bridge-domain** command displays the ARP information on the specified bridge domain.

Format

show ip arp bridge-domain *domain-id*

Parameter

Parameter	Description	Value
domain-id	Specifies the ID of the bridge domain.	The value is an integer ranging from 1 to 16777215.

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

View the ARP information on the specified bridge domain.

```
Switch>show ip arp bridge-domain 1
Switch>
```

3.4 Link Aggregation Configuration Commands

3.4.1 add

Function

The **add** command adds a member interface in the trunk interface configuration view.

Format

```
add { ethernet | xgigaethernet | 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet } interface-number
```

Parameter

Parameter	Description	Value
interface-number	Specifies an Ethernet interface number.	The value is an integer in the range of <1-1>/<0-1>/<1-48>.

Default Value

The Trunk group does not contain any member interface by default.

View

Interface configuration view (Trunk), Peerlink configuration view

Usage Guidelines

You can use this command to bind multiple physical interfaces into a logical interface (trunk interface). Each physical interface is called a member interface. Link aggregation technology (trunk) can increase link bandwidth, enhance link reliability, and implement load balancing.

Before running this command, you must run **interface trunk** to create a Trunk interface.

The Switch supports cross-card trunk interfaces. That is, interfaces on different line cards can be bound to one trunk interface.

The Switch supports a maximum of 128 trunk interfaces and allows each trunk interface to have a maximum of 16 member interfaces. Member interfaces of the same trunk interface must have the same settings of the following attributes. Otherwise, they cannot be bound to the same trunk interface.

- Link type
- Speed
- Duplex mode
- Flow control mode

You are also advised to use the same settings for other interface attributes, including but not limited to:

- Rate limits for broadcast, multicast, and unknown unicast packets for storm control
- Dropping of broadcast, multicast, and unknown unicast packets for storm control
- VLAN ID of a ports

- VLAN mapping
- QinQ
- Interface priority
- Whether to allow BPDU packets to pass
- MAC address learning function
- Static multicast group membership

Attributes of member interfaces cannot be changed individually. You can only change the attributes of the trunk interface, which will change the corresponding attributes of all member interfaces.

To ensure normal communication between the devices connected by a trunk link, you must ensure consistent settings of the following physical attributes on both ends in addition to consistent physical attribute settings of trunk member interfaces:

- Number of physical interfaces connected on the two ends
- Rate of physical interfaces connected on the two ends
- Duplex mode of physical interfaces connected on the two ends
- Flow control mode of physical interfaces connected on the two ends

Example

Add member interface gigaethernet1/0/1 to trunk 1.

```
Switch(config-eth-trunk1)#add gigaethernet 1/0/1
Switch(config-trunk1/1)#
```

3.4.2 active-linknumber

Function

The **active-linknumber** command sets the maximum and minimum numbers of active member interfaces in a link aggregation group.

Format

- **active-linknumber min** { *min-number* | **default** }
- **active-linknumber max** { *max-number* | **default** }

Parameter

Parameter	Description	Value

Parameter	Description	Value
min-number default	Specifies the minimum number of active member interfaces.	The value is an integer ranging from 1 to 100. The default value is 1.
max-number default	Specifies the maximum number of active member interfaces.	The value is an integer ranging from 1 to 100. The default value is 16.

Default Value

By default, the minimum number of active interfaces in a link aggregation interface is 1 and the maximum number of active interfaces is 8.

View

Interface configuration view (Trunk), Peerlink configuration view

Usage Guidelines

The number of active member links in a link aggregation group (trunk interface) affects the state and bandwidth of the trunk interface. To ensure stability of the trunk interface, set the minimum or maximum number of active member interfaces, thereby reducing the impact of member link state changes on the trunk interface.

If the number of member links in Up state is smaller than the minimum number, the trunk interface state changes to Down. Setting the minimum value of active links ensures the minimum bandwidth of the trunk interface.

If the number of member links in Up state reaches the maximum value, the bandwidth of the trunk interface will not increase after more member links change to Up state. Setting the maximum number of active links improves network reliability while ensuring sufficient bandwidth on the trunk interface.

The minimum number of active member interfaces must be smaller than the maximum number of active member interfaces that has been configured for the trunk interface.

If the minimum or maximum number of active member interfaces is configured multiple times, the last configuration takes effect.

Example

On trunk 1, set the maximum number of active member interfaces to 6 and the minimum number of active member interfaces to 2.

```
Switch(config-eth-trunk1)#active-linknumber max 6
Switch(config-eth-trunk1)#
Switch(config-eth-trunk1)#active-linknumber min 2
Switch(config-eth-trunk1)#
```


3.4.3 interface eth-trunk

Function

The **interface eth-trunk** command creates a trunk interface and displays the trunk interface configuration view.

The **no interface eth-trunk** command deletes an existing trunk interface.

Format

- **interface eth-trunk** *trunk-number*
- **interface eth-trunk** *trunk-number.channel-number*
- **no interface eth-trunk** *trunk-number*
- **no interface eth-trunk** *trunk-number.channel-number*

Parameter

Parameter	Description	Value
trunk-number	Specifies the number of a Trunk interface.	The value is an integer ranging from 1 to 128.
subinterface-number	Specifies a sub-interface number.	The value is an integer ranging from 1 to 4094.

Default Value

NA

View

Global configuration view

Usage Guidelines

If the specified trunk interface has been created, this command displays the trunk interface configuration view directly.

When you use the **no** form of the command to delete an existing trunk interface, the system first deletes member interfaces of the trunk interface. You do not need to delete the member interfaces manually.

Example

Create trunk 1 and display its configuration view.

```
Switch(config)#interface eth-trunk 1
Switch(config-eth-trunk1)#
```

3.4.4 mode

Function

The **mode** command sets or changes the working mode of a trunk interface.

Format

mode { manual | lacp-static }

Parameter

Parameter	Description	Value
manual	Sets the working mode to manual load balancing.	-
lacp-static	Sets the working mode to static LACP.	-

Default Value

By default, a trunk interface works in manual load balancing mode.

View

Interface configuration view (trunk)

Usage Guidelines

The Switch supports two trunk interface working modes:

Manual load balancing mode: You need to manually create a trunk interface and add member interfaces to it. Multiple member interfaces manually added to the trunk interface can perform load balancing.

Static LACP mode: The two ends of the link use the LACP protocol to negotiate trunk interface parameters and choose active member interfaces to forward data traffic.

Before changing the working mode of a trunk interface, make sure that the trunk interface does not contain any member interfaces.

Example

Create trunk 1 and configure it to work in static LACP mode.

```
Switch(config-eth-trunk1)#mode lacp-static
Switch(config-eth-trunk1)#
```

3.4.5 join eth-trunk

Function

The **join eth-trunk** command adds an interface to a specified trunk interface.

The **no join eth-trunk** command deletes an interface from a specified trunk interface.

Format

- **join eth-trunk** *trunk-number*
- **no join eth-trunk**

Parameter

Parameter	Description	Value
trunk-number	Specifies the number of a Trunk interface.	The value is an integer ranging from 1 to 128.

Default Value

By default, an Ethernet interface does not belong to any trunk interface.

View

Ethernet bridge interface configuration view, Ethernet routing interface configuration view

Usage Guidelines

You can use this command to bind multiple physical interfaces into a logical interface (trunk interface). Each physical interface is called a member interface. Link aggregation technology (trunk) can increase link bandwidth, enhance link reliability, and implement load balancing.

Before using this command, run the **interface trunk** command to create a trunk interface first.

The Switch supports cross-card trunk interfaces. That is, interfaces on different line cards can be bound to one trunk interface.

The Switch supports a maximum of 128 trunk interfaces and allows each trunk interface to have a maximum of 8 member interfaces. Member interfaces of the same trunk interface must have the same settings of the following attributes. Otherwise, they cannot be bound to the same trunk interface.

Link type

Speed

Duplex mode

Flow control mode

You are also advised to use the same settings for other interface attributes, including but not limited to:

Rate limits for broadcast, multicast, and unknown unicast packets for storm control

Dropping of broadcast, multicast, and unknown unicast packets for storm control

VLAN ID of a port

VLAN mapping

QinQ

Interface priority

Whether to allow BPDU packets to pass

MAC address learning function

Static multicast group membership

Attributes of member interfaces cannot be changed individually. You can only change the attributes of the trunk interface, which will change the corresponding attributes of all member interfaces.

To ensure normal communication between the devices connected by a trunk link, you must ensure consistent settings of the following physical attributes on both ends in addition to consistent physical attribute settings of trunk member interfaces:

Number of physical interfaces connected on the two ends

Rate of physical interfaces connected on the two ends

Duplex mode of physical interfaces connected on the two ends

Flow control mode of physical interfaces connected on the two ends

Example

Enter the configuration view of interface xgigaethernet1/0/3 and add it to trunk 1.

```
Switch(config-10ge1/0/3)#join eth-trunk-1
    %Join eth-trunk-1 successfully.
Switch(config-10ge1/0/3)#
```

3.4.6 remove

Function

The **remove** command deletes a member interface from the interface configuration view (Trunk).

Format

- **remove { ethernet | xgigaethernet | 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet } interface-number**
- **remove { ethernet | xgigaethernet | 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet } interface-number to { ethernet | xgigaethernet | 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet } interface-number**

Parameter

Parameter	Description	Value
interface-number	Specifies the number of the Ethernet port.	The value is an integer in the range of <1-1>/<0-1>/<1-48>.

Default Value

The Trunk group does not contain any member interface by default.

View

Interface configuration view (trunk)

Usage Guidelines

NA

Example

Remove member interface gigaehternet1/0/1 to trunk 1.

```
Switch(config-eth-trunk1)#remove gigaehternet 1/0/1
```

```
Switch(config-eth-trunk1)#
```

3.4.7 show interface eth-trunk verbose

Function

The **show interface eth-trunk** command displays the configuration of a trunk interface.

Format

- **show interface eth-trunk trunk-number verbose**
- **show interface eth-trunk verbose**
- **show interface eth-trunk trunk-number**
- **show interface eth-trunk trunk-number config**

Parameter

Parameter	Description	Value
trunk-number	Specifies the number of a Trunk interface.	The value is an integer ranging from 1 to 128.

Default Value

NA

View

Common user view

Usage Guidelines

You can use this command to check the list of physical interfaces bound to a trunk interface and load balancing mode of the trunk interface.

Example

Display the configuration of trunk 1.

```
Switch>show interface eth-trunk verbose
Interface eth-trunk-1:
  Unknown-unicast-Alg:srcdst-mac
  Schedule-Alg:srcdst-mac
  Interface Mode>manual
  Max-BW:(M):6000
  Cur-BW:(M):0
  Port-List:xge 1/0/6, 1/0/5, 1/0/4, 1/0/3, 1/0/2, 1/0/1

Switch>#
```

3.4.8 show interface statistic

Function

The **show interface statistic** command displays statistics on an interface.

Format

- **show interface statistic brief eth-trunk *trunk-number***
- **show interface statistic eth-trunk *trunk-number***

Parameter

Parameter	Description	Value
trunk-number	Specifies the number of a Trunk interface.	The value is an integer ranging from 1 to 128.

Default Value

NA

View

Common user view

Usage Guidelines

Generally, commands described in this section are used to collect traffic statistics or diagnose faults on interfaces.

If you do not specify a slot number when running this command, the command displays statistics about ingress and egress packets on all the working interfaces on the switch in the order of port numbers.

The command output information includes the following:

Port type and number

Total number of packets sent or received by a port

Total number of unicast packets sent or received by a port

Total number of multicast packets sent or received by a port

Total number of broadcast packets sent or received by a port

Total number of error packets sent or received by a port

Example

Display the statistics on Ethernet interface xgigaethernet 1/0/1.

Switch>show interface statistic					
Interface	In(pkts) :Total	UniCast	MultiCast	BroadCast	Err
	Out(pkts):Total	UniCast	MultiCast	BroadCast	Err
xge-1/0/1	0/0	0/0	0/0	0/0	0/0
	0/0	0/0	0/0	0/0	0/0
xge-1/0/2	0/0	0/0	0/0	0/0	0/0
	0/0	0/0	0/0	0/0	0/0
xge-1/0/3	0/0	0/0	0/0	0/0	0/0
	0/0	0/0	0/0	0/0	0/0
xge-1/0/4	0/0	0/0	0/0	0/0	0/0
	0/0	0/0	0/0	0/0	0/0
xge-1/0/5	0/0	0/0	0/0	0/0	0/0
	0/0	0/0	0/0	0/0	0/0
xge-1/0/6	0/0	0/0	0/0	0/0	0/0

	0/0	0/0	0/0	0/0	0/0
xge-1/0/7	0/0	0/0	0/0	0/0	0/0
	0/0	0/0	0/0	0/0	0/0
xge-1/0/8	0/0	0/0	0/0	0/0	0/0
	0/0	0/0	0/0	0/0	0/0
xge-1/0/9	0/0	0/0	0/0	0/0	0/0
	0/0	0/0	0/0	0/0	0/0
xge-1/0/10	0/0	0/0	0/0	0/0	0/0
	0/0	0/0	0/0	0/0	0/0
xge-1/0/11	0/0	0/0	0/0	0/0	0/0
	0/0	0/0	0/0	0/0	0/0
xge-1/0/12	0/0	0/0	0/0	0/0	0/0
	0/0	0/0	0/0	0/0	0/0
xge-1/0/13	0/0	0/0	0/0	0/0	0/0
	0/0	0/0	0/0	0/0	0/0
xge-1/0/14	0/0	0/0	0/0	0/0	0/0
	0/0	0/0	0/0	0/0	0/0
xge-1/0/15	0/0	0/0	0/0	0/0	0/0
	0/0	0/0	0/0	0/0	0/0
xge-1/0/16	0/0	0/0	0/0	0/0	0/0
	0/0	0/0	0/0	0/0	0/0
xge-1/0/17	0/0	0/0	0/0	0/0	0/0
	0/0	0/0	0/0	0/0	0/0
xge-1/0/18	0/0	0/0	0/0	0/0	0/0
	0/0	0/0	0/0	0/0	0/0
xge-1/0/19	0/0	0/0	0/0	0/0	0/0
	0/0	0/0	0/0	0/0	0/0
xge-1/0/20	0/0	0/0	0/0	0/0	0/0
	0/0	0/0	0/0	0/0	0/0
xge-1/0/21	0/0	0/0	0/0	0/0	0/0
	0/0	0/0	0/0	0/0	0/0
xge-1/0/22	0/0	0/0	0/0	0/0	0/0
	0/0	0/0	0/0	0/0	0/0
xge-1/0/23	0/0	0/0	0/0	0/0	0/0
	0/0	0/0	0/0	0/0	0/0
xge-1/0/24	0/0	0/0	0/0	0/0	0/0
	0/0	0/0	0/0	0/0	0/0
Switch>					

3.4.9 debug schedule-profile

Function

The **debug schedule-profile** command enables debugging of the load balancing template.

The **no debug schedule-profile** command disables debugging of the load balancing template.

Format

- **debug schedule-profile { config | event | all }**
- **no debug schedule-profile { config | event | all }**

Parameter

Parameter	Description	Value
config	Specifies the configuration debugging information.	-
event	Specifies the event debugging information.	-
all	Specifies all the debugging information.	-

Default Value

Disable

View

Privileged user view

Usage Guidelines

NA

Example

Enable debugging of the load balancing template.

```
Switch#debug schedule-profile configle
Switch#
```

3.4.10 load-balance

Function

The **load-balance** command sets the load balancing mode for trunk interfaces.

Format

- **load-balance schedule-profile *profile-name***
- **load-balance { src-mac | dst-mac | srcdst-mac | src-ip | dst-ip | srcdst-ip | default }**

Parameter

Parameter	Description	Value
profile-name	Specifies the name of enhanced load balancing profile applied to the trunk interface, valid to all trunk interfaces	The value is a string containing up to 33

Parameter	Description	Value
		characters.
src-mac	Specifies load balancing among trunk member interfaces based on source MAC addresses, valid to all trunk interfaces.	-
dst-mac	Specifies load balancing among trunk member interfaces based on destination MAC addresses, valid to all trunk interfaces.	-
srcdst-mac	Specifies load balancing among trunk member interfaces based on exclusive OR of source and destination MAC addresses, valid to all trunk interfaces.	-
src-ip	Specifies load balancing among trunk member interfaces based on source IP addresses, valid to all trunk interfaces.	-
dst-ip	Specifies load balancing among trunk member interfaces based on destination IP addresses, valid to all trunk interfaces.	-
srcdst-ip	Specifies load balancing among trunk member interfaces based on exclusive OR of source and destination IP addresses, valid to all trunk interfaces.	

Default Value

srcdst-mac

View

Interface configuration view (Trunk), Peerlink configuration view

Usage Guidelines

This command enables data traffic to be distributed on different member links properly and finally reach the same destination, preventing link congestion. Choose an appropriate load balancing mode based on actual situation on your network. Generally, load balancing based on more frequently changing variables can ensure more balanced traffic distribution on member links.

The traffic distribution algorithm configured in global configuration mode is valid to all trunk interfaces.

Load balancing applies only to egress traffic; therefore, different load balancing modes can be set on two ends of the trunk link.

If you run this command multiple times, the last configured load balancing mode takes effect.

Example

Configure global load balancing based on destination IP addresses.

```
Switch(config)#load-balance dst-ip
Switch(config)#
```

3.4.11 ip field

Function

The **ip field** command sets the IPv4 packet load balancing mode in the enhanced template.

The **no ip field** command deletes the IPv4 packet load balancing mode specified in the enhanced template.

Format

- **ip field { src-ip | dst-ip | vlan | l4-srcport | l4-dstport | protocol | src-port | dst-port | all | default }**
- **no ip field { src-ip | dst-ip | vlan | l4-srcport | l4-dstport | protocol | src-port | dst-port }**

Parameter

Parameter	Description	Value
src-ip	Specifies load balancing based on the source IP address.	-
dst-ip	Specifies load balancing based on the destination IP address.	-
vlan	Specifies load balancing based on the VLAN.	-
l4-srcport	Specifies load balancing based on the source port on the transport layer.	-
l4-dstport	Specifies load balancing based on the destination port on the transport layer.	-
protocol	Specifies load balancing based on the protocol.	-
src-port	Specifies load balancing based on the physical source port.	-
dst-port	Specifies load balancing based on the destination physical port.	-
all	Specifies load balancing based on the all of the preceding fields.	-
default	Specifies load balancing based on the source and destination IP addresses by default.	-

Default Value

By default, load balance of IPv4 packets is based on src-ip and dst-ip.

View

Schedule-profile configuration view, ecmp-profile configuration view

Usage Guidelines

NA

Example

Set the load balancing mode of IPv4 packets in the enhanced load balancing template 123 to VLAN-based load balancing.

```
Switch(config-schedule-profile-123)#ip field vlan
Switch(config-schedule-profile-123)#show schedule-profile
```

```

schedule-profile: 1
  Packet      HashField
  L2          src-mac    dst-mac    vlan
  IPV4        src-ip     dst-ip
  IPV6        src-ip     dst-ip
  MPLS        top-label  2nd-label

Trunk interface:
schedule-profile: 123
  Packet      HashField
  L2          src-mac    dst-mac    src-mac    dst-mac    vlan
  IPV4        src-ip     dst-ip     vlan
  IPV6        src-ip     dst-ip
  MPLS        top-label  2nd-label

Trunk interface:
  ecmp load-balance schedule-profile
Switch(config-schedule-profile-123)#

```

3.4.12 ipv6 field

Function

The **ipv6 field** command configures the load balancing mode of IPv6 packets in the enhanced load balancing template.

The **no ipv6 field** command deletes the configured load balancing mode of IPv6 packets in the enhanced load balancing template.

Format

- **ipv6 field { src-ip | dst-ip | srcdst-ip | vlan | l4-srcport | l4-dstport | protocol | src-port | dst-port | flow-lable | all | default }**
- **no ipv6 field { src-ip | dst-ip | srcdst-ip | vlan | l4-srcport | l4-dstport | protocol | src-port | dst-port | flow-lable }**

Parameter

Parameter	Description	Value
src-ip	Specifies load balancing based on the source IP address.	-
dst-ip	Specifies load balancing based on the destination IP address.	-
srcdst-ip	Specifies load balancing based on the source and destination IP addresses.	-
vlan	Specifies load balancing based on the VLAN.	-
l4-srcport	Specifies load balancing based on the source port on the transport layer.	-

Parameter	Description	Value
l4-dstport	Specifies load balancing based on the destination port on the transport layer.	-
protocol	Specifies load balancing based on the protocol.	-
src-port	Specifies load balancing based on the physical source port.	-
dst-port	Specifies load balancing based on the destination physical port.	-
flow-label	Specifies load balancing based on the flow label.	-
all	Specifies load balancing based on the all of the preceding fields.	-
default	Specifies load balancing based on the source and destination IP addresses by default.	-

Default Value

By default, load balance of IPv6 packets is based on src-ip and dst-ip.

View

Schedule-profile configuration view, ecmp-profile configuration view

Usage Guidelines

NA

Example

Set the load balancing mode of IPv6 packets in the enhanced load balancing template 123 to VLAN-based load balancing.

```
Switch(config-schedule-profile-123)#ipv6 field vlan
Switch(config-schedule-profile-123)#show schedule-profile
schedule-profile: 1
  Packet      HashField
  L2          src-mac      dst-mac      vlan
  IPV4        src-ip        dst-ip
  IPV6        src-ip        dst-ip
  MPLS        top-label    2nd-label

Trunk interface:
schedule-profile: 123
  Packet      HashField
  L2          src-mac      dst-mac      src-mac      dst-mac      vlan
  IPV4        src-ip        dst-ip        vlan
  IPV6        src-ip        dst-ip        vlan
  MPLS        top-label    2nd-label

Trunk interface:
ecmp load-balance schedule-profile
```

```
Switch(config-schedule-profile-123)#
```

3.4.13 l2 field

Function

The **l2 field** command configures the load balancing mode of L2 packets in the enhanced load balancing template.

The **no l2 field** command deletes the configured load balancing mode of L2 packets in the enhanced load balancing template.

Format

- **l2 field** { **src-mac** | **dst-mac** | **l2-protocol** | **vlan** | **src-port** | **dst-port** | **eth-type** | **outer-vlan** | **srcdst-mac** | **all** | **default** }
- **no l2 field** { **src-mac** | **dst-mac** | **l2-protocol** | **vlan** | **src-port** | **dst-port** | **eth-type** | **outer-vlan** | **srcdst-mac** }

Parameter

Parameter	Description	Value
src-mac	Specifies load balancing based on the source MAC address.	-
dst-mac	Specifies load balancing based on the destination MAC address.	-
l2-protocol	Specifies load balancing based on the L2 protocol.	-
vlan	Specifies load balancing based on the VLAN.	-
src-port	Specifies load balancing based on the physical source port.	-
dst-port	Specifies load balancing based on the physical destination port.	-
eth-type	Specifies load balancing based on the Ethernet type.	-
outer-vlan	Specifies load balancing based on the outer VLAN.	-
srcdst-mac	Specifies load balancing based on the source and destination MAC addresses.	-
default	Restores default settings.	-
all	Specifies load balancing based on all of the preceding fields.	-

Default Value

By default, load balance of L2 packets is based on src-mac, dst-mac, and vlan.

View

Schedule-profile configuration view

Usage Guidelines

If this command is executed for multiple times, the load balancing mode configured for L2 packets by the last command applies.

If you run the `no l2 field` command to delete all configuration of the L2 field, the configuration restores to the default configuration.

Example

Set the load balancing mode of L2 packets in the enhanced load balancing template to l2-protocol.

```
Switch(config-schedule-profile-1)#l2 field l2-protocol
Switch(config-schedule-profile-1)#
```

3.4.14 mpls field

Function

The **mpls field** command configures the load balancing mode of MPLS packets in the enhanced load balancing template.

The **no mpls field** command deletes the configured load balancing mode of MPLS packets in the enhanced load balancing template.

Format

- **mpls field** { **top-label** | **2nd-label** | **src-ip** | **dst-ip** | **vlan** | **src-port** | **dst-port** | **all** | **default** }
- **no mpls field** { **top-label** | **2nd-label** | **src-ip** | **dst-ip** | **vlan** | **src-port** | **dst-port** }

Parameter

Parameter	Description	Value
top-label	Specifies load balancing based on the outer label.	-
2nd-label	Specifies load balancing based on the inner label.	-
src-ip	Specifies load balancing based on the source IP address.	-
dst-ip	Specifies load balancing based on the destination IP address.	-
vlan	Specifies load balancing based on the VLAN.	-
src-port	Specifies load balancing based on the source port.	-
dst-port	Specifies load balancing based on the destination port.	-
default	Restores default settings.	-
all	Specifies load balancing based on all of the preceding parameters.	-

Default Value

By default, load balancing of MPLS packets is based on top-label or 2nd-label.

View

Schedule-profile configuration view

Usage Guidelines

NA

Example

Set the load balancing mode of MPLS packets in the enhanced load balancing template 123 to vlan.

```
Switch(config-schedule-profile-1)#mpls field top-label
Switch(config-schedule-profile-1)#
```

3.4.15 schedule-profile

Function

The **schedule-profile** command creates an enhanced load balancing template and enters the template view.

The **no schedule-profile** command deletes the enhanced load balancing template.

Format

- **schedule-profile** { *profile-name* | **default** }
- **no schedule-profile** *profile-name*

Parameter

Parameter	Description	Value
profile-name	Specifies the name of the enhanced load balancing template.	The value is a string consisting of 1 to 33 characters.

Default Value

NA

View

Global configuration view

Usage Guidelines

NA

Example

Create an enhanced load balancing template named 1 and enter the template view.


```
Switch(config)#schedule-profile 1
Switch(config-schedule-profile-1)#
```

3.4.16 show schedule-profile

Function

The **show schedule-profile** command displays details about the enhanced load balancing template.

Format

- **show schedule-profile**
- **show schedule-profile** *profile-name*

Parameter

Parameter	Description	Value
profile-name	Specifies the name of the enhanced load balancing template.	The value is a string containing up to 33 characters.

Default Value

NA

View

Common user view

Usage Guidelines

You can run this command to view details of the enhanced load balancing template, including load balancing modes of the Layer-3 IPv4 and IPv6 packets, layer-2 packets, and MPLS packets.

Example

Display details of the enhanced load balancing template.

```
Switch>show schedule-profile
Version : SCHEDULEPROFILE_VB3.00.00.00
schedule-profile: a
Packet      HashField
-----
L2          src-mac    dst-mac    vlan
IP          src-ip      dst-ip
IPV6        src-ip      dst-ip
MPLS        top-label   2nd-label
```

```
Switch>
```

3.4.17 lacp timeout

Function

The **lacp timeout** command sets the timeout duration for the Eth-Trunk interface to receive LACP packets in LACP mode.

Format

lacp timeout { **fast** | **slow** | *timeout-value* }

Parameter

Parameter	Description	Value
fast	Sets the timeout duration to 3s. If fast is specified, the peer sends one LACP packet every one second and the device responds quickly but occupies more system resources than the slow configuration.	-
slow	Sets the timeout duration to 90s. If slow is specified, the peer sends one LACP packet every 30 seconds and the device responds slowly but occupies less system resources than the fast configuration. The timeout duration at two ends can be inconsistent. However, for maintenance convenience, set the timeout duration at two ends to be the same.	-
timeout-value	Sets the timeout duration for the Eth-Trunk interface to receive packets when fast is specified.	The value is an integer ranging from 10 to 90, in seconds.

Default Value

NA

View

Eth-trunk interface configuration view, Peerlink configuration view

Usage Guidelines

NA

Example

Set the timeout duration for the Eth-Trunk interface to receive LACP packets in LACP mode.

```
Switch(config-eth-trunk1)#mode lacp-static
Switch(config-eth-trunk1)#lacp timeout fast
```

3.4.18 debug lacp

Function

The **debug lacp** command enables debugging of the Link Aggregation Control Protocol (LACP) module.

The **no debug lacp** command disables debugging of the LACP module.

Format

- **debug lacp { timer | event | churn | mux | rx | tx | config | logic | sync | all }**
- **no debug lacp { timer | event | churn | mux | rx | tx | config | logic | sync | all }**

Parameter

Parameter	Description	Value
timer	Specifies debugging of the LACP timer.	-
event	Specifies debugging of the LACP function.	-
churn	Specifies debugging of the LACP churn function.	-
mux	Specifies debugging of the LACP aggregator function.	-
rx	Specifies errors that may occur in received LACP packets.	-
tx	Specifies errors that may occur in sent LACP packets.	-
config	Specifies debugging of the LACP configuration function.	-
logic	Specifies debugging of the LACP logic function.	-
sync	Specifies debugging of the LACP synchronization function.	-
all	Specifies debugging of all LACP functions.	-

Default Value

NA

View

Privileged user view

Usage Guidelines

NA

Example

Enables debugging of the LACP timer.

```
Switch#debug lacp timer
Switch#
```

3.4.19 lacp system-priority

Function

The **lacp system-priority** command sets the priority for all the LACP systems.

Format

lacp system-priority { *priority* | **default** }

Parameter

Parameter	Description	Value
priority	Specifies the LACP system priority.	The value is an integer ranging from 0 to 65535.
default	Uses the default priority value.	32768

Default Value

32768

View

Global configuration view

Usage Guidelines

NA

Example

Set the LACP system priority to 100.

```
Switch(config)#lacp system-priority 100
Switch(config)#
```

3.4.20 lacp port-id extension {enable|disable}

Function

The **lacp port-id extension {enable|disable}** command enables or disables the LACP port ID for a Trunk interface.

Format

lacp port-id extension { **enable** | **disable** }

Parameter

NA

Default Value

NA

View

Interface configuration view (Trunk), Peerlink configuration view

Usage Guidelines

NA

Example

Enable the LACP port ID for a Trunk interface.

```
Switch(config-eth-trunk1)#lacp port-id extension enable
Switch(config-eth-trunk1)#
```

3.4.21 lacp system-id**Function**The **lacp system-id** command configures the LACP system ID for an Eth-Trunk interface.**Format****lacp system-id** *system-id-address***Parameter**

Parameter	Description	Value
system-id-address	Specifies an IPv6 address.	The value is in 32-bit hexadecimal format, such as X:X::X:X, where Xs are hexadecimal digits 0-9 and A-F. The value cannot be all 0s or all Fs.

Default Value

NA

View

Interface configuration view (Trunk), Peerlink configuration view

Usage Guidelines

NA

Example

Configure the LACP system ID for an Eth-Trunk interface.

```
Switch(config-eth-trunk1)#lacp system-id 00:04:67:00:00:22
```

```
Switch(config-eth-trunk1)#
```

3.4.22 reset lacp statistic

Function

The **reset lacp statistic** command clears the LACP statistic of all interfaces.

Format

reset lacp statistic

Parameter

NA

Default Value

NA

View

Global configuration view

Usage Guidelines

NA

Example

Clear the LACP statistic of all interfaces.

```
Switch(config)#reset lacp statistic
Switch(config)#
```

3.4.23 reset lacp statistic interface

Function

The **reset lacp statistic interface** command clears the LACP statistic of an interface.

Format

reset lacp statistic interface { ethernet | xgigaethernet | 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet } interface-number

Parameter

Parameter	Description	Value
interface-number	Specifies an Ethernet interface number.	The value is an integer in the range of <1-128>/<0-2>/<1-256> (For reference only. The

Parameter	Description	Value
		specific value range depends on the slot number and card type).

Default Value

NA

View

Global configuration view

Usage Guidelines

NA

Example

Clear the LACP statistic of all interfaces.

```
Switch(config)#reset lacp statistic interface 10gigaethernet 1/0/1
Switch(config)#
```

3.4.24 reset lacp statistic interface eth-trunk**Function**

The **reset lacp statistic interface eth-trunk** command clears the LACP statistic of all Trunk interfaces.

Format**reset lacp statistic interface eth-trunk** *trunk-number***Parameter**

Parameter	Description	Value
trunk-number	Specifies the number of a Trunk interface.	The value is an integer ranging from 1 to 128.

Default Value

NA

View

Global configuration view

Usage Guidelines

NA

Example

Clear statistics on sent and received LACP packets in LACP mode.

```
Switch(config)#reset lacp statistic interface eth-trunk 1
Switch(config)#
```

3.4.25 show lacp config**Function**

The **show lacp config** command displays the LACP configuration on the switch.

Format

show lacp config

Parameter

NA

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

Display LACP system information.

```
Switch>show lacp config
lacp system-priority 1

interface eth-trunk-1
mode lacp-static
Switch>
```

3.4.26 show lacp eth-trunk**Function**

The **show lacp eth-trunk** command displays information about an LACP trunk interface.

Format

- **show lacp eth-trunk**
- **show lacp eth-trunk** *trunk-number*

Parameter

Parameter	Description	Value
trunk-number	Specifies the number of a Trunk interface.	The value is an integer ranging from 1 to 128.

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

Display information about an LACP trunk interface.

```
Switch>show lacp eth-trunk
  Interface      Status    PortNum  MainPort  MaxActiveIfNum
  eth-trunk-1    master    0        -----   8
Switch>show lacp eth-trunk-1
eth-trunk-1:
  LACP Status: master
  System Priority: 1
  System Mac Address: 00:04:67:90:ff:ff
  Number Of Port In Trunk: 0
  Max Active port number: 8
Switch>
```

3.4.27 show lacp statistic interface eth-trunk**Function**

The **show lacp statistic interface eth-trunk** command displays statistics on sent and received LACP packets in LACP mode.

Format

show lacp statistic interface eth-trunk *trunk-number*

Parameter

Parameter	Description	Value
trunk-number	Specifies the number of a Trunk interface.	The value is an integer ranging from 1 to 128.

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

View statistics on sent and received LACP packets in LACP mode.

Switch>show lacp statistic interface eth-trunk 1

Interface eth-trunk1 PDU statistic info :

Port	LacpRevPdu	LacpSentPdu	MarkerRevPdu	MarkerSentPdu
25ge1/0/3	0	0	0	0
25ge1/0/2	0	0	0	0

Switch>

3.4.28 show lacp system**Function**The **show lacp system** command displays LACP system information.**Format****show lacp system****Parameter**

NA

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

Display LACP system information.

```
Switch>show lacp system
LACP system information:
    Max AG number: 128
    System Priority: 32768
    System Mac Address: 00:04:67:90:ff:ff
    Fast Periodic Time: 1(s)
    Slow Periodic Time: 30(s)
    Short Timeout Time: 3(s)
    Long Timeout Time: 90(s)
    Churn Detection Time: 60(s)
    Join Ag waiting time: 2(s)

Switch>
```

3.4.29 show interface eth-trunk**Function**The **show interface** command displays attributes of an interface and related information.**Format**

- **show interface eth-trunk** *trunk-number*
- **show interface eth-trunk** *trunk-number config*

Parameter

Parameter	Description	Value
verbose	Displays information about all interfaces.	-
trunk-number	Specifies the number of a Trunk interface.	The value is an integer ranging from 1 to 128.

Default Value

NA

View

Common user view

Usage Guidelines

When checking interface attributes and related information:

If no interface number is specified in **show interface trunk**, the Trunk group, stream allocation algorithm and number of interfaces joined the Trunk group are displayed. If an interface number is specified, the basic statistics of the specified Trunk interface is displayed. If **config** is specified, other function configurations of the specified Trunk interface are displayed.

The **show interface verbose** command displays the basic information on all Ethernet and Trunk interfaces (if configured) of the current device.

Generally, commands described in this section are used to collect traffic statistics or diagnose faults on interfaces.

Example

Display the configuration of Ethernet interface xgigaethernet 1/0/1.

```
Switch> show interface eth-trunk xgigaethernet 1/0/1
Interface xgigaethernet-1/0/1
  Admin state is up,operation state is down
  Negotiation auto enable
  flow-control negotiation disable
  Duplex is half
  Speed is 1000M(bps)
  Mtu is 1522
  Connector is electronic
  Priority is 0
  In direction filter-group is disable
  Out direction filter-group is disable
  Bandwidth granularity is 64000(bps)
  In direction bandwidth is disable
  Out direction bandwidth is disable
  Broadcast-storm packet-ctrl is disable
  Multicast-storm packet-ctrl is disable
  Dlf-storm packet-ctrl is disable
  Broadcast-storm bps-ctrl is disable
  Multicast-storm bps-ctrl is disable
  Dlf-storm bps-ctrl is disable
  Pvid is 1
  Dot1q-tunnel disable
  Port link-type is hybrid
  Mdi is auto
  Flow-control disable
```

```
Flow-statistic include-interframe disable
port-security disable
port-security mac-address sticky disable
Port-down holdoff-timer 0
Last 5 minutes input rate:0 Bps, 0 pps
Last 5 minutes output rate:0 Bps, 0 pps
Last 5 minutes input link utilization rate: 0.00%
Last 5 minutes output link utilization rate: 0.00%
Rx statistic:
    octets:0/0
    packets:0/0
    unicast:0/0
    multicast:0/0
    broadcast:0/0
Packets statistic:
    64 octets:0/0
    65-127 octets:0/0
    128-255 octets:0/0
    256-511 octets:0/0
    512-1023 octets:0/0
    1024-1518 octets:0/0
    >1518 octets:0/0
Tx statistic:
    octets:0/0
    packets:0/0
    unicast:0/0
    multicast:0/0
    broadcast:0/0
Packets statistic:
    64 octets:0/0
    65-127 octets:0/0
    128-255 octets:0/0
    256-511 octets:0/0
    512-1023 octets:0/0
    1024-1518 octets:0/0
    >1518 octets:0/0
Other statistic:
    fragments:0/0
    Jabbers:0/0
    CRC errors:0/0
    Collisions:0/0
    Undersize:0/0
    Oversize:0/0
```

```
Switch>
```

3.4.30 unknown-unicast load-balance

Function

The **unknown-unicast load-balance** command sets the load balancing mode for unknown unicast packets on the Trunk interface when the packets are forwarded by the aggregation port VLAN.

Format

- **unknown-unicast load-balance { dst-mac | src-mac | srcdst-mac | default }**
- **unknown-unicast load-balance schedule-profile *name***

Parameter

Parameter	Description	Value
schedule-profile	Enhanced load sharing profile mode that has been created	-
name	Specific profile name	-
src-mac	Specifies load balancing among trunk member interfaces based on source MAC addresses.	-
dst-mac	Specifies load balancing among trunk member interfaces based on destination MAC addresses.	-
srcdst-mac	Specifies load balancing among trunk member interfaces based on the exclusive OR result of source and destination MAC addresses.	-
default	Default mode	The default load balancing mode is srcdst-mac.

Default Value

The default mode is srcdst-mac.

View

Global configuration view

Usage Guidelines

Before setting the load balancing mode of the Trunk interface to **schedule-profile**, run the **schedule-profile** command to configure the enhanced algorithm template.

Example

Set the load balancing mode for all Trunk interfaces to **src-mac**.

```
Switch(config)#unknown-unicast load-balance src-mac
```

```
Switch(config)#
```

3.4.31 show unknown-unicast load-balance

Function

The **show unknown-unicast load-balance** command displays the configuration of unknown unicast load balancing.

Format

show unknown-unicast load-balance

Parameter

NA

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

Configure the unknow unicast load balancing mode to source MAC and display the configuration of unknown unicast load balancing.

```
Switch(config)#unknown-unicast load-balance src-mac
Switch(config)#exit
Switch#disable
Switch>show unknown-unicast load-balance
unknown-unicast load-balance src-mac
Switch>
```

3.5 VLAN Configuration Commands

3.5.1 port default vlan

Function

The **port default vlan** command specifies the default VLAN of a port and adds the port to the VLAN.

The **no port default vlan** command deletes the default VLAN of a port and exits the VLAN.

Format

- **port default vlan** *vlan-id*
- **no port default vlan**

Parameter

Parameter	Description	Value
vlan-id	Specifies the default VLAN ID of a port.	The value is an integer ranging from 1 to 4094.

Default Value

The default VLAN of a port is VLAN 1, and ports are added to VLAN 1 in untagged mode.

View

Ethernet bridge interface configuration view, interface configuration view (Trunk)

Usage Guidelines

This command is valid only to ports of the access and QinQ types. The VLAN specified by *vlan-id* must exist.

A port can belong to multiple VLANs. If a default VLAN is configured, a port handles the packets in the following ways:

Upon receiving packets without VLAN tags, a port adds VLAN tags to the packets and sets the VID in the tag to the default VLAN ID of the port.

When a port receives a VLAN tagged packet carrying the same VLAN ID as the default VLAN ID of the port, the packet is forwarded through the port. If the VLAN ID of the packet is different from the default VLAN ID of the port, the packet is dropped.

When a port receives a VLAN tagged packet carrying the same VLAN ID as the default VLAN ID of the port, the port removes the VLAN tag from the packet and then sends the packet.

Example

Set default VLAN of interface xgigaethernet 1/0/1 to VLAN 2.

```
Switch(config-10ge1/0/1)#port link-type access
Switch(config-10ge1/0/1)#port default vlan 2
```



```
Switch(config-10ge1/0/1)#
```

3.5.2 port hybrid vlan

Function

The **port hybrid vlan** command sets a single or multiple VLANs for the Hybrid port.

The **no port hybrid vlan** command deletes a single or multiple VLANs for the Hybrid port.

Format

- **port hybrid vlan** *vlan-list* { **tagged** | **untagged** }
- **no port hybrid vlan** *vlan-list*
- **no port hybrid vlan all**

Parameter

Parameter	Description	Value
vlan-list	Mandatory. Specifies the VLAN sequence of the Hybrid port.	The value is an integer ranging from 1 to 4094.
tagged	Specifies marking the VLAN frame as Tagged before forwarding it from this port.	-
untagged	Specifies marking the VLAN frame as Untagged before forwarding it from this port.	-

Default Value

NA

View

Ethernet bridge interface configuration view, interface configuration view (Trunk)

Usage Guidelines

This command marks the Hybrid port as Tagged or Untagged and adds a port to the VLAN. Where,

tagged: indicates a port sends frames without removing VLAN Tag from frames.

untagged: indicates a port removes VLAN Tag from frames before sending frames.

You can run this command to add one Hybrid port to multiple VLANs at a time.

Example

Enable a port to remove Tag from the frame before sending the frame to VLAN2.

```
Switch(config-10ge1/0/1)#port hybrid vlan 2 untagged
```

```
Switch(config-10ge1/0/1)#
```

3.5.3 port hybrid pvid

Function

The **port hybrid pvid** command specifies the default VLAN of a hybrid port.

Format

port hybrid pvid { *vlan-id* | **default** }

Parameter

Parameter	Description	Value
vlan-id	Configures the default VLAN ID of the hybrid port.	The value is an integer ranging from 1 to 4094.
default	Configures the default VLAN ID of the hybrid port.	The default value is VLAN 1.

Default Value

The default VLAN of a hybrid port is VLAN 1.

View

Ethernet bridge interface configuration view, interface configuration view (Trunk)

Usage Guidelines

After the default VLAN ID is configured for a hybrid port, you must add a port to the default VLAN so that a port can send packets with the default VLAN tag.

For details about how to add a Hybrid port to VLAN, see **port hybrid vlan**.

Example

Set the default VLAN of hybrid port xgigaethernet 1/0/1 to VLAN 25.

```
Switch(config-10ge1/0/1)#port hybrid pvid 25
Switch(config-10ge1/0/1)#
```

3.5.4 port link-type

Function

The **port link-type** command sets the link type (interface type) of an interface.

Format

port link-type { **access** | **trunk** | **hybrid** | **dot1q-tunnel** | **default** }

Parameter

Parameter	Description	Value
access	Sets the interface type to Access.	-
trunk	Sets the interface type to Trunk.	-
hybrid	Sets the interface type to Hybrid.	-
dot1q-tunnel	Sets the interface type to dot1q-tunnel.	-
default	Restores the interface type to the default value, that is, Hybrid.	-

Default Value

Hybrid

View

Ethernet bridge interface configuration view, interface configuration view (Trunk)

Usage Guidelines

Access interface: Generally, it is connected to the host. It can only connect to the access link and transmit Ethernet frames without VLAN tags. If the access interface is configured with a default VLAN, packets are added with the default VLAN tag. The link allows Ethernet frames matching the default VLAN tag to pass through.

Trunk interface: Generally, it is connected to network devices such as the switch or router. It can connect to only the trunk link. It allows multiple VLAN frames to pass through the link.

Hybrid interface: It can be connected to both a host (access link) and a network device (trunk link). It allows multiple VLAN frames to pass through and removes tags of certain VLAN frames in the outbound direction.



Note:

Before changing the interface type, delete the original VLAN configuration. That is, restore the setting of the interface to the default configuration for adding to VLAN 1.

Example

Set the interface type to Access.

```
Switch(config-10ge1/0/1)#port link-type access
Switch(config-10ge1/0/1)#
```

3.5.5 port trunk allow-pass vlan

Function

The **port trunk allow-pass vlan** command adds a trunk interface to specified VLANs.

The **no port trunk allow-pass vlan** command removes a trunk interface from specified VLANs.

Format

- **port trunk allow-pass vlan** *vlan-list*
- **port trunk allow-pass vlan all**
- **no port trunk allow-pass vlan** *vlan-list*
- **no port trunk allow-pass vlan all**

Parameter

Parameter	Description	Value
vlan-list	Specifies a list of VLANs to which the trunk interface belongs.	The format is 1,3,5 to 8. The value is an integer ranging from 1 to 4094.

Default Value

NA

View

Ethernet bridge interface configuration view, interface configuration view (Trunk)

Usage Guidelines

You can use this command to add the trunk interface to the VLAN in a tagged mode. In this way, the interface does not remove the VLAN tags from frames when sending frames.

The VLAN specified in the VLAN list must exist. Otherwise, the configuration is invalid.

You cannot use this command for physical interfaces added to the aggregation interface.

Example

Set the default VLAN of trunk interface xgigaethernet 1/0/1 to VLAN 2.

```
Switch(config-10ge1/0/1)#port link-type trunk
Switch(config-10ge1/0/1)#port trunk allow-pass vlan 2
Switch(config-10ge1/0/1)#
```

3.5.6 port trunk pvid

Function

The **port trunk pvid** command specifies the default VLAN of a trunk interface.

Format

port trunk pvid { *vlan-id* | **default** }

Parameter

Parameter	Description	Value
vlan-id	Configures the default VLAN ID of a trunk interface.	The value is an integer ranging from 1 to 4094.
default	Restores the VLAN ID of a trunk interface to the default value.	The default value is VLAN 1.

Default Value

The default VLAN ID of a trunk interface is VLAN 1.

View

Ethernet bridge interface configuration view, interface configuration view (Trunk)

Usage Guidelines

After the default VLAN ID is configured for a trunk interface, you must add the interface to the default VLAN so that the interface can send packets with the default VLAN tag.

For details for adding a Trunk interface to the VLAN, see `port trunk pvid`.

Example

Set the default VLAN of trunk interface xgigaethernet 1/0/1 to VLAN 2.

```
Switch(config-10ge1/0/1)#port link-type trunk
Switch(config-10ge1/0/1)#port trunk pvid 2
Switch(config-10ge1/0/1)#
```

3.5.7 show vlan

Function

The **show vlan** command displays VLAN information on the switch.

Format

- **show vlan**
- **show vlan all**
- **show vlan all** *vlan-list*

- **show vlan property**
- **show vlan property *vlan-list***
- **show vlan verbose**
- **show vlan *vlan-id* verbose**

Parameter

Parameter	Description	Value
vlan-id	Specifies a VLAN ID.	The value is an integer ranging from 1 to 4094.
vlan-list	Specifies a VLAN list.	The value is an integer in the format of 1,2,3 to 5.

Default Value

NA

View

Common user view

Usage Guidelines

The **show vlan** command displays all VLAN configuration information, including the VLAN ID, type, state, and MAC address learning state.

The **show vlan verbose** command displays detailed information about all VLAN.

The **show vlan *vlan-id* verbose** command displays details about a specific VLAN, including the VLAN ID, type, description, state, statistics collection state, member interfaces, and interface joining mode.

Example

Display all VLAN-related information.

```
Switch>show vlan
Total :4094    Static :4094    Dynamic :0
-=-None, M=Member,U=Untagged
VID   10ge1/0/1-10ge1/0/48                40ge1/1/1-40ge1/1/6
1     U-UU UUUU UUUU UUUU UUUU UUUU UUUU UUUU UUUU UUUU UUUU UU-  UUUU
UU
VID   10ge1/0/1-10ge1/0/48                40ge1/1/1-40ge1/1/6
10    -----UUU- -----
VID   10ge1/0/1-10ge1/0/48                40ge1/1/1-40ge1/1/6
20    -----U-----
```

```

VID    10ge1/0/1-10ge1/0/48                                40ge1/1/1-40ge1/1/6
300    -----U-----
Switch>

```

Display all VLAN attribute information.

```

Switch>show vlan property
The total number of vlans is :4094
UMcast=UnknownMcast
VID    UMcast    Unicast Type    Alias
1      forward forward static  N/A
2      forward forward static  N/A
3      forward forward static  N/A
4      forward forward static  N/A
5      forward forward static  N/A
6      forward forward static  N/A
7      forward forward static  N/A
8      forward forward static  N/A
9      forward forward static  N/A
10     drop      drop      static  N/A
11     forward forward static  N/A
12     forward forward static  N/A
13     forward forward static  N/A
14     forward forward static  N/A
15     forward forward static  N/A
16     forward forward static  N/A
17     forward forward static  N/A
18     forward forward static  N/A
19     forward forward static  N/A
Switch>

```

Display details about all VLANs.

```

Switch>show vlan verbose

VLAN ID:1
  Vlan alias:N/A
  The total number of ipv4 address is:0,ipv6 address is:0
  Unknown-multicast:forward
  Unknown-unicast:forward
  Admin status:up
  Physical status:down
  Vlan-type:normal
  Vlan-status:static
  Member(s):

```

Interface	Tagged
40ge1/1/6	Untag
40ge1/1/5	Untag
40ge1/1/4	Untag
40ge1/1/3	Untag
40ge1/1/2	Untag
40ge1/1/1	Untag
10ge1/0/47	Untag
10ge1/0/46	Untag
10ge1/0/45	Untag
10ge1/0/44	Untag
10ge1/0/43	Untag
10ge1/0/42	Untag
10ge1/0/41	Untag

Switch>

3.5.8 show port vlan

Function

The **show port vlan** command displays information on an interface in the VLAN.

Format

show port vlan

Parameter

NA

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

View information on an interface in the VLAN.

Switch>show port vlan			
Interface	Link Type	PVID	VLAN List
mgt-eth 0/0/0	hybrid	0	

10gigaethernet 1/0/1	hybrid	1	1
10gigaethernet 1/0/2	hybrid	200	200,1001-1255
10gigaethernet 1/0/3	hybrid	1	1
10gigaethernet 1/0/4	hybrid	200	200,1001-1255
10gigaethernet 1/0/5	hybrid	1	1
10gigaethernet 1/0/6	hybrid	1	1
10gigaethernet 1/0/7	hybrid	1	1
10gigaethernet 1/0/8	hybrid	1	1
10gigaethernet 1/0/9	hybrid	1	1
10gigaethernet 1/0/10	hybrid	1	1
10gigaethernet 1/0/11	hybrid	1	1
10gigaethernet 1/0/12	hybrid	1	1
10gigaethernet 1/0/13	hybrid	1	1
10gigaethernet 1/0/14	hybrid	1	1
10gigaethernet 1/0/15	hybrid	1	1
10gigaethernet 1/0/16	hybrid	1	1
10gigaethernet 1/0/17	hybrid	1	1
10gigaethernet 1/0/18	hybrid	1	1
10gigaethernet 1/0/19	hybrid	1	1
10gigaethernet 1/0/20	hybrid	1	1
Switch>			

3.5.9 unknown-multicast {forward|drop}

Function

The **unknown-multicast {forward|drop}** command sets how the VLAN processes an unknown multicast packet before forwarding the packet.

Format

unknown-multicast { forward | drop }

Parameter

Parameter	Description	Value
forward	Forwards unknown multicast packets.	-
drop	Drops unknown multicast packets.	-

Default Value

The default value is forward.

View

VLAN configuration view

Usage Guidelines

NA

Example

Set VLAN10 to drop unknown unicast packets.

```
Switch(vlan-10)#unknown-multicast drop
Switch(vlan-10)#
```

3.5.10 unknown-unicast {forward|drop}**Function**

The **unknown-unicast {forward|drop}** command sets how the VLAN processes an unknown unicast packet before forwarding the packet.

Format

unknown-unicast { forward | drop }

Parameter

Parameter	Description	Value
forward	Forwards unknown multicast packets.	-
drop	Drops unknown multicast packets.	-

Default Value

The default value is forward.

View

VLAN configuration view

Usage Guidelines

You can run this command to drop or forward an unknown unicast packet.

Example

Set VLAN10 to drop unknown unicast packets.

```
Switch(vlan-10)#unknown-unicast drop
Switch(vlan-10)#
```

3.5.11 no vlan**Function**

The **no vlan** command deletes a specific VLAN and exits the current VLAN configuration view.

Format

no vlan *vlan-id*

Parameter

Parameter	Description	Value
vlan-id	Specifies a VLAN ID.	The value is an integer ranging from 1 to 4094.

Default Value

NA

View

VLAN configuration view, global configuration view

Usage Guidelines

NA

Example

Delete VLAN 2 in the VLAN 10 configuration view and exit the VLAN 10 configuration view.

```
Switch(vlan-10)#no vlan 2
Switch(config)#
```

3.5.12 vlan

Function

The **vlan** command creates a VLAN and accesses the corresponding VLAN configuration view.

Format

vlan *vlan-id*

Parameter

Parameter	Description	Value
vlan-id	Specifies a VLAN ID.	The value is an integer ranging from 1 to 4094.

Default Value

NA

View

VLAN configuration view

Usage Guidelines

NA

Example

Create VLAN 2 in the VLAN 10 configuration view and access the VLAN 2 configuration view.

```
Switch(vlan-10)#vlan 2
Switch(vlan-2)#
```

3.5.13 protocol up-delay-time

Function

The **protocol up-delay-time** command configures the delay UP time for Layer-3 interfaces.

Format

protocol up-delay-time { time | default }

Parameter

Parameter	Description	Value
time	Specifies a delay UP time for Layer-3 interfaces.	The value is an integer ranging from 0 to 65535, in seconds.
default	Specifies the default delay UP time for Layer-3 interfaces.	0s

Default Value

The default value is 0s, that is, the delay UP functions is disabled for Layer-3 interfaces by default.

View

Global configuration view, Ethernet routing interface configuration view, VLAN interface configuration view, and BD interface configuration view

Usage Guidelines

This command can be configured and take effect only when the mode of the interface is Layer-3 router mode.

**Caution**

When the interface is in Layer-3 router mode, the delay UP function is also valid to the layer-2 interface, that is, the delay UP time is also applied to the layer-2 bridge interface.

Example

Configure the delay UP time for the interface VLAN 100 to 30s.

```
Switch(config)#interface vlan 100
Switch(config-vlanif-100)#protocol up-delay-time 30
```

3.5.14 protocol-vlan**Function**

The **protocol-vlan** command sets to allocate VLANs by protocol and specifies the associated protocol.

The **no protocol-vlan** command cancels VLANs allocated by protocol.

Format

- **protocol-vlan** *protocol-index1* { **ethernet2** | **snap** } *ethernet-typevalue*
- **protocol-vlan** *protocol-index1* **llc dsap** *dsap-value* **ssap** *ssap-value*
- **no protocol-vlan** *protocol-index*
- **no protocol-vlan** **all**

Parameter

Parameter	Description	Value
protocol-index1	Specifies a protocol index value.	The value is an integer ranging from 0 to 16.
protocol-index	Specifies a protocol index value.	The value is an integer ranging from 0 to 16.
ethernet-typevalue	Specifies allocating VLANs by other protocol types which are indicated by a hexadecimal number.	The value is a hexadecimal number ranging from 0x600 to 0xffff.
ethernet2	Specifies the encapsulation mode of Ethernet packets to Ethernet 2.	-
snap	Specifies the encapsulation mode of Ethernet packets to SNAP.	-

Parameter	Description	Value
llc	Specifies the encapsulation mode of Ethernet packets to LLC.	-
ssap	Specifies a source service access point.	-
dsap	Specifies a destination service access point.	-
ssap-value	Specifies the value of a source service access point.	The value is a hexadecimal number ranging from 0x0 to 0xff.
dsap-value	Specifies the value of a destination service access point.	The value is a hexadecimal number ranging from 0x0 to 0xff.

Default Value

NA

View

Global configuration view, Ethernet bridge interface configuration view (not applicable for 10G interface)

Usage Guidelines

When configuring the source and destination access points, pay attention to the following points:

- **dsap** and **ssap** cannot be set to **aa** at the same time because **aa** indicates the SNAP encapsulation mode.
- **dsap** and **ssap** cannot be set to **e0** at the same time because **e0** indicates the LLC encapsulation mode for IPX packets.
- **dsap** and **ssap** cannot be set to **ff** at the same time because **ff** indicates the RAW encapsulation mode for IPX packets..

Example

Set to allocate VLANs by ethernet2.

```
Switch(config)#protocol-vlan 2 ethernet2 0x700
Switch(config)#
```

3.5.15 protocol-vlan vid

Function

The **protocol-vlan vid** command sets the interface associated protocol to VLAN.

The **no protocol-vlan vid** command deletes the protocol VLAN associated with the interface.

Format

- **protocol-vlan** *protocol-index* **vid** *vlan-id*
- **protocol-vlan** *protocol-index* **vid** *vlan-id* **priority** *priority*
- **no protocol-vlan** *protocol-index*
- **no protocol-vlan** **all**

Parameter

Parameter	Description	Value
protocol-index	Specifies a protocol index value.	The value is an integer ranging from 1 to 16.
vlan-id	Specifies the VLAN ID of an associated protocol VLAN.	The value is an integer ranging from 1 to 4094.
priority	Specifies the priority of an associated protocol VLAN ID.	The value is an integer ranging from 0 to 7.

Default Value

NA

View

Ethernet bridge interface configuration view (not applicable for 10G interface)

Usage Guidelines

Before running this command, you must enable protocol-based VLAN allocation and set the protocol index value.

After the interface associated protocol VLAN is set, when packets based on the associated protocol enters this interface, the system automatically allocates a VLAN for this protocol. This function is applied for networks in which different protocols have different transmission paths.

Example

Set the associated protocol of the interface **trunk1** to **VLAN2** and the protocol index value to **10**.

```
Switch(config-eth-trunk1)#protocol-vlan 10 vid 2 priority 2
Switch(config-eth-trunk1)#
```

3.5.16 debug protocol-vlan

Function

The **debug protocol-vlan** command enables the protocol VLAN debugging function.

The **no debug protocol-vlan** command disables the protocol VLAN debugging function.

Format

- **debug protocol-vlan**
- **no debug protocol-vlan**

Parameter

NA

Default Value

NA

View

Privileged user view

Usage Guidelines

NA

Example

Enable the protocol VLAN debugging function.

```
Switch#debug protocol-vlan
Switch#
```

3.5.17 show protocol-vlan**Function**The **show protocol-vlan** command displays the configuration of VLANs allocated by protocol.**Format**

- **show protocol-vlan**
- **show protocol-vlan** *protocol-index*
- **show protocol-vlan interface**

Parameter

Parameter	Description	Value
protocol-index	Specifies the ID of a protocol VLAN instance.	The value is an integer ranging from 1 to 1024.

Default Value

NA

View

Common user view

Usage Guidelines

The **show protocol-vlan interface** command displays the configuration of VLANs allocated by the protocol associated with the interface, including the interface number, protocol index value, VLAN ID, and priority of the associated protocol VLAN.

The **show protocol-vlan protocol-index** command displays information on the protocol and protocol index configured for the VLAN.

Example

View information on the protocol and protocol index configured for the VLAN10.

```
Switch>show protocol-vlan 10
  Index  EncapType  ProtoID
  ----  -
  1      snap       0x0x781
Switch>
```

3.5.18 debug mac-vlan**Function**

The **debug mac-vlan** command enables the MAC-based VLAN debugging function.

The **no debug mac-vlan** command disables the MAC-based VLAN debugging function.

Format

- **debug mac-vlan**
- **no debug mac-vlan**

Parameter

NA

Default Value

NA

View

Privileged user view

Usage Guidelines

NA

Example

Enable the MAC-based VLAN debugging function.

```
Switch#debug mac-vlan
Switch#
```

3.5.19 mac-vlan {enable|disable}**Function**

The **mac-vlan {enable|disable}** command enables or disables MAC address-based VLAN assignment on an interface.

Format

mac-vlan { enable | disable }

Parameter

Parameter	Description	Value
enable	Enables MAC address-based VLAN assignment.	-
disable	Disables MAC address-based VLAN assignment.	-

Default Value

By default, MAC address-based VLAN assignment is disabled on an interface.

View

Ethernet bridge interface configuration view (not applicable for 10G interface)

Usage Guidelines

VLANs need to be reassigned frequently when physical locations of users keep changing. To avoid frequent VLAN reassignment, you can enable MAC address-based VLAN assignment. This function removes the need for VLAN reassignment after changes of users' physical locations, reducing your workload.

This function must be enabled before other associated parameters can be configured.

Example

Enable MAC address-based VLAN assignment on an interface.

```
Switch(config-10ge1/0/1)#mac-vlan enable
Switch(config-10ge1/0/1)#
```

3.5.20 mac-vlan priority

Function

The **mac-vlan priority** command associates a MAC address with a VLAN and sets the 802.1p priority of the VLAN corresponding to the MAC address.

The **no mac-vlan** command deassociates a MAC address from a VLAN.

Format

- **mac-vlan** *mac-address* *vlan-id* **priority** *priority*
- **mac-vlan** *mac-address* *vlan-id*
- **no mac-vlan** *mac-address*
- **no mac-vlan** **all**

Parameter

Parameter	Description	Value
mac-address	Specifies a MAC address to be associated with the VLAN.	The format is AA:BB:CC:DD:EE:FF, where A to F are hexadecimal digits.
vlan-id	Specifies the ID of a VLAN with which the MAC address is associated.	The value is an integer ranging from 1 to 4094.
priority	Specifies the 802.1p priority of the VLAN corresponding to the MAC address.	The value is an integer ranging from 0 to 7.

Default Value

NA

View

Global configuration view

Usage Guidelines

After you set to allocate VLANs to the interface based on the MAC address, Switch checks whether the source MAC address of the untagged packet or packet of which the priority is tagged is consistent with the configured MAC address. If yes, add a VLAN Tag and priority to the packet (keep the priority of packets of which the priority is Tag unchanged). If not, the packet forwards the packet to the allocated VLAN. MAC address-based VLAN assignment is usually used together with security features to enable secure and flexible terminal access.

Example

Associate a MAC address with a VLAN.

```
Switch(config-10ge1/0/1)#mac-vlan 00:00:00:00:00:01 1 priority 1
Switch(config-10ge1/0/1)#
```

3.5.21 show mac-vlan

Function

The **show mac-vlan** command displays configuration of MAC address-based VLAN assignment on interfaces.

Format

- **show mac-vlan**
- **show mac-vlan** *vlan-id*
- **show mac-vlan interface**

Parameter

Parameter	Description	Value
vlan-id	Specifies a VLAN ID.	The value is an integer ranging from 1 to 4094.

Default Value

NA

View

Common user view

Usage Guidelines

You can use this command to specify the VLAN or interface to view configuration of VLANs allocated based on the MAC address.

Information queried based on the MAC address includes: MAC address, VLAN ID, priority, and state.

Information queried based on the interface includes: interface ID, state, and precedence.

Example

Display configuration of MAC address-based VLAN assignment on all interfaces.

```
Switch>show mac-vlan interface
If          Mac-vlan-state  Precedence
xge-1/0/1   disable        mac-vlan
xge-1/0/2   disable        mac-vlan
xge-1/0/3   disable        mac-vlan
```

```

xge-1/0/4    disable    mac-vlan
xge-1/0/5    disable    mac-vlan
xge-1/0/6    disable    mac-vlan
xge-1/0/7    disable    mac-vlan
xge-1/0/8    disable    mac-vlan
xge-1/0/9    disable    mac-vlan
xge-1/0/10   disable    mac-vlan
xge-1/0/11   disable    mac-vlan
xge-1/0/12   disable    mac-vlan
xge-1/0/13   disable    mac-vlan
xge-1/0/14   disable    mac-vlan
xge-1/0/15   disable    mac-vlan
xge-1/0/16   disable    mac-vlan
xge-1/0/17   disable    mac-vlan
xge-1/0/18   disable    mac-vlan
xge-1/0/19   disable    mac-vlan
xge-1/0/20   disable    mac-vlan
xge-1/0/21   disable    mac-vlan
xge-1/0/22   disable    mac-vlan
xge-1/0/23   disable    mac-vlan
xge-1/0/24   disable    mac-vlan

```

```
Switch>
```

3.5.22 vlan precedence

Function

The **vlan precedence** command sets the preferred method for adding an interface to a VLAN when both mac-vlan and ip-subnet-vlan match.

Format

vlan precedence { mac-vlan | ip-subnet-vlan }

Parameter

Parameter	Description	Value
mac-vlan	Matches the VLAN based on the MAC address first.	-
ip-subnet-vlan	Matches the VLAN based on the subnet IP address.	-

Default Value

By default, VLAN matching is based on MAC addresses.

View

Ethernet bridge interface configuration view (not applicable for 10G interface)

Usage Guidelines

NA

Example

Match the VLAN based on the subnet IP address.

```
Switch(config-25ge1/0/1)#work-mode bridge
Switch(config-25ge1/0/1)#vlan precedence ip-subnet-vlan
Switch(config-25ge1/0/1)#
```

3.5.23 debug ip-subnet-vlan**Function**

The **debug ip-subnet-vlan** command enables VLAN debugging for an IP subnet.

The **no debug ip-subnet-vlan** command disables VLAN debugging for an IP subnet.

Format

- **debug ip-subnet-vlan**
- **no debug ip-subnet-vlan**

Parameter

NA

Default Value

NA

View

Privileged user view

Usage Guidelines

NA

Example

Enable VLAN debugging for the IP subnet.

```
Switch#debug ip-subnet-vlan
Switch#
```

3.5.24 vlan-mode {normal|super}

Function

The **vlan-mode {normal|super}** command sets the VLAN mode.

Format

vlan-mode { normal | super }

Parameter

Parameter	Description	Value
normal	Specifies a normal VLAN mode.	-
super	Specifies a VLAN aggregation mode.	-

Default Value

normal

View

VLAN configuration view

Usage Guidelines

NA

Example

Set the VLAN mode.

```
Switch(vlan-2)#vlan-mode super
Switch(vlan-2)#
```

3.6 VLAN Mapping Configuration Commands

3.6.1 debug vlan-mapping

Function

The **debug vlan-mapping** command enables VLAN mapping debugging.

The **no debug vlan-mapping** command disables VLAN mapping debugging.

Format

- **debug vlan-mapping**
- **no debug vlan-mapping**

Parameter

NA

Default Value

By default, VLAN mapping debugging is disabled.

View

Privileged user view

Usage Guidelines

NA

Example

Enable VLAN mapping debugging.

```
Switch#debug vlan-mapping
```

```
Switch#
```

3.6.2 vlan-mapping {enable|disable}**Function**

The **vlan-mapping {enable|disable}** command enables or disables the interface-VLAN mapping function.

Format

vlan-mapping { enable | disable }

Parameter

Parameter	Description	Value
enable	Enables the interface-VLAN mapping function.	-
disable	Disables the interface-VLAN mapping function.	-

Default Value

Disable

View

Ethernet bridge interface configuration view, interface configuration view (Trunk)

Usage Guidelines

NA

Example

Enable the interface-VLAN mapping function.

```
Switch(config-10ge1/0/1)#vlan-mapping enable
Switch(config-10ge1/0/1)#
```

3.6.3 vlan-mapping vlan map-vlan**Function**

The **vlan-mapping inner-vlan map-inner-vlan** command sets the action of replacing the packet VLAN ID in the flow action.

The **vlan-mapping vlan map-vlan (remark-8021p)** command configures a 1:1 VLAN mapping entry and matches the outer VLAN ID in a packet to change the outer VLAN ID and priority.

The **vlan-mapping vlan to map-vlan (remark-8021p)** command sets an N:1 VLAN mapping entry and matches the outer VLAN ID in a packet to change the outer VLAN ID and priority. N:1 means mapping multiple user-side VLAN ID labels within the specified range to a network-side VLAN ID label.

The **vlan-mapping vlan inner-vlan map-vlan (remark-8021p)** command matches the outer VLAN ID and inner VLAN ID in a packet to change the outer VLAN and priority, and matches the outer VLAN ID in a packet to change the outer VLAN ID and priority.

The **vlan-mapping vlan inner-vlan to map-vlan (remark-8021p)** command matches the outer VLAN ID and N:1 inner VLAN ID in a packet to modify the outer VLAN ID and priority, and matches the inner and outer VLAN IDs in a packet to change the outer VLAN ID and priority. N:1 means mapping multiple inner VLAN IDs to the outer label of the VLAN to which the interface belong.

The **no vlan-mapping all** command deletes all the configured VLAN mapping entries.

The **no vlan-mapping vlan** command deletes the specified VLAN mapping entry.

Format

- **vlan-mapping inner-vlan** *outside-vlan-id* **map-inner-vlan** *outside-mapping-vlan-id*
- **vlan-mapping inner-vlan** *outside-vlan-id* **map-inner-vlan** *outside-mapping-vlan-id* **remark-8021p** *priority*
- **vlan-mapping inner-vlan** *outside-vlan-id1* **to** *outside-vlan-id2* **map-inner-vlan** *inner-mapping-vlan-id*

- **vlan-mapping inner-vlan outside-vlan-id1 to outside-vlan-id2 map-inner-vlan inner-mapping-vlan-id remark-8021p priority**
- **vlan-mapping 8021p priority map-vlan outside-mapping-vlan-id**
- **vlan-mapping vlan outside-vlan-id map-vlan outside-mapping-vlan-id**
- **vlan-mapping vlan outside-vlan-id map-vlan outside-mapping-vlan-id remark-8021p priority**
- **vlan-mapping vlan outside-vlan-id1 to outside-vlan-id2 map-vlan outside-mapping-vlan-id**
- **vlan-mapping vlan outside-vlan-id1 to outside-vlan-id2 map-vlan outside-mapping-vlan-id remark-8021p priority**
- **vlan-mapping vlan outside-vlan-id 8021p priority map-vlan outside-mapping-vlan-id remark-8021p priority**
- **vlan-mapping vlan outside-vlan-id 8021p priority map-vlan outside-mapping-vlan-id**
- **vlan-mapping vlan outside-vlan-id 8021p priority to priority map-vlan outside-mapping-vlan-id**
- **vlan-mapping vlan outside-vlan-id 8021p priority to priority map-vlan outside-mapping-vlan-id remark-8021p priority**
- **vlan-mapping vlan outside-vlan-id1 to outside-vlan-id2 8021p priority map-vlan outside-mapping-vlan-id**
- **vlan-mapping vlan outside-vlan-id1 to outside-vlan-id2 8021p priority to priority map-vlan outside-mapping-vlan-id remark-8021p priority**
- **vlan-mapping vlan outside-vlan-id1 to outside-vlan-id2 8021p priority to priority map-vlan outside-mapping-vlan-id**
- **vlan-mapping vlan outside-vlan-id inner-vlan inner-mapping-vlan-id map-single-vlan single-vlan**
- **vlan-mapping vlan outside-vlan-id inner-vlan inner-mapping-vlan-id map-vlan map-vlan**
- **vlan-mapping vlan outside-vlan-id inner-vlan inner-mapping-vlan-id map-vlan map-vlan map-inner-vlan map-inner-vlan**
- **vlan-mapping vlan outside-vlan-id inner-vlan inner-mapping-vlan-id map-vlan map-vlan map-inner-vlan map-inner-vlan remark-8021p priority**
- **vlan-mapping vlan outside-vlan-id inner-vlan inner-mapping-vlan-id map-vlan map-vlan remark-8021p priority**

- **vlan-mapping** **vlan** *outside-vlan-id* **inner-vlan** *inner-mapping-vlan-id1* **to** *inner-mapping-vlan-id2* **map-vlan** *map-vlan*
- **vlan-mapping** **vlan** *outside-vlan-id* **inner-vlan** *inner-mapping-vlan-id1* **to** *inner-mapping-vlan-id2* **map-vlan** *map-vlan* **remark-8021p** *priority*
- **no** **vlan-mapping** **all**
- **no** **vlan-mapping** **8021p** *priority*
- **no** **vlan-mapping** **vlan** *outside-vlan-id* **8021p** *priority* **map-vlan** *outside-mapping-vlan-id*
- **no** **vlan-mapping** **vlan** *outside-vlan-id* **8021p** *priority* **to** *priority* **map-vlan** *outside-mapping-vlan-id*
- **no** **vlan-mapping** **vlan** *outside-vlan-id1* **to** *outside-vlan-id2* **8021p** *priority* **map-vlan** *outside-mapping-vlan-id*
- **no** **vlan-mapping** **vlan** *outside-vlan-id* **inner-vlan** *inner-mapping-vlan-id*
- **no** **vlan-mapping** **vlan** *outside-vlan-id* **inner-vlan** *inner-mapping-vlan-id1* **to** *inner-mapping-vlan-id2*
- **no** **vlan-mapping** **vlan** *outside-vlan-id1* **to** *outside-vlan-id2* **8021p** *priority* **to** *priority* **map-vlan** *outside-mapping-vlan-id*
- **no** **vlan-mapping** **inner-vlan** *inner-mapping-vlan-id*
- **no** **vlan-mapping** **inner-vlan** *inner-mapping-vlan-id1* **to** *inner-mapping-vlan-id2*
- **no** **vlan-mapping** **vlan** *outside-vlan-id*
- **no** **vlan-mapping** **vlan** *outside-vlan-id* **to** *outside-mapping-vlan-id*

Parameter

Parameter	Description	Value
outside-vlan-id	Specifies the outer VLAN ID of an interface.	The value is an integer ranging from 1 to 4094.
outside-mapping-vlan-id	Specifies the mapped outer VLAN ID of an interface.	
priority	Specifies a VLAN priority.	The value is an integer ranging from 1 to 7.
inner-vlan-id	Specifies the inner VLAN ID of an interface.	The value is an integer ranging from 1 to 4094.
inner-mapping-vlan-id	Maps the inner VLAN ID to the outer label of the VLAN to which	

Parameter	Description	Value
	the port belongs.	
inner-mapping-vlan-id1	Specifies a start inner VLAN ID.	
inner-mapping-vlan-id2	Specifies an end inner VLAN ID.	
map-vlan	Maps the VLAN ID.	
map-inner-vlan	Maps the inner VLAN ID.	

Default Value

NA

View

Ethernet bridge interface configuration view, interface configuration view (Trunk)

Usage Guidelines

The switch supports 1:1 and N:1 mapping of a single-layer VLAN.

Example

Configure a VLAN mapping entry.

```
Switch(config-10ge1/0/1)#vlan-mapping vlan 10 map-vlan 100
Switch(config-10ge1/0/1)#
```

3.6.4 show vlan-mapping

Function

The **show vlan-mapping** command displays VLAN mapping information, including configuration and interface information.

Format

- **show vlan-mapping**
- **show vlan-mapping config**
- **show vlan-mapping interface { ethernet | xgigaethernet | 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet } interface-number**
- **show vlan-mapping interface eth-trunk trunk-number**

Parameter

Parameter	Description	Value
interface-number	Specifies an Ethernet	The value is an integer in the range of <1-1>/<0-1>/<1-48>.

Parameter	Description	Value
	interface number.	
trunk-number	Specifies the ID of a Trunk group.	The value is an integer ranging from 1 to 128.

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

Display VLAN mapping information.

```
Switch>show vlan-mapping
  Support Max Interface Number    :24
  Support Max Map List Number     :128
  Current Map List Number        :1
  Interface      Out-VID  Map-OutVID
  xgigaethernet 1/0/2  10/10    100
Switch>
```

3.7 VLAN STACKING Configuration Commands

3.7.1 debug vlan-stacking

Function

The **debug vlan-stacking** command enables debugging of selective QinQ.

The **no debug vlan-stacking** command disables debugging of selective QinQ.

Format

- **debug vlan-stacking**
- **no debug vlan-stacking**

Parameter

NA

Default Value

NA

View

Privileged user view

Usage Guidelines

NA

Example

Enable debugging of selective QinQ.

```
Switch#debug vlan-stacking
Switch#
```

3.8 QinQ Configuration Commands

3.8.1 vlan-stacking {enable|disable}

FunctionThe **vlan-stacking {enable|disable}** command enables or disables VLAN stacking.**Format****vlan-stacking { enable | disable }****Parameter**

Parameter	Description	Value
enable	Enables VLAN stacking.	-
disable	Disables VLAN stacking.	-

Default Value

NA

View

Interface group configuration view (Trunk), Ethernet bridge interface configuration view

Usage Guidelines

NA

Example

Enable flexible QinQ for the interface **XGE1/0/1** and add the outer VLAN20 to the user **VLAN2**.

```
Switch(config-10ge1/0/1)#vlan-stacking enable
Switch(config-10ge1/0/1)#
```

3.8.2 vlan-stacking vlan stack-vlan

Function

The **vlan-stacking vlan stack-vlan** command enables flexible QinQ for a single or multiple VLANs.

The **vlan-stacking vlan stack-vlan remark-8021p** command enables flexible QinQ based on a single or multiple VLAN IDs and 802.1p priorities.

The **no vlan-stacking** command deletes the configured flexible QinQ.

Format

- **vlan-stacking vlan *vlan-id1* stack-vlan *vlan-id2***
- **vlan-stacking vlan *vlan-id3* to *vlan-id4* stack-vlan *vlan-id2***
- **vlan-stacking vlan *vlan-id1* stack-vlan *vlan-id2* remark-8021p *priority***
- **vlan-stacking vlan *vlan-id3* to *vlan-id4* stack-vlan *vlan-id2* remark-8021p *priority***
- **vlan-stacking vlan *vlan-id1* 8021p *priority* stack-vlan *vlan-id2***
- **vlan-stacking vlan *vlan-id1* 8021p *priority* stack-vlan *vlan-id2* remark-8021p *priority***
- **vlan-stacking vlan *vlan-id3* to *vlan-id4* 8021p *priority* stack-vlan *vlan-id2***
- **vlan-stacking vlan *vlan-id3* to *vlan-id4* 8021p *priority* stack-vlan *vlan-id2* remark-8021p *priority***
- **vlan-stacking 8021p *priority* stack-vlan *vlan-id2* remark-8021p *priority***
- **vlan-stacking 8021p *priority* stack-vlan *vlan-id2***
- **vlan-stacking 8021p *priority* to *priority* stack-vlan *vlan-id2* remark-8021p *priority***
- **vlan-stacking 8021p *priority* to *priority* stack-vlan *vlan-id2***
- **vlan-stacking untagged stack-vlan *vlan-id2* stack-inner-vlan *vlan-id5***
- **vlan-stacking vlan *vlan-id1* 8021p *priority* stack-vlan *vlan-id2* remark-8021p *priority***
- **vlan-stacking vlan *vlan-id1* 8021p *priority* stack-vlan *vlan-id2***
- **vlan-stacking vlan *vlan-id3* 8021p *priority* to *priority* stack-vlan *vlan-id4***

- **vlan-stacking** **vlan** *vlan-id3* **8021p** *priority* **to** *priority* **stack-vlan** *vlan-id4* **remark-8021p** *priority*
- **no** **vlan-stacking** **all**
- **no** **vlan-stacking** **vlan** *vlan-id1*
- **no** **vlan-stacking** **vlan** *vlan-id1* **to** *vlan-id2*
- **no** **vlan-stacking** **vlan** *vlan-id1* **8021p** *priority*
- **no** **vlan-stacking** **vlan** *vlan-id3* **to** *vlan-id4* **8021p** *priority*
- **no** **vlan-stacking** **8021p** *priority* **to** *priority*
- **no** **vlan-stacking** **8021p** *priority*
- **no** **vlan-stacking** **untagged**
- **no** **vlan-stacking** **vlan** *vlan-id3* **to** *vlan-id4* **8021p** *priority* **to** *priority*

Parameter

Parameter	Description	Value
vlan-id1	Specifies the first user VLAN ID to be mapped or indicates a single VLAN.	The value is an integer ranging from 1 to 4094.
vlan-id2	Specifies an outer VLAN ID tag.	
vlan-id3	Specifies the first VLAN ID among the user VLAN IDs to be mapped.	
vlan-id4	Specifies the last VLAN ID among the user VLAN IDs to be mapped.	
vlan-id5	Stacks an inner VLAN ID tag.	
priority	Specifies the 802.1p priority.	The value is an integer ranging from 0 to 7.

Default Value

NA

View

Interface group configuration view (Trunk), Ethernet bridge interface configuration view, Ethernet routing interface configuration view

Usage Guidelines

When a packet in this VLAN needs to traverse the carrier's network, you can use this command to add a VLAN tag to the packet to form a dual-layer VLAN.

When enabling flexible QinQ, pay attention to the following points:

The interface must be a hybrid interface and is valid only in the inbound direction.

The stacked outer VLAN must exist, and the current interface must be added to the stack VLAN in untagged mode.

Example

Enable flexible QinQ for the interface **XGE1/0/1** and add the outer VLAN20 to the user **VLAN2**.

```
Switch(config-10ge1/0/1)#vlan-stacking vlan 2 stack-vlan 20
Switch(config-10ge1/0/1)#
```

3.8.3 show vlan-stacking

Function

The **show vlan-stacking** command displays information about selective QinQ.

Format

- **show vlan-stacking**
- **show vlan-stacking config interface**
- **show vlan-stacking config interface { ethernet | xgigaethernet | 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet } interface-number**
- **show vlan-stacking interface**
- **show vlan-stacking interface { ethernet | xgigaethernet | 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet } interface-number**
- **show vlan-stacking interface eth-trunk trunk-number**
- **show vlan-stacking config interface eth-trunk trunk-number**

Parameter

Parameter	Description	Value
interface-number	Specifies an Ethernet interface number.	The value is an integer in the range of <1-1>/<0-1>/<1-48>.
trunk-number	Specifies an ID of the Trunk group.	The value is an integer ranging from 1 to 128.

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

View information about flexible QinQ

```
Switch>show vlan-stacking
  Max interface number      :332
  Max qinq items            :8192
  Current qinq items        :0
Switch>
```

3.9 ARP Proxy Configuration Commands

3.9.1 show arp-proxy config

Function

The **show arp-proxy config** command displays the ARP proxy configuration.

Format

show arp-proxy config

Parameter

NA

Default Value

NA

View

Common user view

Usage Guidelines

This command displays information such as the voice VLAN ID.

Example

Display the ARP proxy configuration.

```
Switch>show arp-proxy config
```

```

vlan 2
arp-proxy enable
arp-proxy inner-sub-vlan-proxy enable
Switch>

```

3.9.2 show arp-proxy interface

Function

The **show arp-proxy interface** command displays the interface information on the ARP proxy.

Format

show arp-proxy interface

Parameter

NA

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

Display the ARP proxy configuration in VLANs.

```

Switch>show arp-proxy interface

```

Interface	ArpProxy
xgigaethernet 1/0/1	disable
xgigaethernet 1/0/2	disable
xgigaethernet 1/0/3	disable
xgigaethernet 1/0/4	disable
xgigaethernet 1/0/5	disable
xgigaethernet 1/0/6	disable
xgigaethernet 1/0/7	disable
xgigaethernet 1/0/8	disable
xgigaethernet 1/0/9	disable
xgigaethernet 1/0/10	disable
xgigaethernet 1/0/11	disable

```

xgigaethernet 1/0/12    disable
xgigaethernet 1/0/13    disable
xgigaethernet 1/0/14    disable
xgigaethernet 1/0/15    disable
xgigaethernet 1/0/16    disable
xgigaethernet 1/0/17    disable
xgigaethernet 1/0/18    disable
xgigaethernet 1/0/19    disable
xgigaethernet 1/0/20    disable
xgigaethernet 1/0/21    disable
xgigaethernet 1/0/22    disable
xgigaethernet 1/0/23    disable
xgigaethernet 1/0/24    disable
xgigaethernet 1/0/25    disable
xgigaethernet 1/0/26    disable
xgigaethernet 1/0/27    disable
xgigaethernet 1/0/28    disable
xgigaethernet 1/0/29    disable
xgigaethernet 1/0/30    disable
xgigaethernet 1/0/31    disable
xgigaethernet 1/0/32    disable
xgigaethernet 1/0/33    disable
xgigaethernet 1/0/34    disable
xgigaethernet 1/0/35    disable
xgigaethernet 1/0/36    disable
xgigaethernet 1/0/37    disable
xgigaethernet 1/0/38    disable
xgigaethernet 1/0/39    disable
xgigaethernet 1/0/40    disable
vlan 1                  disable
Switch>

```

3.9.3 show arp-proxy vlan

Function

The **show arp-proxy vlan** command displays the ARP proxy configuration in VLANs.

Format

show arp-proxy vlan

Parameter

NA

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

Display the ARP proxy configuration in VLANs.

```
Switch>show arp-proxy vlan
Vlan ArpProxy  InnerSubVlanProxy  InterSubVlanProxy
  1    disable    disable                disable
  2    enable     enable                disable
Switch>
```

3.9.4 debug arp-proxy**Function**The **debug arp-proxy** command enables synchronous debugging of Proxy ARP.The **no debug arp-proxy** command disables synchronous debugging of Proxy ARP.**Format**

- **debug arp-proxy**
- **no debug arp-proxy**

Parameter

NA

Default Value

By default, ARP proxy debugging is disabled.

View

Privileged user view

Usage Guidelines

NA

Example

Disable ARP proxy debugging.

```
Switch#no debug arp-proxy
Switch#
```

3.9.5 arp-proxy {enable|disable}**Function**

The **arp-proxy {enable|disable}** command enables or disables the routed ARP proxy function on a VLAN interface.

Format

arp-proxy { enable | disable }

Parameter

Parameter	Description	Value
enable	Enables the routed ARP proxy function on the VLAN interface.	-
disable	Disables the routed ARP proxy function on the VLAN interface.	-

Default Value

By default, the routed ARP proxy function is disabled on a VLAN interface.

View

VLANIF configuration view, Ethernet routing interface configuration view

Usage Guidelines

When two hosts are located in different networks physically, with their IP addresses in different subnets of the same IP network and without a gateway configured, you can run the **arp-proxy enable** to enable ARP proxy on the switch connecting the two hosts. The switch can then provide IP address resolution between the hosts.

Example

Enable the routed ARP proxy function on a VLAN interface.

```
Switch(config-vlanif-2)#arp-proxy enable
Switch(config-vlanif-2)#
```

3.9.6 arp-proxy inner-sub-vlan-proxy {enable|disable}

Function

The **arp-proxy inner-sub-vlan-proxy {enable|disable}** command enables or disables the ARP proxy function on a VLAN.

Format

arp-proxy inner-sub-vlan-proxy { enable | disable }

Parameter

Parameter	Description	Value
enable	Enables the ARP proxy function on a VLAN.	-
disable	Disables the ARP proxy function on a VLAN.	-

Default Value

NA

View

VLANIF configuration view

Usage Guidelines

NA

Example

Enable the ARP proxy function on a VLAN.

```
Switch(config-vlanif-2)#arp-proxy inner-sub-vlan-proxy enable
Switch(config-vlanif-2)#
```

3.9.7 arp-proxy inter-sub-vlan-proxy {enable|disable}

Function

The **arp-proxy inter-sub-vlan-proxy {enable|disable}** command enables or disables the ARP proxy function between VLANs.

Format

arp-proxy inter-sub-vlan-proxy { enable | disable }

Parameter

Parameter	Description	Value
enable	Enables the ARP proxy function between VLANs.	-

Parameter	Description	Value
disable	Disables the ARP proxy function between VLANs.	-

Default Value

NA

View

VLANIF configuration view

Usage Guidelines

NA

Example

Enable the ARP proxy function between VLANs.

```
Switch(config-vlanif-2)#arp-proxy inter-sub-vlan-proxy enable
Switch(config-vlanif-2)#
```

3.10 MAM Configuration Commands

3.10.1 debug mam

Function

The **debug mam** command enables debugging of the MAM module.

The **no debug mam** command enables debugging of the MAM module.

Format

- **debug mam { error | mac | flush | mac-limit | sync | hw | nm | event | if | history | aging | all }**
- **no debug mam { error | mac | flush | mac-limit | sync | hw | nm | event | if | history | aging | all }**

Parameter

Parameter	Description	Value
error	Debugs the error information.	-
mac	Displays MAC address changes.	-
flush	Displays flush operations.	-
mac-limit	Displays the MAC address limit.	-
sync	Displays the synchronization information.	-

Parameter	Description	Value
hw	Displays hardware information.	-
nm	Displays network management operations.	-
event	Displays event handling information.	-
if	Displays the interface.	-
history	Displays the MAC address record.	-
aging	Displays the MAC address aging time.	-
all	Displays all debugging information.	-

Default Value

By default, debugging for received and sent ARP packets is disabled.

View

Privileged user view

Usage Guidelines

NA

Example

Enable debugging of the MAM module.

```
Switch#debug mam nm
Switch#
```

3.11 Port Security Configuration Commands

3.11.1 port-security {enable|disable}

Function

The **port-security {enable|disable}** command enables or disables port security.

Format

port-security { enable | disable }

Parameter

Parameter	Description	Value
enable	Enables port security.	-
disable	Disables port security.	-

Default Value

Port security is disabled by default.

View

Ethernet bridge interface configuration view, interface configuration view (Trunk)

Usage Guidelines

NA

Example

Enable the security function for **gigaethernet1/0/1**.

```
Switch(config-10ge1/0/1)#port-security enable
Switch(config-10ge1/0/1)#
```

3.11.2 port-security mac-address sticky {enable|disable}

Function

The **port-security mac-address sticky {enable|disable}** command enables or disables the sticky MAC address.

Format

port-security mac-address sticky { enable | disable }

Parameter

Parameter	Description	Value
enable	Enables the sticky MAC address.	-
disable	Disables the sticky MAC address.	-

Default Value

The sticky MAC address is disabled by default.

View

Ethernet bridge interface configuration view, interface configuration view (Trunk)

Usage Guidelines

NA

Example

Enable the sticky MAC address for **gigaethernet 1/0/1**.

```
Switch(config-10ge1/0/1)#port-security enable
```

```
Switch(config-10ge1/0/1)#port-security mac-address sticky enable
Switch(config-10ge1/0/1)#
```

3.11.3 port-security maximum

Function

The **port-security maximum** command sets the maximum number of secure MAC addresses for a port.

Format

port-security maximum { *mac-number* | **default** }

Parameter

Parameter	Description	Value
mac-number	Specifies the maximum number of secure MAC addresses for a port.	The value is an integer ranging from 1 to 4094, in seconds.
default	Specifies the default value.	1

Default Value

The maximum number of secure MAC addresses for a port is 1 by default.

View

Ethernet bridge interface configuration view, interface configuration view (Trunk)

Usage Guidelines

NA

Example

Set the maximum number of secure MAC addresses for the port **gigaehternet 1/0/1**.

```
Switch(config-10ge1/0/1)#port-security enable
Switch(config-10ge1/0/1)#port-security maximum 10
Switch(config-10ge1/0/1)#
```

3.11.4 port-security mac-address sticky vlan

Function

The **port-security mac-address sticky vlan** command creates a secure MAC address entry.

The **no port-security mac-address sticky vlan** command deletes a secure MAC address entry.

Format

- **port-security mac-address sticky vlan** *vlan-id mac-address*
- **no port-security mac-address sticky**
- **no port-security mac-address sticky vlan** *vlan-id*
- **no port-security mac-address sticky vlan** *vlan-id mac-address*

Parameter

Parameter	Description	Value
vlan-id	Specifies a VLAN ID.	The value is an integer ranging from 1 to 4094.
mac-address	Specifies a secure MAC address.	The format is AA:BB:CC:DD:EE:FF, where A to F are hexadecimal digits.

Default Value

NA

View

Ethernet bridge interface configuration view, interface configuration view (Trunk)

Usage Guidelines

Before running this command, you must run the **port-security mac-address sticky enable** command to enable the **sticky-mac** function.

Example

Create a secure MAC address.

```
Switch(config-10ge1/0/1)#port-security enable
Switch(config-10ge1/0/1)#port-security mac-address sticky enable
Switch(config-10ge1/0/1)#port-security mac-address sticky vlan 1 00:00:00:00:00:01
```

3.11.5 port-security protect-action

Function

The **port-security protect-action** command sets a protection action for the port security function on an interface.

Format

port-security protect-action { protect | restrict | shutdown }

Parameter

Parameter	Description	Value
protect	Drops the packets with source MAC addresses out of the MAC address table when the number of learned MAC addresses reaches the limit on the interface.	-
restrict	Drops the packets with source MAC addresses out of the MAC address table and sends traps when the number of learned MAC addresses reaches the limit on the interface.	-
shutdown	Shuts down the interface when the number of learned MAC addresses reaches the limit on the interface.	-

Default Value

The default protection action is **restrict**.

View

Ethernet bridge interface configuration view, interface configuration view (Trunk)

Usage Guidelines

Before using this command, run the **port-security enable** command to enable port security.

Example

Set a protection action for the port security function.

```
Switch(config-10ge1/0/1)#port-security enable
Switch(config-10ge1/0/1)#port-security protect-action protect
Switch(config-10ge1/0/1)#
```

3.12 Port Isolation Configuration Commands

3.12.1 debug port-isolate

Function

The **debug port-isolate** command enables debugging of Layer-2 and Layer-3 port isolation.

The **no debug port-isolate** command disables debugging of Layer-2 and Layer-3 port isolation.

Format

- **debug port-isolate**
- **no debug port-isolate**

Parameter

NA

Default Value

NA

View

Privileged user view

Usage Guidelines

NA

Example

Enable debugging of Layer-2 and Layer-3 port isolation.

Switch#debug port-isolate

Switch#

3.12.2 port-isolate mode**Function**The **port-isolate mode** command configures Layer 2 or Layer 3 port isolation.**Format****port-isolate mode { l2 | all }****Parameter**

Parameter	Description	Value
l2	Sets the port isolation mode to Layer 2 port isolation.	-
all	Sets the port isolation mode to both Layer 2 and Layer 3 isolation.	-

Default Value

NA

View

Global configuration view

Usage Guidelines

NA

Example

Set the port isolation mode to Layer-2 port isolation.

```
Switch(config)#port-isolate mode l2
Switch(config)#
```

3.12.3 port-isolate group

Function

The **port-isolate group** command creates a port isolation group.

Format

port-isolate group *group-number*

Parameter

Parameter	Description	Value
group-number	Specifies the number of a port isolation group.	The value is an integer ranging from 1 to 8.

Default Value

NA

View

Global configuration view, isolation group configuration view

Usage Guidelines

NA

Example

Create port isolation group 1.

```
Switch(config)#port-isolate group 1
Switch(config-isolate-group1)#
```

3.12.4 port-uniisolate

Function

The **port-uniisolate** command configures unidirectional port isolation.

Format

- **port-uniisolate interface** { **ethernet** | **xgigaethernet** | **10gigaethernet** | **25gigaethernet** | **40gigaethernet** | **100gigaethernet** } *interface-number*
- **port-uniisolate interface eth-trunk** *trunk-number*

- **no port-uniisolate interface** { **ethernet** | **xgigaethernet** | **10gigaethernet** | **25gigaethernet** | **40gigaethernet** | **100gigaethernet** } *interface-number*
- **no port-uniisolate interface eth-trunk** *trunk-number*

Parameter

Parameter	Description	Value
interface-number	Specifies an Ethernet interface number.	The value is an integer in the range of <1-1>/<0-1>/<1-48>.
trunk-number	Specifies the number of a Trunk interface.	The value is an integer ranging from 1 to 128.

Default Value

NA

View

Ethernet bridge interface configuration view, Ethernet routing interface configuration view, interface configuration view (Trunk)

Usage Guidelines

NA

Example

Set unidirectional port isolation for the port **gigaethernet 1/0/1**.

```
Switch(config-10ge1/0/1)#port-uniisolate interface gigaethernet 1/0/1
Switch(config-10ge1/0/1)#
```

3.12.5 join port-isolate group

Function

The **join port-isolate group** command adds an interface to an isolation group.

The **no join port-isolate group** command deletes an interface from an isolation group.

Format

- **join port-isolate group** *group-id*
- **join port-isolate group** *group-list*
- **no join port-isolate group** *group-id*
- **no join port-isolate group** *group-list*

- **no join port-isolate group all**

Parameter

Parameter	Description	Value
group-id	Specifies an isolation group ID.	The value is an integer ranging from 1 to 8.
group-list	Specifies a sequence ID of the isolation group. You can enter multiple VLAN IDs.	The format is 1,3,5 to 10. VLAN IDs are separated by a comma (,) or an en dash (-, indicating a range).

Default Value

NA

View

Ethernet bridge interface configuration view, Ethernet routing interface configuration view, interface configuration view (Trunk)

Usage Guidelines

This command adds an interface to a port isolation group. Interfaces in an isolation group can communicate with interfaces out of the isolation group but cannot communicate with interfaces in the same isolation group.

Example

Add the interface **gigaehternet1/0/1** to the isolation group 4.

```
Switch(config-10ge1/0/1)#join port-isolate group 4
Switch(config-10ge1/0/1)#
```

3.12.6 add interface

Function

The **add interface** command adds an interface to an isolation group.

The **no interface** command deletes a port from an isolation group.

Format

- **add interface** { **ethernet** | **xgigaethernet** | **10gigaethernet** | **25gigaethernet** | **40gigaethernet** | **100gigaethernet** } *interface-number*
- **add interface eth-trunk** *trunk-number*
- **no interface** { **ethernet** | **xgigaethernet** | **10gigaethernet** | **25gigaethernet** | **40gigaethernet** | **100gigaethernet** } *interface-number*

- **no interface eth-trunk** *trunk-number*

Parameter

Parameter	Description	Value
interface-number	Specifies an Ethernet interface number.	The value is an integer in the range of <1-1>/<0-1>/<1-48>.
trunk-number	Specifies the number of a Trunk interface.	The value is an integer ranging from 1 to 128.

Default Value

NA

View

Isolation group configuration view

Usage Guidelines

NA

Example

Add interface gigaethernet1/0/1 to isolation group 1.

```
Switch(config)#port-isolate group 1
Switch(config-isolate-group1)#add interface gigaethernet 1/0/1
Switch(config-isolate-group1)#
```

3.12.7 show port-isolate group

Function

The **show port-isolate group** command displays information about all or specified port isolation groups.

Format

- **show port-isolate group**
- **show port-isolate group** *group-number*

Parameter

Parameter	Description	Value

group-number	Specifies the number of a port isolation group.	The value is an integer ranging from 1 to 256.

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

Display information about port isolation group 2.

Switch>show port-isolate group 2

The interfaces in isolate group 2:

gigaethernet-1/0/1

Switch>

3.12.8 show port-isolate information**Function**The **show port-isolate information** command displays information about all port isolation groups.**Format****show port-isolate information****Parameter**

NA

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

Display information about all port isolation groups.

```
Switch>show port-isolate information
Isolate Mode : allIsolate
Support Max Port Isolate Group Count: 8
Support Max Interface Count for Each Group : 256
Current Used Interface-Group Node Count: 0
Current Free Interface-Group Node Count: 2048
Support Max Interface Count : 256
Support Max Unidirectional Isolate target Interface Count : 16
Current Used Unidirectional-Isolate Node Count: 0
Current Used Bidirectional-Isolate Node Count: 0
Current Free Isolate Node Count: 32640
Switch>
```

3.12.9 show port-uniisolate interface**Function**

The **show port-uniisolate interface** command displays the configuration of unidirectional port isolation.

The **show port-uniisolate online interface** command displays the configuration of online unidirectionally isolated port pairs.

Format

- **show port-uniisolate interface**
- **show port-uniisolate online interface**
- **show port-uniisolate interface { ethernet | xgigaethernet | 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet } interface-number**
- **show port-uniisolate interface eth-trunk trunk-number**

Parameter

Parameter	Description	Value
interface-number	Specifies an Ethernet interface number.	The value is an integer in the range of <1-1>/<0-1>/<1-48>.

trunk-number	Specifies the number of a Trunk interface.	The value is an integer ranging from 1 to 128.

Default Value

NA

View

Common user view

Usage Guidelines

The switch supports a maximum of 64 unidirectional port isolation groups.

Example

Display the configuration of unidirectional port isolation.

```
Switch>show port-uniisolate interface
uniisolate -port      being uniisolated-port
gigaethernet-1/0/1    gigaethernet-1/0/2
Switch>
```

3.12.10 show port-isolate config**Function**

The **show port-isolate config** command displays the isolation group configuration as a configuration file.

Format

show port-isolate config

Parameter

NA

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

Display configuration of all port isolation groups.

```
Switch>show port-isolate config
Version                :PORTISOLATE_VB3.00.08.00
Switch>
```

3.13 Storm Control Configuration Commands

3.13.1 storm-control

Function

The **storm-control** command enables an Ethernet interface to perform storm control on broadcast, multicast or unknown unicast packets.

The **no storm-control** command disables the storm control function.

Format

- **no storm-control** { **broadcast** | **multicast** | **dlf** }
- **storm-control** { **broadcast** | **multicast** | **dlf** } **percent** *value*
- **storm-control** { **broadcast** | **multicast** | **dlf** } **cir** { **kbps** | **mbps** | **gbps** } *cir-value* **cbs** { **bytes** | **kbytes** | **mbytes** } *cbs-value*
- **storm-control** { **broadcast** | **multicast** | **dlf** } **pps** *pps-value*

Parameter

Parameter	Description	Value
broadcast	Configures storm control for broadcast packets.	-
multicast	Configures storm control for multicast packets.	-
dlf	Configures storm control for unknown unicast packets.	-
value	Specifies a rate limit value.	The value is an integer ranging from 0 to 100.
pps-value	Specifies the number of packets per second.	The value is an integer ranging from 0 to 148810000.
cir-value	Specifies the committed information rate (CIR).	The value is an integer ranging from 0 to 10000000.
cbs-value	Specifies the committed burst size (CBS).	The value is an integer ranging from 10000 to 4294967295.

Default Value

Rate control is not performed for broadcast, multicast or unknown unicast packets by default.

View

Ethernet bridge interface configuration view, Ethernet routing interface configuration view, Trunk interface configuration view

Usage Guidelines

To avoid network resource waste, you can run this command to prevent the broadcast, multicast or unknown unicast packets on the network from occupying too much bandwidth to ensure the service.

Example

Configure an Ethernet interface to perform storm control on broadcast packets.

```
Switch(config-10ge1/0/1)#storm-control broadcast percent 50
Switch(config-10ge1/0/1)#
```

3.13.2 debug storm-control**Function**

The **debug storm-control** command enables storm control debugging.

The **no debug storm-control** command disables storm control debugging.

Format

- **debug storm-control { nm | if | vlan | vsi | event | all }**
- **no debug storm-control { nm | if | vlan | vsi | event | all }**

Parameter

Parameter	Description	Value
nm	Indicates storm control network management.	-
If	Indicates the storm control interface node.	-
vlan	Indicates the storm control VLAN node.	-
vsi	Indicates the storm control VSI node.	-
event	Indicates storm control events.	-
all	Displays all debugging information.	-

Default Value

NA

View

Privileged user view

Usage Guidelines

NA

Example

Enable storm control debugging.

```
Switch#debug storm-control event
Switch#
```

3.13.3 show storm-control**Function**

The **show storm-control interface** command displays the storm control information on an interface.

The **show storm-control vlan** command displays the storm control information on a VLAN interface.

The **show storm-control vsi** command displays the storm control information on a VSI interface.

The **show storm-control config** command displays the storm control configuration.

Format

- **show storm-control interface**
- **show storm-control interface { ethernet | xgigaethernet | 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet } interface-number**
- **show storm-control vlan**
- **show storm-control vlan [vlan-id]**
- **show storm-control vsi**
- **show storm-control vsi [vsi-name]**
- **show storm-control config**

Parameter

Parameter	Description	Value
interface-number	Specifies an Ethernet interface number.	The value is an integer in the range of <1-1>/<0-1>/<1-48>.

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

Display the storm control information on an interface.

Switch>show storm-control interface

Interface	Type	Status	Limit	Mode	CIR(bps)	CBS(bytes)

Switch>

3.14 MLAG Configuration Commands

3.14.1 debug mlag

FunctionThe **debug mlag** command enables MLAG debugging.The **no debug mlag** command disables MLAG debugging.**Format**

- **debug mlag { in | out | timer | notify | global | if | packet | error | all }**
- **no debug mlag { in | out | timer | notify | global | if | packet | error | all }**

Parameter

Parameter	Description	Value
in	Displays debugging information about egress packets.	-
out	Displays debugging information about ingress packets.	-
timer	Displays timer information.	-
notify	Displays notification information.	-
global	Specifies global information.	-
if	Displays interface information.	-
packet	Displays packet information.	-
error	Debugs error information.	-
all	Displays all the preceding information.	-

Default Value

Disable

View

Privileged user view

Usage Guidelines

NA

Example

Enable MLAG debugging.

```
Switch#debug mlag all
Switch#
```

3.14.2 lacp mlag priority**Function**

The **lacp mlag priority** command sets the LACP MLAG priority.

Format

lacp mlag priority { *priority-value* | **default** }

Parameter

Parameter	Description	Value
priority-value	Specifies an LACP MLAG priority. A smaller value indicates a higher priority.	The value is an integer ranging from 1 to 65535.
default	Specifies the default LACP MLAG priority.	32768

Default Value

NA

View

Global configuration view

Usage Guidelines

The LACP MLAG priority configured in the global configuration view is applicable to all Eth-Trunk interfaces.

The priority of devices at two ends of the Eth-Trunk interface based on LACP MLAG is distinguished by the LACP MLAG priority. The device with a higher priority acts as the active

LACP end, and the other end selects the active interface based on the priority of the LACP active end's priority, to make the active interfaces of two ends consistent.

Example

Set the LACP MLAG priority.

```
Switch(config)#lacp mlag priority 10
Switch(config)#
```

3.14.3 lacp mlag system-id

Function

The **lacp mlag system-id** command sets the LACP MLAG system ID.

Format

lacp mlag system-id *mac-address*

Parameter

Parameter	Description	Value
mac-address	Specifies an LACP MLAG ID. A lower ID indicates a higher priority.	The format is AA:BB:CC:DD:EE:FF, where A to F are hexadecimal digits.

Default Value

MAC address of the switch.

View

Global configuration view

Usage Guidelines

The LACP MLAG ID configured in the global configuration view is applicable to all Eth-Trunk interfaces.

When the LACP MLAG priorities at two ends of the Eth-Trunk interface are the same, run **lacp mlag system-id** to set the LACP MLAG ID to determine the priority of devices at the two ends and make the active interfaces of devices at the two ends are the same.

Example

Set the LACP MLAG ID.

```
Switch(config)#lacp mlag system-id 04:f8:f8:e5:b8:ba
Switch(config)#
```

3.14.4 mlag exclude interface

Function

The **mlag exclude interface** command sets a reserved MLAG interface.

The **no mlag exclude interface** command deletes the configured reserved MLAG interface.

Format

- **mlag exclude interface** { **ethernet** | **xgigaethernet** | **10gigaethernet** | **25gigaethernet** | **40gigaethernet** | **100gigaethernet** } *interface-number*
- **mlag exclude interface eth-trunk** *trunk-number*
- **no mlag exclude interface** { **ethernet** | **xgigaethernet** | **10gigaethernet** | **25gigaethernet** | **40gigaethernet** | **100gigaethernet** } *interface-number*
- **no mlag exclude interface eth-trunk** *trunk-number*

Parameter

Parameter	Description	Value
interface-number	Specifies an Ethernet interface number.	The value is an integer in the range of <1-1>/<0-1>/<1-48>.
trunk-number	Specifies the number of a Trunk interface.	The value is an integer ranging from 1 to 128.
vlan-id	Specifies a VLAN ID.	The value is an integer ranging from 1 to 4094.

Default Value

NA

View

Global configuration view

Usage Guidelines

NA

Example

Set a reserved MLAG interface.

```
Switch(config)#mlag exclude interface xgigaethernet 1/0/1
Switch(config)#
```

3.14.5 mlag-group

Function

The **mlag-group** command creates an MLAG group.

The **no join mlag** command deletes an MLAG group.

Format

- **mlag-group** *mlag-group*
- **no mlag-group** *mlag-group*

Parameter

Parameter	Description	Value
mlag-group	Specifies the index of an MLAG group.	The value is an integer ranging <1-1>. Only group 1 is supported currently.

Default Value

NA

View

Global configuration view

Usage Guidelines

NA

Example

Create an MLAG group.

```
Switch(config)#mlag-group 1
Switch(config-mlag-1)#
```

3.14.6 mlag interface eth-trunk

Function

The **mlag interface eth-trunk** command sets an Eth-trunk interface for an MLAG member aggregation group.

The **no mlag** command deletes the configured MLAG member aggregation group.

Format

- **mlag** *mlag-member* **interface eth-trunk** *trunk-number*
- **no mlag** *mlag-member*

Parameter

Parameter	Description	Value
trunk-number	Specifies the number of an Eth-trunk interface.	The value is an integer ranging from 1 to 128.
mrag-member	Specifies the ID of an MLAG member aggregation group.	The value is an integer ranging from 1 to 128.

Default Value

NA

View

MLAG configuration view

Usage Guidelines

NA

Example

Set an Eth-trunk interface for an MLAG member aggregation group.

```
Switch(config-mrag-1)#mrag 1 interface eth-trunk 1
Switch(config-mrag-1)#
```

3.14.7 peerlink exclude vlan**Function**

The **peerlink exclude vlan** command configures a list of VLANs through which the MLAG links cannot pass.

The **no peerlink exclude vlan** command deletes the configuration.

Format

- **peerlink exclude vlan** *vlan-list*
- **no peerlink exclude vlan** *vlan-list*

Parameter

Parameter	Description	Value
vlan-list	Specifies a list of VLANs through which the MLAG links cannot pass.	The value is an integer ranging from 1 to 4094.

Default Value

NA

View

MLAG configuration view

Usage Guidelines

NA

Example

Set a list of VLANs through which the MLAG links cannot pass.

```
Switch(config-mlag-1)#peerlink exclude vlan 2
Switch(config-mlag-1)#
```

3.14.8 peerlink interface eth-trunk

Function

The **peerlink interface eth-trunk** command sets an Eth-trunk interface to be a peer-link interface.

The **no peerlink interface** command cancels the configuration of setting the specified interface to be a peer-link interface.

Format

- **peerlink interface eth-trunk** *trunk-number*
- **no peerlink interface**

Parameter

Parameter	Description	Value
trunk-number	Specifies the number of an Eth-trunk interface.	The value is an integer ranging from 1 to 128.

Default Value

NA

View

MLAG configuration view

Usage Guidelines

NA

Example

Set an Eth-trunk interface to be a peer-link interface.

```
Switch(config-mlag-1)#peerlink interface eth-trunk 1
Switch(config-mlag-1)#
```

3.14.9 priority

Function

The **priority** command sets the MLAG priority.

Format

priority { *priority-value* | **default** }

Parameter

Parameter	Description	Value
priority-value	Specifies an MLAG priority.	The value is an integer ranging from 1 to 255.
default	Specifies the default MLAG priority.	1

Default Value

1

View

MLAG configuration view

Usage Guidelines

Two devices for which MLAG is enabled to negotiate to determine which one is the active and which one is the standby based on the negotiation packet. During negotiation, MLAG determines the active and standby devices based on the priority and system MAC address. The device of a higher priority is active. Then, you can run **priority** to set the MLAG priority for the device to determine its active and standby state.

Example

Set the MLAG priority.

```
Switch(config-mlag-1)#priority 10
Switch(config-mlag-1)#
```

3.14.10 reset counter

Function

The **reset counter** command clears the MLAG counter.

Format

reset counter

Parameter

NA

Default Value

NA

View

MLAG configuration view

Usage Guidelines

NA

Example

Clear the MLAG counter.

Switch(config-mlag-1)#reset counter

Switch(config-mlag-1)#

3.14.11 security-key**Function**The **security-key** command sets a security password.The **no security-key** command deletes the configured security password.**Format**

- **security-key** { **simple** | **md5** } { **plain** | **cipher** } *key*
- **no security-key**

Parameter

Parameter	Description	Value
simple	Specifies a simple text password.	-
md5	Specifies an MD5 cipher password.	-
key	Specifies a security password string.	The value is a string consisting of up to 15 characters.

Default Value

NA

View

MLAG configuration view

Usage Guidelines

NA

Example

Set a security password.

```
Switch(config-mlag-1)#security-key simple abcdefg
Switch(config-mlag-1)#
```

3.14.12 show mlag**Function**The **show mlag** command displays the MLAG system information.**Format****show mlag****Parameter**

NA

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

Display MLAG system information.

```
Switch>show mlag
Max mlag group number      :1
Current mlag group number:1
lacp system-id             :68:21:5f:dc:25:02
lacp priority              :32768
The MLAG group 1 information:
  Priority                  :10
  Peerlink                 :eth-trunk 128
  Role                     :BACKUP           PeerRole           :MASTER
  Send-Period (1s)        :3                 Fail-Time (1s)         :9
```

ProtoType	:layer2	Peer-Priority	:1
Peer-Send-Time	:3	Peer-Fail-Time	:9
Security-Key-Type	:md5	Security-Key	:switch
Source-IP	:2000:100::2	Peer-IP	:2000:100::1
DAD detect state	:OK	DAD conflict state	:NORMAL
In	:5797	Out	:5797
InDrop	:0	OutDrop	:2
In DAD	:10433	Out DAD	:17346
In DAD error	:0	Out DAD fail	:3
Switch>			

3.14.13 show mlag config

Function

The **show mlag config** command displays the MLAG configuration file.

Format

show mlag config

Parameter

NA

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

Display MLAG system information.

```
Switch> show mlag config
!
lacp mlag system-id 68:21:5f:dc:25:02
mlag-group 1
peerlink interface eth-trunk 128
priority 10
source-address 2000:100::2 vpn-instance mlag
security-key md5 plain switch
```

```
mlag 1 interface eth-trunk 1
Switch>
```

3.14.14 show mlag consistency

Function

The **show mlag consistency** command displays the MLAG configuration consistency.

Format

show mlag consistency

Parameter

NA

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

View the MLAG configuration consistency.

```
Switch>show mlag consistency
-----
Configuration      Local value          Peer value
-----
----- STP -----
----- VLAN -----

VLAN:3858
VLANIF(STATUS)      up                   N/A
VLANIF(VRRP)        ipv6 vrrpv3         N/A

VLAN:3859
VLANIF(STATUS)      up                   N/A
VLANIF(VRRP)        ipv6 vrrpv3         N/A

VLAN:3860
```

```

VLANIF(STATUS)      up      N/A
VLANIF(VRRP)        ipv6 vrrpv3  N/A

VLAN:3861
VLANIF(STATUS)      up      N/A
VLANIF(VRRP)        ipv6 vrrpv3  N/A
...
Switch>

```

3.14.15 show mlag exclude interface

Function

The **show mlag exclude interface** command displays the MLAG reserved interface information.

Format

show mlag exclude interface

Parameter

NA

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

View the MLAG reserved interface information.

```

Switch>show mlag exclude interface
  Mlag Default Exclude Interface
                25ge1/0/5
                25ge1/0/48
                100ge1/1/2

Switch>

```

3.14.16 show mlag-group

Function

The **show mlag-group** command displays the MLAG information.

Format

- **show mlag-group** *mlag-group*

Parameter

Parameter	Description	Value
mlag-group	Specifies an index of the MLAG group.	The value is an integer ranging <1-1>. Only group 1 is supported currently.

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

View the MLAG information.

```
Switch>show mlag-group 1
The MLAG group 1 information:
  Priority           :10
  Peerlink           :eth-trunk 128
  Role               :BACKUP           PeerRole           :MASTER
  Send-Period (1s)  :3                Fail-Time (1s)      :9
  ProtoType          :layer2           Peer-Priority        :1
  Peer-Send-Time     :3                Peer-Fail-Time       :9
  Security-Key-Type  :md5              Security-Key         :switch
  Source-IP          :2000:100::2      Peer-IP              :2000:100::1
  DAD detect state   :OK                DAD conflict state   :NORMAL
  In                 :5852              Out                  :5853
  InDrop             :0                OutDrop              :2
  In DAD             :10534             Out DAD              :17513
  In DAD error       :0                Out DAD fail         :3

                The Member information(Total number 1)
  MLAG ID   Trunk ID   State(a/o)   PeerValid   Peer ID   PeerState
  1         1         down/down    VALID       1         up

Switch>
```

3.14.17 source-address

Function

The **source-address** command sets detecting the local IPv4 or IPv6 address and VPN instance in active-active mode.

The **no source-address** command cancels the configuration.

Format

- **source-address** *ipv4-address*
- **source-address** *ipv4-address* **peer-address** *peer-ipv4-address*
- **source-address** *ipv4-address* **vpn-instance** *name*
- **source-address** *ipv4-address* **vpn-instance** *name* **peer-address** *peer-ipv4-address*
- **source-address** *ipv6-address*
- **source-address** *ipv6-address* **peer-address** *peer-ipv6-address*
- **source-address** *ipv6-address* **vpn-instance** *name*
- **source-address** *ipv6-address* **vpn-instance** *name* **peer-address** *peer-ipv6-address*
- **no source-address**

Parameter

Parameter	Description	Value
ipv4-address	Specifies an IPv4 address.	The value is in dotted decimal notation.
peer-ipv4-address	Specifies an IPv4 address of the bound peer device.	The value is in dotted decimal notation.
ipv6-address	Specifies an IPv6 address.	The total length is 128 bits divided into 8 groups. Each group consists of 4 hexadecimal digits. The format is X:X:X:X:X:X:X.
peer-ipv6-address	Specifies an IPv6 address of the bound peer device.	The total length is 128 bits divided into 8 groups. Each group consists of 4 hexadecimal digits. The format is X:X:X:X:X:X:X.
name	Specifies a VPN instance name.	The value is a character string.

Default Value

NA

View

MLAG configuration view

Usage Guidelines

NA

Example

Set detecting the local IPv4 or IPv6 address in active-active mode.

```
Switch(config-mlag-1)#source-address 10.18.12.11
Switch(config-mlag-1)#
```

3.14.18 timer hello**Function**

The **timer hello** command sets the sending interval timer for the Hello packets.

Format

timer hello { *hello-interval* | **default** }

Parameter

Parameter	Description	Value
hello-interval	Specifies a sending interval of Hello packets.	The value is an integer ranging from 3 to 30, in seconds.
default	Specifies the default sending interval of Hello packets.	3 seconds

Default Value

3 seconds

View

MLAG configuration view

Usage Guidelines

NA

Example

Set the sending interval timer of Hello packets.

```
Switch(config-mlag-1)#timer hello 10
Switch(config-mlag-1)#
```


3.14.19 timer hold-on-failure multiplier

Function

The **timer hold-on-failure multiplier** command sets the multiplier timer for Hello packet sending interval.

Format

timer hold-on-failure multiplier { *value* | **default** }

Parameter

Parameter	Description	Value
value	Specifies a multiplier of the Hello sending interval.	The value is an integer ranging from 3 to 15.
default	Specifies the default multiplier 3.	3

Default Value

3

View

MLAG configuration view

Usage Guidelines

NA

Example

Set a multiplier of the Hello sending interval.

```
Switch(config-mlag-1)#timer hold-on-failure multiplier 5
Switch(config-mlag-1)#
```

3.14.20 up-delay

Function

The **up-delay** command sets the delay for an MLAG member interface to report the UP state.

Format

up-delay { *delay-value* | **default** } [**auto-recovery interval** { *interval-value* | **default** }]

Parameter

Parameter	Description	Value
delay-value	Specifies a delay for an MLAG member	The value is an integer ranging from 0 to

Parameter	Description	Value
	interface to report the UP state.	3600, in seconds.
default	Specifies the default delay for an MLAG member interface to report the UP state.	240s
interval-value	Specifies the delay for MLAG member interfaces to automatically restore the connection based on the delay for reporting the UP state.	The value is an integer ranging from 0 to 180, in seconds.
default	Specifies the default delay for automatic restoration.	0

Default Value

3

View

MLAG configuration view

Usage Guidelines

NA

Example

Set the delay for an MLAG member interface to report the UP state to 90s.

```
Switch(config-mlag-1)#up-delay 90
Switch(config-mlag-1)#
```

3.14.21 dad enhance {enable|disable}

Function

The **dad enhance {enable|disable}** command enables or disables the DAD enhancing function in MLAG mode.

Format

dad enhance { enable | disable }

Parameter

Parameter	Description	Value
enable	Enables the DAD enhancing function in MLAG mode.	-
disable	Disables the DAD enhancing function in MLAG mode.	-

Default Value

Disable

View

MLAG configuration view

Usage Guidelines

NA

Example

Enable the DAD enhancing function in MLAG mode.

```
Switch(config-mlag-1)#dad enhance enable
Switch(config-mlag-1)#
```

3.14.22 mlag ip address

Function

The **mlag ip address** command configures the IPv4 slave address specific for OSPF/BGP over MLAG.

The **no mlag ip address** command deletes the IPv4 slave address specific for OSPF/BGP over MLAG.

Format

- **mlag ip address** *ipv4-address mask-address*
- **mlag ip address** *ipv4-address mask-address*
- **no mlag ip address**

Parameter

Parameter	Description	Value
ipv4-address	Specifies an IPv4 address.	The value is in dotted decimal notation, such as A.B.C.D, where each of A to D is a decimal number ranging from 0 to 255.
mask-address	Specifies a mask address.	The value is in dotted decimal notation.
M	Specifies the number of mask digits.	The value is an integer ranging from 1 to 32.

Default Value

By default, no IPv4 slave address specific for OSPF/BGP over MLAG is configured.

View

VLANIF configuration view, BD interface configuration view

Usage Guidelines

- Each interface can have only one MLAG IPv4 slave address.
- You must configure the master address first.
- The MLAG slave address must be in the same network segment of the master address.
- A new MLAG slave address directly overwrites the old MLAG slave address.

Example

Configure the IPv4 slave address specific for OSPF/BGP over MLAG to 10.1.1.10/24.

```
Switch(config-vlanif-10)#ip address 10.1.1.1/24
Switch(config-vlanif-10)#mlag ip address 10.1.1.10/24
Switch(config-vlanif-10)#
```

3.14.23 mlag ipv6 address

Function

The **mlag ipv6 address** command configures the IPv6 slave address specific for OSPFv3/BGP over MLAG.

The **no mlag ipv6 address** command deletes the IPv6 slave address specific for OSPFv3/BGP over MLAG.

Format

- **mlag ipv6 address** *ipv6-address/M*
- **no mlag ipv6 address**

Parameter

Parameter	Description	Value
ipv6-address	Specifies an IPv6 address.	The value is in 32-bit hexadecimal format, such as X:X::X:X, where Xs are hexadecimal digits 0-9 and A-F. The value cannot be all 0s or all Fs.
M	Specifies the number of mask digits.	The value is an integer ranging from 1 to 128.

Default Value

By default, no IPv6 slave address specific for OSPFv3/BGP over MLAG is configured.

View

VLANIF configuration view, BD interface configuration view

Usage Guidelines

- Each interface can have only one MLAG IPv6 slave address.
- You must configure the master address first.
- The MLAG IPv6 slave address must be in the same network segment of the master address.
- A new MLAG IPv6 slave address overwrites the old MLAG IPv6 slave address.

Example

Configure the IPv6 slave address specific for OSPFv3/BGP over MLAG to 1001::10/64.

```
Switch(config-vlanif-10)#ipv6 address 1001::1/64
Switch(config-vlanif-10)#mlag ipv6 address 1001::10/64
Switch(config-vlanif-10)#
```

3.14.24 mlag ipv6 address link-local**Function**

The **mlag ipv6 address linklocal** command configures the IPv6 link-local address specific for OSPFv3/BGP over MLAG.

The **no mlag ipv6 address linklocal** command deletes the IPv6 link-local address specific for OSPFv3/BGP over MLAG.

Format

- **mlag ipv6 address** *ipv6-address* **link-local**
- **no mlag ipv6 address link-local**

Parameter

Parameter	Description	Value
ipv6-address	Specifies an IPv6 link-local address.	The value is in 32-bit hexadecimal format, such as X:X::X:X, where Xs are hexadecimal digits 0-9 and A-F. The value cannot be all 0s or all Fs.

Default Value

By default, no IPv6 link-local address specific for OSPFv3/BGP over MLAG is configured for an interface.

View

VLANIF configuration view, BD interface configuration view

Usage Guidelines

Each interface can have at most one link-local address.

Example

Configure the IPv6 link-local address specific for OSPFv3/BGP over MLAG to fe80:1::1.

```
Switch(config-vlanif-10)#mlag ipv6 address fe80:1::1 link-local
Switch(config-vlanif-10)#
```

Chapter 4 IP Commands

This chapter introduces commands for configuring IPv4/IPv6 addresses and DHCP functions.

4.1 IPv4 Address Configuration Commands

4.1.1 ip address

Function

The **ip address** command configures an IP address for a VLAN interface.

The **no ip address** command deletes all IP addresses or an IP address for VLAN interface.

Format

- **ip address** *ip-address/mask-length*
- **ip address** *ip-address mask-address*
- **ip address** *ip-address mask-address sub*
- **ip address** *ip-address/mask-length sub*
- **no ip address** *ip-address*
- **no ip address**

Parameter

Parameter	Description	Value
ip-address	Specifies the IP address of a VLAN interface.	The value is in dotted decimal notation.
mask-address	Specifies a mask address.	The value is in dotted decimal notation.
ip-address/mask-length	Specifies an IP address and a mask length.	The value is in dotted decimal notation. mask-length specifies the mask length, which is an integer ranging from 1 to 32.

Default Value

By default, no IP address is configured in each VLAN view.

View

VLANIF configuration view, out-of-band interface configuration view, Loopback interface configuration view, Tunnel interface configuration view, BD interface configuration view, Ethernet routing interface configuration view

Usage Guidelines

This command assigns an IP address and mask to a VLAN interface to ensure network connectivity. To enable an interface to connect to multiple subnets, you can configure multiple IP address for the interface, where one IP address functions as a primary IP address and other IP addresses function as secondary IP addresses. If the interface already has a primary IP address, when you configure a primary IP address for the interface, its original primary IP address is deleted, and the new one takes effect. Before deleting the primary IP address, you must delete all secondary IP addresses.

Example

Set the primary IP address to 10.18.13.200 and subnet mask length to 24 in VLAN 3.

```
Switch(config-vlanif-3)#ip address 10.18.13.200/24
Switch(config-vlanif-3)#
```

4.1.2 ip tcp max-connect

Function

The **ip tcp max-connect** command sets the maximum number of TCP connections allowed on the switch.

Format

ip tcp max-connect { *max-num* | **default** }

Parameter

Parameter	Description	Value
max-num	Specifies the maximum number of TCP connections.	The value is an integer ranging from 1 to 300.
default	Restores the maximum number of TCP connections to the default value.	300

Default Value

By default, the maximum number of TCP connections is 300.

View

Global configuration view

Usage Guidelines

You can use this command to limit the maximum number of TCP connections. For example, when a Telnet service is enabled on the switch, you can set the maximum number of connections.

Example

Set the maximum number of TCP connections to 25.

```
Switch(config)#ip tcp max-connect 25
```

```
Switch(config)#
```

4.1.3 debug ip

Function

The **debug ip** command enables sent or received IP packet debugging.

The **no debug ip** command disables sent or received IP packet debugging.

Format

- **debug ip { in | out | error | all | source check }**
- **no debug ip { in | out | error | all | source check }**

Parameter

Parameter	Description	Value
in	Displays debugging information about received packets.	-
out	Displays debugging information about sent packets.	-
error	Displays debugging information about error packets.	-
all	Displays debugging information about all IP packets.	-

Default Value

By default, IP debugging is disabled.

View

Privileged user view

Usage Guidelines

This command is used to maintain and debug IP functions of the switch.

Example

Enable the IP packet debugging function.

```
Switch#debug ip in
Switch#
```

4.1.4 debug ip dst-addr

Function

The **debug ip dst-addr** command enables the debugging for sent and received packets with the specified destination IP address.

The **no debug ip dst-addr** command disables the debugging for sent and received packets with the specified destination IP address.

Format

- **debug ip dst-addr** *dst-addr*
- **no debug ip dst-addr**

Parameter

Parameter	Description	Value
dst-addr	Specifies a destination IP address.	The value is in dotted decimal notation.

Default Value

By default, debugging for received and sent packets with the specified destination IP address is disabled.

View

Privileged user view

Usage Guidelines

NA

Example

Enable the debugging for sent and received packets with the specified destination IP address.

```
Switch#debug ip dst-addr 10.12.3.23
Switch#
```

4.1.5 debug ip src-addr

Function

The **debug ip src-addr** command enables the debugging for sent and received packets with the specified source IP address.

The **no debug ip src-addr** command disables the debugging for sent and received packets with the specified source IP address.

Format

- **debug ip src-addr** *src-addr*
- **no debug ip src-addr**

Parameter

Parameter	Description	Value
src-addr	Specifies a source IP address.	The value is in dotted decimal notation.

Default Value

By default, debugging for received and sent packets with the specified source IP address is disabled.

View

Privileged user view

Usage Guidelines

NA

Example

Enable the debugging for sent and received packets with the specified source IP address.

```
Switch#debug ip src-addr 10.12.3.23
Switch#
```

4.1.6 show ip config

Function

The **show ip config** command displays the IP address configuration.

Format

show ip config

Parameter

NA

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

Display the IP address configuration.

```
Switch>show ip config
!ip address configuration
  outband ip address 10.18.12.120/24
!
!Ip Configuration
  ip arp aging-time 600
Switch>
```

4.1.7 show ip connect-table

Function

The **show ip connect-table** command displays the TCP/UDP connection information.

Format

show ip connect-table

Parameter

NA

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

Display the TCP/UDP connection information.

```

Switch>show ip connect-table

rawip socket :
so_fibnum[0],inc_fibnum[0],so_name[],Recv-Q[0],Recv-mb[0],Recv-lowat[1],Recv-space[1],Recv-hiwait[1],Send
-Q[0],Send-mb[0],Send-lowat[2048],Send-space[9216],Send-hiwait[9216]
    Local Address: 0.0.0.0
    Foreign Address: 0.0.0.0

rawip socket :
so_fibnum[0],inc_fibnum[0],so_name[],Recv-Q[0],Recv-mb[0],Recv-lowat[1],Recv-space[9216],Recv-hiwait[921
6],Send-Q[0],Send-mb[0],Send-lowat[2048],Send-space[9216],Send-hiwait[9216]
    Local Address:::.0

    Foreign Address:::.0

rawip socket :
so_fibnum[0],inc_fibnum[0],so_name[],Recv-Q[0],Recv-mb[0],Recv-lowat[1],Recv-space[1],Recv-hiwait[1],Send
-Q[0],Send-mb[0],Send-lowat[2048],Send-space[9216],Send-hiwait[9216]
    Local Address: 0.0.0.0
    Foreign Address: 0.0.0.0

tcp socket :
tp[0x73fed2d0],unused[0],t_state[1],so_fibnum[0],inc_fibnum[0],so_name[],Recv-Q[0],so_rcv.sb_acc[0],tqh_first
[0],so_error[0],Recv-mb[0],Recv-lowat[1],Recv-space[8192],Recv-hiwait[8192],Send-Q[0],Send-mb[0],Send-low
at[2048],Send-space[16384],Send-hiwait[16384]
    Local Address: 0.0.0.0.23
    Foreign Address: 0.0.0.0

    State: LISTEN

tcp socket :
tp[0x73fed000],unused[0],t_state[1],so_fibnum[0],inc_fibnum[0],so_name[],Recv-Q[0],so_rcv.sb_acc[0],tqh_first
[0],so_error[0],Recv-mb[0],Recv-lowat[1],Recv-space[8192],Recv-hiwait[8192],Send-Q[0],Send-mb[0],Send-low
at[2048],Send-space[16384],Send-hiwait[16384]
    Local Address:::.23

    Foreign Address:::.0

    State: LISTEN

udp socket :
so_fibnum[0],inc_fibnum[0],so_name[],Recv-Q[0],Recv-mb[0],Recv-lowat[1],Recv-space[42400],Recv-hiwait[42
400],Send-Q[0],Send-mb[0],Send-lowat[2048],Send-space[8192],Send-hiwait[8192]
    Local Address:::.0

    Foreign Address:::.0

```

```

udp socket :
so_fibnum[0],inc_fibnum[0],so_name[],Recv-Q[0],Recv-mb[0],Recv-lowat[1],Recv-space[42400],Recv-hiwait[42
400],Send-Q[0],Send-mb[0],Send-lowat[2048],Send-space[9216],Send-hiwait[9216]
    Local Address:::.161

    Foreign Address:::.0

udp socket :
so_fibnum[0],inc_fibnum[0],so_name[],Recv-Q[0],Recv-mb[0],Recv-lowat[1],Recv-space[42400],Recv-hiwait[42
400],Send-Q[0],Send-mb[0],Send-lowat[2048],Send-space[8192],Send-hiwait[8192]
    Local Address: 0.0.0.0
    Foreign Address: 0.0.0.0

udp socket :
so_fibnum[0],inc_fibnum[0],so_name[],Recv-Q[0],Recv-mb[0],Recv-lowat[1],Recv-space[42400],Recv-hiwait[42
400],Send-Q[0],Send-mb[0],Send-lowat[2048],Send-space[9216],Send-hiwait[9216]
    Local Address: 0.0.0.0.161
    Foreign Address: 0.0.0.0

udp socket :
so_fibnum[0],inc_fibnum[0],so_name[],Recv-Q[0],Recv-mb[0],Recv-lowat[1],Recv-space[42400],Recv-hiwait[42
400],Send-Q[0],Send-mb[0],Send-lowat[2048],Send-space[9216],Send-hiwait[9216]
    Local Address:::.546

    Foreign Address:::.0

udp socket :
so_fibnum[0],inc_fibnum[0],so_name[],Recv-Q[0],Recv-mb[0],Recv-lowat[1],Recv-space[42400],Recv-hiwait[42
400],Send-Q[0],Send-mb[0],Send-lowat[2048],Send-space[9216],Send-hiwait[9216]
    Local Address:::.547

    Foreign Address:::.0

udp socket :
so_fibnum[0],inc_fibnum[0],so_name[],Recv-Q[0],Recv-mb[0],Recv-lowat[1],Recv-space[1],Recv-hiwait[1],Send
-Q[0],Send-mb[0],Send-lowat[2048],Send-space[1024000],Send-hiwait[1024000]
    Local Address: 0.0.0.0.68
    Foreign Address: 0.0.0.0

udp socket :
so_fibnum[0],inc_fibnum[0],so_name[],Recv-Q[0],Recv-mb[0],Recv-lowat[1],Recv-space[1],Recv-hiwait[1],Send
-Q[0],Send-mb[0],Send-lowat[2048],Send-space[1024000],Send-hiwait[1024000]
    Local Address: 0.0.0.0.67
    Foreign Address: 0.0.0.0

udp socket :

```

```

so_fibnum[0],inc_fibnum[0],so_name[],Recv-Q[0],Recv-mb[0],Recv-lowat[1],Recv-space[42400],Recv-hiwait[42
400],Send-Q[0],Send-mb[0],Send-lowat[2048],Send-space[9216],Send-hiwait[9216]

    Local Address:::.123

    Foreign Address:::.0

udp socket :
so_fibnum[0],inc_fibnum[0],so_name[],Recv-Q[0],Recv-mb[0],Recv-lowat[1],Recv-space[42400],Recv-hiwait[42
400],Send-Q[0],Send-mb[0],Send-lowat[2048],Send-space[9216],Send-hiwait[9216]

    Local Address: 0.0.0.0.123
    Foreign Address: 0.0.0.0.0

Switch>

```

4.1.8 show ip interface

Function

The **show ip interface** command displays IPv4 interface information or interface information in VPN instances.

Format

- **show ip interface**
- **show ip interface vpn-instance *name***

Parameter

Parameter	Description	Value
name	Specifies a VPN instance name.	The value is a string of up to 64 characters.

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

View the IPv4 interface information.

```

Switch>show ip interface

The total number of ip address: 267

```

Ip-Address	Interface	IPIndex	State(a/o)	Role	Type	Vpn-instance
1.1.1.1/32	loopback1	1	up/up	primary	static	N/A
10.1.1.1/24	vlan100	2	up/up	primary	static	N/A
10.1.2.1/24	vlan200	3	up/down	primary	static	N/A
10.1.5.1/24	vlan500	4	up/up	primary	static	N/A
10.1.6.1/24	vlan600	5	up/up	primary	static	N/A
101.1.1.2/24	vlan1001	6	up/down	primary	static	N/A
101.1.2.2/24	vlan1002	7	up/down	primary	static	N/A
101.1.3.2/24	vlan1003	8	up/down	primary	static	N/A
101.1.4.2/24	vlan1004	9	up/down	primary	static	N/A
101.1.5.2/24	vlan1005	10	up/down	primary	static	N/A
101.1.6.2/24	vlan1006	11	up/down	primary	static	N/A
101.1.7.2/24	vlan1007	12	up/down	primary	static	N/A
101.1.8.2/24	vlan1008	13	up/down	primary	static	N/A
101.1.9.2/24	vlan1009	14	up/down	primary	static	N/A
101.1.10.2/24	vlan1010	15	up/down	primary	static	N/A
101.1.11.2/24	vlan1011	16	up/down	primary	static	N/A
101.1.12.2/24	vlan1012	17	up/down	primary	static	N/A
101.1.13.2/24	vlan1013	18	up/down	primary	static	N/A
101.1.14.2/24	vlan1014	19	up/down	primary	static	N/A
101.1.15.2/24	vlan1015	20	up/down	primary	static	N/A

Switch>

4.1.9 show ip statistic

Function

The **show ip statistic** command displays IP statistics.

Format

- **show ip statistic**
- **show ip tcp statistic**
- **show ip udp statistic**
- **show ip icmp statistic**

Parameter

NA

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

Display IP statistics.

```
Switch>show ip statistic
total:                    52475
badsum:                   0
tooshort:                 0
toosmall:                 0
badhlen:                  0
badlen:                   0
infragments:             5419
fragdropped:              0
fragtimeout:              0
forward:                  0
fastforward:              0
cantforward:              0
redirectsent:             0
unknownprotocol:          0
delivered:                28783
localout:                 6161
nobuffers:                0
reassembled:              4104
fragmented:               0
outfragments:             9505
cantfrag:                 0
badoptions:               0
noroute:                  7279
badvers:                  0
rawout:                   6161
toolong:                  0
notmember:                0
nogif:                    0
badaddr:                  0
Switch>
```

4.2 IPv6 Address Configuration Commands

4.2.1 debug ipv6

Function

The **debug ipv6** command enables debugging for received and sent IPv6 packets.

The **no debug ipv6** command disables debugging for received and sent IPv6 packets.

Format

- **debug ipv6 { in | out | error | all | nd l2-proxy | pim }**
- **no debug ipv6 { in | out | error | all | nd l2-proxy | pim }**

Parameter

Parameter	Description	Value
in	Displays debugging information about received packets.	-
out	Displays debugging information about sent packets.	-
error	Displays debugging information about error packets.	-
all	Displays debugging information about all IP packets.	-

Default Value

By default, IPv6 debugging is disabled.

View

Privileged user view

Usage Guidelines

You can run this command to maintain and debug the device IPv6 functions.

Example

Enable IPv6 debugging and display the received packets.

```
Switch#debug ipv6 in
Switch#
```

4.2.2 ipv6 {enable|disable}

Function

The **ipv6 {enable|disable}** command enables or disables the IPv6 function for an interface.

Format

ipv6 { enable | disable }

Parameter

NA

Default Value

Disable

View

VLANIF configuration view, out-of-band interface configuration view, Tunnel interface configuration view, BD interface configuration view, Ethernet routing interface configuration view, and Loopback interface configuration view

Usage Guidelines

NA

Example

Enable the IPv6 function for an interface.

```
Switch(config-vlanif-3)#ipv6 enable
Switch(config-vlanif-3)#
```

4.2.3 ipv6 nd direct-route {enable|disable}

Function

The **ipv6 nd direct-route {enable|disable}** command enables IPv6 neighbors to forward host routes or disables such forwarding.

Format

ipv6 nd direct-route { enable | disable }

Parameter

Parameter	Description	Value
enable	Enables IPv6 neighbors to forward host routes.	-
disable	Disables such forwarding.	-

Default Value

By default, IPv6 neighbors forwarding host routes is disabled.

View

VLANIF configuration view, BD interface configuration view

Usage Guidelines

You must run the **ipv6 enable** command to enable IPv6 for the interface first.

Example

Enable IPv6 neighbors to forward host routes.

```
Switch(config-bridge-domain-10)#ipv6 enable
Switch(config-bridge-domain-10)#ipv6 nd direct-route enable
```

4.2.4 ipv6 address

Function

The **ipv6 address** command sets the primary and secondary IPv6 addresses.

The **no ipv6 address** command deletes a specified or all IPv6 addresses.

Format

- **ipv6 address** *ipv6-address/mask-length*
- **ipv6 address** *ipv6-address/mask-length* **sub**
- **no ipv6 address** *ipv6-address*
- **no ipv6 address**

Parameter

Parameter	Description	Value
ipv6-address	Specifies the IPv6 address of an interface.	In this format, a 128-digit IP address is divided into 8 segments. Each segment consists of 16 digits and is represented by 4 hexadecimal characters (0-9 and A-F). Segments are separated by colons (:). Every "X" represents a group of hexadecimal digits.
mask-length	Specifies the mask length of an IPv6 address.	The value is an integer ranging from 0 to 128.

Default Value

By default, the global unicast address is generated based on the system MAC address.

View

VLANIF configuration view, out-of-band interface configuration view, Tunnel interface configuration view, BD interface configuration view, Ethernet routing interface configuration view, and Loopback interface configuration view

Usage Guidelines

You can set only one primary address, but can set multiple secondary addresses. Different VLANIF must have different IPv6 addresses.

When the port is not VLANIF, you need to judge the work mode. If the work mode is **bridge**, the IPv6 address cannot be set.

Before running this command, you must run `ipv6 {enable|disable}` to enable the IPv6 function for the interface.

Example

Set the primary IPv6 address to **21DA:D3:0:2F3B:2AA:FF:FE28:9C5A** and mask length to **2**.

```
Switch(config-vlanif-3)#ipv6 address 21DA:D3:0:2F3B:2AA:FF:FE28:9C5A/2
```

```
Switch(config-vlanif-3)#
```

4.2.5 ipv6 address eui

Function

The **ipv6 address eui** command sets a global unicast address command in the format of EUI-64.

The **no ipv6 address eui** command deletes the global unicast address command in the format of EUI-64.

Format

- **ipv6 address *ipv6-address/mask-length* eui-64**
- **ipv6 address *ipv6-address/mask-length* eui-64 sub**
- **no ipv6 address *ipv6-address* eui-64**

Parameter

Parameter	Description	Value
ipv6-address	Specifies the IPv6 address of an interface.	In this format, a 128-digit IP address is divided into 8 segments. Each segment consists of 16 digits and is represented by 4 hexadecimal characters (0-9 and A-F). Segments are separated by colons (:). Every "X" represents a group of hexadecimal digits.
mask-length	Specifies the mask length of an IPv6 address.	The value is an integer ranging from 0 to 128.

Default Value

NA

View

VLANIF configuration view, out-of-band interface configuration view, Tunnel interface configuration view, BD interface configuration view, Ethernet routing interface configuration view, and Loopback interface configuration view

Usage Guidelines

sub specifies the secondary command and the address mask length is no more than 64.

Before running this command, you must run `ipv6 {enable|disable}` to enable the IPv6 function for the interface.

Example

Set an address of the EUI-64 format for the interface **VLAN10**.

```
Switch(config-vlanif-10)#ipv6 enable
Switch(config-vlanif-10)#ipv6 address 2000::1/64 eui-64
Switch(config-vlanif-10)#
```

4.2.6 ipv6 address link-local

Function

The **ipv6 address link-local** command sets a local IPv6 address for a link.

Format

- **ipv6 address** *ipv6-address* **link-local**
- **no ipv6 address link-local**

Parameter

Parameter	Description	Value
ipv6-address	Specifies a local IPv6 address for the link.	In this format, a 128-digit IP address is divided into 8 segments. Each segment consists of 16 digits and is represented by 4 hexadecimal characters (0-9 and A-F). Segments are separated by colons (:). Every "X" represents a group of hexadecimal digits.

Default Value

NA

View

VLANIF configuration view, out-of-band interface configuration view, Tunnel interface configuration view, BD interface configuration view, Ethernet routing interface configuration view, and Loopback interface configuration view

Usage Guidelines

Before configuring a local IPv6 address for the link, run this command to enable the IPv6 function.

Before deleting the local IPv6 address of the interface, set the link local address generation mode to **Manual** and set the address prefix to **FE80::/10**.

Example

Set the local IPv6 address of the interface to **fe80::204:6717:3c90:ffff**.

```
Switch(config-vlanif-2)#ipv6 address fe80::204:6717:3c90:ffff link-local
Switch(config-vlanif-2)#
```

4.2.7 ipv6 address auto link-local

Function

The **ipv6 address auto link-local** command sets to automatically generate a local address for the link.

The **no ipv6 address auto link-local** command deletes the automatically generated local link address.

Format

- **ipv6 address auto link-local**
- **no ipv6 address auto link-local**

Parameter

NA

Default Value

By default, the local link address is generated based on the system MAC address.

View

VLANIF configuration view, out-of-band interface configuration view, Tunnel interface configuration view, BD interface configuration view, Ethernet routing interface configuration view, and Loopback interface configuration view

Usage Guidelines

NA

Example

Set to automatically generate a local address for the link.

```
Switch(config-vlanif-3)#ipv6 address auto link-local
Switch(config-vlanif-3)#
```

4.2.8 ipv6 hop-limit

Function

The **ipv6 hop-limit** command sets the IPv6 hop limit.

Format

ipv6 hop-limit { *hop-limit-number* | **default** }

Parameter

Parameter	Description	Value
hop-limit-number	Specifies the maximum number of IPv6 hops.	The value is an integer ranging from 1 to 255.
default	Specifies the default maximum number of IPv6 hops.	64

Default Value

64

View

Global configuration view

Usage Guidelines

NA

Example

Set the maximum number of IPv6 hops to 5.

```
Switch(config)#ipv6 hop-limit 5
Switch(config)#
```

4.2.9 ipv6 neighbor

Function

The **ipv6 neighbor** command sets a neighbor to detect the static neighbor information in the cache.

The **no ipv6 neighbor** command deletes the neighbor entries in the static cache.

Format

- **ipv6 neighbor** *ipv6-address mac-address* { **ethernet** | **xgigaethernet** | **10gigaethernet** | **25gigaethernet** | **40gigaethernet** | **100gigaethernet** } *interface-number* [**vpn-instance name**]
- **ipv6 neighbor** *ipv6-address mac-address eth-trunk trunk-number* [**vpn-instance name**]
- **no ipv6 neighbor** *ipv6-address*

Parameter

Parameter	Description	Value
ipv6-address	Specifies a destination IPv6 address.	In this format, a 128-digit IP address is divided into 8 segments. Each segment consists of 16 digits and is represented by 4 hexadecimal characters (0-9 and A-F). Segments are separated by colons (:). Every "X" represents a group of hexadecimal digits.
mac-address	Specifies a destination MAC address.	The format is AA:BB:CC:DD:EE:FF, where A to F are hexadecimal digits.
interface-number	Specifies an Ethernet interface number.	The value is an integer in the range of <1-1>/<0-1>/<1-48>.
trunk-number	Specifies the number of a Trunk interface.	The value is an integer ranging from 1 to 128.
name	Specifies a VPN instance name.	The value is a character string.

Default Value

NA

View

VLANIF configuration view, BD interface configuration view, Ethernet routing interface configuration view, ad Loopback interface configuration view

Usage Guidelines

NA

Example

Set the address of the interface **xgigaethernet 1/0/1** where the neighbor of IPv6 resides to **21DA:D3:0:2F3B:2AA:FF:FE28:9C5A** and the subnet mask address to **00:04:67:00:00:01**.

```
Switch(config-vlanif-3)#ipv6 neighbor 21DA:D3:0:2F3B:2AA:FF:FE28:9C5A 00:04:67:00:00:01
```

```
xgigaethernet 1/0/1
Switch(config-vlanif-3)#
```

4.2.10 ipv6 mtu

Function

The **ipv6 mtu** command sets an MTU value for an IPv6 interface.

Format

ipv6 mtu { *mtu-value* | **default** }

Parameter

Parameter	Description	Value
mtu-value	Specifies an MTU size.	The value is an integer ranging from 1280 to 9216, in bytes.
default	Specifies the default MTU value.	1500 bytes

Default Value

The default MTU value is 1500 bytes.

View

VLANIF configuration view, out-of-band interface configuration view, Tunnel interface configuration view, and Ethernet routing interface configuration view

Usage Guidelines

NA

Example

Set the MTU value of an IPv6 interface to **1280**.

```
Switch(config-vlanif-3)#ipv6 mtu 1280
Switch(config-vlanif-3)#
```

4.2.11 ipv6 nd lifetime

Function

The **ipv6 nd lifetime** command sets the life cycle of IPv6 neighbors.

Format

ipv6 nd lifetime { *life-time* | **default** }

Parameter

Parameter	Description	Value
life-time	Specifies the lifetime of the detected IPv6 neighbor.	The value is an integer ranging from 30 to 86400, in seconds.
default	Specifies the default lifetime.	The default value is 1200s.

Default Value

The default value is 1200s.

View

Global configuration view

Usage Guidelines

NA

Example

Set the lifetime to 1140s.

```
Switch(config)#ipv6 nd lifetime 1140
Switch(config)#
```

4.2.12 show ipv6 interface loopback

Function

The **show ipv6 interface loopback** command displays the loopback interface information on an IPv6 address.

Format

show ipv6 interface loopback *loopback-number*

Parameter

Parameter	Description	Value
loopback-number	Specifies a loopback interface number.	The value is an integer ranging from 1 to 127.

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

Set the IPv6 address of **loopbak 1** to **2001::1/64** and view the loopback interface information on the IPv6 address.

```
Switch>show ipv6 interface loopback 1
Interface loopback-1
    Physical Address: 00:00:00:00:00:00    description: N/A
    Admin state:up    Oper state:up
    IPv6 Addr :2001::/64    Role:primary    Type:static
    IPv6 Addr :fe80::250:1ff:febd:7ce/64    Role:linklocal    Type:auto
    NDP RA MTU :1536
    NDP RA MTU :1536    Vpn instance :N/A

Switch>
```

4.2.13 show ipv6 interface vlan

Function

The **show ipv6 interface vlan** command displays the VLAN interface information on an IPv6 address.

Format

show ipv6 interface vlan *vlan-id*

Parameter

Parameter	Description	Value
vlan-id	Specifies a VLAN ID.	The value is an integer ranging from 1 to 4094.

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

View the VLAN interface information on the IPv6 address.

```
Switch>show ipv6 interface vlan 2
```

```

Interface vlan-2
    Physical Address: 00:00:00:00:DE:AD    Admin state:UP,Oper state:down
    IPv6 Addr :fe80::204:6717:3c90:ffff/64  Role:linklocal  Type:unknown
    NDP RA MTU :1500
Switch>

```

4.2.14 show ipv6 neighbor

Function

The **show ipv6 neighbor** command displays the neighbor information on an IPv6 address or displays information on a multi-instance VLAN.

Format

- **show ipv6 neighbor**
- **show ipv6 neighbor vpn-instance *name***
- **show ipv6 neighbor vpn-instance**

Parameter

Parameter	Description	Value
name	Specifies a VPN instance name.	The value is a string of up to 64 characters.

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

View the neighbor information on the IPv6 address.

```

Switch>show ipv6 neighbor
-----
    Total: 0      Dynamic:0      Static:0
Switch>

```

4.2.15 show ipv6 neighbor summary

Function

The **show ipv6 neighbor summary** displays the neighbor route summary of an IPv6 address.

Format

show ipv6 neighbor summary

Parameter

NA

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

View the neighbor route summary of the IPv6 address.

```
Switch>show ipv6 neighbor summary
Software route: 0
Hardware route: 0
Switch>
```

4.2.16 show ipv6 route summary

Function

The **show ipv6 route summary** command displays the IPv6 route summary.

Format

show ipv6 route summary

Parameter

NA

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

View the IPv6 route summary.

```
Switch>show ipv6 route summary
Bad routing redirect: 0
Dynamically created route: 0
New gateway due to redirects: 0
Destination found unreachable: 1916
Use of a wildcard route: 0
Software route: 3
Hardware route: 6
Switch>
```

4.2.17 show ipv6 statistic**Function**The **show ipv6 statistic** command displays the IPv6 statistics.**Format**

- **show ipv6 statistic**
- **show ipv6 statistic interface** *vlan* *vlan-id*
- **show ipv6 statistic interface** { **ethernet** | **xgigaethernet** | **10gigaethernet** | **25gigaethernet** | **40gigaethernet** | **100gigaethernet** } *interface-number*
- **show ipv6 statistic interface** { **ethernet** | **xgigaethernet** | **10gigaethernet** | **25gigaethernet** | **40gigaethernet** | **100gigaethernet** } *interface-number.subinterface*

Parameter

Parameter	Description	Value
vlan-id	Specifies a VLAN ID.	The value is an integer ranging from 1 to 4094.
interface-number	Specifies an Ethernet interface number.	The value is an integer in the range of <1-1>/<0-1>/<1-48>.
subinterface	Specifies a sub-interface number.	The value is an integer ranging from 1 to 4094.

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

View the IPv6 statistics.

```
Switch>show ipv6 statistic
IPv6 Protocol:
Interface:loopback0

Sent packets:
    Total                : 1745850256
    Forwarded            : 1476540656   Discarded            : 1476540544
    Fragments            : 1476540736   Fragmented            : 1476540704
    Fragments failed     : 1476540720   Multicast              : 1476540816
    Raw packets          : 1476540672

Received packets:
    Total                : 1476540512   Header error           : 1476540528
    Too big              : 1476540544   Routing failed         : 1476540560
    Address error        : 1476540576   Protocol error         : 1476540592
    Truncated            : 1476540608   Discarded              : 1476540624
    Delivers             : 1476540640   Multicast              : 1476540800
    Reassembly           : 1476540784   Reassembled            : 1476540768
    Reassemble failed   : 1476540752
    Received packets:
        Total            : 6             Header error           : 0
        Too big          : 0             Routing failed         : 0
        Address error    : 0             Protocol error         : 0
        Truncated        : 0             Discarded              : 0
        Delivers         : 6             Multicast              : 1
        Reassembly       : 0             Reassembled            : 0
        Reassemble failed : 0

Switch>
```

4.2.18 show ipv6 route

Function

The **show ipv6 route** command displays the route of an IPv6 address or displays information on a multi-instance VLAN.

Format

- **show ipv6 route**
- **show ipv6 route *ipv6-address***
- **show ipv6 route *ipv6-address/M***
- **show ipv6 route local**
- **show ipv6 route vpn-instance**
- **show ipv6 route vpn-instance *name***
- **show ipv6 route *ipv6-address* vpn-instance *name***
- **show ipv6 route static**
- **show ipv6 route statistic**

Parameter

Parameter	Description	Value
ipv6-address	Specifies an IPv6 address.	In this format, a 128-digit IP address is divided into 8 segments. Each segment consists of 16 digits and is represented by 4 hexadecimal characters (0-9 and A-F). Segments are separated by colons (:). Every "X" represents a group of hexadecimal digits.
name	Specifies a VPN instance name.	The value is a string of up to 64 characters.
M	Specifies a mask of the IPv6 address.	The value is an integer ranging from 1 to 128.

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

View the IPv6 route information.

Switch>show ipv6 route		
Routing Tables: Public		
Dest/Prefixlen	Nexthop	Interface

```

Proto      Cost
-----
::1/128          ::1          loopback0
local          0
fe80::/64        fe80::6a21:5fff:fedc:2300    loopback0
local          0
fe80::6a21:5fff:fedc:2300/128    fe80::6a21:5fff:fedc:2300    loopback0
local          0
-----
Total: 3          Static: 0
Switch>

```

4.3 DHCP Configuration Commands

4.3.1 debug dhcp relay

Function

The **debug dhcp relay** command enables DHCP relay debugging.

The **no debug dhcp relay** command disables DHCP relay debugging.

Format

- **debug dhcp relay { event | packet | info | error | all }**
- **no debug dhcp relay { event | packet | info | error | all }**

Parameter

Parameter	Description	Value
event	Specifies timer expiration information and NMS configuration information.	-
packet	Specifies sent and received packet information.	-
info	Specifies specific sent and received packet information in the user entry information.	-
error	Debugs error information.	-
all	Displays all information.	-

Default Value

By default, DHCP relay debugging is disabled.

View

Privileged user view

Usage Guidelines

NA

Example

```
# Enable debugging of all DHCP Relay information.
```

```
Switch#debug dhcp relay all
Switch#
```

4.3.2 debug dhcp server**Function**

The **debug dhcp server** command enables DHCP server debugging.

The **no debug dhcp server** command disables DHCP server debugging.

Format

- **debug dhcp server { event | packet | info | error | all }**
- **no debug dhcp server { event | packet | info | error | all }**

Parameter

Parameter	Description	Value
event	Specifies timer expiration information and NMS configuration information.	-
packet	Specifies sent and received packet information.	-
info	Specifies specific sent and received packet information in the user entry information.	-
error	Debugs error information.	-
all	Displays all information.	-

Default Value

By default, DHCP server debugging is disabled.

View

Privileged user view

Usage Guidelines

NA

Example

```
# Enable debugging of the sent and received packets of the DHCP server.
```

```
Switch#debug dhcp server packet
Switch#
```

4.3.3 dhcp {start|stop}

Function

The **dhcp {start|stop}** command enables or disables the DHCP function on the switch.

Format

dhcp { start | stop }

Parameter

Parameter	Description	Value
start	Enables the DHCP function.	-
stop	Disables the DHCP function.	-

Default Value

By default, the DHCP function is disabled.

View

Global configuration view

Usage Guidelines

You can use this command to enable the DHCP function. This command must be executed before all the other DHCP configuration commands. Other DHCP attribute configurations takes effect only after the DHCP function is enabled.

Example

Enable the DHCP function.

```
Switch(config)#dhcp start
Switch(config)#
```

4.3.4 dhcp relay server-ip

Function

The **dhcp relay server-ip** command configures the IP address of the DHCP server served by the DHCP relay.

The **no dhcp relay server-ip** command deletes the IP address of the DHCP relay server.

Format

- **dhcp relay server-ip** *ip-address*
- **no dhcp relay server-ip** *ip-address*

Parameter

Parameter	Description	Value
ip-address	Specifies the IP address of the DHCP server for which the DHCP relay is a proxy.	The value is in dotted decimal notation.

Default Value

By default, the IP address of the DHCP server served by the DHCP relay is not configured.

View

VLANIF configuration view, Ethernet routing interface configuration view

Usage Guidelines

If the Switch acts as a DHCP relay agent and a DHCP server IP address is configured on its interface using this command, this interface will forward the broadcast DHCP request packets received from clients to the specified DHCP server. This enables clients to be served by a DHCP server on a different network segment.

Example

Configure the IP address of the DHCP server served by the DHCP relay.

```
Switch(config-vlanif-3)#dhcp relay server-ip 10.16.13.23
Switch(config-vlanif-3)#
```

4.3.5 dhcp relay user refresh-interval

Function

The **dhcp relay user refresh-interval** command sets the scheduled update period for the DHCP relay user table entry.

Format

dhcp relay user refresh-interval { *interval* | **default** }

Parameter

Parameter	Description	Value
interval	Specifies the scheduled update period for the DHCP relay user table entry.	The value is an integer ranging from 60 to 3600, in seconds.
default	Specifies the default scheduled update period for the	-

Parameter	Description	Value
	DHCP relay user table entry, which is 1800s.	

Default Value

By default, the scheduled update period for the DHCP relay user table entry is set to 1800s.

View

Global configuration view

Usage Guidelines

NA

Example

Set the scheduled update period for the DHCP relay user table entry to 600s.

```
Switch(config)#dhcp relay user refresh-interval 600
```

```
Switch(config)#
```

4.3.6 ip dhcp

Function

The **ip dhcp** command configures the DHCP working mode.

The **no ip dhcp** command deletes the DHCP interface, and the interface does not work in any mode.

Format

- **ip dhcp { relay | server }**
- **no ip dhcp**

Parameter

Parameter	Description	Value
relay	Indicates the relay mode.	-
server	Indicates the server mode.	-

Default Value

By default, no work mode is specified for the interface.

View

VLANIF configuration view, Ethernet routing interface configuration view

Usage Guidelines

When the DHCP works in relay mode, upon receiving a DHCP packet from a DHCP client, the switch forwards the packet to the DHCP server. Upon receiving a DHCP response packet from the DHCP server, the switch forwards it to the DHCP client.

Example

Set the DHCP working mode to relay.

```
Switch(config-vlanif-3)#ip dhcp relay
Switch(config-vlanif-3)#
```

4.3.7 reset dhcp relay statistic

Function

The **reset dhcp relay statistic** command clears DHCP relay statistics.

Format

reset dhcp relay statistic

Parameter

NA

Default Value

NA

View

Global configuration view

Usage Guidelines

You can use this command to re-collect information in received packets.

After this command is successfully executed, all statistics of packets on the DHCP relay is cleared.

Example

Clear the statistics of the DHCP relay.

```
Switch(config)#reset dhcp relay statistic
Switch(config)#
```

4.3.8 show dhcp

Function

The **show dhcp** command displays DHCP server information on the switch.

Format

- **show dhcp**
- **show dhcp { bind-entry | fake-server | lease-entry | pool }**
- **show dhcp server {conflict | expired | statistic }**

Parameter

NA

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

Display DHCP configuration parameters and state information.

```
Switch>show dhcp
Version : DHCP_VB3.00.02.00
Switch>
```

4.3.9 show dhcp config**Function**The **show dhcp config** command displays the DHCP configuration on the switch.**Format**

- **show dhcp config**
- **show dhcp { ethernet | xgigaethernet | 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet } interface-number config**
- **show dhcp { ethernet | xgigaethernet | 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet } interface-number.subinterface-number config**

Parameter

Parameter	Description	Value

Parameter	Description	Value
interface-number	Specifies an Ethernet interface number.	The value is an integer in the range of <1-1>/<0-1>/<1-48>.
subinterface-number	Specifies a sub-interface number.	The value is an integer ranging from 1 to 4094.

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

Display the DHCP configuration.

```
Switch>show dhcp config
Switch>
```

4.3.10 show dhcp relay statistic**Function**The **show dhcp relay statistic** command displays DHCP relay statistics.**Format****show dhcp relay statistic****Parameter**

NA

Default Value

NA

View

Common user view

Usage Guidelines

You can use this command to view DHCP relay statistics, including:

- DHCP packets from the client

- Received DHCP DISCOVER packets, DHCP REQUEST packets, DHCP RELEASE packets, DHCP INFORM packets, and DHCP DECLINE packets
- DHCP packets, unicast packets, and broadcast packets sent to the DHCP client
- DHCP packets, DHCP OFFER packets, DHCP ACK packets, and DHCP NAK packets from the DHCP server
- DHCP packets sent to the DHCP server
- DHCP error packets from the DHCP server. Error packets received by the relay include error packets from both the server and client.

Example

Display DHCP relay statistics.

```
Switch>show dhcp relay statistic
Bad Packets received : 0
packets received from clients : 0
DISCOVER received : 0
REQUEST received : 0
INFORM received : 0
DECLINE received : 0
RELEASE received : 0
packets received from servers : 0
OFFER received : 0
ACK received : 0
NAK received : 0
packets sent to servers : 0
packets sent to clients : 0
Unicast sent to clients : 0
Broadcast sent to clients : 0
Switch>
```

4.3.11 show dhcp relay

Function

The **show dhcp relay** command displays the configuration of a DHCP relay server.

Format

show dhcp relay

Parameter

NA

Default Value

NA

View

Common user view

Usage Guidelines

The DHCP relay function can transparently transmit DHCP broadcast packets across the networks, so that broadcast packets of the DHCP client or server can be transparently transmitted to the DHCP server or client on another network segment.

Multiple DHCP clients on the network can use the same DHCP server, which saves costs and facilitates centralized management.

You can use this command to view the DHCP relay configuration, including whether DHCP relay is enabled, interface that provides the relay function, and IP address of the DHCP server served by the relay.

Example

View the configuration of the DHCP relay server.

```
Switch>show dhcp relay
DHCP relay Configure!
Switch>
```

4.3.12 show dhcp vlan config**Function**

The **show dhcp vlan config** command displays the DHCP configuration on a specific VLAN interface.

Format

show dhcp vlan *vlan-id* config

Parameter

Parameter	Description	Value
vlan-id	Specifies a VLAN ID associated with DHCP.	The value is an integer ranging from 1 to 4094.

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

Display the DHCP configuration of the VLAN interface.

```
Switch>show dhcp vlan 1 config
Switch>
```

4.4 DHCP Client Configuration Commands

4.4.1 ip address dhcp {enable|disable}

Function

The **ip address dhcp {enable|disable}** command enables the DHCP client to automatically obtain an IP address or disables this function.

Format

ip address dhcp { enable | disable }

Parameter

Parameter	Description	Value
enable	Enables the DHCP client to automatically obtain an IP address.	-
disable	Disables the DHCP client function.	-

Default Value

Disable

View

VLANIF configuration view, Ethernet routing interface configuration view

Usage Guidelines

The DHCP client, DHCP server, and DHCP relay functions are mutually exclusive on a VLAN interface. If the DHCP client is enabled on a VLAN interface, the DHCP server or DHCP relay function cannot be enabled on this VLAN interface.

Example

Enable the DHCP client to automatically obtain an IP address.

```
Switch(config-vlanif-3)#ip address dhcp enable
Switch(config-vlanif-3)#
```

4.4.2 ip address dhcp release**Function**

The **ip address dhcp release** command releases the IP address obtained by the DHCP client.

Format

ip address dhcp release

Parameter

NA

Default Value

NA

View

VLANIF configuration view, Ethernet routing interface configuration view

Usage Guidelines

Before using this command, you must run the **ip address dhcp {enable|disable}** command.

Example

Release the IP address obtained by the DHCP client.

```
Switch(config-vlanif-3)#ip address dhcp release
Switch(config-vlanif-3)#
```

4.4.3 ip address dhcp renew**Function**

The **ip address dhcp renew** command renews the IP address obtained by the DHCP client.

Format

ip address dhcp renew

Parameter

NA

Default Value

NA

View

VLANIF configuration view, Ethernet routing interface configuration view

Usage Guidelines

Before using this command, you must run the `ip address dhcp {enable|disable}` command.

Example

Renew the IP address obtained by the DHCP client.

```
Switch(config-vlanif-3)#ip address dhcp renew
Switch(config-vlanif-3)#
```

4.4.4 reset dhcp client statistic

Function

The **reset dhcp client statistic** command resets counters of packets sent and received on a VLAN interface.

Format

reset dhcp client statistic

Parameter

NA

Default Value

NA

View

VLANIF configuration view, Ethernet routing interface configuration view

Usage Guidelines

NA

Example

Clear statistics of packets sent and received on the interface **VLAN 3**.

```
Switch(config-vlanif-3)#reset dhcp client statistic
Switch(config-vlanif-3)#
```

4.4.5 show dhcp client

Function

The **show dhcp client** command displays DHCP client state information on a single or all VLAN interfaces.

Format

- **show dhcp client**
- **show dhcp client vlan** *vlan-id*
- **show dhcp client auto-config vlan** *vlan-id*
- **show dhcp client auto-config { ethernet | xgigaethernet | 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet } interface-number**
- **show dhcp client { ethernet | xgigaethernet | 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet } interface-number**

Parameter

Parameter	Description	Value
vlan-id	Specifies the VLAN ID of an interface.	The value is an integer ranging from 1 to 4094.
interface-number	Specifies an Ethernet interface number.	The value is an integer in the range of <1-1>/<0-1>/<1-48>.

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

Display the DHCP client state information.

```
Switch>show dhcp client
Switch>
```

4.4.6 show dhcp client statistic

Function

The **show dhcp client statistic** command displays statistics about packets sent and received by the DHCP client on a single or all VLAN interfaces.

Format

- **show dhcp client statistic**
- **show dhcp client statistic vlan** *vlan-id*
- **show dhcp client statistic { ethernet | xgigaethernet | 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet } interface-number**

Parameter

Parameter	Description	Value
vlan-id	Specifies the VLAN ID of an interface.	The value is an integer ranging from 1 to 4094.
interface-number	Specifies an Ethernet interface number.	The value is an integer in the range of <1-1>/<0-1>/<1-48>.

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

Display statistics about packets sent and received by the DHCP client on VLAN interface 3.

```
Switch>show dhcp client statistic
Switch>
```

4.4.7 show dhcpv6 relay

Function

The **show dhcpv6 relay** command displays the DHCPv6 relay interface information.

Format

- **show dhcpv6 relay**
- **show dhcpv6 relay interface { ethernet | xgigaethernet | 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet } interface-number**
- **show dhcpv6 relay interface { ethernet | xgigaethernet | 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet } interface-number.subinterface**

Parameter

Parameter	Description	Value
interface-number	Specifies an Ethernet interface number.	The value is an integer in the range of <1-1>/<0-1>/<1-48> (For reference only. The specific value range depends on the slot number and card type).
subinterface	Specifies a sub-interface number.	The value is an integer ranging from 1 to 4094.

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

Display the DHCPv6 relay interface information.

```
Switch>show dhcpv6 relay
Switch>
```

4.4.8 show dhcpv6 statistic

Function

The **show dhcpv6 statistic** command displays the DHCPv6 statistics.

Format

- **show dhcpv6 statistic**
- **show dhcpv6 statistic interface vlan vlan-id**
- **show dhcpv6 statistic interface { ethernet | xgigaethernet | 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet } interface-number.subinterface**

Parameter

Parameter	Description	Value
vlan-id	Specifies the VLAN ID of an interface.	The value is an integer ranging from 1 to 4094.
interface-number	Specifies an Ethernet interface number.	The value is an integer in the range of <1-1>/<0-1>/<1-48> (For reference only. The specific value range depends on the slot number and card type).
subinterface	Specifies a sub-interface number.	The value is an integer ranging from 1 to 4094.

Default Value

NA

View

Common user view

Usage Guidelines

You can use this command to view DHCP V6 server statistics, including:

- Statistics of the DHCP V6 server
- The number of messages sent by the DHCP V6 client to the DHCP V6 server.
- Statistics of DHCP V6 packets sent by the DHCP V6 client to the DHCP V6 server.
- The number of messages sent by the DHCP V6 client to the DHCP V6P server.
- Statistics of DHCP V6 packets sent by the DHCP V6 client to the DHCP V6 server.
- Number of unrecognized packets

Example

Show statistics of the DHCP V6 server.

```
Switch>show dhcpv6 statistic
Switch>
```

4.4.9 show dhcpv6 interface**Function**

The **show dhcpv6 interface** command displays DHCPv6 interface information.

Format

- **show dhcpv6 interface**

- **show dhcpv6 interface vlan** *vlan-id*
- **show dhcpv6 interface** { **ethernet** | **xgigaethernet** | **10gigaethernet** | **25gigaethernet** | **40gigaethernet** | **100gigaethernet** } *interface-number.subinterface*

Parameter

Parameter	Description	Value
vlan-id	Specifies the VLAN ID of an interface.	The value is an integer ranging from 1 to 4094.
interface-number	Specifies an Ethernet interface number.	The value is an integer in the range of <1-1>/<0-1>/<1-48> (For reference only. The specific value range depends on the slot number and card type).
subinterface	Specifies a sub-interface number.	The value is an integer ranging from 1 to 4094.

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

Display DHCPv6 interface information.

```
Switch>show dhcpv6 interface
Switch>
```

Chapter 5 Routing Commands

This chapter introduces commands for routing configuration of the Switch series switch.

5.1 Basic IP Routing Commands

5.1.1 show ecmp-profile

Function

The **show ecmp-profile** command displays the configuration of the Equal Cost Multi-path (ECMP) template.

Format

- **show ecmp-profile** *profile-name*
- **show ecmp-profile**

Parameter

Parameter	Description	Value
profile-name	Specifies an ECMP template.	The value is a string consisting of up to 32 characters.

Default Value

NA

View

Common user view

Usage Guidelines

If no ECMP template is configured, no information is displayed after you run **show ecmp-profile**.

If an ECMP template is configured, after you run **show ecmp-profile**, the ECMP template name and ECMP load balancing mode are displayed.

Example

View the configuration of the ECMP template.

```
Switch>show ecmp-profile
Version : SCHEDULEPROFILE_VB3.00.00.00
```

```
Switch>
```

5.1.2 show ecmp load-balance

Function

The **show ecmp load-balance** command displays the ECMP load balancing information.

Format

show ecmp load-balance

Parameter

NA

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

View the ECMP load balancing information.

```
Switch>show ecmp load-balance
    ecmp load-balance configuration: default
Switch>#
```

5.1.3 ecmp-profile

Function

The **ecmp-profile** command creates an ECMP enhanced template and enters the ECMP template view.

The **no ecmp-profile** command deletes an ECMP enhanced template.

Format

- **ecmp-profile** *profile-name*
- **no ecmp-profile** *profile-name*

Parameter

Parameter	Description	Value
profile-name	Specifies the name of an ECMP template.	The value is a string consisting of up to 32 characters.

Default Value

By default, no ECMP load balancing template is created.

View

Global configuration view

Usage Guidelines

NA

Example

Bind or unbind an ECMP load balancing template.

```
Switch(config)#ecmp profile aaa
Switch(config-ecmp-profile-aaa)#
```

5.1.4 ecmp hash-mode**Function**

The **ecmp hash-mode** command sets the HASH value for the ECMP load balancing.

Format

ecmp hash-mode { *mode-value* | **default** }

Parameter

Parameter	Description	Value
mode-value	Sets the HASH value for ECMP load balancing.	The value is an integer ranging from 1 to 13.
default	Sets the default HASH value for ECMP load balancing.	7

Default Value

The default HASH value for ECMP load balancing is 7.

View

ECMP Profile configuration view

Usage Guidelines

Different HASH values have different load balancing effects. You can set an appropriate HASH value for load balancing based on the traffic model.

Example

Set the HASH value for ECMP load balancing to 6.

```
Switch(config)#ecmp profile aaa
Switch(config-ecmp-profile-aaa)#ecmp hash-mode 6
```

5.1.5 ecmp load-balance profile**Function**

The **ecmp load-balance profile** command binds or unbinds an ECMP load balancing mode to or from a profile.

Format

- **ecmp load-balance profile** *profile-name*
- **no ecmp load-balance profile** *profile-name*

Parameter

Parameter	Description	Value
profile-name	Specifies the name of the ECMP load balancing profile.	The value is a character string of no more than 32 characters.

Default Value

Disable

View

Global configuration view

Usage Guidelines

NA

Example

Bind or unbind an ECMP load balancing mode to or from a profile.

```
Switch(config)#ecmp load-balance profile aaa
Switch(config)#
```

5.1.6 ecmp load-balance {src-ip|default}

Function

The **ecmp load-balance {src-ip|default}** command sets the ECMP load balancing mode.

Format

- **ecmp load-balance { src-ip | default }**

Parameter

NA

Default Value

NA

View

Global configuration view

Usage Guidelines

NA

Example

Set the ECMP load balancing mode.

```
Switch(config)#ecmp load-balance src-ip
Switch(config)#
```

5.2 DID Configuration Commands

5.2.1 debug did

Function

The **debug did** command debugs DID.

Format

debug did { event | detect | cmd | off | all }

Parameter

Parameter	Description	Value
event	Debugs the DID event function.	-
detect	Debugs the DID detection function.	-

Parameter	Description	Value
cmd	Debugs the CMD.	-
off	Debugs Off information.	-
all	Specifies all the debugging information.	-

Default Value

DID debugging is disabled by default.

View

Privileged user view

Usage Guidelines

NA

Example

Debug DID.

```
Switch#debug did all
Switch#
```

5.2.2 show did resource**Function**

The **show did resource** command displays the DID resource information.

Format

show did resource

Parameter

NA

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

Display information about DID resources.

```
Switch>show did resource
  DID resource:
    detect interval:10
    max peer:256
    free number of peer:256
    max nexthop:256
    free number of nexthop:0
Switch>
```

5.2.3 show did peer

Function

The **show did peer** command displays the DID peer information.

Format

show did peer

Parameter

NA

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

View the DID peer information.

```
Switch>show did peer
Switch>
```

5.3 Static Route Configuration Commands

5.3.1 ip route-static

Function

The **ip route-static** command creates a static IPv4 route. It supports multi-instance VPN.

The **no ip route-static** command deletes a static IPv4 route.

The **no ip route-static all** command deletes all static IPv4 routes.

Format

- **ip route-static** *ip-address mask-address nexthop-address*
- **ip route-static preference** { *preference-value* | **default** }
- **ip route-static** *ip-address mask-address nexthop-address preference* { *preference-value* | **default** }
- **ip route-static** *ip-address mask-address interface null null-number*
- **ip route-static** *ip-address mask-address vpn-instance name nexthop-address preference preference-value*
- **ip route-static** *ip-address mask-address nexthop-address track bfd track-number*
- **ip route-static** *ip-address mask-address vpn-instance name nexthop-address*
- **ip route-static** *ip-address mask-address vpn-instance name nexthop-address track bfd track-number*
- **ip route-static vpn-instance name ip-address mask-address nexthop-address**
- **ip route-static vpn-instance name ip-address mask-address nexthop-address preference preference-value**
- **ip route-static vpn-instance name ip-address mask-address nexthop-address track bfd track-number**
- **ip route-static vpn-instance name ip-address mask-address vpn-instance name nexthop-address**
- **ip route-static vpn-instance name ip-address mask-address vpn-instance name nexthop-address preference preference-value**
- **ip route-static vpn-instance name ip-address mask-address vpn-instance name nexthop-address track bfd track-number**
- **no ip route-static** *ip-address mask-address*
- **no ip route-static** *ip-address mask-address nexthop-address*
- **no ip route-static** *ip-address mask-address nexthop-address track bfd*

- **no ip route-static** *ip-address mask-address vpn-instance name*
- **no ip route-static** *ip-address mask-address vpn-instance name nexthop-address*
- **no ip route-static** *ip-address mask-address vpn-instance name nexthop-address track bfd*
- **no ip route-static all**
- **no ip route-static track bfd all**
- **no ip route-static vpn-instance name all**
- **no ip route-static vpn-instance name** *ip-address mask-address*
- **no ip route-static vpn-instance name** *ip-address mask-address nexthop-address*
- **no ip route-static vpn-instance name** *ip-address mask-address nexthop-address track bfd*
- **no ip route-static vpn-instance name** *ip-address mask-address vpn-instance name nexthop-address*
- **no ip route-static vpn-instance name** *ip-address mask-address vpn-instance name nexthop-address track bfd*

Parameter

Parameter	Description	Value
ip-address	Specifies a destination IP address.	The value is in dotted decimal notation, for example, <i>A.B.C.D</i> , in which <i>A</i> to <i>D</i> are decimal digits ranging from 0 to 255.
mask-address	Specifies the mask of a destination IP address.	The value is in dotted decimal notation, for example, <i>A.B.C.D</i> , in which <i>A</i> to <i>D</i> are decimal digits ranging from 0 to 255.
nexthop-address	Specifies the next-hop IP address of a route.	The value is in dotted decimal notation, for example, <i>A.B.C.D</i> , in which <i>A</i> to <i>D</i> are decimal digits ranging from 0 to 255.
name	Specifies a VPN instance name.	The value is a string of up to 64 characters.
track-number	Specifies the ID of a static BFD session.	The value is an integer ranging from 1 to 512.
preference-value	Specifies a preference value.	The value is an integer ranging from 1 to 255.
null-number	Specifies the ID of a NULL interface.	The value is an integer ranging from 0.

Default Value

By default, no static routing entry is configured in the system.

View

Global configuration view

Usage Guidelines

NA

Example

Configure an IPv4 route with destination IP address 220.181.111.88 and next-hop address 220.181.111.89. Delete the preceding static route and all static routes.

```
Switch(config)#ip route-static 220.181.111.88 255.255.255.255 220.181.111.89
Switch(config)#
Switch(config)#no ip route-static 220.181.111.88 255.255.255.255 220.181.111.89
Switch(config)#
Switch(config)#no ip route-static all
Switch(config)#
```

5.3.2 ipv6 route-static

Function

The **ipv6 route-static** command sets an IPv6 static route. Configuration under multi-instance VPN is also supported.

The **no ipv6 route-static** command deletes an IPv6 static route.

The **no ipv6 route-static all** command deletes all IPv6 static routes.

Format

- **ipv6 route-static** *ipv6-address mask-length ipv6-nexthop-address*
- **ipv6 route-static** *ipv6-address mask-length ipv6-nexthop-address preference preference-value*
- **ipv6 route-static** *ipv6-address mask-length ipv6-nexthop-address preference preference-value vpn-instance name*
- **ipv6 route-static** *ipv6-address mask-length ipv6-nexthop-address track bfd track-number*
- **ipv6 route-static** *ipv6-address mask-length ipv6-nexthop-address vpn-instance name*
- **ipv6 route-static** *ipv6-address mask-length ipv6-nexthop-address vpn-instance name track bfd track-number*
- **ipv6 route-static** *ipv6-address mask-length interface { ethernet | xgigaethernet | 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet } interface-number link-local link-local-address*

- **ipv6 route-static** *ipv6-address mask-length interface* { **ethernet** | **xgigaethernet** | **10gigaethernet** | **25gigaethernet** | **40gigaethernet** | **100gigaethernet** } *interface-number.subinterface link-local link-local-address*
- **ipv6 route-static** *ipv6-address mask-length interface vlan vlan-id link-local link-local-address*
- **ipv6 route-static** *ipv6-address mask-length interface null null-number*
- **ipv6 route-static** *ipv6-address mask-length interface tunnel tunnel-number*
- **ipv6 route-static preference** { *preference-value* | **default** }
- **no ipv6 route-static** *ipv6-address mask-length*
- **no ipv6 route-static** *ipv6-address mask-length ipv6-nexthop-address*
- **no ipv6 route-static** *ipv6-address mask-length ipv6-nexthop-address track bfd*
- **no ipv6 route-static** *ipv6-address mask-length vpn-instance name*
- **no ipv6 route-static** *ipv6-address mask-length ipv6-nexthop-address vpn-instance name*
- **no ipv6 route-static** *ipv6-address mask-length ipv6-nexthop-address vpn-instance name track bfd*
- **no ipv6 route-static track bfd all**
- **no ipv6 route-static all**

Parameter

Parameter	Description	Value
ipv6-address	Specifies a destination IPv6 address.	In this format, a 128-digit IP address is divided into 8 segments. Each segment consists of 16 digits and is represented by 4 hexadecimal characters (0-9 and A-F). Segments are separated by colons (:). Every "X" represents a group of hexadecimal digits.
mask-length	Specifies the mask length of a destination IP address.	The value is an integer ranging from 0 to 128.
ipv6- nexthop-address	Specifies the next-hop IPv6 address of a route.	In this format, a 128-digit IP address is divided into 8 segments. Each segment consists of 16 digits and is represented by 4 hexadecimal characters (0-9 and A-F). Segments are separated by colons (:). Every "X" represents a group of hexadecimal digits.
name	Specifies a VPN instance name.	The value is a string of up to 64 characters.

Parameter	Description	Value
track-number	Specifies the ID of a static BFD session.	The value is an integer ranging from 1 to 512.
preference-value	Specifies a preference value.	The value is an integer ranging from 1 to 255.
null-number	Specifies the ID of a NULL interface.	The value is an integer ranging from 0 to 0.
tunnel-number	Specifies the ID of a Tunnel interface.	The value is an integer ranging from 1 to 5.
interface-number	Specifies an Ethernet interface number.	The value is an integer in the range of <1-1>/<0-1>/<1-48> (For reference only. The specific value range depends on the slot number and card type).
link-local-address	Specifies the local IPv6 address for a link.	In this format, a 128-digit IP address is divided into 8 segments. Each segment consists of 16 digits and is represented by 4 hexadecimal characters (0-9 and A-F). Segments are separated by colons (:). Every "X" represents a group of hexadecimal digits.

Default Value

By default, no static IPv6 route is configured in the system.

View

Global configuration view

Usage Guidelines

When deleting an IPv6 route, you cannot delete the following routes:

Filter host routes with a 128-bit mask

Multicast routes of which the first byte is 0xff

Routes of which the destination address is the link's local address

Local routes of which the protocol type is local

Example

Set the route of the IPv6 address to **21DA:D3:0:2F3B:2AA:FF:FE28:9C5A** and the next hop address is **21DA:D3:0:2F3B:2AA:FF:FE20:8C6A**.

```
Switch(config)#ipv6 route-static 21DA:D3:0:2F3B:2AA:FF:FE28:9C5A 24
21DA:D3:0:2F3B:2AA:FF:FE20:8C6A
Switch(config)#
```

5.3.3 ipv6 route-static interface vlan link-local

Function

The **ipv6 route-static interface vlan link-local** command sets an IPv6 static route and specifies the next hop address of the outbound interface is the local address of the link.

Format

ipv6 route-static *ipv6-address mask-length* **interface vlan** *vlan-id* **link-local** *link-local-address*

Parameter

Parameter	Description	Value
ipv6-address	Specifies a destination IPv6 address.	In this format, a 128-digit IP address is divided into 8 segments. Each segment consists of 16 digits and is represented by 4 hexadecimal characters (0-9 and A-F). Segments are separated by colons (:). Every "X" represents a group of hexadecimal digits.
mask- length	Specifies the mask length of a destination IP address.	The value is an integer ranging from 0 to 128.
vlan-id	Specifies a VLAN ID.	The value is an integer ranging from 1 to 4094.
link-local-address	Specifies the local IPv6 address for a link.	In this format, a 128-digit IP address is divided into 8 segments. Each segment consists of 16 digits and is represented by 4 hexadecimal characters (0-9 and A-F). Segments are separated by colons (:). Every "X" represents a group of hexadecimal digits.

Default Value

NA

View

Global configuration view

Usage Guidelines

NA

Example

Set a static route of which the destination address is **21DA:D3:0:2F3B:2AA:FF:FE28:9C5A** and the next hop address is the local address **FE80::9CC5:FF28** of the outbound interface **VLAN 10**.

```
Switch(config)#ipv6 route-static 21DA:D3:0:2F3B:2AA:FF:FE28:9C5A 24 interface vlan 10 link-local
FE80::9CC5:FF28
Switch(config)#
```


5.3.4 show ip route

Function

The **show ip route** command displays routing information. It can also display routing information in VPN instances.

Format

- **show ip route**
- **show ip route vpn-instance name**
- **show ip route vpn-instance**
- **show ip route vpn-instance name ip-address1**
- **show ip route vpn-instance name ip-address1 ip-address2**
- **show ip route ip-address**
- **show ip route ip-address1 ip-address2 [vpn-instance name]**
- **show ip route ip-address1 ip-address2 ip-address3**
- **show ip route ip-address1 ip-address2 brief**
- **show ip route ip-address/M**

Parameter

Parameter	Description	Value
ip-address ip-address1	Specifies a destination IP address.	The value is in dotted decimal notation, for example, <i>A.B.C.D</i> , in which <i>A</i> to <i>D</i> are decimal digits ranging from 0 to 255.
ip-address2	Specifies a mask address.	The value is in dotted decimal notation.
ip-address3	Specifies a next hop address.	The value is in dotted decimal notation.
name	Specifies a VPN instance name.	The value is a string of up to 64 characters.
string	Specifies a character string used for filtering the configuration information to be displayed.	The value is a character string.
M	Specifies the mask of an IP address.	The value is an integer ranging from 1 to 32.

Default Value

NA

View

Common user view

Usage Guidelines

The destination IP address suffixed to this command specify information about a specified route.

Example

Display local routing information.

```
Switch>show ip route
Routing Tables: Public
  Destination            Gateway         Preference/Metric   Interface        Proto  Mpls
Vpn-Instance
-----
  10.1.1.0/24            10.1.1.1        0/0                 vlan100           local  no    N/A
  10.1.1.1/32            10.1.1.1        0/0                 vlan100           local  no    N/A
  127.0.0.1/32          127.0.0.1        0/0                 loopback0         local  no    N/A
  150.1.1.0/24          150.1.1.102     0/0                 mgt-eth0/0/0     local  no    N/A
  150.1.1.102/32        150.1.1.102     0/0                 mgt-eth0/0/0     local  no    N/A
-----
Total: 5                Static: 0        Down: 0
Switch>
```

5.3.5 show ip route {static|local}**Function**

The **show ip route {static|local}** command displays the static or local IPv4 routing table.

Format

show ip route { static | local }

Parameter

NA

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

Display the static IPv4 routing table.

```
Switch>show ip route static
-----
Total: 0          Static: 0          Down: 0
Switch>
```

5.3.6 show {ip|ipv6} route statistic

Function

The **show {ip|ipv6} route statistic** command displays route statistics in the IPv4 routing table.

Format

- **show {ip|ipv6} route statistic**
- **show {ip|ipv6} route statistic all**
- **show {ip|ipv6} route statistic vpn-instance**
- **show {ip|ipv6} route statistic vpn-instance *name***

Parameter

Parameter	Description	Value
name	Specifies a VPN instance name.	The value is a string of no more than 64 characters.

Default Value

NA

View

Common user view

Usage Guidelines

The output of this command includes:

Proto: Routing protocol

total routes: Total number of routes in the current routing table

active routes: Number of active routes in the routing table

added routes: Number of routes added to the routing table (active and inactive)

deleted routes: Number of routes with deletion tags in the routing table

freed routes: Indicates the number of routes freed (permanently deleted) from the routing table.

Example

Display route statistics in the IPv4 routing table.

Switch>show ip route statistic				
Proto	total	active	added	deleted
	routes	routes	routes	routes
DIRECT	1	1	2	1
STATIC	0	0	0	0
RIP	0	0	0	0
OSPF	0	0	0	0
IS-IS	0	0	0	0
BGP	0	0	0	0
Other	0	0	0	0
Switch>				

5.3.7 show ip route summary

Function

The **show ip route summary** command displays the summarized routing information.

Format

show ip route summary

Parameter

NA

Default Value

NA

View

Common user view

Usage Guidelines

The output of this command includes:

Total route entry

Bad routing redirect

Dynamically created route

New gateway due to redirects

Destination found unreachable

Use of a wildcard route

Example

Display summarized routing information.

```
Switch>show ip route summary
SoftDestware route      :1
HardDestware route      :1
Software route           :1
Hardware route           :1
Software ILM             :0
Hardware ILM             :0
Switch>
```

5.3.8 show ipv6 route

Function

The **show ipv6 route** command displays the route of an IPv6 address or displays information on a multi-instance VLAN.

Format

- **show ipv6 route**
- **show ipv6 route *ipv6-address***
- **show ipv6 route *ipv6-address/M***
- **show ipv6 route *vpn-instance***
- **show ipv6 route *ipv6-address vpn-instance***
- **show ipv6 route { *static* | *local* }**
- **show ipv6 route summary**
- **show ipv6 route statistic**
- **show ipv6 route statistic *vpn-instance***
- **show ipv6 route statistic *vpn-instance name***

Parameter

Parameter	Description	Value

Parameter	Description	Value
ipv6-address	Specifies an IPv6 address.	In this format, a 128-digit IP address is divided into 8 segments. Each segment consists of 16 digits and is represented by 4 hexadecimal characters (0-9 and A-F). Segments are separated by colons (:). Every "X" represents a group of hexadecimal digits.
name	Specifies a VPN instance name.	The value is a string of up to 64 characters.
M	Specifies the mask of an IPv6 address.	The value is an integer ranging from 1 to 128.

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

View the IPv6 route information.

Switch>show ipv6 route				
Routing Tables: Public				
	Dest/Prefixlen		Nexthop	Interface
Proto	Pre/Cost	Vpn-Instance		

	::1/128		::1	loopback0
local	0/0	N/A		
	fe80::/64		fe80::216:16ff:fe02:8564	loopback0
local	0/0	N/A		
	fe80::216:16ff:fe02:8564/128		fe80::216:16ff:fe02:8564	loopback0
local	0/0	N/A		
	fe80::/64		fe80::216:16ff:fe02:8564	vlan1
local	0/0	N/A		
	fe80::216:16ff:fe02:8564/128		fe80::216:16ff:fe02:8564	vlan1
local	0/0	N/A		
	fe80::/64		fe80::216:16ff:fe02:8564	loopback1
local	0/0	N/A		
	fe80::216:16ff:fe02:8564/128		fe80::216:16ff:fe02:8564	loopback1
local	0/0	N/A		

Total: 7	Static: 0
Switch>	

5.3.9 show ip hwroute summary

Function

The **show ip hwroute summary** command displays the summarized hardware routing information.

Format

show ip hwroute summary

Parameter

NA

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

View the summarized hardware routing information.

Switch>show ip hwroute summary
Switch>

5.3.10 show ipv6 hwroute summary

Function

The **show ipv6 hwroute summary** command displays the summarized IPv6 hardware routing information.

Format

show ipv6 hwroute summary

Parameter

NA

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

View the summarized IPv6 hardware routing information.

Switch>show ipv6 hwroute summary

Switch>

5.4 OSPFv2 Configuration Commands

5.4.1 debug ospf

FunctionThe **debug ospf** command enables OSPF debugging.The **no debug ospf** command disables OSPF debugging.**Format**

- **debug ospf { global | all | lsa | hello | packet | neighbor | interface | ip-route | rtm | spf | syn | graceful-restart | nbrchange | frr | error }**
- **no debug ospf { global | all | lsa | hello | packet | neighbor | interface | ip-route | rtm | spf | syn | graceful-restart | nbrchange | frr | error }**
- **debug ospf { global | all | lsa | hello | packet | neighbor | interface | ip-route | rtm | spf | syn | graceful-restart | nbrchange | frr | error } process *process-id***
- **no debug ospf { global | all | lsa | hello | packet | neighbor | interface | ip-route | rtm | spf | syn | graceful-restart | nbrchange | frr | error } process *process-id***
- **debug ospf { global | all | lsa | hello | packet | neighbor | interface | ip-route | rtm | spf | syn | graceful-restart | nbrchange | frr | error } process all**
- **no debug ospf { global | all | lsa | hello | packet | neighbor | interface | ip-route | rtm | spf | syn | graceful-restart | nbrchange | frr | error } process all**

Parameter

Parameter	Description	Value
process	Specifies a process ID.	The value is an integer ranging from 1 to 256.

Default Value

By default, OSPF debugging is disabled.

View

Privileged user view

Usage Guidelines

You can use this command to debug and locate OSPF faults.

Example

Enable OSPF debugging.

```
Switch#debug ospf all
Switch#
```

5.4.2 maxage-lsa route-calculate-delay**Function**

The **maxage-lsa route-calculate-delay** command specifies the delay for route calculation when OSPF LSA oscillates frequently.

The **no maxage-lsa route-calculate-delay** command deletes the configuration.

Format

- **maxage-lsa route-calculate-delay** *delay-value*
- **no maxage-lsa route-calculate-delay**

Parameter

Parameter	Description	Value
delay-value	Specifies a delay for route calculation.	The value is an integer ranging from 1 to 65535, in seconds.

Default Value

NA

View

OSPFv2 route configuration view

Usage Guidelines

If the peer OSPF LSA oscillates frequently, the local device route also oscillates, affecting the service traffic. In this case, run **maxage-lsa route-calculate-delay** on the local device to delay route calculation for the local device to suppress route oscillation on the local device.

Example

Set the delay for route calculation when OSPF LSA oscillates frequently.

```
Switch(config-ospf-1)#maxage-lsa route-calculate-delay 100
Switch(config-ospf-1)#
```

5.4.3 preference

Function

The **preference** command sets the priority of the OSPF protocol.

The **no preference** command cancels the priority configuration for the OSPF protocol.

Format

- **preference** *preference-value*
- **preference** *preference-value* **route-policy** *policy-name*
- **preference ase** *preference-value*
- **preference ase** *preference-value* **route-policy** *policy-name*
- **no preference**
- **no preference ase**

Parameter

Parameter	Description	Value
preference-value	Specifies the priority of the OSPF protocol. A smaller value indicates a higher priority.	The value is an integer ranging from 1 to 255.
policy-name	Specifies a routing policy name.	The length is no more than 20 characters.
ase	Sets the priority of AS-external routes.	-

Default Value

The default priority of OSPF routes is 10. When the **ase** keyword is specified, the default priority is 150.

View

OSPFv2 route configuration view

Usage Guidelines

A switch may run multiple dynamic routing protocols simultaneously. In this case, the switch needs to implement routing information sharing among these protocols and select routes of them. Therefore, you need to set a priority value for each routing protocol. When different protocols discover the same route, the switch selects the protocol with highest priority. This command sets the priority of the OSPF protocol.

Example

Set the priority of the OSPF protocol to 30.

```
Switch(config-ospf-1)#preference 30
Switch(config-ospf-1)#
```

5.4.4 filter route-policy**Function**

The **filter route-policy** command configures the routing protocol filter policy. Only filtered routes can be used to generate routes in the routing table.

The **no filter router-policy** command cancels the routing protocol filter policy.

Format

- **filter route-policy** *route-policy-name*
- **no filter router-policy** *route-policy-name*

Parameter

Parameter	Description	Value
route-policy-name	Specifies the name of the routing policy, which must be specified in the routing policy.	The length is no more than 20 characters.

Default Value

By default, the value is a null character string, indicating not referring to any routing policy.

View

OSPFv2 configuration view

Usage Guidelines

Only routing information in compliance with certain conditions can be used to generate routes in the routing table.

You can use this command to set filter conditions for routing information. Only filtered information can be used to generate routes in the routing table.

Before running this command, you must create a routing policy first.

Example

Configure filter policy fhn1 for the routing protocol.

```
Switch(config-ospf-1)#filter route-policy fhn1
Switch(config-ospf-1)#
```

5.4.5 valid-ttl-hops

Function

The **valid-ttl-hops** command sets the valid TTL value of OSPF.

Format

valid-ttl-hops { *hops-number* | **default** }

Parameter

Parameter	Description	Value
hops-number	Specifies the number of hops.	The value is an integer ranging from 1 to 255.
default	Specifies the default number of hops.	The default value is 0.

Default Value

The default value is 0.

View

OSPFv2 configuration view

Usage Guidelines

If the TTL is not configured, OSPF does not detect the TTL by default. When the TTL is configured and the TTL of a received packet is smaller than 255-hops number+1, the switch discards the packet.

Example

Set the valid TTL of OSPF to 200.

```
Switch(config-ospf-1)#valid-ttl-hops 200
```

```
Switch(config-ospf-1)#
```

5.4.6 area authentication

Function

The **area authentication** command configures plain-text authentication or MD5 authentication for an OSPF area.

The **no area authentication** command cancels the OSPF area authentication configuration.

Format

- **area** *area-id* **authentication simple-password** *text-key*
- **area** *area-id* **authentication simple-password** { **cipher** | **plain** } *text-key*
- **area** *area-id* **authentication md5** *key-id* { **cipher** | **plain** } *md5-key*
- **area** *area-id* **authentication md5** *key-id* *md5-key*
- **no area** *area-id* **authentication**

Parameter

Parameter	Description	Value
simple-password	Specifies the plain-text authentication mode.	-
text-key	Specifies the keyword for plain-text authentication.	The value is a string of less than nine characters.
md5	Specifies the MD5 cipher-text authentication mode.	-
key-id	Specifies the authentication ID of the MD5 key.	The value is an integer ranging from 1 to 255.
md5-key	Specifies the key word for ciphertext authentication.	The value is an integer ranging from 1 to 16, in character string format.
area-id	Specifies an area ID.	The value is a dotted decimal number or an integer. Generally, for an area with ID smaller than 65535, the value is an integer. For an area with ID larger than 65535, the value is an IP address. The value ranges from 0 to 4294967295.

Default Value

By default, OSPF area authentication is not configured.

View

OSPFv2 configuration view

Usage Guidelines

You can use this command to configure MD5 authentication for an area. After configuration, all interfaces within the area use the same MD5 authentication password. You can run the `no area authentication` command to cancel the area authentication. Then, all interfaces within the area do not perform authentication.

Before running this command, you must create an area.

Example

Set MD5 authentication password of area 0 to aaa and KEY ID to 100.

```
Switch#configure
    %Enter configuration commands.End with Ctrl+Z or command "quit" & "end"
Switch(config)#router ospf
Switch(config-ospf-1)#network 1.1.1.0 255.255.255.0 area 0
Switch(config-ospf-1)#area 0 authentication md5 100 aaa
Switch(config-ospf-1)#
```

5.4.7 area nssa default-cost

Function

The **area nssa default-cost** command configures the default NSSA LSA cost.

Format

area *area-id* **nssa default-cost** { *cost-value* | **default** }

Parameter

Parameter	Description	Value
area-id	Specifies an area ID.	The value is a dotted decimal number or an integer. Generally, for an area with ID smaller than 65535, the value is an integer. For an area with ID larger than 65535, the value is an IP address. The value ranges from 0 to 4294967295.
cost-value	Specifies a cost.	The value is an integer ranging from 0 to 65535.

Default Value

The default value is 1.

View

OSPFv2 configuration view

Usage Guidelines

Before running this command, you must create an area.

Example

Set the default NSSA LSA cost to 3000.

```
Switch(config)#router ospf
Switch(config-ospf-1)#network 2.2.2.0 255.255.255.0 area 1
Switch(config-ospf-1)#area 1 nssa
Switch(config-ospf-1)#area 1 nssa default-cost 3000
Switch(config-ospf-1)#
```

5.4.8 area nssa translator

Function

The **area nssa translator** command specifies a transition router or a candidate transition router for the ABR in the NSSA area.

Format

area *area-id* **nssa translator** { **always** | **candidate** }

Parameter

Parameter	Description	Value
area-id	Specifies an area ID.	The value is a dotted decimal number or an integer. Generally, for an area with ID smaller than 65535, the value is an integer. For an area with ID larger than 65535, the value is an IP address. The value ranges from 0 to 4294967295.
always	Specifies a transition router for the ABR in the NSSA area. Multiple ABRs in the NSSA area can be configured as the transition router.	-
candidate	Specifies a candidate transition router for the ABR in the NSSA area. If no conversion router is designated in the current area, the conversion router is elected from all the candidate routers.	-

Default Value

NA

View

OSPFv2 configuration view

Usage Guidelines

Before running this command, you must create an area.

Example

Specify a transition router for the ABR in the NSSA area.

```
Switch(config-ospf-1)#network 1.1.1.0 255.255.255.0 area 10000
Switch(config-ospf-1)#area 10000 nssa translator always
Switch(config-ospf-1)#
```

5.4.9 area nssa

Function

The **area nssa** command configures an OSPF area as an NSSA area.

The **no area nssa** command restores an NSSA area as a common area.

Format

- **area** *area-id* **nssa**
- **no area** *area-id* **nssa**

Parameter

Parameter	Description	Value
area-id	Specifies an area ID.	The value is a dotted decimal number or an integer. Generally, for an area with ID smaller than 65535, the value is an integer. For an area with ID larger than 65535, the value is an IP address. The value ranges from 0 to 4294967295.

Default Value

By default, the NSSA area is disabled in OSPF areas.

View

OSPFv2 configuration view

Usage Guidelines

An NSSA area is similar to a stub area, except that the NSSA area can send external routes but does not accept external routes. The router in the NSSA area generates Type7 LSAs for external routes, which are used for route calculation within the area. The ABR converts Type7 LSAs into Type5 LSAs and sends them to other areas. The ABR also generates a default summary LSA for the NSSA area.

NSSA area configuration has the following limitations:

The backbone area cannot be configured as an NSSA area.

A stub area cannot be configured as an NSSA area.

A virtual link transit area cannot be configured as an NSSA area.

Example

Configure area 1 as an NSSA area.

```
Switch(config)#router ospf
Switch(config-ospf-1)#network 2.2.2.0 255.255.255.0 area 1
Switch(config-ospf-1)#area 1 nssa
Switch(config-ospf-1)#
```

5.4.10 area nssa range

Function

The **area nssa range** command configures the aggregation route entry in the NSSA area.

The **no area nssa range** command deletes the aggregation route entry configured for the NSSA area.

Format

- **area** *area-id* **nssa range** *dst-address dst-mask* { **advertise** | **no-advertise** }
- **no area** *area-id* **nssa range** *dst-address dst-mask*

Parameter

Parameter	Description	Value
area-id	Specifies an area ID.	The value is a dotted decimal number or an integer. Generally, for an area with ID smaller than 65535, the value is an integer. For an area with ID larger than 65535, the value is an IP address. The value ranges from 0 to 4294967295.
dst-address	Specifies an aggregation address.	The value is in dotted decimal notation.
dst-mask	Specifies an aggregation mask.	The value is in dotted decimal notation.

Parameter	Description	Value
advertise	Indicates that the switch receives aggregation entries.	-
no-advertise	Indicates that the switch rejects aggregation entries.	-

Default Value

By default, the NSSA area does not include any aggregation entry.

View

OSPFv2 configuration view

Usage Guidelines

Before running this command, you must create an area.

You can use this command to configure an aggregation route entry for an area. You can use the no area range command to delete an aggregation entry configured for an area.

When the ABR calculates the route for area A, it advertises the internal routes of area A to other areas, and generates a Summary LSA for each area. If the internal route scale is large, the number of Summary LSA entries is large. You can configure aggregation entry for area A to control the number of Summary LSAs.

After the aggregation entry is configured, routes matching the aggregation entry in area A will not be included in the Summary LSAs of other areas. According to different advertise attributes of the aggregation entries, the following situations may exist:

1. The advertise operation is specified for the aggregation entry, and the Summary LSA is generated for the aggregation entry.
2. The not-advertise operation is specified for the aggregation entry, and the Summary LSA is not generated for the aggregation entry.



Caution

This command can only be used for an existing area.

Example

```
# Enable area 0 to include only Summary LSA of 1.1.0.0/16.
```

```
Switch(config-ospf-1)#network 1.1.0.0 255.255.255.0 area 0
Switch (config-ospf-1)#area 0 nssa range 1.1.0.0 255.255.0.0 advertise
```

The following command enables area 1 not include any Summary LSA of 1.1.0.0/16.

```
Switch(config-ospf-1)#network 1.1.0.0 255.255.255.0 area 1
Switch (config-ospf-1)#area 0 nssa range 1.1.0.0 255.255.0.0 not-advertise
```

5.4.11 area range

Function

The **area range** command configures the aggregation route entry in an area.

The **no area range** command deletes the aggregation route entry configured for an area.

Format

- **area** *area-id* **range** *dst-address dst-mask* { **advertise** | **no-advertise** }
- **no area** *area-id* **range** *dst-address dst-mask*

Parameter

Parameter	Description	Value
area-id	Specifies an area ID.	The value is a dotted decimal number or an integer. Generally, for an area with ID smaller than 65535, the value is an integer. For an area with ID larger than 65535, the value is an IP address. The value ranges from 0 to 4294967295.
dst-address	Specifies an aggregation address.	The value is in dotted decimal notation.
dst-mask	Specifies an aggregation mask.	The value is in dotted decimal notation.
advertise	Indicates that the switch receives aggregation entries.	-
no-advertise	Indicates that the switch rejects aggregation entries.	-

Default Value

By default, the OSPF area has no aggregation entry.

View

OSPFv2 configuration view

Usage Guidelines

Before running this command, you must create an area.

You can use this command to configure an aggregation route entry for an area. You can use the `no area range` command to delete an aggregation entry configured for an area.

When the ABR calculates the route for area A, it advertises the internal routes of area A to other areas, and generates a Summary LSA for each area. If the internal route scale is large, the number of Summary LSA entries is large. You can configure aggregation entry for area A to control the number of Summary LSAs.

After the aggregation entry is configured, routes matching the aggregation entry in area A will not be included in the Summary LSAs of other areas. According to different advertise attributes of the aggregation entries, the following situations may exist:

1. The advertise operation is specified for the aggregation entry, and the Summary LSA is generated for the aggregation entry.
2. The not-advertise operation is specified for the aggregation entry, and the Summary LSA is not generated for the aggregation entry.



Caution

This command can only be used for an existing area.

Example

Enable area 0 to include only Summary LSA of 1.1.0.0/16.

```
Switch(config-ospf-1)#network 1.1.0.0 255.255.255.0 area 0
Switch (config-ospf-1)#area 0 range 1.1.0.0 255.255.0.0 advertise
```

The following command enables area 1 not include any Summary LSA of 1.1.0.0/16.

```
Switch(config-ospf-1)#network 1.1.0.0 255.255.255.0 area 1
Switch (config-ospf-1)#area 0 range 1.1.0.0 255.255.0.0 not-advertise
```

5.4.12 area stub

Function

The **area stub** command configures an OSPF area as a stub area.

The **no area stub** command restores a stub area as a common area.

Format

- **area *area-id* stub**
- **no area *area-id* stub**

Parameter

Parameter	Description	Value
area-id	Specifies an area ID.	The value is a dotted decimal number or an integer. Generally, for an area with ID smaller than 65535, the value is an integer. For an area with ID larger than 65535, the value is an IP address. The value ranges from 0 to 4294967295.

Default Value

By default, the OSPF area is not a stub area.

View

OSPFv2 configuration view

Usage Guidelines

You can use this command to configure an area as a stub area. The stub area does not include external routes (Type 5 LSA) and does not generate external routes. The stub area configuration has the following limitations:

The backbone area cannot be configured as a stub area.

If an area is a virtual link transit area, you cannot configure this area as a stub area. Otherwise, the area works abnormally.

After a stub area is configured, the ABR generates a default Summary LSA for the area. The generation process of other summary LSAs remains unchanged. If the no-summary attribute is configured, the ABR clears other non-default Summary LSAs and includes only one default Summary LSA.

A stub area can control the number of LSAs within an area. If an area has limited router memory and cannot receive a large amount of LSAs, you can configure this area as a stub area.

A stub area cannot be used as the virtual link transit area. All routers within a stub area must have the same stub attributes. Otherwise, a neighbor relation cannot be established.

Example

```
# Restore a stub area as a common area.
```

```
Switch(config-ospf-1)#no area 1 stub
Switch(config-ospf-1)#
```

5.4.13 area stub no-summary

Function

The **area stub no-summary** command configures an area as a total stub area.

Format

area *area-id* **stub no-summary**

Parameter

Parameter	Description	Value
area-id	Specifies an area ID.	The value is a dotted decimal number or an integer. Generally, for an area with ID smaller than 65535, the value is an integer. For an area with ID larger than 65535, the value is an IP address. The value ranges from 0 to 4294967295.

Default Value

NA

View

OSPFv2 configuration view

Usage Guidelines

Before running this command, you must create an area.

The ABR in an area can stop generating other summary LSAs for the stub area to further compress the LSA scale. At this time, the stub area is known as a total stub area.

Example

Configure area 1.3.2.1 as a totally stub area.

```
Switch(config-ospf-1)#area 1.3.2.1 stub no-summary
Switch(config-ospf-1)#
```

5.4.14 area nssa no-summary

Function

The **area nssa no-summary** command configures an area as a totally NSSA area.

Format

area *area-id* **nssa no-summary**

Parameter

Parameter	Description	Value
area-id	Specifies an area ID.	The value is a dotted decimal number or an integer. Generally, for an area with ID smaller than 65535, the value is an integer. For an area with ID larger than 65535, the value is an IP address. The value ranges from 0 to 4294967295.

Default Value

NA

View

OSPFv2 configuration view

Usage Guidelines

Before running this command, you must create an area.

Example

Configure area 1 as a total NSSA area.

```
Switch(config-ospf-1)#area 1 nssa no-summary
Switch(config-ospf-1)#
```

5.4.15 area virtual-link**Function**

The **area virtual-link** command configures an OSPF virtual link.

The **no area virtual-link** command deletes an OSPF virtual link.

Format

- **area** *area-id* **virtual-link** *neighbor-address*
- **area** *area-id* **virtual-link** *neighbor-address* **dead-interval** { *dead-interval-time* | **default** }
- **area** *area-id* **virtual-link** *neighbor-address* **hello-interval** { *hello-interval-time* | **default** }
- **area** *area-id* **virtual-link** *neighbor-address* **retransmit-interval** { *retransmit-interval-time* | **default** }

- **area** *area-id* **virtual-link** *neighbor-address* **transmit-delay** { *transmit-interval-time* | **default** }
- **no area** *area-id* **virtual-link** *neighbor-address*

Parameter

Parameter	Description	Value
area-id	Specifies the area ID of a transit area.	The value is a dotted decimal number or an integer. Generally, for an area with ID smaller than 65535, the value is an integer. For an area with ID larger than 65535, the value is an IP address. The value ranges from 0 to 4294967295.
neighbor-address	Specifies the router ID of a virtual neighbor.	The value is in dotted decimal notation.
dead-interval-time	Specifies the dead interval of a virtual neighbor.	The value is a dead-interval integer ranging from 0 to 2147483647, in seconds.
transmit- interval-time	Specifies the transmission delay of the link state notification.	The value is an integer ranging from 0 to 3600, in seconds.
hello- interval-time	Specifies the interval for calling a virtual neighbor.	The value is an integer ranging from 1 to 65535, in seconds.
retransmit-interval-time	Specifies the retransmission interval of the link state notification.	The value is an integer ranging from 1 to 3600, in seconds.

Default Value

By default, virtual links are established based on the default parameters.

View

OSPFv2 configuration view

Usage Guidelines

In OSPF, the backbone area summarizes topology information on areas to form inter-domain routes. Therefore, all inter-domain communication traffic passes through the backbone area, while non-backbone areas cannot directly exchange data packets. On an OSPF network, all non-backbone areas should be connected to the backbone area. Some routes cannot be calculated if non-backbone areas are not connected to the backbone area or the backbone area itself is not continuous due to network lines or design. Therefore, virtual links can be configured to address such problem.

Virtual link configuration must comply with the following rules:

The virtual link must be configured on the boundary switch between two areas.

An area through which the virtual link passes is known as a transit area. The transit area must have all route selection information, so that the switch can identify a physical route destined for the backbone area to transmit virtual link information.

The transit area cannot be a stub area.

Example

Configure the virtual link for area 1.

```
Switch(config-ospf-1)#area 1 virtual-link 1.1.1.0
Switch(config-ospf-1)#
```

5.4.16 area virtual-link authentication

Function

The **area virtual-link authentication** command configures virtual link authentication, MD5 authentication, and simple password authentication.

The **no area virtual-link authentication** command deletes virtual link authentication, MD5 authentication, and simple password authentication.

Format

- **area** *area-id* **virtual-link** *neighbor-address* **authentication md5** *md5* { **cipher** | **plain** } *md5-key*
- **area** *area-id* **virtual-link** *neighbor-address* **authentication simple-password** { **cipher** | **plain** } *md5-key*
- **area** *area-id* **virtual-link** *neighbor-address* **authentication md5** *md5* *md5-key*
- **area** *area-id* **virtual-link** *neighbor-address* **authentication simple-password** *md5-key*
- **no area** *area-id* **virtual-link** *neighbor-address* **authentication**

Parameter

Parameter	Description	Value
area-id	Specifies the area ID of a transit area.	The value is a dotted decimal number or an integer. Generally, for an area with ID smaller than 65535, the value is an integer. For an area with ID larger than 65535, the value is an IP address. The value ranges from 0 to 4294967295.
neighbor-address	Specifies the router ID of a virtual neighbor.	The value is in dotted decimal notation.
md5	Configures MD5	The value is an integer ranging from 1 to 255.

Parameter	Description	Value
	authentication for the interface.	
simple-password	Configures simple password authentication for an interface.	The value is a string consisting of 1 to 8 characters.
md5-key	Specifies the key word for ciphertext authentication.	The value is an integer ranging from 1 to 16, in character string format.

Default Value

NA

View

OSPFv2 route configuration view

Usage Guidelines

Before configuring the virtual link authentication, you must configure the virtual link. For details, see [area virtual-link](#).

Example

Configure MD5 authentication for the virtual neighbor.

```
Switch(config-ospf-1)#area 1 virtual-link 1.1.1.0
Switch(config-ospf-1)#area 1 virtual-link 1.1.1.0 authentication md5 123
```

5.4.17 bandwidth-reference

Function

The **bandwidth-reference** command configures the reference bandwidth of an interface, used to dynamically calculate the interface cost.

Format

bandwidth-reference { *bandwidth* | **default** }

Parameter

Parameter	Description	Value
bandwidth	Specifies the reference bandwidth of an interface.	The value is an integer ranging from 1 to 2147483647.
default	Uses the default value.	By default, the reference link bandwidth is 100 Mbit/s.

Default Value

By default, the reference link bandwidth is 100 Mbit/s.

View

OSPFv2 configuration view

Usage Guidelines

NA

Example

Set the reference bandwidth of an interface to 1000 Mbit/s.

```
Switch(config-ospf-1)#bandwidth-reference 1000
Switch(config-ospf-1)#
```

5.4.18 default-route-advertise always

Function

The **default-route-advertise always** command forcibly advertises default routes to common OSPF areas. The switch generates and advertises a Category-5 LSA describing the default routes. In addition, the switch does not calculate default routes of other devices.

The **no default-route-advertise** command cancels default route advertisement to the common OSPF route areas.

Format

- **default-route-advertise always**
- **default-route-advertise always cost** *cost-value*
- **default-route-advertise always cost** *cost-value* **type** *type-value*
- **default-route-advertise always type** *type-value*
- **no default-route-advertise**

Parameter

Parameter	Description	Value
always	Indicates that the switch generates and advertises an LSA describing default routes regardless of whether another OSPF process has an active default route.	-
cost-value	Specifies a route cost.	The value is an integer ranging from 1 to 65535.

Parameter	Description	Value
type-value	Specifies a route cost type.	The value is an integer ranging from 1 to 2.

Default Value

By default, default-route-advertise always is disabled.

View

OSPFv2 configuration view

Usage Guidelines

NA

Example

Configure the switch to advertise default routes to common OSPF route areas.

```
Switch(config-ospf-1)#default-route-advertise always
Switch(config-ospf-1)
```

5.4.19 graceful-restart begin

Function

The **graceful-restart begin** command performs a graceful restart.

Format

graceful-restart begin

Parameter

NA

Default Value

NA

View

OSPFv2 configuration view

Usage Guidelines

NA

Example

Perform a graceful restart.

```
Switch(config-ospf)#graceful-restart begin
Switch(config-ospf)#
```

5.4.20 graceful-restart helper

Function

The **graceful-restart helper** command enables the OSPF graceful restart helper.

The **graceful-restart helper** command disables the OSPF graceful restart helper.

Format

- **graceful-restart helper**
- **no graceful-restart helper**

Parameter

NA

Default Value

NA

View

OSPFv2 configuration view

Usage Guidelines

NA

Example

Enable the OSPF graceful restart helper.

```
Switch(config-ospf)#graceful-restart helper
Switch(config-ospf)#
```

5.4.21 graceful-restart

Function

The **graceful-restart** command enables the graceful restart function.

The **graceful-restart period** command sets the graceful restart period.

The **no graceful-restart** command disables the graceful restart function.

Format

- **graceful-restart**
- **graceful-restart period** *restart-time*
- **no graceful-restart**

Parameter

Parameter	Description	Value
restart time	Specifies the restart period.	The value is an integer ranging from 40 to 1800, in seconds.
period	Sets the restart period.	-

Default Value

NA

View

OSPFv2 configuration view

Usage Guidelines

Before running **gr**, manually enable opaque.

Example

Enable the graceful restart function.

```
Switch(config-ospf)#graceful-restart
Switch(config-ospf)#
```

5.4.22 ip ospf dead-interval

Function

The **ip ospf dead-interval** command configures the neighbor expiration time of an IPv4 OSPF interface.

Format

ip ospf dead-interval { *interval* | **default** }

Parameter

Parameter	Description	Value
interval	Specifies the neighbor expiration time of an OSPF interface.	The value is an integer ranging from 0 to 2147483647.
default	Specifies the default neighbor expiration time of an OSPF interface.	40 seconds

Default Value

By default, the neighbor expiration time of an OSPF interface is 40s.

View

VLANIF configuration view, loopback interface configuration view, Ethernet routing interface configuration view, BD interface configuration view

Usage Guidelines

You can use this command to change the default neighbor expiration time of the OSPF interface. Note that the same expiration time must be configured for both parties and the value must be larger than three times the interval for sending Hello packets.

Example

Set the neighbor expiration time of an OSPF interface to 30s.

```
Switch(config-vlanif-3)#ip ospf dead-interval 30
Switch(config-vlanif-3)#
```

5.4.23 ip ospf hello-interval**Function**

The **ip ospf hello-interval** command configures the interval for sending Hello packets by an IPv4 OSPF interface.

Format

ip ospf hello-interval { *hello-interval* | **default** }

Parameter

Parameter	Description	Value
hello-interval	Specifies the interval for sending Hello packets by an OSPF interface.	The value is an integer ranging from 1 to 65535.
default	Specifies the default interval for sending Hello packets by an OSPF interface.	10 seconds

Default Value

The default value is 10s.

View

VLANIF configuration view, loopback interface configuration view, Ethernet routing interface configuration view, BD interface configuration view

Usage Guidelines

By default, the interval for sending Hello packets by an OSPF interface is 10s. You can modify the default value, but the interval configured for both parties must be the same. The interval must be smaller than neighbor expiration time/3.

Example

Set the interval for sending Hello packets by the OSPF interface to 20s.

```
Switch(config-vlanif-3)#ip ospf hello-interval 20
Switch(config-vlanif-3)#
```

5.4.24 ip ospf if-type

Function

The **ip ospf if-type** command sets the network type for the OSPF interface.

Format

ip ospf if-type { broadcast | nbma | p2p | p2multip }

Parameter

Parameter	Description	Value
broadcast	Specifies the broadcast type for the interface.	-
nbma	Specifies the NBMA type for the interface.	
p2p	Specifies the point-to-point (P2P) type for the interface.	-
p2multip	Specifies the point-to-multi-point (p2multip) type for the interface.	

Default Value

By default, all OSPF interfaces are of the broadcast type.

View

VLANIF configuration view, loopback interface configuration view, Ethernet routing interface configuration view, BD interface configuration view

Usage Guidelines

All switch interfaces are Ethernet interfaces. By default, all OSPF interfaces are of the broadcast type. Broadcast interfaces are more complex than P2P interfaces in operation. If the switch uses P2P connections, change the OSPF interface to P2P. P2P interfaces are recommended for both neighbors; otherwise, the operation may fail.

Example

Set the OSPF interface type to P2P.

```
Switch(config-vlanif-3)#ip ospf if-type p2p
Switch(config-vlanif-3)#
```

5.4.25 ip ospf authentication**Function**

The **ip ospf authentication** command configures the OSPF interface authentication mode.

Format

- **ip ospf authentication md5** *key-id* { **cipher** | **plain** } *md5-key*
- **ip ospf authentication md5** *key-id* *md5-key*
- **ip ospf authentication simple-password** *key-value*
- **ip ospf authentication simple-password** { **cipher** | **plain** } *key-value*
- **no ip ospf authentication**

Parameter

Parameter	Description	Value
simple-password	Configures simple password authentication for an interface.	The value is a string consisting of 1 to 8 characters.
md5	Configures MD5 authentication for an interface.	-
key-id	Specifies the authentication ID of the MD5 key.	The value is an integer ranging from 1 to 255.
md5-key	Specifies the key word for ciphertext authentication.	The value is a string consisting of 1 to 16 characters, without spaces. The value is case sensitive.
key-value	Specifies the authentication key of a simple password.	The value is a character string.

Default Value

NA

View

VLANIF configuration view, loopback interface configuration view, Ethernet routing interface configuration view, BD interface configuration view

Usage Guidelines

The interface authentication configuration shall prevail if the interface authentication configuration and area authentication configuration co-exist.

Example

Configure MD5 authentication for an OSPF interface.

```
Switch(config-vlanif-3)#ip ospf authentication md5 100 key
Switch(config-vlanif-3)#
```

Configure simple password authentication for an OSPF interface.

```
Switch(config-vlanif-3)#ip ospf authentication simple-password key
Switch(config-vlanif-3)#
```

5.4.26 ip ospf bfd {enable|disable}**Function**

The **ip ospf bfd {enable|disable}** command enables or disables the BFD feature for a VLAN interface.

Format

ip ospf bfd { enable | disable }

Parameter

Parameter	Description	Value
enable	Enables the BFD feature to quickly detect OSPF neighbor disconnection.	-
disable	Disables the BFD feature.	-

Default Value

NA

View

VLANIF configuration view, loopback interface configuration view, Ethernet routing interface configuration view, BD interface configuration view

Usage Guidelines

NA

Example

Enable the BFD feature.

```
Switch(config-vlanif-3)#ip ospf bfd enable
Switch(config-vlanif-3)#
```

5.4.27 ip ospf cost

Function

The **ip ospf cost** command configures the cost of an OSPF interface.

Format

ip ospf cost { *cost-value* | **default** }

Parameter

Parameter	Description	Value
cost-value	Specifies the cost required for running the OSPF protocol.	The value is an integer ranging from 1 to 65535.
default	Specifies the default cost required for running the OSPF protocol.	The value is an integer and automatically set by the switch.

Default Value

By default, the default value is automatically set by the switch.

View

VLANIF configuration view, loopback interface configuration view, Ethernet routing interface configuration view, BD interface configuration view

Usage Guidelines

Costs of OSPF interfaces are used for route selection control.

Example

Set the cost of an OSPF interface to 20000.

```
Switch(config-vlanif-3)#ip ospf cost 20000
Switch(config-vlanif-3)#
```

5.4.28 ip ospf fast-change

Function

The **ip ospf fast-change** command enables or disables fast neighbor establishment for an OSPF interface.

Format

ip ospf fast-change { enable | disable }

Parameter

Parameter	Description	Value
enable	Enable the fast neighbor establishment for an OSPF interface.	-
disable	Disables the fast neighbor establishment for an OSPF interface.	-

Default Value

NA

View

VLANIF configuration view, loopback interface configuration view, Ethernet routing interface configuration view, BD interface configuration view

Usage Guidelines

NA

Example

Enable fast neighbor establishment for an OSPF interface.

```
Switch(config-vlanif-3)#ip ospf fast-change enable
Switch(config-vlanif-3)#
```

5.4.29 ip ospf flooding-group

Function

The **ip ospf flooding-group** command configures the OSPF flooding group.

Format

ip ospf flooding-group { flooding-group-number | default }

Parameter

Parameter	Description	Value
flooding-group-number	Non-0: If the value is not 0, interfaces within the same flooding group do not spread the LSA. If the value is 0, the configuration restores to the normal mode.	The value is an integer ranging from 0 to 64.

Parameter	Description	Value
default	Specifies the default value.	0

Default Value

The default value is 0.

View

VLANIF configuration view, loopback interface configuration view, Ethernet routing interface configuration view, BD interface configuration view

Usage Guidelines

NA

Example

Configure OSPF flooding group 1.

```
Switch(config-vlanif-3)#ip ospf flooding-group 1
Switch(config-vlanif-3)#
```

5.4.30 ip ospf mtu

Function

The **ip ospf mtu** command configures the MTU for an OSPF interface.

Format

ip ospf mtu { *mtu* | **default** }

Parameter

Parameter	Description	Value
mtu	Specifies the MTU value for the OSPF interface.	The value is an integer ranging from 128 to 9216.
default	Specifies the default MTU value for the OSPF interface.	The value is 1500.

Default Value

The default value is 1500.

View

VLANIF configuration view, loopback interface configuration view, Ethernet routing interface configuration view, BD interface configuration view

Usage Guidelines

The default MTU of the OSPF interface is the IPMTU of the interface. If the interface does not support MTU configuration, the value is 0 by default. You can use this command to modify the MTU of the OSPF interface. Note that this command is not used to modify the MTU of an IP interface.

You must configure the same MTU value for both parties in a neighbor relation.

Example

Set the MTU value of an OSPF interface to 1000.

```
Switch(config-vlanif-3)#ip ospf mtu 1000
Switch(config-vlanif-3)#
```

5.4.31 ip ospf mtu-ignore {enable|disable}**Function**

The **ip ospf mtu-ignore {enable|disable}** command enables or disables MTU detection ignorance on an interface.

Format

ip ospf mtu-ignore { enable | disable }

Parameter

Parameter	Description	Value
enable	Enables MTU detection ignorance.	-
disable	Disables MTU detection ignorance.	-

Default Value

Disable

View

VLANIF configuration view, loopback interface configuration view, Ethernet routing interface configuration view, BD interface configuration view

Usage Guidelines

NA

Example

Enables MTU detection ignorance.

```
Switch(config-ospf-1)#network 1.1.1.0 255.255.255.0 area 0
```

```
Switch(config-ospf-1)#quit
Switch(config-vlanif-1)#ip ospf mtu-ignore enable
Switch(config-vlanif-1)#
```

5.4.32 ip ospf passive-interface

Function

The **ip ospf passive-interface** command configures an OSPF passive interface.

The **no ip ospf passive-interface** command cancels an OSPF passive interface.

Format

- **ip ospf passive-interface**
- **no ip ospf passive-interface**

Parameter

NA

Default Value

NA

View

VLANIF configuration view, loopback interface configuration view, Ethernet routing interface configuration view, BD interface configuration view

Usage Guidelines

A passive interface refers to an OSPF interface that does not send or receive protocol messages and does not establish any neighbor relation. However, the interface route is included in the Router LSA for internal route propagation. It can be used for the stub route.

Example

Configure OSPF interface VLAN3 as a passive interface.

```
Switch(config-vlanif-3)#ip ospf passive-interface
Switch(config-vlanif-3)#
```

5.4.33 ip ospf poll-interval

Function

The **ip ospf poll-interval** command specifies the interval for sending Hello packets by a neighbor router on the NBMA network.

Format

ip ospf poll-interval { *poll-interval-time* | **default** }

Parameter

Parameter	Description	Value
poll-interval-time	Specifies the interval for sending Hello packets by a neighbor router on the NBMA network.	The value is an integer ranging from 1 to 3600, in seconds.
default	Specifies the default value.	120s

Default Value

The default value is 120.

View

VLANIF configuration view, loopback interface configuration view, Ethernet routing interface configuration view, BD interface configuration view

Usage Guidelines

NA

Example

Set the interval for sending Hello packets by a neighboring router on the NBMA network to 1500 seconds.

```
Switch(config-vlanif-3)#ip ospf poll-interval 1500
Switch(config-vlanif-3)#
```

5.4.34 ip ospf priority**Function**

The **ip ospf priority** command configures the OSPF interface priority.

Format

ip ospf priority { *priority* | **default** }

Parameter

Parameter	Description	Value
priority	Specifies an OSPF interface priority.	The value is an integer ranging from 0 to 255, in BPS.
default	Specifies the default OSPF interface priority.	The value is 1.

Default Value

The default value is 1.

View

VLANIF configuration view, loopback interface configuration view, Ethernet routing interface configuration view, BD interface configuration view

Usage Guidelines

The OSPF interface priority is used for DR election. Generally, it does not need to be configured, especially in a point-to-point connection scenario where the interface priority is basically useless. However, if you require a specific interface functioning as the DR, you can set a higher priority for the interface. Note that the DR of OSPF interfaces cannot be preempted. If a device serves as the DR, it constantly serves as the DR unless it is faulty or disabled.

Example

Set OSPF interface priority to 125.

```
Switch(config-vlanif-3)#ip ospf priority 125
Switch(config-vlanif-3)#
```

5.4.35 ip ospf retransmit-interval**Function**

The **ip ospf retransmit-interval** command configures the retransmission interval for an OSPF interface.

Format

ip ospf retransmit-interval { *interval-time* | **default** }

Parameter

Parameter	Description	Value
interval-time	Specifies a retransmission interval.	The value is an integer ranging from 1 to 3600, in seconds.
default	Specifies the default retransmission interval.	The value is 5s.

Default Value

The default value is 5s.

View

VLANIF configuration view, loopback interface configuration view, Ethernet routing interface configuration view, BD interface configuration view

Usage Guidelines

OSPF packets are directly encapsulated based on IP for transmission. There is a probability of packet loss. Therefore, packet retransmission is required. The default retransmission interval is 5s. You can adjust the retransmission interval according to the network conditions.

The retransmission interval is a variable and does not need synchronization. You can configure different retransmission intervals for both parties in a neighbor relation.

Example

Set the retransmission interval on an OSPF interface to 2s.

```
Switch(config-vlanif-3)#ip ospf retransmit-interval 2
Switch(config-vlanif-3)#
```

5.4.36 ip ospf transmit-delay

Function

The **ip ospf transmit-delay** command configures the transmission delay on an OSPF interface.

Format

ip ospf transmit-delay { *transmit-delay-time* | **default** }

Parameter

Parameter	Description	Value
transmit-delay-time	Specifies the transmission delay on an interface.	The value is an integer ranging from 0 to 500, in seconds.
default	Specifies the default value.	1

Default Value

The default value is 1.

View

VLANIF configuration view, loopback interface configuration view, Ethernet routing interface configuration view, BD interface configuration view

Usage Guidelines

OSPF assumes that a delay is generated during message transmission. The default delay is 1s. Delay is set to better control the LSA update. For example, when an LSA with Age set to 0 is transmitted

over an interface, Age should be set to the delay of the interface. However, considering the aging time of the LSA is 3600s, which is much larger than the actual transmission delay of the interface, the transmission delay is not important.

The retransmission delay is a variable and does not need synchronization. You can configure different retransmission delay values for both parties in a neighbor relation.

Example

Set the transmission delay on an OSPF interface to 2s.

```
Switch(config-vlanif-3)#ip ospf transmit-delay 2
Switch(config-vlanif-3)#
```

5.4.37 loop-prevent {enable|disable}

Function

The **loop-prevent {enable|disable}** command enables or disables DN bit check to avoid routing loops.

Format

loop-prevent { enable | disable }

Parameter

Parameter	Description	Value
enable	Enables DN bit check.	-
disable	Disables DN bit check.	-

Default Value

By default, loop-prevent is disabled.

View

OSPFv2 configuration view

Usage Guidelines

In OSPF multi-VPN instance, if the DN bit is set in Type 3, Type 5, or Type 7 LSAs and loop prevention is enabled, the OSPF routes in these LSAs are not calculated.

Example

Enable loop prevention.

```
Switch(config-ospf-1001)#loop-prevent enable
Switch(config-ospf-1001)#
```

5.4.38 maximum load-balancing

Function

The **maximum load-balancing** command sets the maximum number of ECMP routes for load balancing.

Format

maximum load-balancing { *load-balancing-number* | **default** }

Parameter

Parameter	Description	Value
load-balancing-number	Specifies the maximum number of ECMP routes for load balancing.	The value is an integer ranging from 1 to 16.
default	Specifies the default maximum number of ECMP routes for load balancing.	16

Default Value

16

View

OSPFv2 configuration view

Usage Guidelines

When the routing table contains multiple routes that have the same destination address and reference bandwidth and are detected by the same routing protocol, then load balancing can be performed by these routes. You can **run maximum load-balancing** to set the maximum number of ECMP routes for load balancing to optimize the routing policy and meet the requirements of a complex network environment.

Example

Set the maximum number of ECMP routes for load balancing.

```
Switch(config-ospf-1)#maximum load-balancing 2
Switch(config-ospf-1)#
```

5.4.39 network area

Function

The **network area** command configures the OSPF area.

The **no network area** command deletes the OSPF area.

Format

- **network** *network-address network-mask* **area** *area-id*
- **no network** *network-address network-mask* **area** *area-id*

Parameter

Parameter	Description	Value
area-id	Specifies an area ID.	The value is a dotted decimal number or an integer. Generally, for an area with ID smaller than 65535, the value is an integer. For an area with ID larger than 65535, the value is an IP address. The value ranges from 0 to 4294967295.
network-address	Specifies the network address to be joined.	The value is in dotted decimal notation.
network-mask	Specifies the subnet mask of a network address.	The value is in dotted decimal notation.

Default Value

NA

View

OSPFv2 configuration view

Usage Guidelines

One OSPF interface can belong to only one area, but the area can contain multiple interfaces. Before you run this command, if the specified area does not exist, the command automatically creates an area. If the specified interface does not exist, the configuration is still reserved. When the interface appears, an OSPF interface is automatically created.

Example

Configure network segment 2.2.2.0/24 for area 2.

```
Switch(config-ospf-1)#network 2.2.2.0 255.255.255.0 area 2
Switch(config-ospf-1)#
```

5.4.40 peer priority

Function

The **peer priority** command configures the IPv4 address and priority of an adjacent switch on the NBMA network.

The **no peer** command deletes the IPv4 address of an adjacent switch on the NBMA network.

Format

- **peer** *ipv4-address* **priority** *priority*
- **no peer** *ipv4-address*

Parameter

Parameter	Description	Value
ipv4-address	Specifies the IPv4 address of an adjacent switch.	The value is in dotted decimal notation.
priority	Specifies the priority of a network neighbor.	The value is an integer ranging from 0 to 255.

Default Value

NA

View

OSPFv2 configuration view

Usage Guidelines

If you use this command to set the priority of a peer router, the peer switch must have the same priority as the local switch.

Example

Set the IPv4 address of an adjacent switch on the OSPF network to 10.18.13.1 and priority to 1.

```
Switch(config-ospf-1)#peer 10.18.13.1 priority 1
Switch(config-ospf-1)#
```

5.4.41 redistribute

Function

The **redistribute** command enables redistributing the BGP routes, direct routes, and static routes.

The **no redistribute** command disables redistributing the BGP routes, direct routes, and static routes.

Format

- **redistribute** { **connect** | **static** | **bgp** }

- **no redistribute { connect | static | bgp }**

Parameter

Parameter	Description	Value
static	Redistributes static routes to the OSPF protocol.	-
connect	Redistributes direct routes to the OSPF protocol.	-
bgp	Redistributes BGP routes to the OSPF protocol.	-

Default Value

By default, no route is redistributed.

View

OSPFv2 configuration view

Usage Guidelines

NA

Example

Configure static route redistribution.

```
Switch(config-ospf-1)#redistribute static
Switch(config-ospf-1)#
```

5.4.42 redistribute {rip|isis|ospf}

Function

The **redistribute {rip|isis|ospf}** command enables redistributing RIP, ISIS, and OSPF instance routes.

The **no redistribute {rip|isis|ospf}** command disables redistributing RIP, ISIS, and OSPF instance routes.

Format

- **redistribute { rip | isis | ospf } process-id**
- **no redistribute { rip | isis | ospf } process-id**
- **no redistribute { rip | isis | ospf } process-id dst-address dst-mask**

Parameter

Parameter	Description	Value
process-id	Specifies an IPv4 OSPF process ID.	The value is an integer ranging from 1 to 256.
dst-address	Specifies a destination network address.	The value is in dotted decimal notation.
dst-mask	Specifies a network mask address.	The value is in dotted decimal notation.

Default Value

Redistribution of OSPF instance routes is disabled.

View

OSPFv2 configuration view

Usage Guidelines

NA

Example

Enable redistributing OSPF instance routes.

```
Switch(config-ospf-1)#redistribute ospf 10
Switch(config-ospf-1)#
```

5.4.43 redistribute range

Function

The **redistribute range** command aggregates re-distributed routes that match the specified network segment.

The **no redistribute range** command deletes an aggregate redistributed route entry.

Format

- **redistribute** { **connect** | **static** | **rip** | **bgp** | **isis** | **ospf** } **range** *dst-address dst-mask*
- **no redistribute** { **connect** | **static** | **rip** | **bgp** | **isis** | **ospf** } **range** *dst-address dst-mask*
- **redistribute** { **connect** | **static** | **rip** | **bgp** | **isis** | **ospf** } **range** *dst-address dst-mask* **not-advertise**
- **redistribute** { **connect** | **static** | **rip** | **bgp** | **isis** | **ospf** } **range** *dst-address dst-mask* **no-translate**

- **redistribute { connect | static | rip | bgp | isis | ospf } range dst-address dst-mask type cost-type not-advertise**
- **redistribute { connect | static | rip | bgp | isis | ospf } range dst-address dst-mask type cost-type no-translate**
- **redistribute { connect | static | rip | bgp | isis | ospf } range dst-address dst-mask type cost-type**

Parameter

Parameter	Description	Value
static	Configures a policy for importing static routes.	-
connect	Configures a policy for importing direct routes.	-
rip	Configures a policy for importing RIP routes.	-
bgp	Configures a policy for importing BGP routes.	-
isis	Configures a policy for importing ISIS routes.	-
ospf	Configures a policy for importing OSPF routes.	-
dst-address	Specifies a destination network address.	The value is in dotted decimal notation.
dst-mask	Specifies a network mask address.	The value is in dotted decimal notation.
cost-type	Specifies an external cost type.	The value is an integer ranging from 1 to 2.

Default Value

By default, the OSPF area has no aggregation entry.

View

OSPFv2 configuration view

Usage Guidelines

NA

Example

Configure re-allocated aggregation route entry 10.0.0.0 255.255.0.0.

```
Switch(config-ospf-1)#redistribute connect range 10.0.0.0 255.255.0.0
Switch(config-ospf-1)#
```

5.4.44 redistribute route-policy

Function

The **redistribute route-policy** command configures a route import policy.

The **no redistribute route-policy** command deletes a route import policy.

Format

- **redistribute** { **connect** | **static** | **rip** | **bgp** | **isis** | **ospf** } **route-policy** *policy-name*
- **no redistribute** { **connect** | **static** | **rip** | **bgp** | **isis** | **ospf** } **route-policy** *policy-name*

Parameter

Parameter	Description	Value
static	Configures a policy for importing static routes.	-
connect	Configures a policy for importing direct routes.	-
rip	Configures a policy for importing RIP routes.	-
bgp	Configures a policy for importing BGP routes.	-
isis	Configures a policy for importing ISIS routes.	-
ospf	Configures a policy for importing OSPF routes.	-
policy-name	Specifies the name of a routing policy.	The value is a string consisting of up to 20 bytes.

Default Value

By default, the value is a null character string, indicating not referring to any routing policy.

View

OSPFv2 configuration view

Usage Guidelines

NA

Example

Configure routing policy 2 for importing static routes.

```
Switch(config-ospf-1)#redistribute static route-policy 2
Switch(config-ospf-1)#
```

5.4.45 redistribute metric

Function

The **redistribute metric** command configures OSPF to redistribute imported direct, static, and BGP routes and sets the cost of the routes.

The **no redistribute metric** command cancels route redistribution.

Format

- **redistribute** { **connect** | **static** | **rip** | **bgp** | **isis** | **ospf** } *dst-address dst-mask* **metric** *router-cost* **type** *cost-type*
- **redistribute** { **connect** | **static** | **rip** | **bgp** | **isis** | **ospf** } **metric** *router-cost* **type** *cost-type*
- **no redistribute** { **connect** | **static** | **rip** | **bgp** | **isis** | **ospf** } *dst-address dst-mask*
- **redistribute** { **rip** | **isis** | **ospf** } *process-id* *dst-address dst-mask* **metric** *router-cost* **type** *cost-type*
- **redistribute** { **rip** | **isis** | **ospf** } *process-id* **metric** *router-cost* **type** *cost-type*
- **redistribute** { **connect** | **static** | **rip** | **bgp** | **isis** | **ospf** } **range** *dst-address dst-mask* **metric** *router-cost* **not-advertise**
- **redistribute** { **connect** | **static** | **rip** | **bgp** | **isis** | **ospf** } **range** *dst-address dst-mask* **metric** *router-cost* **no-translate**
- **redistribute** { **connect** | **static** | **rip** | **bgp** | **isis** | **ospf** } **range** *dst-address dst-mask* **metric** *router-cost* **type** *cost-type* **not-advertise** **no-translate**
- **redistribute** { **connect** | **static** | **rip** | **bgp** | **isis** | **ospf** } **range** *dst-address dst-mask* **metric** *router-cost* **type** *cost-type* **not-advertise**
- **redistribute** { **connect** | **static** | **rip** | **bgp** | **isis** | **ospf** } **range** *dst-address dst-mask* **metric** *router-cost* **type** *cost-type* **no-translate** **not-advertise**
- **redistribute** { **connect** | **static** | **rip** | **bgp** | **isis** | **ospf** } **range** *dst-address dst-mask* **metric** *router-cost* **type** *cost-type* **no-translate**
- **redistribute** { **connect** | **static** | **rip** | **bgp** | **isis** | **ospf** } **range** *dst-address dst-mask* **metric** *router-cost* **type** *cost-type*
- **redistribute** { **connect** | **static** | **rip** | **bgp** | **isis** | **ospf** } **range** *dst-address dst-mask* **metric** *router-cost*

Parameter

Parameter	Description	Value
dst-address	Specifies a destination network address.	The value is in dotted decimal notation.
dst-mask	Specifies a network mask address.	The value is in dotted decimal notation.
router-cost	Specifies a route cost.	The value is an integer ranging from 1 to 65535.
cost-type	Specifies an external cost type.	The value is an integer ranging from 1 to 2.
process-id	Specifies an IPv4 OSPF process ID.	The value is an integer ranging from 1 to 256.

Default Value

By default, OSPF route redistribution is not configured.

View

OSPFv2 configuration view

Usage Guidelines

After you run this command, OSPF can advertise the imported static and direct routes to the adjacent routers.

By default, all external routes of the same protocol have the same attribute. You can specify the cost of a specific route.

Example

Set the OSPF to redistribute the direct route destined for **1.2.3.1** with subnet mask **255.255.255.0**, and set the route cost to **10** and cost type to **1**.

```
Switch(config-ospf-1)#redistribute connect 1.2.3.1 255.255.255.0 metric 10 type 1
Switch(config-ospf-1)#
```

5.4.46 redistribute not-advertise|advertise**Function**

The **redistribute not-advertise|advertise** command rejects a specific external route.

Format

- **redistribute { connect | static | bgp } dst-address dst-mask { not-advertise | advertise }**
- **redistribute { rip | isis | ospf } process-id dst-address dst-mask { not-advertise | advertise }**

Parameter

Parameter	Description	Value
dst-address	Specifies a destination IP address.	The value is in dotted decimal notation.
dst-mask	Specifies a network mask address.	The value is in dotted decimal notation.
process-id	Specifies an IPv4 OSPF process ID.	The value is an integer ranging from 1 to 256.

Default Value

By default, OSPF route redistribution is not configured.

View

OSPFv2 configuration view

Usage Guidelines

You can use this command to filter out certain external routes during route import.

Example

Set OSPF to reject a specified static route destined for **10.2.3.1** with subnet mask **255.255.255.0**.

```
Switch(config-ospf-1)#redistribute static 10.2.3.1 255.255.255.0 not-advertise
Switch(config-ospf-1)#
```

5.4.47 redistribute translate|no-translate

Function

The **redistribute translate|no-translate** command determines whether to set the translate bit when the switch generates NSSA LSAs for route redistribution.

Format

- **redistribute { connect | static | bgp } *dst-address dst-mask* { translate | no-translate }**
- **redistribute { connect | static | bgp } { translate | no-translate }**
- **redistribute { rip | isis | ospf } *process-id dst-address dst-mask* { translate | no-translate }**

Parameter

Parameter	Description	Value
dst-address	Specifies a destination network address.	The value is in dotted decimal notation.
dst-mask	Specifies a network mask address.	The value is in dotted decimal notation.
process-id	Specifies an IPv4 OSPF process ID.	The value is an integer ranging from 1 to 256.

Default Value

By default, OSPF route redistribution is not configured.

View

OSPFv2 configuration view

Usage Guidelines

NA

Example

Configure OSPF to set the translation bit when generating an NSSA LSA to redistribute the direct route destined for **10.13.3.1** with mask **255.255.255.0**.

```
Switch(config-ospf-1)#redistribute connect 10.1.3.1 255.255.255.0 no-translate
Switch(config-ospf-1)#
```

5.4.48 router-id

Function

The **router-id** command configures a router ID for the switch.

Format

router-id *ip-address*

no router-id

Parameter

Parameter	Description	Value
ip-address	Specifies the router ID of the switch.	The value is in dotted decimal notation.

Default Value

By default, no router ID is configured for the system, and the switch selects an interface IP address as its router ID.

View

OSPFv2 configuration view, BGP-VPN IPv4 address family configuration view, and BGP-VPN IPv6 address family configuration view

Usage Guidelines

The router ID selection rules are as follows:

- 1) Minimum static loopback address
- 2) Minimum static primary address
- 3) Minimum static secondary address
- 4) Minimum static link local address
- 5) Minimum address allocated by the DHCP
- 6) Error return

Example

Set the router ID to 1.1.1.1.

```
Switch(config-vlanif-3)#ip address 1.1.1.1/24
Switch(config-vlanif-3)#quit
Switch(config)#router ospf
Switch(config-ospf-1)#router-id 1.1.1.1
Switch(config-ospf-1)#
```

5.4.49 router ospf

Function

The **router ospf** command enables IPv4 OSPF and enters the OSPF configuration view. The switch supports multiple IPv4 OSPF instances and VPN instances.

The **no router ospf** command disables IPv4 OSPF.

Format

- **router ospf**
- **router ospf** *process-id*
- **router ospf vpn-instance** *name*
- **router ospf** *process-id* **vpn-instance** *name*
- **no router ospf** [*process-id*]
- **no router ospf**
- **no router ospf all**

Parameter

Parameter	Description	Value
name	Specifies a VPN instance name.	The value is a string of up to 64 characters.
process-id	Specifies an IPv4 OSPF process ID.	The value is an integer ranging from 1 to 256. If you do not enter a process ID, the default process ID 1 is used.

Default Value

By default, IPv4 OSPF is disabled.

View

Global configuration view

Usage Guidelines

NA

Example

Enable OSPF on the switch.

```
Switch(config-vlanif-3)#ip address 1.1.1.1/24
Switch(config-vlanif-3)#quit
Switch(config)#router ospf
Switch(config-ospf-1)#
```

5.4.50 reset ospf**Function**The **reset ospf** command restarts the OSPF process.**Format**

- **reset ospf**
- **reset ospf** *process-id*

Parameter

Parameter	Description	Value
process-id	Specifies an OSPF process ID.	The value is an integer ranging from 1 to 256.

Default Value

NA

View

Privileged user view, OSPFv2 configuration view, global configuration view

Usage Guidelines

NA

Example

Restart OSPF process 1.

```
Switch(config-ospf-1)#reset ospf 1
Switch(config-ospf-1)#
```

5.4.51 reset ospf counters**Function**

The **reset ospf counters** command sets the OSPF counters.

Format

- **reset ospf counters**
- **reset ospf *process-id* counters**

Parameter

Parameter	Description	Value
process-id	Specifies an OSPF process ID.	The value is an integer ranging from 1 to 256.

Default Value

NA

View

Privileged user view, OSPFv2 configuration view, global configuration view

Usage Guidelines

NA

Example

Zero the OSPF counter.

```
Switch#reset ospf counters
Switch#
```

5.4.52 rfc1583 compatible

Function

The **rfc1583 compatible** command enables or disables preferential route selection rules compatible with RFC1583.

Format

rfc1583 compatible { enable | disable }

Parameter

Parameter	Description	Value
enable	Enable the RFC1583 compatible function.	-
disable	Disable the RFC1583 compatible function.	-

Default Value

By default, the preferential route selection rules compatible with RFC1583 are disabled.

View

OSPFv2 configuration view

Usage Guidelines

NA

Example

Enable preferential route selection rules compatible with RFC1583.

```
Switch(config-ospf-1)#rfc1583 compatible enable
Switch(config-ospf-1)#
```

5.4.53 route-tag

Function

The **route-tag** command configures a tag for imported VPN routes.

Format

route-tag { *tag* | **default** }

Parameter

Parameter	Description	Value
tag	Specifies a tag for imported VPN routes.	The value is an integer ranging from 1 to 65535.
default	Disables loop detection using a tag.	-

Default Value

NA

View

OSPFv2 configuration view

Usage Guidelines

NA

Example

Set the route tag of OSPF process 1001 to 1000.

```
Switch(config-ospf-1001)#route-tag 1000
Switch(config-ospf-1001)#
```

5.4.54 show ip ospf area

Function

The **show ip ospf area** command displays all areas directly connected to the switch.

Format

- **show ip ospf area** [*area-id*]
- **show ip ospf area**
- **show ip ospf area process** *process-id*

Parameter

Parameter	Description	Value
area-id	Specifies an area ID.	The value is a dotted decimal number or an integer. Generally, for an area with ID smaller than 65535, the value is an integer. For an area with ID larger than 65535, the value is an IP address. The value ranges from 0 to 4294967295.
process-id	Specifies a process ID.	The value is an integer ranging from 1 to 256.

Default Value

NA

View

Common user view

Usage Guidelines

You can use this command to learn whether the OSPF area is correctly set and perform OSPF fault locating.

Example

View all areas directly connected to the switch.

```
Switch>show ip ospf area
OSPF Process 16
```

AreaId	Type	Summary	RouteUpdates	ABR	ASBR	LSACount
0	normal	summary	6430	0	0	5

```
Switch>
```

5.4.55 show ip ospf bfd session

Function

The **show ip ospf bfd session** command displays information on the neighbor for which the BFD feature is enabled.

Format

show ip ospf bfd session

Parameter

NA

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

View information on the neighbor for which the BFD feature is enabled.

```
Switch>show ip ospf bfd session
OSPF Process 16
Neighbor      :10.1.2.1      NeighborId    :1.1.1.1
Interface     :vlan200      BFDState      :up
Min TX        :1000        Min RX        :1000
Multiplier    :3           BFD Local Dis :1
LocalIpAdd    :0.0.0.0      RemoteIpAdd   :1.2.1.10
Diagnostic Info:noDiagnostic
Switch>
```

5.4.56 show ip ospf brief

Function

The **show ip ospf brief** command displays global OSPF parameter information.

Format

- **show ip ospf brief**
- **show ip ospf brief process** *process-id*

Parameter

Parameter	Description	Value
process-id	Specifies a process ID.	The value is an integer ranging from 1 to 256.

Default Value

NA

View

Common user view

Usage Guidelines

You can use this command to learn whether the OSPF area is correctly set and perform OSPF fault locating.

Example

View all areas directly connected to the switch.

```
Switch>show ip ospf brief
Version                               :OSPFV2_VB3.00.07.03
OSPF Process 16
-----
OSPF General Parameters
Admin Status                          :enable
Vpn Name                             :
Valid Ttl                             :0
Router ID                             :2.2.2.2
Version                               :2
Area Border Router                    :false
AS Border Router                      :false
External LSA Count                     :32000
External LSA Checksum Sum              :0x3ebd77a9
TOS Support                           :false
New LSA Received                       :32005
External LSDB Limit                   :-1 No Limited
Exit Overflow Interval                 :0(s)
Opaque Enable                          :no
Redistribute Static Enable             :no
Redistribute Rip Enable                :no
Redistribute Local Enable              :no
Redistribute Bgp Enable                :no
Redistribute Isis Enable               :no
Originate New LSA                      :3446
Multicast Extensions                   :no multicast forwarding is enabled
```

```

Demand Extensions           :false
Reference Bandwidth         :100(Mbits/s)
Spf Running Interval       :2(s)
Rfc1583 Compatible         :no
Default Route Advertise    :disable
Default Route Advertise Cost :1
Default Route Advertise Type :2
Fast Reroute               :disable
Loop Prevent               :disable
Restart Strict LSA Check   :no
Stub Router Support        :yes
Stub Router Advertisement  :doNotAdvertise
Discontinuity Time        :2
Preference                 :10
Preference RoutePolicy     :
Ase Preference             :150
Ase Preference RoutePolicy :
Switch>

```

5.4.57 show ip ospf config

Function

The **show ip ospf config** command displays general OSPF running information.

Format

show ip ospf config

Parameter

NA

Default Value

NA

View

Common user view

Usage Guidelines

You can use this command to view overall OSPF information, and therefore helping you monitor the protocol running in a macro manner.

Example

Display general OSPF running information.

```
Switch>show ip ospf config
Version:OSPFV2_VB3.00.07.03
!
router ospf 16
router-id 2.2.2.2
network 2.2.2.2 255.255.255.255 area 0
network 10.1.2.0 255.255.255.0 area 0
network 10.1.3.0 255.255.255.0 area 0
network 101.1.1.0 255.255.255.0 area 0
network 101.1.2.0 255.255.255.0 area 0
network 101.1.3.0 255.255.255.0 area 0
network 101.1.4.0 255.255.255.0 area 0
interface vlan 200
ip ospf hello-interval 1
ip ospf dead-interval 4
ip ospf bfd enable
Switch>
```

5.4.58 show ip ospf database

Function

The **show ip ospf database** command displays OSPF database information.

Format

- **show ip ospf database**
- **show ip ospf database area** *area-id*
- **show ip ospf database area** *area-id* **process** *process-id*
- **show ip ospf database { as-external-lsa | type9 | type11 }** *Ls-id* *adver-router-id*
- **show ip ospf database { as-external-lsa | type9 | type11 }** *Ls-id* *adver-router-id* *process-id*
- **show ip ospf database { router | network | summary-network | summary-asbr | as-external-lsa | nssa-lsa | type9 | type10 | type11 }**
- **show ip ospf database { router | network | summary-network | summary-asbr | as-external-lsa | nssa-lsa | type9 | type10 | type11 }** **process** *process-id*
- **show ip ospf database { router | network | summary-network | summary-asbr | nssa-lsa | type10 }** *LS-id* *adver-router-id* *area-id*

- **show ip ospf database { router | network | summary-network | summary-asbr | nssa-lsa | type10 }** *LS-id adver-router-id area-id process-id*
- **show ip ospf database age** *min-age max-age*
- **show ip ospf database age** *min-age max-age count*
- **show ip ospf database count**
- **show ip ospf database count process** *process-id*
- **show ip ospf database expire**
- **show ip ospf database expire count**
- **show ip ospf database expire process** *process-id*
- **show ip ospf database process** *process-id*
- **show ip ospf database total count**

Parameter

Parameter	Description	Value
area-id	Specifies an area ID.	The value is a dotted decimal number or an integer. Generally, for an area with ID smaller than 65535, the value is an integer. For an area with ID larger than 65535, the value is an IP address. The value ranges from 0 to 4294967295.
LS-id	Specifies an LS ID.	The value is in dotted decimal notation.
adverrouter-id	Specifies an advertising route ID.	The value is in dotted decimal notation.
as-external-lsa type9 type11 type10 router network summary-network summary-asbr nssa-lsa	Specifies an LSA type.	-
process-id	Specifies a process ID.	The value is an integer ranging from 1 to 256.
min-age	Specifies the minimum database aging time.	The value is an integer ranging from 1 to 3600.
max-age	Specifies the maximum database aging time.	The value is an integer ranging from 1 to 3600.

Default Value

NA

View

Common user view

Usage Guidelines

You can use this command to view information about the OSPF link state database, helping you implement fault diagnosis.

Example

Display the OSPF database information.

```
Switch>show ip ospf database network
```

Database of OSPF Process 16

Network LSA (area 0)

LinkId	ADV Router	Age	Seq#	CheckSum	Len
10.1.2.2	2.2.2.2	319	0x80000001	0x334	32

```
Switch>
```

5.4.59 show ip ospf graceful-restart**Function**

The **show ip ospf graceful-restart** command displays information about OSPF graceful restart of the switch.

Format

show ip ospf graceful-restart

Parameter

NA

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

Display information about OSPF graceful restart of the switch.

```
Switch>show ip ospf graceful-restart
OSPF Process 16
-----
Restart Capability           :Not Support
Restart Helper Capability    :Not Support
Restart State                :Not in Restarting
Restart Period               :120 seconds
Restart Exit Reason          :none
Restart Age                  :0
Switch>
```

5.4.60 show ip ospf import-route

Function

The **show ip ospf import-route** command displays the routes imported by the OSPF protocol.

Format

- **show ip ospf import-route**

Parameter

NA

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

View the routes imported by the OSPF protocol.

```
Switch>show ip ospf import-route
Switch>
```

5.4.61 show ip ospf interface

Function

The **show ip ospf interface** command displays information about OSPF interface table of the switch.

Format

- **show ip ospf interface** [*ip-address*]
- **show ip ospf interface count**
- **show ip ospf interface process** *process-id*
- **show ip ospf interface**

Parameter

Parameter	Description	Value
[<i>ip-address</i>]	Specifies the IP address of an interface. It is optional.	The value is in dotted decimal notation.
process	Specifies a process ID.	The value is an integer ranging from 1 to 256.

Default Value

NA

View

Common user view

Usage Guidelines

You can use this command to check the OSPF running status on an interface, whether OSPF configuration is correct, and whether OSPF faults occur.

Example

Display information about the OSPF interface table of the switch.

```
Switch>show ip ospf interface
OSPF Process 16
  Interface      IpAddr      AreaId      State          Cost
  loopback 1    2.2.2.2     0           designatedRouter 1
  vlan 200      10.1.2.2    0           designatedRouter 1
Switch>
```

5.4.62 show ip ospf log

Function

The **show ip ospf log** command displays the switch OSPF logs.

Format

show ip ospf log

Parameter

NA

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

View the switch OSPF logs.

```
Switch>show ip ospf log
Switch>
```

5.4.63 show ip ospf neighbor**Function**

The **show ip ospf neighbor** command displays information about the adjacent station table of the switch.

Format

- **show ip ospf neighbor** [*ip-address*]
- **show ip ospf neighbor process** *process-id*
- **show ip ospf neighbor state count**
- **show ip ospf neighbor state statistic**
- **show ip ospf neighbor state statistic process** *process-id*

Parameter

Parameter	Description	Value
ip-address	Specifies the IP address of a neighbor. It is optional.	The value is in dotted decimal notation.

Parameter	Description	Value
process-id	Specifies a process ID.	The value is an integer ranging from 1 to 256.

Default Value

NA

View

Common user view

Usage Guidelines

You can use this command to learn the OSPF neighbor situations, helping you determine whether the OSPF neighbor is correct and whether OSPF fault identification is performed.

Example

Display information about the adjacent station table of the switch.

```
Switch>show ip ospf neighbor
OSPF Process 16
IpAddress      NeighborID      Priority  State      Aging    UpTime      Interface
10.1.2.1       1.1.1.1         1        full       3        0:20:46     vlan 200
Switch>
```

5.4.64 show ip ospf route**Function**

The **show ip ospf route** command displays the OSPF routing information.

Format

- **show ip ospf route**
- **show ip ospf route process** *process-id*
- **show ip ospf route vpn-instance** *name*

Parameter

Parameter	Description	Value
process	Specifies a process ID.	The value is an integer ranging from 1 to 256.
name	Specifies a VPN instance name.	The value is a string of no more than 64 characters.

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

View the OSPF routing information.

```
Switch>show ip ospf route
OSPF Process 16
  RoutType  Prefix                PathType  Cost    Cost2      NextHop
BackupNextHop  AreaId  Time
Network  1.1.1.1/32                INTRA     2        0        10.1.2.1      0.0.0.0
N/A      0:04:39
Network  2.2.2.2/32                INTRA     1        0        2.2.2.2      0.0.0.0
N/A      0:36:13
Network  10.1.2.0/24               INTRA     1        0        10.1.2.2      0.0.0.0
N/A      0:04:40
Switch>
```

5.4.65 show ip ospf route count**Function**

The **show ip ospf route count** command displays the number of OSPF routes.

Format

- **show ip ospf route count**
- **show ip ospf route count process** *process-id*
- **show ip ospf route total count**
- **show ip ospf route vpn-instance** *name* **count**

Parameter

Parameter	Description	Value
process-id	Specifies a process ID.	The value is an integer ranging from 1 to 256.
name	Specifies a VPN instance name.	The value is a string of no more than 64 characters.

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

View the OSPF routing information.

```
Switch>show ip ospf route count
OSPF Process 16
-----
Route :
ABR      ASBR      Network  Intra    Inter    External
0        0          3        3        0        0

Path :
ABR      ASBR      Network  Intra    Inter    External
0        0          3        3        0        0

Switch>
```

5.4.66 show ip ospf trap**Function**

The **show ip ospf trap** command displays information about the configured traps.

Format

show ip ospf trap

Parameter

NA

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

Display information about the configured traps.

```
Switch>show ip ospf trap
```

```
-----
OSPF Process 1
```

```
Trap Number : 20
-----
```

Trap Name	Status	Excessive Flag
ospfvirtifstatechange	off	N
ospfnbrstatechange	off	N
ospfvirtnbrstatechange	off	N
ospfifconfigerror	off	Y
ospfvirtifconfigerror	off	Y
ospfifauthfailure	off	N
ospfvirtifauthfailure	off	N
ospfifrxbadpacket	off	N
ospfvirtifrxbadpacket	off	N
ospftxretransmit	off	Y
ospfvirtiftxretransmit	off	Y
ospforiginatelsa	off	Y
ospfmaxagelsa	off	Y
ospflsdboverflow	off	N
ospflsdbapproachingoverflow	off	N
ospfifstatechange	off	N
ospfnssatranslatorstatuschange	off	N

```
Switch>
```

5.4.67 show ip ospf virtual interface**Function**

The **show ip ospf virtual interface** command displays interfaces of the configured virtual links.

Format

- **show ip ospf virtual interface**
- **show ip ospf virtual interface process** *process-id*
- **show ip ospf virtual interface** { *virtual-interface-area-id1* | *virtual-link-neighbor-router-id* }
- **show ip ospf virtual interface** { *virtual-interface-area-id2* | *virtual-link-neighbor-router-id* }

Parameter

Parameter	Description	Value
virtual-interface-area-id1	Specifies the area ID of the virtual interface.	The value is a decimal number ranging from 0 to 4294967295.
virtual-interface-area-id2	Specifies the area ID of the virtual interface.	The value is in dotted decimal notation.
virtual-link-neighbor-router-id	Specifies the ID of the virtual link neighbor router.	The value is in dotted decimal notation.
process-id	Specifies a process ID.	The value is an integer ranging from 1 to 256.

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

Display interfaces of the virtual link interfaces.

```
Switch>show ip ospf virtual interface
  OSPF Process 1
  OSPF Process 16
Switch>
```

5.4.68 show ip ospf virtual neighbor

Function

The **show ip ospf virtual neighbor** command displays information about virtual neighbors of the configured virtual links.

Format

- **show ip ospf virtual neighbor**
- **show ip ospf virtual neighbor process** *process-id*

Parameter

Parameter	Description	Value
process-id	Specifies a process ID.	The value is an integer ranging from 1 to 256.

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

Display information about virtual neighbors of the configured virtual links.

```
Switch>show ip ospf virtual neighbor
OSPF Process 1
-----
Neighbor Address           :0.0.0.0
Neighbor Id                :2.1.1.2
Neighbor State             :Full
Neighbor Event Count       :8
Neighbor Retransmit Queue Length :0
Neighbor Options           :0
Switch#
```

5.4.69 show ip ospf statistic bfd**Function**The **show ip ospf statistic bfd** command displays statistics about BFD state changes.**Format**

- **show ip ospf statistic bfd**
- **show ip ospf statistic bfd** *start-item*

Parameter

Parameter	Description	Value
start-item	Specifies the start index for statistics.	The value ranges from 1 to 3000.

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

Display statistics about BFD state changes.

```
Switch>show ip ospf statistic bfd
process time          nbr addr      state      diag
16      2008/04/13 01:05:11 10.1.2.1    Down      control detection time expired
16      2008/04/13 01:05:14 10.1.2.1    Down      neighbor signaled session down
16      2008/04/13 01:06:50 10.1.2.1    Down      control detection time expired
16      2008/04/13 06:28:38 10.1.2.1    Down      neighbor signaled session down
16      2008/04/13 06:28:38 10.1.2.1    Down      administratively down
16      2008/04/13 06:38:42 10.1.2.1    Down      neighbor signaled session down
16      2008/04/13 06:38:42 10.1.2.1    Down      administratively down
16      2008/04/13 06:48:47 10.1.2.1    Down      neighbor signaled session down
16      2008/04/13 06:48:47 10.1.2.1    Down      administratively down
16      2008/04/13 06:58:51 10.1.2.1    Down      neighbor signaled session down
16      2008/04/13 06:58:51 10.1.2.1    Down      administratively down
16      2008/04/13 07:08:56 10.1.2.1    Down      neighbor signaled session down
16      2008/04/13 07:08:56 10.1.2.1    Down      administratively down
Switch>
```

5.4.70 show ip ospf statistic global

Function

The **show ip ospf statistic global** command displays the global protocol statistics.

Format

show ip ospf statistic global

Parameter

NA

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

Display the global protocol statistics.

```

Switch>show ip ospf statistic global
  OSPF Global Statistic

  Working Mode:NOMAL
  RawSocket   :141  RouteSocket :142

  Memory Statistics
  Configuration Params
  Process    : 64
  Interface: 128
  Neighbor   : 64
  Area       : 64
  LSA        : 20480
  Route      : 49452

  OSPF System Statistics
  kernel Route Table Statistic
  System Route Add: Success: 0          Failed: 0
  System Route Del: Success: 0          Failed: 0
  Backup Route Add: Success: 0          Failed: 0
  Backup Route Del: Success: 0          Failed: 0          Not Need Del: 0
  System Error
  Current Errno: 0 Normal Errno: 0 Normal Error Count: 0
Switch>

```

5.4.71 show ip ospf statistic interface**Function**

The **show ip ospf statistic interface** command displays statistics about an OSPF interface.

Format

show ip ospf statistic interface *ip-address*

Parameter

Parameter	Description	Value
ip-address	Specifies an interface IP address.	The value is in dotted decimal notation.

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

View statistics about an OSPF interface.

```

Switch>show ip ospf statistic interface 1.1.1. 2
  OSPF Process 1
    Interface xge-4/0/1 Statistics information:
    -----
    IP address           :1.1.1.2
    Area ID              :1
    Ifnet Unit           :2
    Vrid                 :0
    Rcv pkt      Send pkt  Rcv bytes  Send bytes  Rcv Lsa  Send Lsa
    HELLO        0         0         0         0         0         0
    DD           0         0         0         0         0         0
    REQUEST      0         0         0         0         0         0
    UPDATE       0         0         0         0         0         0
    ACK          0         0         0         0         0         0
    rcv packet total count :0
    send packet total count :0
    Rxd Unicast           :0
    Rxd Multicast         :0
    Txd Unicast           :0
    Txd Multicast         :0
    Init DD Retransmit    :0
    DD Retransmit         :0
    Mcast Update          :0
    Ucast Update          :0
    - Request Retransmit  :0
    Packet from invalid source :0
    Packet from unkown neighbor :0
    Packet with error auth type :0(last 0)
    Packet with error auth info :0
    Bad network mask in Hello :0(last 0)

```

```

Bad hello interval in hello :0(last 0)
Bad dead interval in hello  :0(last 0)
Bad External bit in hello   :0
Bad NSSA bit in hello       :0
Neighbor negodone           :0
Neighbor exchange done      :0
Neighbor bad lsa request    :0
Neighbor loading done       :0
Neighbor sequence mismatch  :0
Neighbor shutdown or timeout:0
Interface up times          :0
Interface down times        :0
Interface neighbor changed  :0
Mismatch MTU in DD packet   :0(last 0)

```

Switch>

5.4.72 show ip ospf statistic lsa

Function

The **show ip ospf statistic lsa** command displays statistics about LSAs generated by the OSPF protocol.

Format

- **show ip ospf statistic lsa**
- **show ip ospf statistic lsa** *start-item*

Parameter

Parameter	Description	Value
start-item	Specifies the start index for statistics.	The value ranges from 1 to 3000.

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

View statistics about LSAs generated by the OSPF protocol.

```
Switch>show ip ospf statistic lsa
```

	process	time	t id	adv	seqnum	age	len	action
16	2008/04/13 17:26:24	1	2.2.2.2	2.2.2.2	80000587	0	3108	mod
16	2008/04/13 17:26:24	2	101.1.244.1	2.2.2.2	80000004	0	32	mod
16	2008/04/13 17:26:25	1	1.1.1.1	1.1.1.1	80000684	1	3108	mod
16	2008/04/13 17:26:25	1	2.2.2.2	2.2.2.2	80000588	0	3108	mod
16	2008/04/13 17:26:25	2	101.1.166.1	2.2.2.2	80000002	0	32	mod
16	2008/04/13 17:26:25	2	101.1.151.2	1.1.1.1	80000001	3600	32	mod
16	2008/04/13 17:26:26	1	2.2.2.2	2.2.2.2	80000589	0	3108	mod
16	2008/04/13 17:26:26	2	101.1.117.1	2.2.2.2	80000004	0	32	mod
16	2008/04/13 17:26:26	1	1.1.1.1	1.1.1.1	80000689	1	3108	mod
16	2008/04/13 17:26:26	1	2.2.2.2	2.2.2.2	8000058a	0	3108	mod

```
Switch>
```

5.4.73 show ip ospf statistic memory

Function

The **show ip ospf statistic memory** command displays statistics about the OSPF memory.

Format

show ip ospf statistic memory

Parameter

NA

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

Display statistics about the OSPF memory.

```
Switch>show ip ospf statistic memory
```

Detailed Memory Operation:

Index	Add	Fail	Free	Current	Size	Description
0	391950	0	391949	1	2800	Packet

1	1	0	0	1	1072	Area
2	51509	0	51254	255	344	SPF Node
3	257	0	0	257	1136	Interface
4	0	0	0	0	72	Redistribute Route
5	6950048	0	6949632	416	104	Retransmit Node
6	90631	0	90631	0	1600	DD summary packet
7	92640	0	92216	424	1600	LSA
8	393122	0	392863	259	152	Route Entry
9	3326	0	3074	252	736	Neighbor
10	0	0	0	0	80	Address Range
11	324781	0	324781	0	64	Request Node
12	257	0	0	257	72	Network Config
13	0	0	0	0	72	Redistribute Config
14	0	0	0	0	80	Redistribute Range
15	2	0	0	2	3648	Process
16	4143	0	3885	258	224	Nexthop
17	0	0	0	0	232	Route Policy
18	6	0	0	6	216	Lsa Table

Switch>

5.4.74 show ip ospf statistic neighbor

Function

The **show ip ospf statistic neighbor** command displays statistics about the OSPF neighbor state.

Format

- **show ip ospf statistic neighbor**
- **show ip ospf statistic neighbor** *start-item*

Parameter

Parameter	Description	Value
start-item	Specifies the start index for statistics.	The value ranges from 1 to 3000.

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

View statistics about the OSPF neighbor state.

```
Switch>show ip ospf statistic neighbor
```

process	time	nbr_addr	last_state	state	event
16	2008/04/13 17:33:22	101.1.28.2	Down	Init	hello-rcvd
16	2008/04/13 17:33:22	101.1.28.2	Init	ExStart	2-way
16	2008/04/13 17:33:22	101.1.28.2	ExStart	Exchange	neg-done
16	2008/04/13 17:33:22	101.1.28.2	Exchange	Loading	exchange-done
16	2008/04/13 17:33:23	101.1.128.2	Down	Init	hello-rcvd
16	2008/04/13 17:33:23	101.1.128.2	Init	ExStart	2-way
16	2008/04/13 17:33:23	101.1.128.2	ExStart	Exchange	neg-done
16	2008/04/13 17:33:23	101.1.128.2	Exchange	Loading	exchange-done
16	2008/04/13 17:33:23	101.1.28.2	Loading	Full	loading-done
16	2008/04/13 17:33:23	101.1.133.2	Down	Init	hello-rcvd
16	2008/04/13 17:33:23	101.1.133.2	Init	ExStart	2-way

```
Switch>
```

5.4.75 show ip ospf statistic route process**Function**

The **show ip ospf statistic route process** command displays statistics about the OSPF routes of a specified instance.

Format

show ip ospf statistic route process *process-id*

Parameter

Parameter	Description	Value
process-id	Specifies the ID of an OSPF instance.	The value is an integer ranging from 1 to 256.

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

View statistics about the OSPF routes of a specified instance.

```
Switch>show ip ospf statistic route process 1
OSPF Process 1

      SPF Table (area 1)
type    id          nexthop          cost    ifunit    parent          role
router  1.1.1.2      N/A              0        0         N/A             main

      Network Route Table
type    dest          nexthop          cost    ifunit    role
INTRA   1.1.1.0/24         1.1.1.2          1        2         main
Switch>
```

5.4.76 show ip ospf statistic route

Function

The **show ip ospf statistic route** command displays statistics about the OSPF routes.

Format

show ip ospf statistic route

Parameter

NA

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

View statistics about the OSPF routes.

```
Switch>show ip ospf statistic route

OSPF Process 1

OSPF Process 16

      SPF Table (area 0)
```

type	id	nexthop	cost	ifunit	parent	role
router	1.1.1.1	10.1.2.1	1	12488	10.1.2.2	main
router	1.1.1.1	101.1.1.2	1	13289	10.1.2.2	main
router	1.1.1.1	101.1.2.2	1	13290	10.1.2.2	main
router	1.1.1.1	101.1.3.2	1	13291	10.1.2.2	main
router	1.1.1.1	101.1.4.2	1	13292	10.1.2.2	main
router	1.1.1.1	101.1.5.2	1	13293	10.1.2.2	main
router	1.1.1.1	101.1.6.2	1	13294	10.1.2.2	main
router	1.1.1.1	101.1.7.2	1	13295	10.1.2.2	main
router	1.1.1.1	101.1.8.2	1	13296	10.1.2.2	main
router	1.1.1.1	101.1.9.2	1	13297	10.1.2.2	main
router	1.1.1.1	101.1.10.2	1	13298	10.1.2.2	main
router	1.1.1.1	101.1.11.2	1	13299	10.1.2.2	main
router	1.1.1.1	101.1.12.2	1	13300	10.1.2.2	main

Switch>

5.4.77 show ip ospf statistic spf

Function

The **show ip ospf statistic spf** command displays statistics about the SPF calculations by the OSPF protocol.

Format

- **show ip ospf statistic spf**
- **show ip ospf statistic spf start-item**

Parameter

Parameter	Description	Value
start-item	Specifies the start index for statistics.	The value ranges from 1 to 3000.

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

View statistics about the SPF calculations by the OSPF protocol.

```

Switch>show ip ospf statistic spf
OSPF SPF Related Log Statistics
2008/04/13 15:18:32(861ms)(ospf-16):spf calc,time 0,sched 0,abr/asbr/net=0/1/3
2008/04/13 15:18:40(946ms)(ospf-16):spf calc,time 0,sched 0,abr/asbr/net=0/1/3
2008/04/13 15:18:40(946ms)(ospf-16):spf calc,time 0,sched 0,abr/asbr/net=0/1/3
2008/04/13 15:18:40(47ms)(ospf-16):spf calc,time 0,sched 0,abr/asbr/net=0/1/3
2008/04/13 15:18:40(47ms)(ospf-16):spf calc,time 0,sched 0,abr/asbr/net=0/1/3
2008/04/13 15:18:44(443ms)(ospf-16):spf calc,time 0,sched 0,abr/asbr/net=0/2/5
2008/04/13 15:18:44(443ms)(ospf-16):sys route update,add 2,del 0
2008/04/13 15:19:21(812ms)(ospf-16):spf calc,time 0,sched 0,abr/asbr/net=0/1/5
2008/04/13 15:19:21(812ms)(ospf-16):sys route update,add 0,del 2
2008/04/13 15:19:21(278ms)(ospf-16):spf calc,time 0,sched 0,abr/asbr/net=0/1/3
2008/04/13 15:19:22(818ms)(ospf-16):spf calc,time 0,sched 0,abr/asbr/net=0/1/3
2008/04/13 15:19:31(583ms)(ospf-16):spf calc,time 0,sched 0,abr/asbr/net=0/1/3
2008/04/13 15:19:31(583ms)(ospf-16):spf calc,time 0,sched 0,abr/asbr/net=0/1/3
2008/04/13 15:19:31(726ms)(ospf-16):spf calc,time 0,sched 0,abr/asbr/net=0/1/3
2008/04/13 15:19:31(726ms)(ospf-16):spf calc,time 0,sched 0,abr/asbr/net=0/1/3
2008/04/13 15:19:32(345ms)(ospf-16):spf calc,time 0,sched 0,abr/asbr/net=0/2/5
2008/04/13 15:19:32(345ms)(ospf-16):sys route update,add 2,del 0
2008/04/13 15:20:11(875ms)(ospf-16):spf calc,time 0,sched 0,abr/asbr/net=0/1/5
2008/04/13 15:20:11(876ms)(ospf-16):sys route update,add 0,del 2
2008/04/13 15:20:11(449ms)(ospf-16):spf calc,time 0,sched 0,abr/asbr/net=0/1/3
2008/04/13 15:20:12(880ms)(ospf-16):spf calc,time 0,sched 0,abr/asbr/net=0/1/3
Switch>

```

5.4.78 snmp-trap

Function

The **snmp-trap** command enables or disables the traps for OSPF.

Format

- **snmp-trap { enable | disable }**
- **snmp-trap { enable | disable } trap-name { ospfifauthfailure | ospfifconfigerror | ospfifrxbadpacket | ospfifstatechange | ospflsdbapproachingoverflow | ospflsdboverflow | ospfmaxagelsa | ospfnbrrestarthelperstatuschange | ospfnbrstatechange | ospfnssatranslatorstatuschange | ospforiginatelsa | ospfrestartstatuschange | ospftxretransmit | ospfvirtifauthfailure | ospfvirtifconfigerror | ospfvirtifrxbadpacket | ospfvirtifstatechange | ospfvirtiftxretransmit | ospfvirtnbrrestarthelperstatuschange | ospfvirtnbrstatechange }**

Parameter

Parameter	Description	Value
enable	Enables the OSPF traps.	-
disable	Disables the OSPF traps.	-

Default Value

NA

View

OSPFv2 configuration view

Usage Guidelines

You can use this command to enable OSPF traps.

Example

Enable SNMP traps for OSPF.

```
Switch(config-ospf-1) #snmp-trap enable
Switch(config-ospf-1) #
```

5.4.79 spf-running-interval

Function

The **spf-running-interval** command configures the interval for route calculation.

Format

spf-running-interval { *interval* | **default** }

Parameter

Parameter	Description	Value
interval	Specifies the route calculation interval.	The value is an integer ranging from 1 to 60, in ms.
default	Specifies the default interval for route calculation.	2

Default Value

The default value is 2.

View

OSPFv2 configuration view

Usage Guidelines

The OSPF database synchronization and route calculation do not have a direct cause-effect relation. The device cannot learn whether the database synchronization is complete. It checks the synchronization based on the specified calculation interval. If it determines route calculation is required, it starts to calculate the route. A complete calculation process is time-consuming. If the network keeps updating the database, the route calculation persists. Therefore, you can set the interval for route calculation to a larger value to reduce the device burden.

The OSPF route does not need to be re-calculated at the end of each interval. It is calculated only when change occurs. Therefore, when the network is stable, the interval for route calculation does not affect OSPF performance.

Example

Set the route calculation interval to 30 ms.

```
Switch(config-ospf-1)#spf-running-interval 30
Switch(config-ospf-1)#
```

5.4.80 opaque

Function

The **opaque** command enables or disables the opaque function.

Format

opaque { enable | disable }

Parameter

Parameter	Description	Value
enable	Enables the opaque function.	-
disable	Disables the opaque function.	-

Default Value

By default, the opaque function is disabled.

View

OSPFv2 configuration view

Usage Guidelines

You can use this command to enable or disable the opaque function. If the opaque function is enabled, the protocol module can process link state notifications of types 9, 10, and 11. If the opaque function is disabled, the protocol module does not process link state notifications of these types.

Example

Enable the opaque function.

```
Switch(config-ospf-1)#opaque enable
Switch(config-ospf-1)#
```

5.4.81 ip ospf source sub-address**Function**

The **ip ospf source sub-address** command specifies a slave IP address as the source IP address.

The **no ip ospf source sub-address** command cancels using a slave IP address as the source IP address.

Format

- **ip ospf source sub-address** *ipv4-address*
- **no ip ospf source sub-address**

Parameter

Parameter	Description	Value
ipv4-address	Specifies a local slave IP address as the source IP address.	The value is in dotted decimal notation, such as A.B.C.D, where each of A to D is a decimal number ranging from 0 to 255.

Default Value

NA

View

VLANIF configuration view, Ethernet sub-interface configuration view, Trunk sub-interface configuration view, Loopback interface configuration view, BD interface configuration view, Ethernet routing interface configuration view, and GRP routing interface configuration view

Usage Guidelines

The slave IP address must be configured. Then, run the **show ip ospf interface** or **router lsa** command to view the current source IP address of the interface.

Example

Specify the slave IP address 11.1.1.3 as the source IP address.

```
Switch#configure
Switch(config)#interface vlan 11
```

```
Switch(config-vlanif-11)#ip ospf source sub-address 11.1.1.3
```

5.4.82 stub-router on-startup

Function

The **stub-router** command configures a stub router.

The **stub-router on-startup** command configures a stub router and sets the interval during which a device acts as a stub router when it is restarted or faulty.

The **no stub-router** command restores the router status and no device serves as a stub router.

Format

- **stub router**
- **stub router on-startup** [*on-startup-time* | **default**]
- **no stub router**

Parameter

Parameter	Description	Value
on-startup-time	Specifies the interval during which a device acts as a stub router when it is restarted or faulty. ● If on-startup-time is configured, the device works as a stub router only when it is restarted or faulty. The hold time of the stub router state is specified by the parameter interval. ● If on-startup-time is not configured or set to the default value, the default interval 500s is applied.	The value is an integer ranging from 5 to 65535, in seconds. The default value is 500s.

Default Value

By default, a device works as a stub router for 500s.

View

OSPFv2 configuration view

Usage Guidelines

If you run the **stub router** command directly, the device is always a stub router, that is, the Cost value of all routes from this device is set to 65535.

This command increases the link metric to 65535 in the LSA generated by the device to notify other OSPF devices of not using this stub router to forward data. However, since the metric is not infinite,

it is still possible to have a route to a stub router. In the Router LSA generated by a stub router, the metric values of all links are set very high.

Example

Configure a device as a stub router.

```
Switch(config)#router ospf 1
Switch(config-ospf-1)#stub-router on-startup 200
```

5.5 OSPFv3 Configuration Commands

5.5.1 area nssa

Function

The **area nssa** command sets an OSPF area as an NSSA area.

The **no area nssa** command restores an NSSA area as a common area.

Format

- **area** *area-id* **nssa**
- **no area** *area-id* **nssa**

Parameter

Parameter	Description	Value
area-id	Specifies an area ID.	The value is a dotted decimal number or an integer. Generally, for an area with ID smaller than 65535, the value is an integer. For an area with ID larger than 65535, the value is an IP address. The value ranges from 0 to 4294967295.

Default Value

By default, the NSSA area is disabled in OSPF areas.

View

OSPFv3 configuration view

Usage Guidelines

An NSSA area is similar to a stub area, except that the NSSA area can send external routes but does not accept external routes. The router in the NSSA area generates Type7 LSAs for external routes, which are used for route calculation within the area. The ABR converts Type7 LSAs into Type5

LSAs and sends them to other areas. The ABR also generates a default summary LSA for the NSSA area.

NSSA area configuration has the following limitations:

- The backbone area cannot be configured as an NSSA area.
- A stub area cannot be configured as an NSSA area.
- A virtual link transit area cannot be configured as an NSSA area.

Example

Set area 1 as an NSSA area.

```
Switch(config-ospfv3-1)#area 1 nssa
Switch(config-ospfv3-1)#
```

5.5.2 area nssa range

Function

The **area nssa range** command sets the aggregation route entry in the NSSA area.

The **no area nssa range** command deletes the aggregation route entry configured for the NSSA area.

Format

- **area** *area-id* **nssa range** *dst-address/dst-mask* { **advertise** | **not-advertise** }
- **no area** *area-id* **nssa range** *dst-address/dst-mask*

Parameter

Parameter	Description	Value
area-id	Specifies an area ID.	The value is a dotted decimal number or an integer. Generally, for an area with ID smaller than 65535, the value is an integer. For an area with ID larger than 65535, the value is an IP address. The value ranges from 0 to 4294967295.
dst-address	Specifies a destination Ipv6 address.	-
dst-mask	Specifies a destination mask.	-
advertise	Indicates that the switch receives aggregation entries.	-
no-advertise	Indicates that the switch rejects aggregation entries.	-

Default Value

NA

View

OSPFv3 route configuration view

Usage Guidelines

Before running this command, you must create an area.

Example

Delete an aggregation route entry.

```
Switch(config-ospfv3-1)#no area 0 nssa range 2000::1/64
Switch(config-ospfv3-1)#
```

5.5.3 area range

Function

The **area range** command sets the aggregation route entry in an area.

The **no area range** command deletes the aggregation route entry configured for an area.

Format

- **area** *area-id* **range** *dst-address/dst-mask* { **advertise** | **not-advertise** }
- **no area** *area-id* **range** *dst-address/dst-mask*

Parameter

Parameter	Description	Value
area-id	Specifies an area ID.	The value is a dotted decimal number or an integer. Generally, for an area with ID smaller than 65535, the value is an integer. For an area with ID larger than 65535, the value is an IP address. The value ranges from 0 to 4294967295.

Default Value

By default, the OSPF area has no aggregation entry.

View

OSPFv3 configuration view

Usage Guidelines

Before running this command, you must run `ipv6 ospf area` to create an area in the VLAN interface.

You can use this command to configure an aggregation route entry for an area. You can use the `no area range` command to delete an aggregation entry configured for an area.

When the ABR calculates the route for area A, it advertises the internal routes of area A to other areas, and generates a Summary LSA for each area. If the internal route scale is large, the number of Summary LSA entries is large. You can configure aggregation entry for area A to control the number of Summary LSAs.

After the aggregation entry is configured, routes matching the aggregation entry in area A will not be included in the Summary LSAs of other areas. According to different advertise attributes of the aggregation entries, the following situations may exist:

1. The advertise operation is specified for the aggregation entry, and the Summary LSA is generated for the aggregation entry.
2. The not-advertise operation is specified for the aggregation entry, and the Summary LSA is not generated for the aggregation entry.



Caution

This command can only be used for an existing area.

Example

Enable area 1 to include only Summary LSA of 2001::1/64.

```
Switch(config-ospfv3-1)#area 1 range 2001::1/64 advertise
Switch(config-ospfv3-1)#
```

Enable area 1 not to include any Summary LSA of 2001::1/64.

```
Switch(config-ospfv3-1)#area 1 range 2001::1/64 not-advertise
Switch (config-ospfv3-1)#
```

5.5.4 area virtual-link

Function

The **area virtual-link** command configures an OSPF virtual link.

The **no area virtual-link** command deletes an OSPF virtual link.

Format

- **area** *area-id* **virtual-link** *neighbor-address*

- **area** *area-id* **virtual-link** *neighbor-address* { **hello-interval** | **retransmit-interval** | **transmit-delay** | **dead-interval** } { *interval-time* | **default** }
- **no area** *area-id* **virtual-link** *neighbor-address*

Parameter

Parameter	Description	Value
area-id	Specifies the area ID of a transit area.	The value is a dotted decimal number or an integer. Generally, for an area with ID smaller than 65535, the value is an integer. For an area with ID larger than 65535, the value is an IP address. The value ranges from 0 to 4294967295.
neighbor-address	Specifies the router ID of a virtual neighbor.	The value is in dotted decimal notation.
hello-interval retransmit-interval transmit-delay dead-interval	Indicates the interval for calling a virtual neighbor, retransmission interval of the link state notification, transmission delay of the link state notification, and dead interval of a virtual neighbor, respectively.	-
interval-time	Specifies an interval.	The value is an integer ranging from 1 to 65535, in seconds.

Default Value

By default:

The default value of hello-interval is 10s.

The default value of retransmit-interval is 5s.

The default value of transmit-delay is 1s.

The default value of dead-interval is 60s.

View

OSPFv3 configuration view

Usage Guidelines

In OSPF, the backbone area summarizes topology information on areas to form inter-domain routes. Therefore, all inter-domain communication traffic passes through the backbone area, while non-backbone areas cannot directly exchange data packets. On an OSPF network, all non-backbone areas should be connected to the backbone area. Some routes cannot be calculated if non-backbone

areas are not connected to the backbone area or the backbone area itself is not continuous due to network lines or design. Therefore, virtual links can be configured to address such problem.

Virtual link configuration must comply with the following rules:

- The virtual link must be configured on the boundary switch between two areas.
- An area through which the virtual link passes is known as a transit area. The transit area must have all route selection information, so that the switch can identify a physical route destined for the backbone area to transmit virtual link information.
- The transit area cannot be a stub area.

Example

Set a virtual link for area 1.

```
Switch(config-ospfv3-1)#area 1 virtual-link 1.1.1.0
Switch(config-ospfv3-1)#
```

5.5.5 area stub

Function

The **area stub** command configures an OSPF area as a stub area.

The **no area stub** command restores a stub area as a common area.

Format

- **area** *area-id* **stub**
- **no area** *area-id* **stub**

Parameter

Parameter	Description	Value
area-id	Specifies an area ID.	The value is a dotted decimal number or an integer. Generally, for an area with ID smaller than 65535, the value is an integer. For an area with ID larger than 65535, the value is an IP address. The value ranges from 0 to 4294967295.

Default Value

By default, the OSPF area is not a stub area.

View

OSPFv3 configuration view

Usage Guidelines

You can use this command to configure an area as a stub area. The stub area does not include external routes (Type 5 LSA) and does not generate external routes. The stub area configuration has the following limitations:

- The backbone area cannot be configured as a stub area.
- If an area is a virtual link transit area, you cannot configure this area as a stub area. Otherwise, the area works abnormally.

After a stub area is configured, the ABR generates a default Summary LSA for the area. The generation process of other summary LSAs remains unchanged. If the no-summary attribute is configured, the ABR clears other non-default Summary LSAs and includes only one default Summary LSA.

A stub area can control the number of LSAs within an area. If an area has limited router memory and cannot receive a large amount of LSAs, you can configure this area as a stub area.

A stub area cannot be used as the virtual link transit area. All routers within a stub area must have the same stub attributes. Otherwise, a neighbor relation cannot be established.

Example

Restore a stub area as a common area.

```
Switch(config-ospfv3-1)# no area 1 stub
Switch(config-ospfv3-1)#
```

5.5.6 area stub no-summary

Function

The **area stub no-summary** command configures an area as a totally stub area.

Format

area *area-id* **stub no-summary**

Parameter

Parameter	Description	Value
area-id	Specifies an area ID.	The value is a dotted decimal number or an integer. Generally, for an area with ID smaller than 65535, the value is an integer. For an area with ID larger than 65535, the value is an IP address. The value ranges from 0 to 4294967295.

Default Value

NA

View

OSPFv3 configuration view

Usage Guidelines

Before running this command, you must create an area.

The ABR in an area can stop generating other summary LSAs for the stub area to further compress the LSA scale. At this time, the stub area is known as a totally stub area.

Example

Configure area 1.3.2.1 as a totally stub area.

```
Switch(config-ospfv3-1)#area 1.3.2.1 stub no-summary
Switch(config-ospfv3-1)#
```

5.5.7 area nssa no-summary

Function

The **area nssa no-summary** command configures an area as a totally NSSA area.

Format

area *area-id* **nssa no-summary**

Parameter

Parameter	Description	Value
area-id	Specifies an area ID.	The value is a dotted decimal number or an integer. Generally, for an area with ID smaller than 65535, the value is an integer. For an area with ID larger than 65535, the value is an IP address. The value ranges from 0 to 4294967295.

Default Value

NA

View

OSPFv3 configuration view

Usage Guidelines

Before running this command, you must create an area.

Example

Configure area 1 as a total NSSA area.

```
Switch(config-ospfv3-1)#area 1 nssa no-summary
Switch(config-ospfv3-1)#
```

5.5.8 area default-cost

Function

The **area default-cost** command configures the cost of an OSPF area.

Format

- **area *area-id1* default-cost { *cost* | **default** }**
- **area *area-id2* default-cost { *cost* | **default** }**

Parameter

Parameter	Description	Value
area-id1	Specifies an area ID.	The value is an integer. Generally, for an area with ID smaller than 65535, the value is an integer ranging from 0 to 4294967295.
area-id2	Specifies an area ID.	Generally, an area with ID larger than 65535 is entered in IP address format.
cost	Specifies a cost.	The value is an integer ranging from 1 to 65535.

Default Value

By default, the LSA cost generated by the OSPF stub area is 1.

View

OSPFv3 configuration view

Usage Guidelines

The ABR in the stub area generates default summary LSA for the area. By default, the LSA cost is 0. You can use this command to set the cost of the summary LSA (for example, you need to differentiate priorities of two ABRs). You can run the no command to restore the cost to default value 0.

Before running this command, you must create an area.

Example

Set the default cost of area 1 to 300.

```
Switch(config-ospfv3-1)#network 2.2.2.0 255.255.255.0 area 1
```

```
Switch(config-ospfv3-1)#area 1 default-cost 300
Switch(config-ospfv3-1)#
```

5.5.9 bandwidth-reference

Function

The **bandwidth-reference** command configures the reference bandwidth of an interface, used to dynamically calculate the interface cost.

Format

bandwidth-reference { *bandwidth* | **default** }

Parameter

Parameter	Description	Value
bandwidth	Specifies the reference bandwidth of an interface.	The value is an integer ranging from 1 to 2147483647.
default	Uses the default value.	By default, the reference link bandwidth is 100 Mbit/s.

Default Value

By default, the reference link bandwidth is 100 Mbit/s.

View

OSPFv3 configuration view

Usage Guidelines

NA

Example

Set the reference bandwidth of an interface to 1000 Mbit/s.

```
Switch(config-ospfv3-1)#bandwidth-reference 1000
Switch(config-ospfv3-1)#
```

5.5.10 debug ospf6

Function

The **debug ospf6** command enables OSPF debugging.

The **no debug ospf6** command disables OSPF debugging.

Format

- **debug ospf6 { global | all | lsa | hello | packet | neighbor | interface | ip-route | rtm | spf | syn | graceful-restart | nbrchange | frr | error }**
- **debug ospf6 { global | all | lsa | hello | packet | neighbor | interface | ip-route | rtm | spf | syn | graceful-restart | nbrchange | frr | error } process *process-id***
- **debug ospf6 { global | all | lsa | hello | packet | neighbor | interface | ip-route | rtm | spf | syn | graceful-restart | nbrchange | frr | error } process all**
- **no debug ospf6 { global | all | lsa | hello | packet | neighbor | interface | ip-route | rtm | spf | syn | graceful-restart | nbrchange | frr | error }**
- **no debug ospf6 { global | all | lsa | hello | packet | neighbor | interface | ip-route | rtm | spf | syn | graceful-restart | nbrchange | frr | error } process *process-id***
- **no debug ospf6 { global | all | lsa | hello | packet | neighbor | interface | ip-route | rtm | spf | syn | graceful-restart | nbrchange | frr | error } process all**

Parameter

Parameter	Description	Value
process-id	Specifies a process ID.	The value is an integer ranging from 1 to 64.

Default Value

By default, OSPF debugging is disabled.

View

Privileged user view

Usage Guidelines

You can use this command to debug and locate OSPF faults.

Example

Enable debugging all OSPF information.

```
Switch#debug ospf6 all
Switch#
```

5.5.11 graceful-restart (OSPFv3)

Function

The **graceful-restart** command enables the graceful restart function.

The **no graceful-restart** command disables the graceful restart function.

Format

- **graceful-restart**
- **graceful-restart period** *restart-time*
- **no graceful-restart**

Parameter

Parameter	Description	Value
restart-time	Specifies the restart period.	The value is an integer ranging from 40 to 1800, in seconds.

Default Value

NA

View

OSPFv3 route configuration view

Usage Guidelines

NA

Example

Enable the graceful restart function.

```
Switch(config-ospfv3-1)#graceful-restart
Switch(config-ospfv3-1)#
```

5.5.12 graceful-restart begin (OSPFv3)**Function**The **graceful-restart begin** command enables graceful OSPFv3 restart.**Format****graceful-restart begin****Parameter**

NA

Default Value

NA

View

OSPFv3 route configuration view

Usage Guidelines

NA

Example

Enable graceful OSPFv3 restart.

```
Switch(config-ospfv3-1)#graceful-restart begin
Switch(config-ospfv3-1)#
```

5.5.13 graceful-restart helper (OSPFv3)

Function

The **graceful-restart helper** command enables or disables the OSPFv3 graceful restart helper.

Format

- **graceful-restart helper**
- **no graceful-restart helper**

Parameter

NA

Default Value

NA

View

OSPFv3 route configuration view

Usage Guidelines

NA

Example

Enable the OSPFv3 graceful restart helper.

```
Switch(config-ospfv3-1)#graceful-restart helper
Switch(config-ospfv3-1)#
```

5.5.14 ipv6 ospf if-type

Function

The **ipv6 ospf if-type** command sets the OSPFv3 interface type.

Format

- **ipv6 ospf if-type { broadcast | p2p }**
- **ipv6 ospf if-type { broadcast | p2p } process *process-id***

Parameter

Parameter	Description	Value
broadcast	Specifies the interface type to broadcast, which is the default type.	-
p2p	Specifies the interface type to P2P.	-
process-id	Specifies the ID of an OSPFv3 process.	The value is an integer ranging from 1 to 64.

Default Value

Broadcast

View

VLANIF configuration view, loopback interface configuration view, Ethernet routing interface configuration view, BD interface configuration view

Usage Guidelines

NA

Example

Set the OSPFv3 interface type to P2P.

```
Switch(config-vlanif-3)#ipv6 ospf if-type p2p
Switch(config-vlanif-3)#
```

5.5.15 ipv6 ospf hello-interval

Function

The **ipv6 ospf hello-interval** command sets the interval for an IPv6 OSPF interface to send Hello packets.

The **ipv6 ospf hello-interval default** command restores the interval for an IPv6 OSPF interface to send Hello packets.

Format

- **ipv6 ospf hello-interval { *hello-interval* | default }**

- **ipv6 ospf hello-interval** { *hello-interval* | **default** } **process** *process-id*

Parameter

Parameter	Description	Value
hello-interval	Specifies the interval for sending Hello packets by an OSPF interface.	The value is an integer ranging from 1 to 65535.
process-id	Specifies a process ID.	The value is an integer ranging from 1 to 64. When no process ID is configured, the default process ID 1 is used.

Default Value

By default, the interval for sending Hello packets by an OSPF interface is 10s.

View

VLANIF configuration view, loopback interface configuration view, Ethernet routing interface configuration view, BD interface configuration view

Usage Guidelines

By default, the interval for sending Hello packets by an OSPF interface is 10s. You can modify the default value, but the interval configured for both parties must be the same. The interval must be smaller than neighbor expiration time/3.

Example

Set the interval for sending Hello packets by the OSPF interface to 20s.

```
Switch(config-vlanif-3)#ipv6 ospf hello-interval 20
Switch(config-vlanif-3)#
```

5.5.16 ipv6 ospf dead-interval

Function

The **ipv6 ospf dead-interval** command sets the neighbor expiration time of an IPv6 OSPF interface.

The **ipv6 ospf dead-interval default** command restores the neighbor expiration time of an IPv6 OSPF interface.

Format

- **ipv6 ospf dead-interval** { *interval* | **default** }
- **ipv6 ospf dead-interval** { *interval* | **default** } **process** *process-id*

Parameter

Parameter	Description	Value
interval	Specifies the neighbor expiration time of an OSPF interface.	The value is an integer ranging from 1 to 65535.
process-id	Specifies a process ID.	The value is an integer ranging from 1 to 64. When no process ID is configured, the default process ID 1 is used.

Default Value

By default, the neighbor expiration time of an OSPF interface is 40s.

View

VLANIF configuration view, loopback interface configuration view, Ethernet routing interface configuration view, BD interface configuration view

Usage Guidelines

You can use this command to change the default neighbor expiration time of the OSPF interface. Note that the same expiration time must be configured for both parties and the value must be larger than three times the interval for sending Hello packets.

Example

Set the neighbor expiration time of an OSPF interface to 30s.

```
Switch(config-vlanif-3)#ipv6 ospf dead-interval 30
Switch(config-vlanif-3)#
```

5.5.17 ipv6 ospf transmit-delay**Function**

The **ipv6 ospf transmit-delay** command sets the transmission delay on an IPv6 OSPF interface.

The **ipv6 ospf transmit-delay default** command restores the transmission delay on an IPv6 OSPF interface.

Format

- **ipv6 ospf transmit-delay** { *transmit-delay-time* | **default** }
- **ipv6 ospf transmit-delay** { *transmit-delay-time* | **default** } **process** *process-id*

Parameter

Parameter	Description	Value
transmit-delay-time	Specifies the transmission delay on an interface.	The value is an integer ranging from 1 to 500.
process-id	Specifies a process ID.	The value is an integer ranging from 1 to 64.

Default Value

The default value is 1.

View

VLANIF configuration view, loopback interface configuration view, Ethernet routing interface configuration view, BD interface configuration view

Usage Guidelines

OSPF assumes that a delay is generated during message transmission. The default delay is 1s. Delay is set to better control the LSA update. For example, when an LSA with Age set to 0 is transmitted over an interface, Age should be set to the delay of the interface. However, considering the aging time of the LSA is 3600s, which is much larger than the actual transmission delay of the interface, the transmission delay is not important.

The retransmission delay is a variable and does not need synchronization. You can configure different retransmission delay values for both parties in a neighbor relation.

Example

Set the transmission delay on an OSPF interface to 2s.

```
Switch(config-vlanif-3)#ipv6 ospf transmit-delay 2
Switch(config-vlanif-3)#
```

5.5.18 ipv6 ospf area

Function

The **ipv6 ospf area** command sets an area directly connected to the switch.

Format

- **ipv6 ospf area** *area-id*
- **ipv6 ospf area** *area-id process* *process-id*
- **ipv6 ospf area** *area-id process* *process-id instance* *instance-id*
- **no ipv6 ospf**
- **no ipv6 ospf process** *process-id*

- **no ipv6 ospf process** *process-id* **instance** *instance-id*

Parameter

Parameter	Description	Value
area-id	Specifies an area ID.	The value is a dotted decimal number or an integer. Generally, for an area with ID smaller than 65535, the value is an integer. For an area with ID larger than 65535, the value is an IP address. The value ranges from 0 to 4294967295.
process-id	Specifies a process ID.	The value is an integer ranging from 1 to 64.
instance-id	Specifies an OSPF instance ID.	The value is an integer ranging from 0 to 255.

Default Value

NA

View

VLANIF configuration view, loopback interface configuration view, Ethernet routing interface configuration view, BD interface configuration view

Usage Guidelines

NA

Example

Set the ID of the area directly connected to the switch to 10000.

```
Switch(config-vlanif-1)#ipv6 ospf area 10000
Switch(config-vlanif-1)#
```

5.5.19 ipv6 ospf bfd {enable|disable}

Function

The **ipv6 ospf bfd {enable|disable}** command enables or disables the BFD feature for a VLAN interface.

Format

- **ipv6 ospf bfd { enable | disable }**
- **ipv6 ospf bfd { enable | disable } process** *process-id*

Parameter

Parameter	Description	Value

Parameter	Description	Value
enable	Enables the BFD feature. After the BFD feature is enabled, the switch can quickly detect OSPF neighbor disconnection.	-
disable	Disables the BFD feature.	-
process-id	Specifies an OSPFv3 process ID.	The value is an integer ranging from 1 to 64.

Default Value

NA

View

VLANIF configuration view, loopback interface configuration view, Ethernet routing interface configuration view, BD interface configuration view

Usage Guidelines

NA

Example

Enable the BFD feature.

```
Switch(config-vlanif-3)#ipv6 ospf bfd enable
Switch(config-vlanif-3)#
```

5.5.20 ipv6 ospf cost

Function

The **ipv6 ospf cost** command sets the cost of an OSPFv3 interface.

Format

- **ipv6 ospf cost** { *cost* | **default** }
- **ipv6 ospf cost** { *cost* | **default** } **process** *process-id*

Parameter

Parameter	Description	Value
cost	Specifies the cost required for running the OSPF protocol.	The value is an integer ranging from 1 to 65535.
process-id	Specifies a process ID.	The value is an integer ranging from 1 to 64. When no process ID is configured, the default process ID 1 is used.

Default Value

The default value is 1.

View

VLANIF configuration view, loopback interface configuration view, Ethernet routing interface configuration view, BD interface configuration view

Usage Guidelines

Costs of OSPF interfaces are used for route selection control. For example, compared with a 100-megabit interface, a 1000-megabit interface has a larger capacity. You can set a smaller cost for a 1000-megabit interface and a larger cost for a 100-megabit interface, so that the switch selects the 1000-megabit interface first. Generally, set the same cost for interfaces of adjacent routers.

Example

Set the cost of the OSPFv3 interface to 20000.

```
Switch(config-vlanif-3)#ipv6 ospf cost 20000
Switch(config-vlanif-3)#
```

5.5.21 ipv6 ospf peer**Function**

The **ipv6 ospf peer** command sets the IPv6 addresses and priority of adjacent switches on an NBMA network.

Format

- **ipv6 ospf peer** *ipv6-address* **priority** *priority*
- **ipv6 ospf peer** *ipv6-address* **priority** *priority* **process** *process-id*

Parameter

Parameter	Description	Value
ipv6-address	Specifies the IPv6 address of an adjacent switch.	The value is in dotted decimal notation.
priority	Specifies the priority of a network neighbor.	The value is an integer ranging from 0 to 255.
process-id	Specifies an OSPFv3 process ID.	The value is an integer ranging from 1 to 64.

Default Value

NA

View

VLANIF configuration view, loopback interface configuration view, Ethernet routing interface configuration view, BD interface configuration view

Usage Guidelines

If you use this command to set the priority of a peer router, the peer switch must have the same priority as the local switch.

Example

Set the IPv6 address of adjacent switches on an OSPF network to 2000::1 and the priority to 1.

```
Switch(config-vlanif-3)#ipv6 ospf peer 2000::1 priority 1
Switch(config-vlanif-3)#
```

5.5.22 ipv6 ospf priority**Function**

The **ipv6 ospf priority** command sets the priority of an OSPFv3 interface.

Format

- **ipv6 ospf priority** { *priority* | **default** }
- **ipv6 ospf priority** { *priority* | **default** } **process** *process-id*

Parameter

Parameter	Description	Value
priority	Interface priority	The value is an integer ranging from 0 to 255.
process-id	Specifies a process ID.	The value is an integer ranging from 1 to 64.

Default Value

The default value is 1.

View

VLANIF configuration view, loopback interface configuration view, Ethernet routing interface configuration view, BD interface configuration view

Usage Guidelines

The OSPF interface priority is used for DR election. Generally, it does not need to be configured, especially in a point-to-point connection scenario where the interface priority is basically useless.

However, if you require a specific interface functioning as the DR, you can set a higher priority for the interface. Note that the DR of OSPF interfaces cannot be preempted. If a device serves as the DR, it constantly serves as the DR unless it is faulty or disabled.

Example

Set the priority of an OSPFv3 interface to 125.

```
Switch(config-vlanif-3)#ipv6 ospf priority 125
Switch(config-vlanif-3)#
```

5.5.23 ipv6 ospf retransmit-interval

Function

The **ipv6 ospf retransmit-interval** command sets the retransmission interval for an OSPFv3 interface.

Format

- **ipv6 ospf retransmit-interval** { *retransmit-interval-time* | **default** }
- **ipv6 ospf retransmit-interval** { *retransmit-interval-time* | **default** } **process** *process-id*

Parameter

Parameter	Description	Value
retransmit-interval-time	Specifies a retransmission interval.	The value is an integer ranging from 1 to 1800, in seconds.
process-id	Specifies a process ID.	The value is an integer ranging from 1 to 64. When no process ID is configured, the default process ID 1 is used.

Default Value

By default, the retransmission interval is 5s.

View

VLANIF configuration view, loopback interface configuration view, Ethernet routing interface configuration view, BD interface configuration view

Usage Guidelines

OSPF packets are directly encapsulated based on IP for transmission. There is a probability of packet loss. Therefore, packet retransmission is required. The default retransmission interval is 5s. You can adjust the retransmission interval according to the network conditions.

The retransmission interval is a variable and does not need synchronization. You can configure different retransmission intervals for both parties in a neighbor relation.

Example

Set the retransmission interval of an OSPFv3 interface to 2s.

```
Switch(config-vlanif-3)#ipv6 ospf retransmit-interval 2
Switch(config-vlanif-3)#
```

5.5.24 ipv6 ospf mtu

Function

The **ipv6 ospf mtu** command sets an MTU value for an OSPFv3 interface.

Format

- **ipv6 ospf mtu** { *mtu* | **default** }
- **ipv6 ospf mtu** { *mtu* | **default** } **process** *process-id*

Parameter

Parameter	Description	Value
mtu	Specifies the MTU value of the OSPFv3 interface.	The value is an integer ranging from 1280 to 9216. The default value is 1500.
process-id	Specifies an OSPFv3 process ID.	The value is an integer ranging from 1 to 64. When no process ID is configured, the default process ID 1 is used.

Default Value

The default value is 1500.

View

VLANIF configuration view, loopback interface configuration view, Ethernet routing interface configuration view, BD interface configuration view

Usage Guidelines

The default MTU of the OSPFv3 interface is the IPMTU of the interface. If the interface does not support MTU configuration, the value is 0 by default. You can use this command to modify the MTU of the OSPFv3 interface. Note that this command is not used to modify the MTU of an IP interface.

You must configure the same MTU value for both parties in a neighbor relation.

Example

Set the MTU value of an OSPFv3 interface to 1000.

```
Switch(config-vlanif-3)#ipv6 ospf mtu 1000
Switch(config-vlanif-3)#
```

5.5.25 ipv6 ospf mtu-ignore

Function

The **ipv6 ospf mtu-ignore {enable|disable}** command enables or disables MTU detection ignorance for DD packets.

Format

- **ipv6 ospf mtu-ignore { enable | disable }**
- **ipv6 ospf mtu-ignore { enable | disable } process *process-id***

Parameter

Parameter	Description	Value
enable	Enables MTU detection ignorance for DD packets.	-
disable	Disables MTU detection ignorance for DD packets.	-
process-id	Specifies an OSPFv3 process ID.	The value is an integer ranging from 1 to 64.

Default Value

Disable

View

VLANIF configuration view, loopback interface configuration view, Ethernet routing interface configuration view, BD interface configuration view

Usage Guidelines

NA

Example

Enable MTU detection ignorance for DD packets.

```
Switch(config-vlanif-3)#ipv6 ospf mtu-ignore enable
Switch(config-vlanif-3)#
```


5.5.26 maximum load-balancing

Function

The **maximum load-balancing** command sets the maximum number of ECMP routes for load balancing.

Format

maximum load-balancing { *load-balancing-number* | **default** }

Parameter

Parameter	Description	Value
load-balancing-number	Specifies the maximum number of ECMP routes for load balancing.	The value is an integer ranging from 1 to 16.
default	Specifies the default maximum number of ECMP routes for load balancing.	16

Default Value

16

View

OSPFv3 configuration view

Usage Guidelines

When the routing table contains multiple routes that have the same destination address and reference bandwidth and are detected by the same routing protocol, then load balancing can be performed by these routes. You can **run maximum load-balancing** to set the maximum number of ECMP routes for load balancing to optimize the routing policy and meet the requirements of a complex network environment.

Example

Set the maximum number of ECMP routes for load balancing.

```
Switch(config-ospfv3-1)#maximum load-balancing 2
Switch(config-ospfv3-1)#
```

5.5.27 router ipv6 ospf

Function

The **router ipv6 ospf** command enables IPv6 OSPF and enters the OSPFv3 configuration view. The system supports configuration of multiple OSPF instances.

The **no router ipv6 ospf** command disables IPv6 OSPF.

Format

- **router ipv6 ospf**
- **router ipv6 ospf** *process-id*
- **no router ipv6 ospf**
- **no router ipv6 ospf** *process-id*

Parameter

Parameter	Description	Value
process-id	Specifies an IPv6 OSPF process ID.	The value is an integer ranging from 1 to 64. If you do not enter a process ID, the default process ID 1 is used.

Default Value

By default, IPv6 OSPF is disabled.

View

Global configuration view

Usage Guidelines

NA

Example

Enable IPv6 OSPF.

```
Switch(config-ospfv3-1)#router ipv6 ospf
Switch(config-ospfv3-1)#
```

5.5.28 router ipv6 ospf vpn-instance

Function

The **router ipv6 ospf vpn-instance** command enables IPv6 OSPF and starts a process of a VPN instance.

Format

- **router ipv6 ospf** *process-id* **vpn-instance** *vpn-instance-name*
- **router ipv6 ospf vpn-instance** *vpn-instance-name*

Parameter

Parameter	Description	Value
process-id	Specifies an IPv6 OSPF process ID.	The value is an integer ranging from 1 to 64. If you do not enter a process ID, the default process ID 1 is used.
vpn-instance-name	Specifies the name of the VPN instance created for MPLS.	The value is a case-sensitive character string.

Default Value

By default, the VPN instance process is not started in the system.

View

Global configuration view

Usage Guidelines

NA

Example

Enable IPv6 OSPF 1 and start a process named VPN11.

```
Switch(config-ospfv3-1)#router ipv6 ospf 1 vpn-instance 11
Switch(config-ospfv3-1)#
```

5.5.29 reset ipv6 ospf**Function**

The **reset ipv6 ospf** command restarts an IPv6 OSPF process.

Format

- **reset ipv6 ospf**
- **reset ipv6 ospf** *process-id*

Parameter

Parameter	Description	Value
process-id	Specifies an IPv6 OSPF process ID.	The value is an integer ranging from 1 to 64.

Parameter

NA

Default Value

NA

View

Privileged configuration view, global configuration view, OSPFv3 route configuration view

Usage Guidelines

NA

Example

Restart an IPv6 OSPF process.

```
Switch(config-ospfv3-1)#reset ipv6 ospf
Switch(config-ospfv3-1)#
```

5.5.30 reset ipv6 ospf counters**Function**The **reset ipv6 ospf counters** command clears the OSPFv3 counter.**Format**

- **reset ipv6 ospf counters**
- **reset ipv6 ospf *process-id* counters**

Parameter

Parameter	Description	Value
process-id	Specifies an OSPFv3 process ID.	The value is an integer ranging from 1 to 64.

Default Value

NA

View

Privileged user view, global configuration view, OSPFv3 configuration view

Usage Guidelines

NA

Example

Clear the OSPFv3 counter.

```
Switch(config-ospfv3-1)#reset ipv6 ospf counters
Switch(config-ospfv3-1)#
```

5.5.31 redistribute

Function

The **redistribute** command enables redistributing the BGP, direct, static, RIP, ISIS, and OSPF routes.

The **no redistribute** command disables redistributing the BGP, direct, static, RIP, ISIS, and OSPF routes.

Format

- **redistribute** { **connect** | **static** | **bgp** | **rip** | **isis** | **ospf** }
- **no redistribute** { **connect** | **static** | **bgp** | **rip** | **isis** | **ospf** }

Parameter

Parameter	Description	Value
static	Redistributes static routes to the OSPF protocol.	-
connect	Redistributes direct routes to the OSPF protocol.	-
bgp	Redistributes BGP routes to the OSPF protocol.	-
rip	Redistributes RIP routes to the OSPF protocol.	-
isis	Redistributes ISIS routes to the OSPF protocol.	-
ospf	Redistributes OSPF routes to the OSPF protocol.	-

Default Value

By default, no route is redistributed.

View

OSPFv3 configuration view

Usage Guidelines

NA

Example

Configure static route redistribution.

```
Switch(config-ospfv3-1)#redistribute static
Switch(config-ospfv3-1)#
```

5.5.32 redistribute route-policy

Function

The **redistribute route-policy** command sets a route import policy.

The **no redistribute route-policy** command deletes a route import policy.

Format

- **redistribute { connect | static | rip | bgp | isis | ospf } route-policy *policy-name***
- **no redistribute { connect | static | rip | bgp | isis | ospf } route-policy**

Parameter

Parameter	Description	Value
static	Configures a policy for importing static routes.	-
connect	Configures a policy for importing direct routes.	-
rip	Configures a policy for importing RIP routes.	-
bgp	Configures a policy for importing BGP routes.	-
isis	Configures a policy for importing ISIS routes.	-
ospf	Configures a policy for importing OSPF routes.	-
policy-name	Specifies the name of a routing policy.	The value is a string consisting of up to 20 bytes.

Default Value

By default, the value is a null character string, indicating not referring to any routing policy.

View

OSPFv3 configuration view

Usage Guidelines

NA

Example

Configure routing policy 2 for importing static routes.

```
Switch(config-ospfv3-1)#redistribute static route-policy 2
Switch(config-ospfv3-1)#
```

5.5.33 router-id

Function

The **router-id** command configures a router ID for the switch.

Format

router-id *ip-address*

Parameter

Parameter	Description	Value
ip-address	Specifies the router ID of the switch.	The value is in dotted decimal notation.

Default Value

By default, no switch ID is configured. The switch selects an interface IP address as its ID during running. The maximum IP address is used.

View

OSPFv3 configuration view

Usage Guidelines

The router ID selection rules are as follows:

- 1) Minimum static loopback address
- 2) Minimum static primary address
- 3) Minimum static secondary address
- 4) Minimum static link local address
- 5) Minimum address allocated by the DHCP
- 6) Error return

Example

Set the switch ID to 10.2.3.1.

```
Switch(config-ospfv3-1)#router-id 10.2.3.1
Switch(config-ospfv3-1)#
```

5.5.34 show ipv6 ospf graceful-restart

Function

The **show ipv6 ospf graceful-restart** command displays information about OSPFv3 graceful restart of the switch and the state of graceful restart.

Format

- **show ipv6 ospf graceful-restart**
- **show ipv6 ospf graceful-restart process** *process-id*

Parameter

Parameter	Description	Value

Parameter	Description	Value
process-id	Specifies a process ID.	The value is an integer ranging from 1 to 64.

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

View information about OSPFv3 graceful restart of the switch and the state of graceful restart.

```
Switch>show ipv6 ospf graceful-restart
OSPFv3 Process 1
Restart Capability          :Not Support
Restart Helper Capability   :Not Support
Restart State               :In Restarting
Restart Period              :120 seconds
Restart Exit Reason         :none
Restart Age                 :0
Restart Strict Lsa Check    :enable
Restart Time                :0
Switch>
```

5.5.35 show ipv6 ospf brief

Function

The **show ipv6 ospf brief** command displays the brief OSPF information.

Format

- **show ipv6 ospf brief process** *process-id*
- **show ipv6 ospf brief**

Parameter

Parameter	Description	Value
process-id	Specifies a process ID.	The value is an integer ranging from 1 to 64.

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

View the brief OSPFv3 information.

```

Switch>show ipv6 ospf brief
  OSPFv3 Process 1
  -----
  Vpn Name           :
  Version            :3
  Routing Id         :1.1.1.1
  AS Scope LSA Number :0
  Checksum Sum       :0x29F30
  External LSA Number :0
  Redistribute Bgp    :Enable
  Area Border Router  :no
  AS Border Router    :yes
  Originate New Lsas  :4
  Receive New Lsas    :5
  External LSDB Limit  :-1 No Limited
  Exit Overflow Interval :0(s)
  Demand Extensions   :no
  Reference Bandwidth  :100(Mbits/s)
  Stub Router Support  :no
  Stub Router Advertisement :DoNotAdvertise
  Spf Running Interval :2(s)
  Discontinuity Time   :0(s)
  Frr State            :disable
Switch>

```

5.5.36 show ipv6 ospf area**Function**

The **show ipv6 ospf area** command displays information about all areas directly connected to the switch.

Format

- **show ipv6 ospf area** [*area-id*]
- **show ipv6 ospf area process** *process-id*
- **show ipv6 ospf area**

Parameter

Parameter	Description	Value
area-id	Specifies an area ID.	The value is a dotted decimal number or an integer. Generally, for an area with ID smaller than 65535, the value is an integer. For an area with ID larger than 65535, the value is an IP address. The value ranges from 0 to 4294967295.
process-id	Specifies an OSPFv3 process ID.	The value is an integer ranging from 1 to 64.

Default Value

NA

View

Common user view

Usage Guidelines

Based on the command output, you can check whether the configuration of an OSPFv3 area is correct and solve the OSPFv3 fault.

Example

View all areas directly connected to the switch.

```
Switch>show ipv6 ospf area
OspfV3 Process 1
AreaId          Type          Summary  RouteUpdates  ABR   ASBR   LSACount
0.0.0.0         normal        summary  3978          0     0      6

Switch>
```

5.5.37 show ipv6 ospf bfd session

Function

The **show ipv6 ospf bfd session** command displays information on the neighbor for which the BFD feature is enabled.

Format

show ipv6 ospf bfd session**Parameter**

NA

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

View information on the neighbor for which the BFD feature is enabled.

```

Switch>show ipv6 ospf bfd session
OSPFv3 Process 1
Neighbor : fe80::b8:2   NeighborId : 1.1.1.2
Interface : ge1/0/1   BFDState : up
Min TX : 200   Min RX : 200
Multiplier : 3   BFD Local Dis : 1
LocalIpAdd : fe80::b8:1 RemoteIpAdd : fe80::b8:2
Diagnostic Info : noDiagnostic
Switch>

```

5.5.38 show ipv6 ospf config**Function**The **show ipv6 ospf config** command displays the general OSPF running information.**Format****show ipv6 ospf config****Parameter**

NA

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

Display general OSPF running information.

```
Switch>show ipv6 ospf config
Version:OSPFV3_VX3.00.07.03
!
router ipv6 ospf 1
  router-id 1.1.1.1
  redistribute bgp

interface vlan 200
  ipv6 ospf area 0.0.0.0
interface loopback 1
  ipv6 ospf area 0.0.0.0
Switch>
```

5.5.39 show ipv6 ospf database

Function

The **show ipv6 ospf database** command displays OSPFv3 database information.

Format

- **show ipv6 ospf database process** *process-id*
- **show ipv6 ospf database**
- **show ipv6 ospf database { router | network | inter-prefix | inter-router | external | link | intra-prefix | nssa | te }**
- **show ipv6 ospf database { router | network | inter-prefix | inter-router | intra-prefix | nssa | te }** *LS-id advertise-router-id area-id*
- **show ipv6 ospf database age** *min-age max-age*
- **show ipv6 ospf database area** *area-id*
- **show ipv6 ospf database area** *area-id process process-id*
- **show ipv6 ospf database external** *LS-id advertise-router-id*

- **show ipv6 ospf database link** *LS-id* *advertise-router-id* **interface** **vlan** *vlan-id*
- **show ipv6 ospf database link** *LS-id* *advertise-router-id* **interface** **loopback** *loopback-id*
- **show ipv6 ospf database link** *LS-id* *advertise-router-id* **interface** { **ethernet** | **xgigaethernet** | **10gigaethernet** | **25gigaethernet** | **40gigaethernet** | **100gigaethernet** } *interface-number*
- **show ipv6 ospf database link** *LS-id* *advertise-router-id* **interface** { **ethernet** | **xgigaethernet** | **10gigaethernet** | **25gigaethernet** | **40gigaethernet** | **100gigaethernet** } *interface-number.subinterface*

Parameter

Parameter	Description	Value
LS-id	Specifies an LS ID.	The value is in dotted decimal notation.
advert-router-id	Specifies an advertising route ID.	The value is in dotted decimal notation.
router network inter-prefix inter-router external link intra-prefix nssa te	Specifies an LSA type.	-
vlan-id	Specifies a VLAN ID.	The value is an integer ranging from 1 to 4094.
loopback-id	Specifies a Loopback ID.	The value is an integer ranging from 1 to 127.
process-id	Specifies a process ID.	The value is an integer ranging from 1 to 64.
min-age	Specifies the minimum aging time.	The value is an integer ranging from 1 to 3600.
max-age	Specifies the maximum aging time.	The value is an integer ranging from 1 to 3600.
area-id	Specifies an area ID.	The value is a dotted decimal number or an integer. Generally, for an area with ID smaller than 65535, the value is an integer. For an area with ID larger than 65535, the value is an IP address. The value ranges from 0 to 4294967295.
interface-number	Specifies an Ethernet interface number.	The value is an integer in the range of <1-1>/<0-1>/<1-48> (For reference only. The specific value range depends on the slot number and card type).
subinterface	Specifies an Ethernet sub-interface number.	The value is an integer ranging from 1 to 4094.

Default Value

NA

View

Common user view

Usage Guidelines

You can use this command to view information about the OSPF link state database, helping you implement fault diagnosis.

Example

View OSPFv3 database information.

```
Switch>show ipv6 ospf database
Database of OSPFv3 Process 1
```

Router Link State (Area 0.0.0.0)

LinkId	ADV Router	Age	Seq#	CheckSum	Len
0.0.0.0	1.1.1.1	252	0x80000f02	0xe635	24

Intra Area Prefix Link State (Area 0.0.0.0)

LinkId	ADV Router	Age	Seq#	CheckSum	Len
0.0.0.1	1.1.1.1	252	0x80000f75	0x83de	64

Link(Type-8) State(interface vlan200 Area 0.0.0.0)

LinkId	ADV Router	Age	Seq#	CheckSum	Len
0.0.48.200	1.1.1.1	647	0x80000005	0x14ad	76

Link(Type-8) State(interface loopback1 Area 0.0.0.0)

LinkId	ADV Router	Age	Seq#	CheckSum	Len
0.0.80.2	1.1.1.1	48	0x80000052	0x79e7	64

```
Switch>
```

5.5.40 show ipv6 ospf database count**Function**

The **show ipv6 ospf database count** command displays the number of OSPFv3 LSAs.

Format

- **show ipv6 ospf database count**
- **show ipv6 ospf database count process *process-id***
- **show ipv6 ospf database total count**

Parameter

Parameter	Description	Value
process-id	Specifies a process ID.	The value is an integer ranging from 1 to 64.

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

View the number of OSPFv3 LSAs.

Switch>show ipv6 ospf database

Database of OSPFv3 Process 1

Router Link State (Area 0.0.0.0)

LinkId	ADV Router	Age	Seq#	Checksum	Len
0.0.0.0	1.1.1.1	252	0x80000f02	0xe635	24

Intra Area Prefix Link State (Area 0.0.0.0)

LinkId	ADV Router	Age	Seq#	Checksum	Len
0.0.0.1	1.1.1.1	252	0x80000f75	0x83de	64

Link(Type-8) State(interface vlan200 Area 0.0.0.0)

LinkId	ADV Router	Age	Seq#	Checksum	Len
0.0.48.200	1.1.1.1	647	0x80000005	0x14ad	76

Link(Type-8) State(interface loopback1 Area 0.0.0.0)

LinkId	ADV Router	Age	Seq#	Checksum	Len
0.0.80.2	1.1.1.1	48	0x80000052	0x79e7	64

DUT1>show ipv6 ospf database count

%δ☐ ->"database" .

DUT1>show ipv6 ospf database count

OSPFv3 Process 1

Extern LSA:0

Unkown LSA:0

Areaid 0.0.0.0

RouteLsa	NetworkLsa	InterPrefix	InterRouter	NssaLsa	IntraLsa	UnKnowLsa
1	0	0	0	0	1	0
Interface N/A						
Link LSA Count: 1						
Interface N/A						
Link LSA Count: 1						
Switch>						

5.5.41 show ipv6 ospf import-route

Function

The **show ipv6 ospf import-route** command displays the routes imported by the OSPFv3 protocol.

Format

- **show ipv6 ospf import-route**

Parameter

NA

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

View the routes imported by the OSPFv3 protocol.

```
Switch>show ipv6 ospf import-route
Switch>
```

5.5.42 show ipv6 ospf interface

Function

The **show ipv6 ospf interface** command displays information about the switch OSPFv3 interface.

Format

- **show ipv6 ospf interface**

- **show ipv6 ospf interface vlan** *vlan-id*
- **show ipv6 ospf interface loopback** *loopback-id*
- **show ipv6 ospf interface count**
- **show ipv6 ospf interface process** *process-id*
- **show ipv6 ospf interface { ethernet | xgigaethernet | 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet } interface-number**
- **show ipv6 ospf interface { ethernet | xgigaethernet | 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet } interface-number.subinterface**

Parameter

Parameter	Description	Value
vlan-id	Specifies a VLAN ID.	The value is an integer ranging from 1 to 4094.
loopback-id	Specifies a Loopback ID.	The value is an integer ranging from 1 to 127.
process-id	Specifies a process ID.	The value is an integer ranging from 1 to 64.
interface-number	Specifies an Ethernet interface number.	The value is an integer in the range of <1-1>/<0-1>/<1-48> (For reference only. The specific value range depends on the slot number and card type).
subinterface	Specifies an Ethernet sub-interface number.	The value is an integer ranging from 1 to 4094.

Default Value

NA

View

Common user view

Usage Guidelines

Based on the command output, you can view the OSPFv3 running information, check whether the configuration is correct, and solve the OSPFv3 fault.

Example

View information about the switch OSPFv3 interface.

```
Switch>show ipv6 ospf interface
Ospf3 Process 1
Interface      AreaId        Type           State          Cost
vlan200        0.0.0.0       BROADCAST     BDR            1
loopback1      0.0.0.0       BROADCAST     DR             1
Switch>
```

5.5.43 show ipv6 ospf log

Function

The **show ipv6 ospf neighbor** command displays the OSPF logs.

Format

- **show ipv6 ospf log**
- **show ipv6 ospf log lsa**
- **show ipv6 ospf log nbr**
- **show ipv6 ospf log spf**

Parameter

Parameter	Description	Value
lsa	Displays logs about important LSA changes.	-
nbr	Displays logs about neighbor state changes.	-
spf	Displays logs about SPF calculation.	-

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

Display the OSPF logs.

```
Switch>show ipv6 ospf log spf
OSPFv3 SPF Log Information
2020/09/17 04:38:54(161ms)(ospf6-1) spf request
2020/09/17 04:38:58(911ms)(ospf6-1) route calc,time 0,sched 7,abr/asbr/net=0/0/2
2020/09/17 04:39:39(290ms)(ospf6-1) spf request
2020/09/17 04:39:42(546ms)(ospf6-1) route calc,time 0,sched 7,abr/asbr/net=0/0/2
2020/09/17 04:39:44(991ms)(ospf6-1) spf request
2020/09/17 04:39:48(760ms)(ospf6-1) route calc,time 0,sched 7,abr/asbr/net=0/0/2
2020/09/17 04:40:30(817ms)(ospf6-1) spf request
2020/09/17 04:40:32(75ms)(ospf6-1) route calc,time 0,sched 7,abr/asbr/net=0/0/2
2020/09/17 04:40:34(161ms)(ospf6-1) spf request
```

```

2020/09/17 04:40:38(932ms)(ospf6-1) route calc,time 0,sched 7,abr/asbr/net=0/0/2
2020/09/17 04:41:21(581ms)(ospf6-1) spf request
2020/09/17 04:41:23(838ms)(ospf6-1) route calc,time 0,sched 7,abr/asbr/net=0/0/2
2020/09/17 04:41:24(178ms)(ospf6-1) spf request
2020/09/17 04:41:28(930ms)(ospf6-1) route calc,time 0,sched 7,abr/asbr/net=0/0/2
Switch>

```

5.5.44 show ipv6 ospf neighbor

Function

The **show ipv6 ospf neighbor** command displays information about the adjacent station table of the switch.

Format

- **show ipv6 ospf neighbor process** *process-id*
- **show ipv6 ospf neighbor ip-address**
- **show ipv6 ospf neighbor state statistic**
- **show ipv6 ospf neighbor**

Parameter

Parameter	Description	Value
ip-address	Specifies the IP address of a neighbor. It is optional.	The value is in dotted decimal notation.
process-id	Specifies a process ID.	The value is an integer ranging from 1 to 64.

Default Value

NA

View

Common user view

Usage Guidelines

Based on the command output, you can view the OSPFv3 neighbor information, check whether the configuration of the OSPFv3 neighbor is correct, and solve the OSPFv3 fault.

Example

Display information about the adjacent station table of the switch.

```

Switch>show ipv6 ospf neighbor
Ospf3 Process 1

```

```

NeighborId      Priority  State   Interface   Instance  Aging   UpTime   IpAddress
2.2.2.2         1          Exchange  vlan200      0         29      0:00:00
fe80::6f8:f8ff:fee5:b8ba
Switch>

```

5.5.45 show ipv6 ospf route

Function

The **show ipv6 ospf route** command displays the OSPFv3 route information.

Format

- **show ipv6 ospf route**
- **show ipv6 ospf route process *process-id***

Parameter

Parameter	Description	Value
process-id	Specifies a process ID.	The value is an integer ranging from 1 to 64.

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

View the OSPFv3 route information.

```

Switch>show ipv6 ospf route

OspfV3 Process 1
RoutType  Prefix                AreaId  PathType  Cost  Cost2  NextHopIf
NextHopNbr BackupNextHop
PREFIX    1000::2/128                0.0.0.0  INTRA     2     0      N/A
fe80::6f8:f8ff:fee5:b8ba      ::
PREFIX    1000:200::/64            0.0.0.0  INTRA     1     0      N/A      ::
::
PREFIX    6600:0:6900:0:2c31::1/128 0.0.0.0  INTRA     1     0      ethernet ::
::

```

```
Switch>
```

5.5.46 show ipv6 ospf route count

Function

The **show ipv6 ospf route count** command displays the number of OSPFv3 routes.

Format

- **show ipv6 ospf route count**
- **show ipv6 ospf route count process** *process-id*
- **show ipv6 ospf route total count**
- **show ipv6 ospf route vpn-instance** *name*
- **show ipv6 ospf route vpn-instance** *name* **count**

Parameter

Parameter	Description	Value
process-id	Specifies a process ID.	The value is an integer ranging from 1 to 64.
name	Specifies a VPN instance name.	The value is a string of no more than 64 characters.

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

View the number of OSPFv3 routes.

```
Switch>show ipv6 ospf route count
```

```
Ospfv3 Process 1
```

```
Route :
```

```
Prefix(Intra  Inter  External)  ABR      ASBR
3          3        0          0          0          0
```

```

Path :
Prefix(Intra  Inter  External)  ABR      ASBR
3      3      0      0          0        0
Switch>

```

5.5.47 show ipv6 ospf statistic global

Function

The **show ipv6 ospf statistic global** command displays the global protocol statistics.

Format

show ipv6 ospf statistic global

Parameter

NA

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

Display the global protocol statistics.

```

Switch>show ipv6 ospf statistic global
OSPF Global Statistic

Working Mode:NOMAL
RawSocket:  144 RouteSocket:145 CmdSocket:  146

Memory Statistics
Configuration Params
Process   : 16
Interface: 64
Neighbor : 16
Area      : 16
LSA       : 32768
Route     : 16384

```

```

OSPF System Statistics
kernel Route Table Statistic
System Route Add: Success: 0          Failed: 0
System Route Del: Success: 0          Failed: 0
Backup Route Add: Success: 0          Failed: 0
Backup Route Del: Success: 0          Failed: 0          Not Need Del: 0
System Error
Current Errno: 0 Normal Errno: 0 Normal Error Count: 0
Switch> 0 Normal Errno: 0 Normal Error Count: 0

```

5.5.48 show ipv6 ospf statistic memory

Function

The **show ipv6 ospf statistic memory** command displays statistics about the OSPF memory.

Format

show ipv6 ospf statistic memory

Parameter

NA

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

Display statistics about the OSPF memory.

```
Switch>show ipv6 ospf statistic memory
```

Detailed Memory Operation:

Index	Add	Fail	Free	Current	Size	Description
0	1	0	0	1	704	Area
1	1985	0	1984	1	680	Neighbor
2	2	0	0	2	1696	Interface
3	1	0	0	1	2472	Instance

4	48560	0	48557	3	56	If prefix
5	17314	0	17314	0	1600	DD Node
6	12506	0	12497	9	88	LSA Database Entry
7	6123	0	6120	3	336	SPF Node
8	354	0	351	3	416	Nexthop
9	128	0	125	3	120	Route Entry
10	878428	0	878428	0	112	Retransmit node
11	0	0	0	0	160	Address Range
12	26981	0	26971	10	0	Buf
13	3000	0	3000	0	88	Redistribute Node
14	5764	0	5764	0	64	Request Node
15	0	0	0	0	224	route policy Node
16	3002	0	0	3002	0	Stat Node
17	8	0	0	8	0	Lsatable Node
18	0	0	0	0	0	Backup Spf

Switch>

5.5.49 show ipv6 ospf trap

Function

The **show ipv6 ospf trap** command displays information about the configured traps.

Format

- **show ipv6 ospf trap**
- **show ipb6 ospf trap process *process-id***

Parameter

Parameter	Description	Value
process-id	Specifies a process ID.	The value is an integer ranging from 1 to 64.

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

View information about the configured traps.


```
Switch>show ipv6 ospf trap
```

```
-----
```

```
OSPFv3 Process 1
```

```
Trap Number : 12
```

```
-----
```

Trap Name	Status	Excessive Flag
virtifstatechange	off	N
nbrstatechange	off	N
virtnbrstatechange	off	N
ifconfigerror	off	Y
virtifconfigerror	off	Y
ifrxbadpacket	off	N
virtifrxbadpacket	off	N
ifstatechange	off	N
nssatranslatorstatuschange	off	N
restartstatuschange	off	N
nbrrestarthelperstatuschange	off	N
virtnbrrestarthelperstatuschange	off	N

```
Switch>
```

5.5.50 show ipv6 ospf virtual interface

Function

The **show ipv6 ospf virtual interface** command displays the virtual links configured for OSPFv3.

Format

- **show ipv6 ospf virtual interface**
- **show ipv6 ospf virtual interface process *process-id***

Parameter

Parameter	Description	Value
process-id	Specifies a process ID.	The value is an integer ranging from 1 to 64.

Default Value

NA

View

Common user view

Usage Guidelines

The command output helps troubleshooting OSPFv3 faults.

Example

View the virtual links of OSPFv3.

```
Switch>show ipv6 ospf interface
Ospf3 Process 1
Interface      AreaId      Type        State        Cost
vlan200        0.0.0.0     BROADCAST   DR           1
loopback1      0.0.0.0     BROADCAST   DR           1
Switch>
```

5.5.51 show ipv6 ospf virtual neighbor**Function**

The **show ipv6 ospf virtual neighbor** command displays information about virtual neighbors of the configured virtual links.

Format

show ipv6 ospf virtual neighbor

Parameter

NA

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

Display information about virtual neighbors of the configured virtual links.

```
Switch>show ipv6 ospf virtual neighbor
Ospf3 Process 1
NeighborId      Priority  State   Interface  Instance  Aging   UpTime   IpAddress
2.2.2.2          1        Full    vlan200    0         36      0:18:39
fe80::6f8:f8ff:fee5:b8ba
Switch>
```

5.5.52 filter route-policy

Function

The **filter route-policy** command sets the routing protocol filter policy. Only filtered routes can be used to generate routes in the routing table.

The **no filter router-policy command** cancels the routing protocol filter policy.

Format

- **filter route-policy** *route-policy-name*
- **no filter route-policy** *route-policy-name*

Parameter

Parameter	Description	Value
route-policy-name	Specifies the name of the routing policy, which must be specified in the routing policy.	The value is a character string.

Default Value

By default, the value is a null character string, indicating not referring to any routing policy.

View

OSPFv3 configuration view

Usage Guidelines

Only routing information in compliance with certain conditions can be used to generate routes in the routing table. You can use this command to set filter conditions for routing information. Only filtered information can be used to generate routes in the routing table.

Before running this command, you must run the route-policy command to create a routing policy.

Example

Set filter policy unv1 for the routing protocol.

```
Switch(config-ospfv3-1)#filter route-policy unv1
Switch(config-ospfv3-1)#
```

5.5.53 spf-running-interval

Function

The **spf-running-interval** command configures the interval for route calculation.

Format

spf-running-interval { *interval* | **default** }

Parameter

Parameter	Description	Value
interval	Specifies the route calculation interval.	The value is an integer ranging from 1 to 60, in ms.
default	Specifies the default route calculation interval.	The default value is 2 ms.

Default Value

The default value is 2 ms.

View

OSPFv3 configuration view

Usage Guidelines

NA

Example

Set the route calculation interval to 30 ms.

```
Switch(config-ospfv3-1)#spf-running-interval 30
Switch(config-ospfv3-1)#
```

5.5.54 area nssa translator

Function

The **area nssa translator** command specifies a transition router or a candidate transition router for the ABR in the NSSA area.

Format

area *area-id* **nssa translator** { **always** | **candidate** }

Parameter

Parameter	Description	Value
area-id	Specifies an area ID.	The value is a dotted decimal number or an integer. Generally, for an area with ID smaller than 65535, the value is an integer. For an area with ID larger than 65535, the value is an IP address. The value ranges from 0 to 4294967295.
always	Specifies a transition router for the ABR in the	-

Parameter	Description	Value
	NSSA area. You can set multiple ABRs in the NSSA area as the transition router.	
candidate	Specifies an ABR in the NSSA area as the transition router. If no conversion router is designated in the current area, the conversion router is elected from all the candidate routers.	-

Default Value

NA

View

OSPFv3 route configuration view

Usage Guidelines

NA

Example

Set an ABR in the NSSA area as the transition router.

```
Switch(config-ospfv3-1)#area 1000 nssa translator always
Switch (config-ospfv3-1)#
```

5.5.55 snmp-trap

Function

The **snmp-trap** command enables or disables the traps for OSPFv3.

Format

- **snmp-trap { enable | disable }**
- **snmp-trap (enable|disable) trap-name { ifconfigerror | ifrxbadpacket | ifstatechange | nbrrestarthelperstatuschange | nbrstatechange | nssatranslatorstatuschange | restartstatuschange | virtifconfigerror | virtifrxbadpacket | virtifstatechange | virtnbrrestarthelperstatuschange | virtnbrstatechange }**

Parameter

Parameter	Description	Value
enable	Enables the traps for OSPFv3.	-
disable	Disables the traps for OSPFv3.	-

Default Value

By default, the traps for OSPFv3 are disabled.

View

OSPFv3 configuration view

Usage Guidelines

NA

Example

Enable the traps for OSPFv3.

```
Switch(config-ospfv3-1)#snmp-trap enable
Switch(config-ospfv3-1)#
```

5.5.56 ipv6 ospf passive-interface

Function

The **ipv6 ospf passive-interface** command disables an interface to receive and send OSPFv3 packets.

The **no ipv6 ospf passive-interface** command resets an interface to receive and send OSPFv3 packets.

Format

- **ipv6 ospf passive-interface**
- **ipv6 ospf passive-interface process** *process-id*
- **no ipv6 ospf passive-interface**
- **no ipv6 ospf passive-interface process** *process-id*

Parameter

Parameter	Description	Value
process-id	Specifies an OSPFv3 process ID.	The value is an integer ranging from 1 to 64.

Default Value

NA

View

VLANIF configuration view, loopback interface configuration view, Ethernet routing interface configuration view, BD interface configuration view

Usage Guidelines

Run this command if you do not want your OSPFv3 route information to be obtained by devices in other networks and enable the local device not to receive route update information released by other devices in the network.

Example

Disable the interface VLANIF 200 to receive and send OSPFv3 packets.

```
Switch(config-vlanif-200)#ipv6 ospf passive-interface
Switch(config-vlanif-200)
```

5.5.57 preference

Function

The **preference** command sets the priority of the OSPF protocol.

The **no preference** command cancels the priority configuration for the OSPF protocol.

Format

- **preference** *preference-value*
- **preference** *preference-value* **route-policy** *policy-name*
- **preference ase** *preference-value*
- **preference ase** *preference-value* **route-policy** *policy-name*
- **no preference**
- **no preference ase**

Parameter

Parameter	Description	Value
preference-value	Specifies the priority of the OSPF protocol. A smaller value indicates a higher priority.	The value is an integer ranging from 1 to 255.
policy-name	Specifies a routing policy name.	The value is a character string.
ase	Sets the priority of AS-external routes.	The value ranges from 1 to 255.

Default Value

The default priority of OSPF routes is 10. When the **ase** keyword is specified, the default priority is 150.

View

OSPFv3 route configuration view

Usage Guidelines

A switch may run multiple dynamic routing protocols simultaneously. In this case, the switch needs to implement routing information sharing among these protocols and select routes of them. Therefore, you need to set a priority value for each routing protocol. When different protocols discover the same route, the switch selects the protocol with highest priority. This command sets the priority of the OSPF protocol.

Example

Set the priority of the OSPF protocol to 30.

```
Switch(config-ospfv3-1)#preference 30
Switch(config-ospfv3-1)#
```

5.5.58 redistribute range

Function

The **redistribute range** command aggregates re-distributed routes that match the specified network segment.

The **no redistribute range** command deletes an aggregate redistributed route entry.

Format

- **redistribute { connect | static | rip | bgp | isis | ospf } range *dst-address/dst-mask***
- **redistribute { connect | static | rip | bgp | isis | ospf } *dst-address/dst-mask* metric *router-cost***
- **redistribute { connect | static | rip | bgp | isis | ospf } *dst-address/dst-mask* metric *router-cost* type *cost-type***
- **redistribute { connect | static | rip | bgp | isis | ospf } range *dst-address/dst-mask* not-advertise**
- **redistribute { connect | static | rip | bgp | isis | ospf } range *dst-address/dst-mask* type *cost-type***
- **no redistribute { connect | static | rip | bgp | isis | ospf } range *dst-address/dst-mask***

Parameter

Parameter	Description	Value
static	Configures a policy for importing static routes.	-
connect	Configures a policy for importing direct routes.	-

Parameter	Description	Value
rip	Configures a policy for importing RIP routes.	-
bgp	Configures a policy for importing BGP routes.	-
isis	Configures a policy for importing ISIS routes.	-
ospf	Configures a policy for importing OSPF routes.	-
dst-address	Specifies a destination network address.	The value is in dotted decimal notation.
dst-mask	Specifies a network mask address.	The value is in dotted decimal notation.
cost-type	Specifies an external cost type.	The value is an integer ranging from 1 to 2.
router-cost	Specifies a route cost.	The value is an integer ranging from 1 to 65535.

Default Value

By default, the OSPF area has no aggregation entry.

View

OSPFv3 configuration view

Usage Guidelines

NA

Example

Configure re-allocated aggregation route entry 10.0.0.0 255.255.0.0.

```
Switch(config-ospfv3-1)#redistribute connect range 10.0.0.0 255.255.0.0
Switch(config-ospfv3-1)#
```

5.5.59 stub-router on-startup

Function

The **stub-router** command configures a stub router.

The **stub-router on-startup** command configures a stub router and sets the interval during which a device acts as a stub router when it is restarted or faulty.

The **no stub-router** command restores the router status and no device serves as a stub router.

Format

- **stub router**
- **stub router on-startup** [*on-startup-time* | **default**]

- **no stub router**

Parameter

Parameter	Description	Value
on-startup-time	Specifies the interval during which a device acts as a stub router when it is restarted or faulty. ● If on-startup-time is configured, the device works as a stub router only when it is restarted or faulty. The hold time of the stub router state is specified by the parameter interval. ● If on-startup-time is not configured or set to the default value, the default interval 500s is applied.	The value is an integer ranging from 5 to 65535, in seconds. The default value is 500s.

Default Value

By default, a device works as a stub router for 500s.

View

OSPFv3 configuration view

Usage Guidelines

If you run the **stub router** command directly, the device is always a stub router, that is, the Cost value of all routes from this device is set to 65535.

This command increases the link metric to 65535 in the LSA generated by the device to notify other OSPF devices of not using this stub router to forward data. However, since the metric is not infinite, it is still possible to have a route to a stub router. In the Router LSA generated by a stub router, the metric values of all links are set very high.

Example

Configure a device as a stub router.

```
Switch(config)#router ipv6 ospf
Switch(config-ospfv3-1)#stub-router on-startup 200
```

5.6 BGP Configuration Commands

5.6.1 aggregate

Function

The **aggregate** command creates an aggregation record in the BGP routing table.

The **no aggregate** command deletes the created record.

Format

BGP configuration view, BGP-VPN IPv4 address family configuration view

- **aggregate** *ipv4-address ipv4-mask-length* { **summaryonly** | **all** }
- **no aggregate** *ipv4-address ipv4-mask-length*

BGP configuration view, BGP-VPN IPv6 address family configuration view

- **aggregate** *ipv6-address ipv6-mask-length* { **summaryonly** | **all** }
- **no aggregate** *ipv6-address ipv6-mask-length*

Parameter

Parameter	Description	Value
ipv4-address	Specifies an aggregated IPv4 address.	The value is in dotted decimal notation, for example, <i>A.B.C.D</i> , in which <i>A</i> to <i>D</i> are decimal digits ranging from 0 to 255.
ipv6-address	Specifies an aggregated IPv6 address.	The address contains 128 bits and is a string of 16-bit hexadecimal digits separated by a colon (:).
ipv4-mask-length	Specifies the mask length of an IPv4 address.	The value is an integer ranging from 0 to 32.
ipv6-mask-length	Specifies the mask length of an IPv6 address.	The value is an integer ranging from 0 to 128.
summaryonly all	Indicates whether to send only aggregated routes or send aggregated routes and specific routes.	-

Default Value

NA

View

BGP configuration view, BGP-VPN IPv4 address family configuration view, BGP-VPN IPv6 address family configuration view

Usage Guidelines

You can run this command to aggregate addresses in a network segment to reduce the number of routes transmitted in the network.

Example

Create an aggregation record with address 10.10.10.10 10 in the BGP routing table

```
Switch(config-bgp)#aggregate 10.10.10.10 10 summaryonly
Switch(config-bgp)#
```

5.6.2 aggregate adminstatus**Function**

The **aggregate adminstatus** command sets to make an aggregation entry valid or invalid.

Format

BGP configuration view, BGP-VPN IPv4 address family configuration view

aggregate *ipv4-address* *ipv4-mask-length* **adminstatus** { **up** | **down** }

BGP configuration view, BGP-VPN IPv6 address family configuration view

aggregate *ipv6-address* *ipv6-mask-length* **adminstatus** { **up** | **down** }

Parameter

Parameter	Description	Value
ipv4-address	Specifies an aggregated IPv4 address.	The value is in dotted decimal notation, for example, <i>A.B.C.D</i> , in which <i>A</i> to <i>D</i> are decimal digits ranging from 0 to 255.
ipv6-address	Specifies an aggregated IPv6 address.	The address contains 128 bits and is a string of 16-bit hexadecimal digits separated by a colon (:).
ipv4-mask-length	Specifies the mask length of an IPv4 address.	The value is an integer ranging from 0 to 32.
ipv6-mask-length	Specifies the mask length of an IPv6 address.	The value is an integer ranging from 0 to 128.
up down	Makes an aggregation entry valid or invalid.	-

Default Value

NA

View

BGP configuration view, BGP-VPN IPv4 address family configuration view, BGP-VPN IPv6 address family configuration view

Usage Guidelines

NA

Example

Make an aggregation entry valid or invalid.

```
Switch(config-bgp)#aggregate 10.10.10.10 10 adminstatus up
Switch(config-bgp)#
```

5.6.3 show ip bgp error-statistics**Function**

The **show ip bgp error-statistics** command displays statistics of errors generated in the BGP process.

Format

- **show ip bgp error-statistics**
- **show ip bgp neighbor *nbr-address* error-statistics**

Parameter

Parameter	Description	Value
nbr-address	Specifies a neighbor IP address.	The value is in dotted decimal notation, such as A.B.C.D, where each of A to D is a decimal number ranging from 0 to 255.

Default Value

NA

View

Global configuration view

Usage Guidelines

When you query error statistics of a specific neighbor, the *nbr-address* is the IP address of the peer neighbor of the BGP.

Example

View statistics of errors generated in the BGP process.

```
Switch(config)#show ip bgp error-statistic
memory allocation failure counts: 0
socket create failure counts: 0
socket bind failure counts: 0
```

```

socket connect failure counts: 35
socket send failure counts: 0
socket receive failure counts: 0
v4 route msg send failure counts: 0
v6 route msg send failure counts: 0
arp/host sys-update failure counts: 0
mac sys-update failure counts: 0
proxy sys-update failure counts: 0
tunnel sys-update failure counts: 0
sync send failure counts: 0
notify send counts: 0
nofity receive counts: 0
import filtered route counts: 0
system route nexthop changed counts: 4
peer down because bfd down counts: 0
bfd bind error counts: 0
peer fsm down event counts: 0
route change in rib-in process counts: 0

```

View statistics of errors of the neighbor whose IP address is 2.2.2.2 generated in the BGP process.

```

Switch(config)#show ip bgp neighbor 2.2.2.2 error-statistic
peer: 2.2.2.2 vrf_id: 0 addr_type: 2
peer fsm change event counts: 0
peer msg length error counts: 0
peer marker error counts: 0
peer rxd open error counts: 0
peer open option len error counts: 0
peer rxd update error counts: 0
peer open msg version error counts: 0
peer open msg router id error counts: 0
peer open msg as number error counts: 0
peer open msg holdtime error counts: 0
peer open msg capability error counts: 0
peer rxd duplicate update attribute counts: 0
peer invalid attribute flag counts: 0
peer invalid attribute len counts: 0
peer some fixed option not appear counts: 0
peer aspath attribute error counts: 0
peer origin attribute error counts: 0
peer nexthop error counts: 0
peer route error counts: 0
peer connection collision counts: 0
peer loop detect fake as counts: 0

```

```

peer loop detect confed as counts: 0
peer loop detect local as counts: 0
peer loop detect originid counts: 0
peer loop detect cluster counts: 0
peer loop detect nhop counts: 0
peer aspath len error counts: 0
peer aspath type error counts: 0
peer nhop subnet error counts: 0
peer nhop is self error counts: 0
peer nhop len error counts: 0
peer mpreach unreachable len error counts: 0
peer mpreach unreachable af error counts: 0
peer mpreach unreachable af mismatch counts: 0
peer mpreach unreachable snpa error counts: 0
peer extcommunity error counts: 0
peer aggregator error counts: 0
peer originatorid error counts: 0
peer update source err counts: 0
peer become collision winner counts: 0
peer become collision loser counts: 0
peer evpn route error counts: 0

```

5.6.4 debug bgp neighbor

Function

The **debug bgp neighbor** command enables neighbor debugging for the BGP protocol.

The **no debug bgp neighbor** command disables neighbor debugging for the BGP protocol.

Format

BGP configuration view, BGP-VPN IPv4 address family configuration view

- **debug bgp neighbor** *ipv4-address*
- **no debug bgp neighbor** *ipv4-address*

BGP configuration view, BGP-VPN IPv6 address family configuration view

- **debug bgp neighbor** *ipv6-address*
- **no debug bgp neighbor** *ipv6-address*

Parameter

Parameter	Description	Value
ipv4-address	Specifies the IPv4 address of an	The value is in dotted decimal notation.

Parameter	Description	Value
	interface.	
ipv6-address	Specifies the IPv6 address of an interface.	In this format, a 128-digit IP address is divided into 8 segments. Each segment consists of 16 digits and is represented by 4 hexadecimal characters (0-9 and A-F). Segments are separated by colons (:). Every "X" represents a group of hexadecimal digits.

Default Value

By default, neighbor debugging is disabled for the BGP protocol.

View

BGP configuration view, BGP-VPN IPv4 address family configuration view, BGP-VPN IPv6 address family configuration view

Usage Guidelines

NA

Example

Enable neighbor debugging for the BGP protocol.

```
Switch#debug bgp neighbor
Switch#
```

5.6.5 filter-policy {export|import} route-policy

Function

The **filter-policy {export|import} route-policy** command sets the route filter policy.

The **no filter-policy {export|import} route-policy** command deletes the configuration.

Format

- **filter-policy { export | import } route-policy route-policy-name**
- **no filter-policy { export | import } route-policy route-policy-name**

Parameter

Parameter	Description	Value
export import	Specifies the route update information applied to notification/learning.	-
route-policy-name	Specifies a routing policy name.	-

Default Value

NA

View

BGP configuration view, bgp-af-ipv4-mcast configuration view, bgp-af-ipv4-vpn-mcast configuration view, BGP-ipv4 address family configuration view, BGP-IPv6 address family configuration view, BGP-VPN IPv4 address family configuration view, BGP-VPN IPv6 address family configuration view

Usage Guidelines

After a protocol is configured, this command can only filter routes of the specified protocol. After a route policy is configured, the filtered route entries must meet the configuration of the route policy.

Example

Set the route filter policy.

```
Switch(config-bgp)#filter-policy export route-policy fhv
Switch(config-bgp)#
```

5.6.6 filter-policy export**Function**

The **filter-policy** command sets the route filter policy.

The **no filter-policy** command deletes the configuration.

Format

- **filter-policy export** { **static** | **connected** | **rip** | **ospf** | **isis** } **route-policy** *route-policy-name*
- **no filter-policy export** { **static** | **connected** | **rip** | **ospf** | **isis** } **route-policy** *route-policy-name*

Parameter

Parameter	Description	Value
static connected rip ospf	Specifies the static, direct, RIP, and OSPF routes.	-
route-policy-name	Specifies a routing policy name.	-

Default Value

NA

View

BGP configuration view, bgp-af-ipv4-mcast configuration view, bgp-af-ipv4-vpn-mcast configuration view, BGP-IPv4 address family configuration view, BGP-IPv6 address family

configuration view, BGP-VPN IPv4 address family configuration view, BGP-VPN IPv6 address family configuration view

Usage Guidelines

After a protocol is configured, this command can only filter routes of the specified protocol. After a route policy is configured, the filtered route entries must meet the configuration of the route policy.

Example

Set the route filter policy.

```
Switch(config-bgp)#filter-policy export route-policy fhn
Switch(config-bgp)#
```

5.6.7 neighbor advertisement-interval

Function

The **neighbor advertisement-interval** command sets the minimum interval for the BGP to generate the route update packet.

Format

BGP configuration view, BGP-VPN IPv4 address family configuration view

neighbor *ipv4-address* **advertisement-interval** { *time-interval* | **default** }

BGP configuration view, BGP-VPN IPv6 address family configuration view

neighbor *ipv6-address* **advertisement-interval** { *time-interval* | **default** }

Parameter

Parameter	Description	Value
ipv4-address	Specifies a neighbor IPv4 address.	The value is in dotted decimal notation, for example, <i>A.B.C.D</i> , in which <i>A</i> to <i>D</i> are decimal digits ranging from 0 to 255.
ipv6-address	Specifies a neighbor IPv6 address.	The address contains 128 bits and is a string of 16-bit hexadecimal digits separated by a colon (:).
time-interval	Specifies a timer interval.	The value is an integer ranging from 1 to 255.
default	Specifies the default value.	The default value for IBGP neighbors and EBGp neighbors is 5 and 30 respectively.

Default Value

The default value for IBGP neighbors and EBGp neighbors is 5 and 30 respectively.

View

BGP configuration view, BGP-VPN IPv4 address family configuration view, BGP-VPN IPv6 address family configuration view

Usage Guidelines

NA

Example

Set the minimum interval for the BGP to generate the route update packet.

```
Switch(config-bgp)#neighbor 1.1.1.1 advertisement-interval 100
Switch(config-bgp)#
```

5.6.8 neighbor as-origin-interval

Function

The **neighbor as-origin-interval** command sets the minimum interval for the BGP to generate the BGP route update packet.

Format

BGP configuration view, BGP-VPN IPv4 address family configuration view

neighbor *ipv4-address* **as-origin-interval** { *origin-interval* | **default** }

BGP configuration view, BGP-VPN IPv6 address family configuration view

neighbor *ipv6-address* **as-origin-interval** { *origin-interval* | **default** }

Parameter

Parameter	Description	Value
ipv4-address	Specifies a neighbor IPv4 address.	The value is in dotted decimal notation, for example, A.B.C.D, in which A to D are decimal digits ranging from 0 to 255.
ipv6-address	Specifies a neighbor IPv6 address.	The address contains 128 bits and is a string of 16-bit hexadecimal digits separated by a colon (:).
origin-interval	Specifies an interval range.	The value is an integer ranging from 1 to 65535.
default	Specifies the default interval.	15

Default Value

NA

View

BGP configuration view, BGP-VPN IPv4 address family configuration view, BGP-VPN IPv6 address family configuration view

Usage Guidelines

NA

Example

Set the minimum interval for the BGP to generate the BGP route update packet.

```
Switch(config-bgp)#neighbor 1.1.1.1 as-origin-interval 100
Switch(config-bgp)#
```

5.6.9 neighbor connect-retry-interval

Function

The **neighbor connect-retry-interval** command sets the interval for sending a reconnection request to the peer after the link is disconnected.

Format

BGP configuration view, BGP-VPN IPv4 address family configuration view

neighbor *ipv4-address* **connect-retry-interval** { *retry-interval* | **default** }

BGP configuration view, BGP-VPN IPv6 address family configuration view

neighbor *ipv6-address* **connect-retry-interval** { *retry-interval* | **default** }

Parameter

Parameter	Description	Value
ipv4-address	Specifies a neighbor IPv4 address.	The value is in dotted decimal notation, for example, A.B.C.D, in which A to D are decimal digits ranging from 0 to 255.
ipv6-address	Specifies a neighbor IPv6 address.	The address contains 128 bits and is a string of 16-bit hexadecimal digits separated by a colon (:).
retry-interval	Specifies an interval range.	The value is an integer ranging from 1 to 65535.
default	Specifies the default interval.	20

Default Value

NA

View

BGP configuration view, BGP-VPN IPv4 address family configuration view, BGP-VPN IPv6 address family configuration view

Usage Guidelines

NA

Example

Set the interval for sending a reconnection request to the peer after the link is disconnected.

```
Switch(config-bgp)#neighbor 1.1.1.1 connect-retry-interval 100
Switch(config-bgp)#
```

5.6.10 neighbor ebgp-multihop

Function

The **neighbor ebgp** command sets a BGP neighbor to support multi-hop EBGp.

The **no neighbor ebgp** command cancels the configuration.

Format

BGP configuration view, BGP-VPN IPv4 address family configuration view

- **neighbor *ipv4-address* ebgp-multihop**
- **neighbor *ipv4-address* ebgp-multihop**

BGP configuration view, BGP-VPN IPv6 address family configuration view

- **neighbor *ipv6-address* ebgp-multihop**
- **neighbor *ipv6-address* ebgp-multihop**

Parameter

Parameter	Description	Value
ipv4-address	Specifies a neighbor IPv4 address.	The value is in dotted decimal notation, for example, A.B.C.D, in which A to D are decimal digits ranging from 0 to 255.
ipv6-address	Specifies a neighbor IPv6 address.	The address contains 128 bits and is a string of 16-bit hexadecimal digits separated by a colon (:).

Default Value

NA

View

BGP configuration view, BGP-VPN IPv4 address family configuration view, BGP-VPN IPv6 address family configuration view

Usage Guidelines

NA

Example

Set a BGP neighbor to support multi-hop EBGp.

```
Switch(config-bgp)#neighbor 1.1.1.1 ebgp-multihop
Switch(config-bgp)#
```

5.6.11 neighbor keepalive-timer hold-timer

Function

The **neighbor keepalive-timer hold-timer** command sets the keep alive time and hold time for the link to the peer.

Format

BGP configuration view, BGP-VPN IPv4 address family configuration view

neighbor *ipv4-address* **keepalive-timer** { *keep-value* | **default** } **hold-timer** { *hold-value* | **default** }

BGP configuration view, BGP-VPN IPv6 address family configuration view

neighbor *ipv6-address* **keepalive-timer** { *keep-value* | **default** } **hold-timer** { *hold-value* | **default** }

Parameter

Parameter	Description	Value
ipv4-address	Specifies a neighbor IPv4 address.	The value is in dotted decimal notation, for example, A.B.C.D, in which A to D are decimal digits ranging from 0 to 255.
ipv6-address	Specifies a neighbor IPv6 address.	The address contains 128 bits and is a string of 16-bit hexadecimal digits separated by a colon (:).
keep-value	Specifies the keep alive time.	The value is an integer ranging from 1 to 21845, in seconds. The default value is 30.
hold-value	Specifies the hold time.	The value is an integer ranging from 3 to 65535, in seconds. The default value is 90.

Default Value

NA

View

BGP configuration view, BGP-VPN IPv4 address family configuration view, BGP-VPN IPv6 address family configuration view

Usage Guidelines

NA

Example

Set the keep alive time and hold time for the link to the peer.

```
Switch(config-bgp)#neighbor 1.1.1.1 keepalive-timer 100 hold-timer 1000
Switch(config-bgp)#
```

5.6.12 neighbor next-hop-local

Function

The **neighbor next-hop-local** command sets the local device as the next hop.

The **no neighbor next-hop-local** command cancels the configuration.

Format

BGP configuration view, BGP-ipv4 address family configuration view, BGP-vpnv4 address family configuration view

- **neighbor** *ipv4-address* **next-hop-local**
- **no neighbor** *ipv4-address* **next-hop-local**

BGP configuration view, BGP-ipv6 address family configuration view

- **neighbor** *ipv6-address* **next-hop-local**
- **no neighbor** *ipv6-address* **next-hop-local**

Parameter

Parameter	Description	Value
ipv4-address	Specifies a neighbor IPv4 address.	The value is in dotted decimal notation, for example, A.B.C.D, in which A to D are decimal digits ranging from 0 to 255.
ipv6-address	Specifies a neighbor IPv6 address.	The address contains 128 bits and is a string of 16-bit hexadecimal digits separated by a colon (:).

Default Value

NA

View

BGP configuration view, BGP-ipv6 address family configuration view, BGP-VPN IPv4 address family configuration view, BGP-vpnv4 address family configuration view

Usage Guidelines

NA

Example

Set the local device as the next hop.

```
Switch(config-bgp)#neighbor 10.18.2.111 next-hop-local
Switch(config-bgp)#
Switch(config-bgp)#no neighbor next-hop-local
Switch(config-bgp)#
```

5.6.13 neighbor password**Function**

The **neighbor password** command sets the BGP peer to perform MD5 authentication on TCP connections and BGP messages.

The **no neighbor password** command cancels this function.

Format

BGP configuration view, BGP-VPN IPv4 address family configuration view

- **neighbor** *ipv4-address* **password** { **cipher** | **plain** } *password*
- **neighbor** *ipv4-address* **password** *password*
- **no neighbor** *ipv4-address* **password**

BGP configuration view, BGP-VPN IPv6 address family configuration view

- **neighbor** *ipv6-address* **password** *password*
- **neighbor** *ipv6-address* **password** { **cipher** | **plain** } *password*
- **no neighbor** *ipv6-address* **password**

Parameter

Parameter	Description	Value
ipv4-address	Specifies a neighbor IPv4 address.	The value is in dotted decimal notation, for example, <i>A.B.C.D</i> , in which <i>A</i> to <i>D</i> are decimal digits ranging from 0 to 255.

Parameter	Description	Value
ipv6-address	Specifies a neighbor IPv6 address.	The address contains 128 bits and is a string of 16-bit hexadecimal digits separated by a colon (:).
password	Specifies a plain text password string.	The value is a string consisting of up to 64 characters, without spaces.

Default Value

NA

View

BGP configuration view, BGP-VPN IPv4 address family configuration view, BGP-VPN IPv6 address family configuration view

Usage Guidelines

NA

Example

Set the BGP peer to perform MD5 authentication on TCP connections and BGP messages.

```
Switch(config-bgp)#neighbor 1.1.1.1 password 12345
Switch(config-bgp)#
```

5.6.14 neighbor remote-as

Function

The **neighbor remote-as** command sets the remote AS number of the peer.

The **no neighbor remote-as** command cancels the configuration.

Format

BGP configuration view, BGP-VPN IPv4 address family configuration view

- **neighbor** *ipv4-address* **remote-as** *as-value*
- **neighbor** *ipv4-address* **remote-as** *string*
- **no neighbor** *ipv4-address*

BGP configuration view, BGP-VPN IPv6 address family configuration view

- **no neighbor** *ipv6-address*
- **neighbor** *ipv6-address* **remote-as** *as-value*
- **neighbor** *ipv6-address* **remote-as** *string*

Parameter

Parameter	Description	Value
ipv4-address	Specifies a neighbor IPv4 address.	The value is in dotted decimal notation, for example, A.B.C.D, in which A to D are decimal digits ranging from 0 to 255.
ipv6-address	Specifies a neighbor IPv6 address.	The address contains 128 bits and is a string of 16-bit hexadecimal digits separated by a colon (:).
as-value	Specifies an AS ID.	The value is an integer ranging from 1 to 65535.
string	Specifies an AS ID.	It is a 4-byte neighbor AS ID in the format of <1-65535>.<0-65535>, for example, 1.2.

Default Value

NA

View

BGP configuration view, BGP-VPN IPv4 address family configuration view, BGP-VPN IPv6 address family configuration view

Usage Guidelines

NA



Caution

Before running **bgp neighbor** commands, run **remote as** first to specify the AS ID of the neighbor.

Example

Set the remote AS ID of the peer.

```
Switch(config-bgp)#neighbor 1.1.1.1 remote-as 100
Switch(config-bgp)#
```

5.6.15 neighbor route-reflector-client**Function**

The **neighbor route-reflector-client** command sets an internal BGP peer as a route reflector client and sets the local device as the route reflector.

The **no neighbor route-reflector-client** command cancels the configuration.

Format

BGP configuration view, BGP-VPN IPv4 address family configuration view, BGP-vpnv4 address family configuration view

- **neighbor *ipv4-address* route-reflector-client**
- **no neighbor *ipv4-address* route-reflector-client**

BGP configuration view, BGP-VPN IPv6 address family configuration view

- **neighbor *ipv6-address* route-reflector-client**
- **no neighbor *ipv6-address* route-reflector-client**

Parameter

Parameter	Description	Value
ipv4-address	Specifies a neighbor IPv4 address.	The value is in dotted decimal notation, for example, <i>A.B.C.D</i> , in which <i>A</i> to <i>D</i> are decimal digits ranging from 0 to 255.
ipv6-address	Specifies a neighbor IPv6 address.	The address contains 128 bits and is a string of 16-bit hexadecimal digits separated by a colon (:).

Default Value

NA

View

BGP configuration view, BGP-ipv6 address family configuration view, BGP-VPN IPv4 address family configuration view, BGP-vpnv4 address family configuration view

Usage Guidelines

NA

Example

Set an internal BGP peer as a route reflector client and set the local device as the route reflector.

```
Switch(config-bgp)#neighbor 1.1.1.1 route-reflector-client
Switch(config-bgp)#
```

5.6.16 neighbor route-refresh

Function

The **neighbor route-refresh** command enables a neighbor to refresh the routes.

The **no neighbor route-refresh** command cancels the configuration.

Format

BGP configuration view, BGP-VPN IPv4 address family configuration view

- **neighbor** *ipv4-address* **route-refresh**
- **no neighbor** *ipv4-address* **route-refresh**

BGP configuration view, BGP-VPN IPv6 address family configuration view

- **neighbor** *ipv6-address* **route-refresh**
- **no neighbor** *ipv6-address* **route-refresh**

Parameter

Parameter	Description	Value
ipv4-address	Specifies a neighbor IPv4 address.	The value is in dotted decimal notation, for example, <i>A.B.C.D</i> , in which <i>A</i> to <i>D</i> are decimal digits ranging from 0 to 255.
ipv6-address	Specifies a neighbor IPv6 address.	The address contains 128 bits and is a string of 16-bit hexadecimal digits separated by a colon (:).

Default Value

NA

View

BGP configuration view, BGP-VPN IPv4 address family configuration view, BGP-VPN IPv6 address family configuration view

Usage Guidelines

NA

Example

Enable a neighbor to refresh the routes.

```
Switch(config-bgp)#neighbor 1.1.1.1 route-refresh
Switch(config-bgp)#
```

5.6.17 neighbor send-community**Function**

The **neighbor send-community** command sets to send the community property to the peer.

The **no neighbor send-community** command cancels sending the community property to the peer.

Format

BGP configuration view, BGP-VPN IPv4 address family configuration view, BGP-vpnv4 address family configuration view

- **neighbor** *ipv4-address* **send-community**
- **no neighbor** *ipv4-address* **send-community**

BGP configuration view, BGP-ipv6 address family configuration view

- **neighbor** *ipv6-address* **send-community**
- **no neighbor** *ipv6-address* **send-community**

Parameter

Parameter	Description	Value
ipv4-address	Specifies a neighbor IPv4 address.	The value is in dotted decimal notation, for example, <i>A.B.C.D</i> , in which <i>A</i> to <i>D</i> are decimal digits ranging from 0 to 255.
ipv6-address	Specifies a neighbor IPv6 address.	The address contains 128 bits and is a string of 16-bit hexadecimal digits separated by a colon (:).

Default Value

NA

View

BGP configuration view, BGP-ipv6 address family configuration view, BGP-VPN IPv4 address family configuration view, BGP-vpnv4 address family configuration view

Usage Guidelines

NA

Example

Set to send the community property to the peer.

```
Switch(config-bgp)#neighbor 1.1.1.1 send-community
Switch(config-bgp)#
```

5.6.18 neighbor send route-refresh**Function**

The **neighbor send route-refresh** command sets to send the route refreshing information.

Format

BGP configuration view, BGP-VPN IPv4 address family configuration view

neighbor *ipv4-address* **send route-refresh** { **ipv4** | **ipv6** } { **unicast** | **multicast** }

BGP configuration view, BGP-VPN IPv6 address family configuration view

neighbor *ipv6-address* **send route-refresh** { **ipv4** | **ipv6** } { **unicast** | **multicast** }

Parameter

Parameter	Description	Value
ipv4-address	Specifies a neighbor IPv4 address.	The value is in dotted decimal notation, for example, <i>A.B.C.D</i> , in which <i>A</i> to <i>D</i> are decimal digits ranging from 0 to 255.
ipv6-address	Specifies a neighbor IPv6 address.	The address contains 128 bits and is a string of 16-bit hexadecimal digits separated by a colon (:).
unicast	Specifies a unicast route.	-
multicast	Specifies a multicast route.	-

Default Value

NA

View

BGP configuration view, BGP-VPN IPv4 address family configuration view, BGP-VPN IPv6 address family configuration view

Usage Guidelines

NA

Example

Send the route refreshing information.

```
Switch(config-bgp)#neighbor 1.1.1.1 route-refresh
Switch(config-bgp)#
```

5.6.19 neighbor shutdown**Function**

The **neighbor shutdown** command disables creating a session with the peer.

The **no neighbor shutdown** command cancels the configuration.

Format

BGP configuration view, BGP-VPN IPv4 address family configuration view

- **neighbor *ipv4-address* shutdown**
- **no neighbor *ipv4-address* shutdown**

BGP configuration view, BGP-VPN IPv6 address family configuration view

- **neighbor *ipv6-address* shutdown**
- **no neighbor *ipv6-address* shutdown**

Parameter

Parameter	Description	Value
ipv4-address	Specifies a neighbor IPv4 address.	The value is in dotted decimal notation, for example, <i>A.B.C.D</i> , in which <i>A</i> to <i>D</i> are decimal digits ranging from 0 to 255.
ipv6-address	Specifies a neighbor IPv6 address.	The address contains 128 bits and is a string of 16-bit hexadecimal digits separated by a colon (:).

Default Value

NA

View

BGP configuration view, BGP-VPN IPv4 address family configuration view, BGP-VPN IPv6 address family configuration view

Usage Guidelines

NA

Example

Disable creating a session with the peer.

```
Switch(config-bgp)#neighbor 1.1.1.1 shutdown
Switch(config-bgp)#
```

5.6.20 neighbor update-source

Function

The **neighbor update-source** command sets the source address for initiating a connection request.

The **no neighbor update-source** command deletes the source address for initiating a connection request.

Format

- **neighbor** *ip-address1* **update-source** *ip-address2*
- **no neighbor** *ip-address1* **update-source**

Parameter

Parameter	Description	Value
ip-address1	Specifies a neighbor IPv4 or IPv6 address.	The value is in dotted decimal notation, for example, <i>A.B.C.D</i> , in which <i>A</i> to <i>D</i> are decimal digits ranging from 0 to 255. The address contains 128 bits and is a string of 16-bit hexadecimal digits separated by a colon (:).
ip-address2	Specifies the local IPv4 or IPv6 address of the neighbor, that is, the source address.	The value is in dotted decimal notation, for example, <i>A.B.C.D</i> , in which <i>A</i> to <i>D</i> are decimal digits ranging from 0 to 255. The address contains 128 bits and is a string of 16-bit hexadecimal digits separated by a colon (:).

Default Value

NA

View

BGP configuration view, BGP-VPN IPv4 address family configuration view, BGP-VPN IPv4 address family configuration view

Usage Guidelines

This command is recommended when you want to create multiple peers between two switches through multiple links.

Example

Set the source address for initiating a connection request.

```
Switch(config-bgp)#neighbor 1.1.1.1 update-source 2.2.2.2
Switch(config-bgp)#
```

5.6.21 neighbor valid-ttl-hops**Function**

The **neighbor valid-ttl-hops** command enables the GTSM function for the peer.

Format

BGP configuration view, BGP-VPN IPv4 address family configuration view

neighbor *ipv4-address* **valid-ttl-hops** { *hops-value* | **default** }

BGP configuration view, BGP-VPN IPv6 address family configuration view

neighbor *ipv6-address* **valid-ttl-hops** { *hops-value* | **default** }

Parameter

Parameter	Description	Value
ipv4-address	Specifies a neighbor IPv4 address.	The value is in dotted decimal notation, such as (A.B.C.D), where each of A to D is a decimal number ranging from 1 to 255.
ipv6-address	Specifies a neighbor IPv6 address.	The address contains 128 bits and is a string of 16-bit hexadecimal digits separated by a colon (:).
hops-value	Specifies the number of TTL hops to be detected.	The value is an integer ranging from 1 to 255.
default	Specifies the default value.	255

Default Value

The default value is 255.

View

BGP configuration view, BGP-VPN IPv4 address family configuration view, BGP-VPN IPv6 address family configuration view

Usage Guidelines

NA

Example

Enable the GTSM function for the peer.

```
Switch(config-bgp)#neighbor 10.10.12.11 valid-ttl-hops 10
Switch(config-bgp)#
```

5.6.22 neighbor connect-interface

Function

The **neighbor connect-interface** command sets the source interface for sending the BGP packet.

The **no neighbor connect-interface** command deletes the configuration.

Format

- **neighbor** *ipv6-address* **connect-interface** *if-name*
- **no neighbor** *ipv6-address* **connect-interface**

Parameter

Parameter	Description	Value
ipv6-address	Specifies the IPv6 link-local address of the neighbor.	The address contains 128 bits and is a string of 16-bit hexadecimal digits separated by a colon (:). When configuring the link local address, the specified IPv6 address must be prefixed with FE80::/10.
if-name	Specifies the name of an IP interface.	The value is a character string.

Default Value

NA

View

BGP configuration view, BGP-VPN IPv6 address family configuration view

Usage Guidelines

NA

Example

Set the source interface for sending the BGP packet.

```
Switch(config-bgp)#neighbor fe80::6f8:f8ff:fee5:b8ba connect-interface vlan200
Switch(config-bgp)#
```

5.6.23 neighbor allow-as-loop

Function

The **neighbor allow-as-loop** command sets the loop number of a local AS ID.

Format

BGP configuration view, BGP-VPN IPv4 address family configuration view

neighbor *ipv4-address* **allow-as-loop** { *loop-number* | **default** }

BGP configuration view, BGP-VPN IPv6 address family configuration view

neighbor *ipv6-address* **allow-as-loop** { *loop-number* | **default** }

Parameter

Parameter	Description	Value
ipv4-address	Specifies a neighbor IPv4 address.	The value is in dotted decimal notation, for example, <i>A.B.C.D</i> , in which <i>A</i> to <i>D</i> are decimal digits ranging from 0 to 255.
ipv6-address	Specifies a neighbor IPv6 address.	The address contains 128 bits and is a string of 16-bit hexadecimal digits separated by a colon (:).
loop-number	Specifies the loop number of a local AS ID.	The value is an integer ranging from 0 to 10.
default	Specifies the default value.	0

Default Value

0

View

BGP configuration view, BGP-VPN IPv4 address family configuration view, BGP-VPN IPv6 address family configuration view

Usage Guidelines

NA

Example

Set the loop number of a local AS ID.

```
Switch(config-bgp)#neighbor 1.1.1.1 allow-as-loop 5
Switch(config-bgp)#
```

5.6.24 neighbor bfd

Function

The **neighbor bfd** command creates or cancels a BFD session for a peer or a group.

Format

BGP configuration view, BGP-VPN IPv4 address family configuration view

neighbor *ipv4-address* **bfd** { **enable** | **disable** }

BGP configuration view, BGP-VPN IPv6 address family configuration view

neighbor *ipv6-address* **bfd** { **enable** | **disable** }

Parameter

Parameter	Description	Value
ipv4-address	Specifies a neighbor IPv4	The value is in dotted decimal notation, for example,

Parameter	Description	Value
	address.	A.B.C.D, in which A to D are decimal digits ranging from 0 to 255.
ipv6-address	Specifies a neighbor IPv6 address.	The address contains 128 bits and is a string of 16-bit hexadecimal digits separated by a colon (:).

Default Value

Disable

View

BGP configuration view, BGP-VPN IPv4 address family configuration view, BGP-VPN IPv6 address family configuration view

Usage Guidelines

NA

Example

Create a BFD session.

```
Switch(config-bgp)#neighbor 1.1.1.1 bfd enable
Switch(config-bgp)#
```

5.6.25 neighbor public-as-only

Function

The **neighbor public-as-only** command sets to carry only the public AS ID, not the private AS ID, in the BGP update packet to be sent.

The **no neighbor public-as-only** command sets to carry the private AS ID in the BGP update packet to be sent.

Format

BGP configuration view, BGP-VPN IPv4 address family configuration view

- **neighbor** *ipv4-address* **public-as-only**
- **no neighbor** *ipv4-address* **public-as-only**

BGP configuration view, BGP-VPN IPv6 address family configuration view

- **neighbor** *ipv6-address* **public-as-only**
- **no neighbor** *ipv6-address* **public-as-only**

Parameter

Parameter	Description	Value
ipv4-address	Specifies a neighbor IPv4 address.	The value is in dotted decimal notation, for example, A.B.C.D, in which A to D are decimal digits ranging from 0 to 255.
ipv6-address	Specifies a neighbor IPv6 address.	The address contains 128 bits and is a string of 16-bit hexadecimal digits separated by a colon (:).

Default Value

NA

View

BGP configuration view, BGP-VPN IPv4 address family configuration view, BGP-VPN IPv6 address family configuration view

Usage Guidelines

Generally, the BGP update packet carries the AS ID (either public or private).

After you run this command, if the AS path property in the BGP route information only contains private AS IDs, BGP deletes the private AS IDs, and then sends the route information.

Example

Set to carry only the public AS ID, not the private AS ID, in the BGP update packet to be sent.

```
Switch(config-bgp)#neighbor 1.1.1.1 public-as-only
Switch(config-bgp)#
```

5.6.26 preference**Function**

The **preference** command sets the priority for an external, internal, and local routing protocol.

Format

preference { *preference1* | **default** } { *preference2* | **default** } { *preference3* | **default** }

Parameter

Parameter	Description	Value
preference1	Specifies the priority of an external EGP routing protocol. The external route is the optimal route learned from a peer outside the AS.	The value is an integer ranging from 1 to 255. The smaller value indicates a higher priority.

Parameter	Description	Value
preference2	Specifies the priority of an internal IBGP routing protocol. The internal route is a route learned from other peers inside the AS.	The value is an integer ranging from 1 to 255. The smaller value indicates a higher priority.
preference3	Specifies the priority of a local BGP route.	The value is an integer ranging from 1 to 255. The smaller value indicates a higher priority.

Default Value

Disable

View

BGP configuration view, BGP-ipv4 address family configuration view, BGP-ipv6 address family configuration view, BGP-VPN IPv4 address family configuration view, BGP-VPN IPv6 address family configuration view, BGP-vpnv4 address family configuration view

Usage Guidelines

You can run **preference** to configure the BGP priority or determine the route selection between BGP and other routing protocols.

You can set a routing policy to set a priority for routes received from the peer that meet the specified conditions. Use the default priority for routes that do not meet the specified conditions. A smaller value indicates a higher priority.

Example

Set the priority for an external, internal, and local routing protocol to 10, 20, and 30 respectively.

```
Switch(config-bgp)#preference 10 20 30
Switch(config-bgp)#
```

5.6.27 neighbor upe

Function

The **neighbor upe** command sets a BGP peer or peer group as UPE of HoVPN or cancels the configuration.

Format

neighbor *ipv4-address* **upe** { **enable** | **disable** }

Parameter

Parameter	Description	Value

Parameter	Description	Value
ipv4-address	Specifies a neighbor IPv4 address.	The value is in dotted decimal notation, for example, <i>A.B.C.D</i> , in which <i>A</i> to <i>D</i> are decimal digits ranging from 0 to 255.

Default Value

Disable

View

BGP configuration view, BGP-VPN IPv6 address family configuration view

Usage Guidelines

When you run this command to specify a UPE on SPE, SPE no longer sends a detailed route to UPE.

Example

Set a BGP peer or peer group as UPE of HoVPN.

```
Switch(config-bgp)#neighbor 1.1.1.1 upe enable
Switch(config-bgp)#
```

5.6.28 redistribute

Function

The **redistribute** command sets a route redistribution command.

Format

- **redistribute** { **static** | **connected** | **isis** | **rip** | **ospf** }
- **redistribute** { **static** | **connected** | **isis** | **rip** | **ospf** } **med** *med-value*
- **no redistribute** { **static** | **connected** | **isis** | **rip** | **ospf** }

Parameter

Parameter	Description	Value
med-value	Specifies the MED value.	The value is an integer ranging from 1 to 4294967295.
static connected rip isis ospf	Specifies the static, direct, ISIS, RIP, and OSPF routes.	-

Default Value

NA

View

BGP configuration view, BGP-ipv4 address family configuration view, BGP-ipv6 address family configuration view, BGP-VPN IPv4 address family configuration view, BGP-VPN IPv6 address family configuration view, bgp-af-ipv4-mcast configuration view, bgp-af-ipv4-vpn-mcast configuration view

Usage Guidelines

By default, the BGP routing protocol does not send any non-BGP route information. To enable BGP routing protocol to send such information, you must enable BGP route redistribution.

When an MED value is configured, only routes with the specified MED value are redistributed.

Example

Set to redistribute routes.

```
Switch(config-bgp)#redistribute isis med 1000
Switch(config-bgp)#
```

5.6.29 redistribute route-policy

Function

The **redistribute route-policy** command sets a route redistribution command.

Format

- **redistribute** { **static** | **connected** | **isis** | **rip** | **ospf** } **route-policy** *route-policy-name*
- **no redistribute** { **static** | **connected** | **isis** | **rip** | **ospf** } **route-policy** *route-policy-name*

Parameter

Parameter	Description	Value
<i>route-policy-name</i>	Specifies a routing policy name.	The value is a character string.
static connected isis rip ospf	Specifies the static, direct, ISIS, RIP, and OSPF routes.	-

Default Value

NA

View

BGP configuration view, BGP-ipv4 address family configuration view, BGP-ipv6 address family configuration view, BGP-VPN IPv4 address family configuration view, BGP-VPN IPv6 address family configuration view, bgp-af-ipv4-mcast configuration view, bgp-af-ipv4-vpn-mcast configuration view

Usage Guidelines

By default, the BGP routing protocol does not send any non-BGP route information. To enable BGP routing protocol to send such information, you must enable BGP route redistribution.

Example

Set to redistribute routes.

```
Switch(config-bgp)#redistribute static route-policy fhv
Switch(config-bgp)#
```

5.6.30 show ip bgp route label**Function**

The **show ip bgp route label** command displays the BGP route label information.

Format

show ip bgp route label

Parameter

NA

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

View the BGP VPNv4 route label information.

```
Switch>show ip bgp route label
```

DestAddr/Prefixlen	NextHop	InLabel	OutLabel
200.8.0.0/24	10.1.1.2	NULL	NULL
200.8.1.0/24	10.1.1.2	NULL	NULL
200.8.2.0/24	10.1.1.2	NULL	NULL
200.8.3.0/24	10.1.1.2	NULL	NULL
200.8.4.0/24	10.1.1.2	NULL	NULL

200.8.5.0/24	10.1.1.2	NULL	NULL
200.8.6.0/24	10.1.1.2	NULL	NULL
200.8.7.0/24	10.1.1.2	NULL	NULL
200.8.8.0/24	10.1.1.2	NULL	NULL
200.8.9.0/24	10.1.1.2	NULL	NULL
200.8.10.0/24	10.1.1.2	NULL	NULL
200.8.11.0/24	10.1.1.2	NULL	NULL
200.8.12.0/24	10.1.1.2	NULL	NULL
200.8.13.0/24	10.1.1.2	NULL	NULL
200.8.14.0/24	10.1.1.2	NULL	NULL
200.8.15.0/24	10.1.1.2	NULL	NULL
200.8.16.0/24	10.1.1.2	NULL	NULL
200.8.17.0/24	10.1.1.2	NULL	NULL
200.8.18.0/24	10.1.1.2	NULL	NULL
200.8.19.0/24	10.1.1.2	NULL	NULL
200.8.20.0/24	10.1.1.2	NULL	NULL
200.8.21.0/24	10.1.1.2	NULL	NULL
200.8.22.0/24	10.1.1.2	NULL	NULL
200.8.23.0/24	10.1.1.2	NULL	NULL
--More--			
Switch>			

5.6.31 show ip bgp aggregate

Function

The **show ip bgp aggregate** command displays the BGP aggregation route entry.

Format

show ip bgp aggregate

Parameter

NA

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

View the BGP aggregation route entry.

```
Switch(config-bgp)#show ip bgp aggregate
  Address                AddrLen  status  Advertise
  1.2.3.1                 19       up      summaryOnly
Switch(config-bgp)#
```

5.6.32 show ip bgp config**Function**

The **show ip bgp config** command displays the BGP configuration information.

Format

show ip bgp config

Parameter

NA

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

View the BGP configuration information.

```
Switch>show ip bgp config
Version : BGP4_VX2.10.84.04
!
router bgp 100
  router-id 1.1.1.1
  neighbor 2.2.2.2 remote-as 200
  neighbor 2.2.2.2 ebgp-multihop
  neighbor 2.2.2.2 update-source 1.1.1.1
  neighbor 2.2.2.2 bfd enable
  neighbor 10.1.1.2 remote-as 200
  neighbor 1000::2 remote-as 200
```

```

neighbor 1000::2 ebgp-multihop
neighbor 1000::2 update-source 1000::1
neighbor 1000::2 bfd enable
ipv4-family unicast
neighbor 2.2.2.2 next-hop-local
neighbor 2.2.2.2 enable
neighbor 10.1.1.2 enable
redistribute static route-policy 2
redistribute isis route-policy 1
ipv6-family unicast
neighbor 1000::2 next-hop-local
neighbor 1000::2 enable
redistribute isis med 1000
Switch>

```

5.6.33 show ip bgp damping-route

Function

The **show ip bgp damping-route** command displays the BGP route dampening information.

Format

- **show ip bgp damping-route**

Parameter

NA

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

View the BGP route dampening information.

```

Switch>show ip bgp damping-route
Switch>

```

5.6.34 show ip bgp log

Function

The **show ip bgp log** command displays the BGP logs.

Format

show ip bgp log

Parameter

NA

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

View the BGP logs.

```
Switch>show ip bgp log
2020/10/22 08:41:19:nm set peer cmd 36,flag 3
2020/10/22 08:41:19:nm set peer cmd 7,flag 3
2020/10/22 08:41:19:nm set peer cmd 5,flag 3
2020/10/22 08:41:19:nm set peer cmd 7,flag 3
2020/10/22 08:41:25:nm set peer cmd 7,flag 3
2020/10/22 08:41:26:nm set peer cmd 37,flag 3
2020/10/22 08:41:26:nm set peer cmd 7,flag 3
2020/10/22 08:41:32:invalid peer inprogress state 0
2020/10/22 08:41:33:invalid peer recv state 1
2020/10/22 08:41:33:nm set peer af cmd 7,flag 3
2020/10/22 08:41:36:invalid peer recv state 1
2020/10/22 08:41:40:system vpn 1 created,af 0
2020/10/22 08:41:40:create vpn instance 1
2020/10/22 08:41:40:system vpn 1 created,af 4
2020/10/22 08:41:40:system vpn 2 created,af 0
2020/10/22 08:41:40:create vpn instance 2
2020/10/22 08:41:40:system vpn 2 created,af 4
2020/10/22 08:41:40:system vpn 3 created,af 0
```

```
2020/10/22 08:41:40:create vpn instance 3
Switch>
```

5.6.35 show ip bgp log period-statistic

Function

The **show ip bgp log period-statistic** command displays the BGP log statistics period.

Format

show ip bgp log period-statistic

Parameter

NA

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

View the BGP log statistics period.

```
Switch> show ip bgp log period-statistic
Time                RxUpdate  RxFea   RxWith  PeerUp  PeerDown  NhopChg  IPv4Add  IPv4Del
IPv6Add IPv6Del
0d:19h:16m:48s      0         0       0       1       0         0       0       0       0
0
0d:19h:14m:32s      0         0       0       0       0         0       0       0       0
0
0d:19h:14m:27s      0         0       0       0       0         0       0       0       0
0
0d:19h:13m:58s      0         0       0       0       0         0       0       0       0
0
0d:19h:13m:2s       0         0       0       0       0         0       0       0       0
0
0d:19h:12m:52s      0         0       0       0       0         0       0       0       0
0
0d:19h:12m:27s      0         0       0       0       0         0       0       0       0
```

0									
0d:19h:12m:22s	0	0	0	0	0	0	0	0	0
0									
0d:19h:12m:7s	0	0	0	0	0	0	0	0	0
0									
0d:19h:11m:26s	0	0	0	0	0	0	0	0	0
0									
0d:19h:11m:21s	0	0	0	0	0	0	0	0	0
0									
0d:19h:11m:1s	0	0	0	0	0	0	0	0	0
0									
0d:19h:8m:35s	0	0	0	0	0	0	0	0	0
0									
0d:19h:5m:24s	0	0	0	0	0	0	0	0	0
0									
0d:19h:5m:10s	0	0	0	0	0	0	0	0	0
0									
0d:19h:5m:5s	0	0	0	0	0	0	0	0	0
0									
0d:19h:4m:22s	0	0	0	0	0	0	0	0	0
0									
0d:19h:4m:9s	0	0	0	0	0	0	0	0	0
0									
0d:19h:3m:8s	0	0	0	0	0	0	0	0	0
0									
0d:19h:2m:48s	1	5	0	0	0	0	5	0	0
0									
0d:19h:2m:43s	0	0	0	0	0	0	0	0	0
0									
0d:18h:58m:51s	0	0	0	0	0	0	0	0	0
0									
0d:18h:55m:19s	0	0	0	0	0	0	0	0	0
0									
0d:18h:54m:26s	0	0	0	0	0	0	0	0	0
0									
0d:18h:54m:21s	0	0	0	0	0	0	0	0	0
0									
0d:18h:51m:9s	0	0	0	0	0	0	0	0	0
0									
0d:18h:50m:37s	0	0	0	0	0	1	5	5	0
0									
0d:18h:49m:49s	0	0	0	0	1	0	0	5	0
0									

0d:18h:49m:19s	1	5	0	1	0	0	5	0	0
0d:18h:49m:10s	0	0	0	0	1	0	0	5	0
0d:18h:49m:2s	1	5	0	1	0	0	5	0	0
0d:18h:48m:52s	0	0	0	0	1	0	0	5	0
0d:18h:48m:44s	1	5	0	1	0	0	5	0	0
0d:18h:48m:32s	1	5	0	0	0	0	5	0	0
0d:18h:48m:24s	0	0	0	0	0	0	0	0	0
0d:18h:48m:13s	1	0	5	0	0	0	0	5	0
0d:18h:48m:2s	1	1	0	0	0	0	0	0	0
0d:18h:47m:57s	3	4	0	0	0	0	5	0	0
Switch>									

5.6.36 show ip bgp neighbor

Function

The **show ip bgp neighbor** command displays the state of a specified BGP peer.

Format

- **show ip bgp neighbor**
- **show ip bgp neighbor *ipv4-address***
- **show ip bgp neighbor *ipv6-address***
- **show ip bgp neighbor orf state**
- **show ipv6 bgp neighbor *ipv6-address* error-statistic**
- **show ip bgp neighbor *ipv4-address/ipv6-address* error-statistic**

Parameter

Parameter	Description	Value
ipv4-address	Specifies a neighbor IPv4 address.	The value is in dotted decimal notation, for example, A.B.C.D, in which A to D are decimal digits ranging

Parameter	Description	Value
		from 0 to 255.
ipv6-address	Specifies the IPv6 address of an interface.	In this format, a 128-digit IP address is divided into 8 segments. Each segment consists of 16 digits and is represented by 4 hexadecimal characters (0-9 and A-F). Segments are separated by colons (:). Every "X" represents a group of hexadecimal digits.

Default Value

NA

View

Common user view

Usage Guidelines

When no parameter is specified in this command, the state of all BGP peers is displayed.

Example

View the state of a specified BGP peer.

```
Switch>show ip bgp neighbor

BGP local router ID :1.1.1.1
Local AS number :100
Total number of neighbors :3          Neighbors in established state:2
Neighbor      Version  AS      MsgIn    MsgOut   Up/Down   State
StateChange  VpnInstance
2.2.2.2       4          200     20       27       00:00:00  Active    2
N/A
10.1.1.2      4          200     483      555      03:57:50  Established 5
N/A
1000::2       4          200     11       10       00:03:46  Established 549
N/A
Switch>
```

5.6.37 show ip bgp orf

Function

The **show ip bgp orf** command displays the filter information on the BGP out-of-band routes.

Format

show ip bgp orf

Parameter

NA

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

View the filter information on the BGP out-of-band routes.

Switch>show ip bgp orf

Switch>

5.6.38 show ip bgp resource**Function**The **show ip bgp resource** command displays statistics about BGP resources.**Format****show ip bgp resource****Parameter**

NA

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

View statistics about BGP resources.

```
Switch>show ip bgp resource
```

Statistic of System Route Update

```
IPv4 Add/Del/Fail          :194000/193000/0
IPv6 Add/Del/Fail          :0/0/0
```

Statistic of BGP Rib to EVPN forwarding table

```
Add/Fail                  :0/0
Add Last Error              :0/0
Delete/Fail                 :0/0
Delete Last Error           :0/0
```

Statistic of BGP MPLS VPN

```
MPLS State                 :enable
VPN Add/Delete              :0/0
VPN Label Alloc/Fail/Release :2/0/1
Import Target Add/Delete    :0/0
Export Target add/Delete     :0/0
MPLS Route Add/Fail         :0/0
MPLS Route Add Last Error    :0
MPLS Route Delete/Fail      :0/0
MPLS Route Delete Last Error :0
NextHop Changed              :0
```

Statistic of BGP Routes

```
Total Use Route/Pend Route/Pend Discard :1000/0/0
Routes Waiting System Update :0
Routes Waiting Advertise     :0
Routes Waiting Delete        :0
Routes Pend Feasible         :0
Routes Pend Withdraw         :0
Routes System Selected       :1000
Routes In Kernal              :0
Routes In Hwroute            :0
Routes In MPLS                :0
Walkup Count During System Update :387000
Walkup Count During Advertise   :1098000
Walkup Count During RIB in Proc :0
RIB in Walkup Not Finish      :0
System Add Update Node        :0
System Delete Update Node     :0
```

Statistic of BGP Messages

```

Update Send/Recv           :1215/237
Keepalive Send/Recv        :2519/2448
Open Send/Recv             :566/560
Notify Send/Recv           :13/560
Bytes Send/Recv            :1660663/984351

```

Memory Table

Id	Size	Total	Avaliable
1	24	5459	5454
2	64	65504	65504
3	184	129584	122991
4	160	0	0
5	320	32311	32311
6	1504	87	73
7	5000	26	22
8	720	0	0

Memory Type Usage

Create	Fail	Delete	Current	Len	Name
4	0	1	3	2632	Peer
421000	0	420000	1000	184	Route
8	0	7	1	552	Path
917491	0	911897	5594	0	Buffer
3	0	0	3	96	Policy
1	0	0	1	1632	VpnInstance
583000	0	583000	0	72	FloodFlag
508	0	508	0	0	Rxbuf
210433	0	210432	1	580	Nexthop
12	0	0	12	984	RIB
1	0	0	1	88	Sync Block
774000	0	774000	0	144	System Update Node

Switch>

5.6.39 show ip bgp route

Function

The **show ip bgp route** command displays the BGP route information. You can specify different parameters to view information on specific routes.

Format

- **show ip bgp route**

- **show ip bgp route *ipv4-address***
- **show ipv6 bgp route *ipv6-address***
- **show ip bgp route vpn-instance *name***
- **show ipv6 bgp route vpn-instance *name***
- **show ip bgp route vpn-instance *name* *ipv4-address***
- **show ipv6 bgp route vpn-instance *name* *ipv6-address***
- **show ip bgp route *ipv4-address* **prefix-match****
- **show ipv6 bgp route *ipv6-address* **prefix-match****
- **show ip bgp route vpn-instance *name* *ipv4-address* **prefix-match****
- **show ipv6 bgp route vpn-instance *name* *ipv6-address* **prefix-match****
- **show ip bgp route { **local** | **best** | **sys-update** | **import-filtered** }**
- **show ip bgp route vpn-instance *name* { **local** | **best** | **sys-update** | **import-filtered** }**
- **show ip bgp route { **peer** | **nexthop** } *ipv4-address***
- **show ip bgp route { **peer** | **nexthop** } *ipv6-address***
- **show ipv6 bgp route vpn-instance *name* { **peer** | **nexthop** } *ipv6-address***
- **show ip bgp route vpn-instance *name* { **peer** | **nexthop** } *ipv4-address***

Parameter

Parameter	Description	Value
ipv4-address	Specifies a neighbor IPv4 address.	The value is in dotted decimal notation, for example, <i>A.B.C.D</i> , in which <i>A</i> to <i>D</i> are decimal digits ranging from 0 to 255.
ipv6-address	Specifies a neighbor IPv6 address.	The value is in dotted decimal notation, such as (<i>X:X::X:X</i>).
name	Specifies a VPN instance name.	The value is a string of up to 64 characters.

Default Value

By default, the BGP routing table is displayed.

View

Common user view

Usage Guidelines

NA

Example

Display the BGP route information.

Switch>show ip bgp route						
Total 1000 Routes						
DestAddr/Prefixlen		Peer		Nexthop	Protocol	Med
LocalPrf	Origin	Vpn-Instance	As-Path			
200.8.0.0/24		10.1.1.2		10.1.1.2	bgp	0 100
IGP	N/A	as-seq 200				
200.8.1.0/24		10.1.1.2		10.1.1.2	bgp	0 100
IGP	N/A	as-seq 200				
200.8.2.0/24		10.1.1.2		10.1.1.2	bgp	0 100
IGP	N/A	as-seq 200				
200.8.3.0/24		10.1.1.2		10.1.1.2	bgp	0 100
IGP	N/A	as-seq 200				
200.8.4.0/24		10.1.1.2		10.1.1.2	bgp	0 100
IGP	N/A	as-seq 200				
200.8.5.0/24		10.1.1.2		10.1.1.2	bgp	0 100
IGP	N/A	as-seq 200				
200.8.6.0/24		10.1.1.2		10.1.1.2	bgp	0 100
IGP	N/A	as-seq 200				
200.8.7.0/24		10.1.1.2		10.1.1.2	bgp	0 100
IGP	N/A	as-seq 200				
200.8.8.0/24		10.1.1.2		10.1.1.2	bgp	0 100
IGP	N/A	as-seq 200				
200.8.9.0/24		10.1.1.2		10.1.1.2	bgp	0 100
IGP	N/A	as-seq 200				
200.8.10.0/24		10.1.1.2		10.1.1.2	bgp	0 100
IGP	N/A	as-seq 200				
200.8.11.0/24		10.1.1.2		10.1.1.2	bgp	0 100
IGP	N/A	as-seq 200				
200.8.12.0/24		10.1.1.2		10.1.1.2	bgp	0 100
IGP	N/A	as-seq 200				
--More--						
Switch>						

5.6.40 show ip bgp summary**Function**The **show ip bgp summary** command displays statistics about the BGP routes.

Format

show ip bgp summary

Parameter

NA

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

View statistics about the BGP routes.

```
Switch>show ip bgp summary
```

Protocol	Peer	NumberofRoute
BGP	10.1.1.2	1000

```
Switch>
```

5.6.41 show ip bgp vpn-instance neighbor**Function**

The **show ip bgp vpn-instance neighbor** command displays the neighbor information on a BGP VPN instance.

Format

show ip bgp vpn-instance *name* neighbor

Parameter

Parameter	Description	Value
name	Specifies a VPN instance name.	The value is a string of up to 64 characters.

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

View the neighbor information on a BGP VPN instance.

```
Switch>show ip bgp vpn-instance 1 neighbor
Address  Rmote-AS   State      StateChange
1.1.1.1   25         Connect    5 (state value of the state machine)
200::1    67         Established 6 (state value of the state machine)
Switch>
```

5.6.42 show ipv6 bgp route

Function

The **show ipv6 bgp route** command displays the BGP for IPv6 route information.

Format

show ipv6 bgp route [*ipv6-address*]

Parameter

Parameter	Description	Value
ipv6-address	Specifies a neighbor IPv6 address.	The value is in dotted decimal notation, such as (X:X::X:X).

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

View the BGP for IPv6 route information.

```
Switch>show ipv6 bgp route
Switch>
```


5.6.43 neighbor tcp

Function

The **neighbor tcp** command sets how to create a TCP connection with a neighbor.

The **no neighbor route-refresh** command cancels the configuration.

Format

BGP configuration view, BGP-VPN IPv4 address family configuration view

- **neighbor ipv4-address tcp { client-only | server-only }**
- **no neighbor ipv4-address tcp { client-only | server-only }**

BGP configuration view, BGP-VPN IPv6 address family configuration view

- **neighbor ipv6-address tcp { client-only | server-only }**
- **no neighbor ipv6-address tcp { client-only | server-only }**

Parameter

Parameter	Description	Value
ipv4-address	Specifies a neighbor IPv4 address.	The value is in dotted decimal notation, for example, <i>A.B.C.D</i> , in which <i>A</i> to <i>D</i> are decimal digits ranging from 0 to 255.
ipv6-address	Specifies a neighbor IPv6 address.	The address contains 128 bits and is a string of 16-bit hexadecimal digits separated by a colon (:).

Default Value

NA

View

BGP configuration view, BGP-VPN IPv4 address family configuration view, BGP-VPN IPv6 address family configuration view

Usage Guidelines

NA

Example

Set how to create a TCP connection with a neighbor.

```
Switch(config-bgp)#neighbor 1.1.1.1 tcp client-only
Switch(config-bgp)#
```

5.6.44 cluster-id

Function

The **cluster-id** command sets the cluster ID of the route reflector.

The **no cluster-id** command cancels the configured cluster ID of the route reflector.

Format

- **cluster-id** *router-id*
- **no cluster-id**

Parameter

Parameter	Description	Value
router-id	Specifies a cluster ID.	The value is in dotted decimal notation, for example, <i>A.B.C.D</i> , in which <i>A</i> to <i>D</i> are decimal digits ranging from 0 to 255.

Default Value

NA

View

BGP-ipv4 address family configuration view, BGP-vpnv4 address family configuration view, BGP-EVPN address family configuration view, BGP-VPNip4 address family configuration view, and BGP-VPN IPv6 address family configuration view

Usage Guidelines

NA

Example

Set the cluster ID of the route reflector.

```
Switch(config-bgp)#cluster-id 20.20.20.20
Switch(config-bgp)#
Switch(config-bgp)#no cluster-id
Switch(config-bgp)#
```

5.6.45 community

Function

The **community** command sets the value of the community property sent to the peer.

The **no community** command cancels the community property configuration.

Format

- **community** { *community-value* | **noadvertise** | **noexport** } { **additive** | **replace** | **none** }
- **no community**

Parameter

Parameter	Description	Value
community-value	Specifies a community property value.	The value is an integer ranging from 0 to 4294967295.
noadvertise noexport	These are two common community parameters with the value of 0Xffffff01 and 0xffffffff02 respectively. When the community value in the received route update message is noadvertise , this route is no longer sent to other peers. When the value is noexport , this route is no longer sent to external peers.	-
additive replace none	Specifies how the community property is sent to the peer. additive means adding the specified property to the original property. replace means sending the specified property value only. none means not sending the community property.	-

Default Value

NA

View

BGP configuration view, BGP-VPN IPv6 address family configuration view, and BGP-vpnv4 address family configuration view

Usage Guidelines

You can run this command to specify the community property to determine whether to notify a route.

Example

Set to send the community property value to the peer.

```
Switch(config-bgp)#community 2000 additive
Switch(config-bgp)#
Switch(config-bgp)#no community
Switch(config-bgp)#
```

5.6.46 confederation identifier

Function

The **confederation identifier** command sets the confederation ID.

The **no confederation identifier** command deletes the configured confederation ID.

Format

- **confederation identifier** { *autonomy-system-number* | *string* }
- **no confederation identifier**

Parameter

Parameter	Description	Value
autonomy-system-number	Specifies an AS ID.	The value is an integer ranging from 1 to 65535.
string	Specifies a 4-byte AS ID.	<1-65535>.<0-65535>

Default Value

NA

View

BGP configuration view

Usage Guidelines

Similar to the reflection function, the BGP confederation function is used to reduce internal connections of a BGP AS. You can run this command to divide a large AS into multiple sub-ASs, but the whole confederation is still an AS to external ASs. You can run this command to set the AS ID of a BGP confederation.

Example

Set a confederation ID.

```
Switch(config-bgp)#confederation identifier 1000
Switch(config-bgp)#
Switch(config-bgp)#no confederation identifier
Switch(config-bgp)#
```

5.6.47 confederation peer-as

Function

The **confederation peer-as** command sets an ID for each sub-AS inside a confederation.

The **no confederation peer-as** command cancels the configuration.

Format

- **confederation peer-as** *autonomy-system-number*
- **no confederation peer-as** *autonomy-system-number*

Parameter

Parameter	Description	Value
autonomy-system-number	Lists the peer ASs.	The value is an integer in the format of 1,3,5 to 7.

Default Value

NA

View

BGP configuration view

Usage Guidelines

NA

Example

Set an ID for each sub-AS inside a confederation.

```
Switch(config-bgp)#confederation peer-as 1000
Switch(config-bgp)#
Switch(config-bgp)#no bgp confederation peers 1000
Switch(config-bgp)#
```

5.6.48 dampening

Function

The **dampening** command sets the BGP route dampening parameters.

Format

dampening { *value1* | **default** } { *value2* | **default** } { *value3* | **default** } { *value4* | **default** }

Parameter

Parameter	Description	Value
value1	Specifies a dampening half-life value.	The value is an integer ranging from 1 to 45, in minutes.
default	Specifies the default dampening	15 minutes

Parameter	Description	Value
	half-life value.	
value2	Specifies the threshold for the route to exit the dampening state.	The value is an integer ranging from 1 to 20000.
default	Specifies the default threshold for the route to exit the dampening state.	750
value3	Specifies the threshold for the route to enter the dampening state.	The value is an integer ranging from 1 to 20000.
default	Specifies the default threshold for the route to enter the dampening state.	2000
value4	Specifies a dampening upper limit.	The value is an integer ranging from 1001 to 20000.
default	Specifies the default dampening upper limit.	16000

Default Value

The default value of above four parameters is 15, 750, 2000, and 2000 respectively.

View

BGP configuration view

Usage Guidelines

You can run this command to set the BGP route dampening parameters. These parameters only take effect when dampening is enabled. Generally, you do not need to modify these parameters.

Example

Set the BGP route dampening parameters.

```
Switch(config-bgp)#dampening 1 100 234 10000
Switch(config-bgp)#
```

5.6.49 dampening {enable|disable}

Function

The **dampening {enable|disable}** command enables or disables the BGP route dampening function.

Format

dampening { enable | disable }

Parameter

Parameter	Description	Value
enable	Enables the BGP route dampening function.	-

Parameter	Description	Value
disable	Disables the BGP route dampening function.	-

Default Value

Disable

View

BGP configuration view

Usage Guidelines

NA

Example

Enable the BGP route dampening function.

```
Switch(config-bgp)#dampening enable
Switch(config-bgp)#
```

5.6.50 debug bgp**Function**

The **debug bgp** command enables the BGP debugging function.

The **no debug bgp** command disables the BGP debugging function.

Format

- **debug bgp**
- **no debug bgp**
- **debug bgp { update | rib-tree | route | event | tcp | packet | all | orf | graceful-restart | error | sync }**
- **no debug bgp { update | rib-tree | route | event | tcp | packet | all | orf | graceful-restart | error | sync }**

Parameter

NA

Default Value

By default, the BGP debugging function is disabled.

View

Privileged user view

Usage Guidelines

NA

Example

Enable the BGP debugging function.

```
Switch#debug bgp update
Switch#
```

5.6.51 default local-med

Function

The **default local-med** command sets the default local MED value for BGP.

Format

default local-med { *local-med* | **default** }

Parameter

Parameter	Description	Value
local-med	Specifies a preference value.	The value is an integer ranging from 0 to 4294967295.
default	Specifies the default local MED value.	The default value is 0.

Default Value

0

View

BGP configuration view

Usage Guidelines

NA

Example

Set the default local MED value for BGP.

```
Switch(config-bgp)#default local-med 200
Switch(config-bgp)#
```


5.6.52 default local-preference

Function

The **default local-preference** command sets the default preference value for BGP.

Format

default local-preference { *preference-value* | **default** }

Parameter

Parameter	Description	Value
preference-value	Specifies a preference value.	The value is an integer ranging from 1 to 4294967295.
default	Specifies the default local preference value.	100

Default Value

100

View

BGP configuration view

Usage Guidelines

NA

Example

Set the default local preference value for BGP.

```
Switch(config-bgp)#default local-preference 100
Switch(config-bgp)#
```

5.6.53 graceful-restart {enable|disable}

Function

The **graceful-restart {enable|disable}** command enables or disables the graceful restart function.

Format

graceful-restart { **enable** | **disable** }

Parameter

Parameter	Description	Value
enable	Enables the graceful restart function.	-
disable	Disables the graceful restart function.	-

Default Value

Disable

View

BGP configuration view

Usage Guidelines

NA

Example

Enable the graceful restart function.

```
Switch(config-bgp)#graceful-restart enable
Switch(config-bgp)#
```

5.6.54 graceful-restart timer restart**Function**

The **graceful-restart timer restart** command sets the maximum wait time from the time when the peer detects restart of the local end to the time when a BGP session is recreated.

Format

graceful-restart timer restart { *restart-time* | **default** }

Parameter

Parameter	Description	Value
restart-time	Specifies a wait time range.	The value is an integer ranging from 3 to 600, in seconds.
default	Specifies the default wait time.	90s

Default Value

The default value is 90 seconds.

View

BGP configuration view

Usage Guidelines

NA

Example

Set the maximum wait time from the time when the peer detects restart of the local end to the time when a BGP session is recreated.

```
Switch(config-bgp)#graceful-restart timer restart 100
Switch(config-bgp)#
```

5.6.55 graceful-restart timer selection-deferral

Function

The **graceful-restart timer selection-deferral** command sets the route selection time for graceful restart delay.

Format

graceful-restart timer selection-deferral { *select-time* | **default** }

Parameter

Parameter	Description	Value
select-time	Specifies a selection wait time.	The value is an integer ranging from 3 to 3000, in seconds.

Default Value

The default value is 600 seconds.

View

BGP configuration view

Usage Guidelines

NA

Example

Set the route selection time for graceful restart delay.

```
Switch(config-bgp)#graceful-restart timer selection-deferral 300
Switch(config-bgp)#
```

5.6.56 ipv4[ipv6]-family

Function

The **ipv4[ipv6]-family** command enters a BGP address family view.

Format

- **ipv4-family unicast**
- **ipv4-family vpn-instance *name***
- **ipv4-family vpn-instance *name* multicast**
- **ipv6-family unicast**
- **ipv6-family vpn-instance *name***

Parameter

Parameter	Description	Value
vpn4	Enters the BGP-VPNv4 address family view.	-
vpn6	Enters the BGP-VPNv6 address family view.	-
unicast	Enters the unicast address family view.	-
name	Associates the specified VPN instance with the IPv4 or IPV6 address family and uses this parameter to enter the BGP-VPN instance view.	The value consists of up to 31 bytes.

Default Value

NA

View

BGP configuration view

Usage Guidelines

If no parameter is specified, the system enters the unicast address family view.

Example

Enter the BGP unicast address family view.

```
Switch(config-bgp)#ipv4-family unicast
Switch(config-bgp-af-ipv4)#
```

5.6.57 advertise l2vpn evpn

Function

The **advertise l2vpn evpn** command advertises a route in a VPN to BGP EVPN.

Format

advertise l2vpn evpn

Parameter

NA

Default Value

NA

View

BGP configuration view

Usage Guidelines

NA

Example

Advertise a route in a VPN to BGP EVPN.

```
Switch(config-bgp)#advertise l2vpn evpn
Switch(config-bgp)#
```

5.6.58 maximum load-balancing**Function**

The **maximum load-balancing** command sets the maximum number of ECMP routes for load balancing.

Format**maximum load-balancing** { *load-balancing-number* | **default** }**Parameter**

Parameter	Description	Value
load-balancing-number	Specifies the maximum number of ECMP routes for load balancing.	The value is an integer ranging from 1 to 16.
default	Specifies the default maximum number of ECMP routes for load balancing.	1

Default Value

1

View

BGP configuration view

Usage Guidelines

NA

Example

Set the maximum number of ECMP routes for load balancing.

```
Switch(config-bgp)#maximum load-balancing 2
Switch(config-bgp)#
```

5.6.59 neighbor next-hop-invariable**Function**

The **neighbor next-hop-invariable** command sets not to change the next hop when a BGP speaker advertises a route to the peer.

The **no neighbor next-hop-invariable** command deletes the configuration.

Format

- **neighbor** *ipv4-address* **next-hop-invariable**
- **neighbor** *ipv6-address* **next-hop-invariable**
- **no neighbor** *ipv4-address* **next-hop-invariable**
- **no neighbor** *ipv6-address* **next-hop-invariable**

Parameter

Parameter	Description	Value
ipv4-address	Specifies a peer IPv4 address.	The value is in dotted decimal notation.
ipv6-address	Specifies a peer IPv6 address.	-

Default Value

NA

View

BGP configuration view, BGP-ipv4 address family configuration view, BGP-ipv6 address family configuration view, BGP-VPNv4 address family view, BGP-VPNv6 address family view, bgp-af-ipv4-mcast address family configuration view

Usage Guidelines

Before running this command, run **neighbor remote-as** to set a remote AS ID for the peer.

Example

Set not to change the next hop when a BGP speaker advertises a route to the peer.

```
Switch(config-bgp)#neighbor 1.1.1.1 remote-as 100
```

```
Switch(config-bgp)#ipv4-family unicast
Switch(config-bgp-af-ipv4)#neighbor 1.1.1.1 next-hop-invariable
Switch(config-bgp-af-ipv4)#
```

5.6.60 neighbor

Function

The **neighbor** command enables or disables exchanging the route information with a specified peer.

Format

BGP configuration view, BGP-ipv4 address family configuration view, BGP-VPNv4 address family view, bgp-af-ipv4-mcast configuration view, bgp-af-ipv4-vpn-mcast configuration view

neighbor *ipv4-address* { **enable** | **disable** }

BGP configuration view, BGP-ipv6 address family configuration view, BGP-VPNv6 address family view

neighbor *ipv6-address* { **enable** | **disable** }

Parameter

Parameter	Description	Value
ipv4-address	Specifies a neighbor IPv4 address.	The value is in dotted decimal notation.
ipv6-address	Specifies a neighbor IPv6 address.	In this format, a 128-digit IP address is divided into 8 segments. Each segment consists of 16 digits and is represented by 4 hexadecimal characters (0-9 and A-F). Segments are separated by colons (:). Every "X" represents a group of hexadecimal digits.

Default Value

Disable

View

BGP configuration view, BGP-ipv4 address family configuration view, BGP-ipv6 address family configuration view, BGP-VPNv4 address family view, BGP-VPNv6 address family view, EVPN address family configuration view, bgp-af-ipv4-mcast configuration view, bgp-af-ipv4-vpn-mcast configuration view

Usage Guidelines

When BGP Peer is enabled or disabled for an address family, if you run **neighbor enable** or **neighbor disable** for a VPNv4 address family, the BGP connection and auto renegotiation of this Peer in other address families are affected.

Example

Enable exchanging the route information with a specified peer.

```
Switch(config-bgp)#neighbor 1.1.1.1 enable
Switch(config-bgp)#
```

5.6.61 neighbor substitute-as

Function

The **neighbor substitute-as** command enables the AS ID substitution function, that is, using the local AS ID to replace the peer AS ID specified in AS_Path.

The **no neighbor substitute-as** command deletes the configuration.

Format

- **neighbor** *ipv4-address* **substitute-as**
- **neighbor** *ipv6-address* **substitute-as**
- **no neighbor** *ipv4-address* **substitute-as**
- **no neighbor** *ipv6-address* **substitute-as**

Parameter

Parameter	Description	Value
ipv4-address	Specifies a peer IPv4 address.	The value is in dotted decimal notation.
ipv6-address	Specifies a peer IPv6 address.	The format is X:X:X:X:X:X:X.

Default Value

NA

View

BGP-VPNv4 family address view, BGP-VPNv6 family address view

Usage Guidelines

Before running this command:

1. Run **ip vpn-instance** to create a VPN and run **route-distinguisher** and **vpn-target** to set an RD and an RT.

2. Run **neighbor remote-as** to set a remote AS ID for the peer.

Example

Set not to change the next hop when a BGP speaker advertises a route to the peer.

```
Switch(config)#ip vpn-instance 1
Switch(config-vpn-instance-1)#ipv4-family
Switch(config-vpn-instance-af-ipv4)#route-distinguisher 1000:1000
Switch(config-vpn-instance-af-ipv4)#vpn-target 1000:1000
Switch(config-vpn-instance-af-ipv4)#quit
Switch(config-vpn-instance-1)#quit
Switch(config)#router bgp
Switch(config-bgp)#neighbor 1.1.1.1 remote-as 100
Switch(config-bgp)#ipv4-family vpn-instance 1
Switch(config-bgp-af-ipv4-1)#neighbor 1.1.1.1 substitute-as
Switch(config-bgp-af-ipv4-1)#
```

5.6.62 neighbor route-policy {export|import}

Function

The **neighbor route-policy {export|import}** command specifies a Route-Policy for the route from the peer or a route advertised to the peer.

The **no neighbor route-policy {export|import}** command cancels the configuration.

Format

BGP-ipv4 address family configuration view, BGP-VPNv4 address family view, and BGP-VPN IPv4 address family configuration view

- **neighbor ipv4-address route-policy route-policy-name { export | import }**
- **no neighbor ipv4-address route-policy route-policy-name { export | import }**

BGP-ipv6 address family configuration view, BGP-VPNv6 address family view

- **neighbor ipv6-address route-policy route-policy-name { export | import }**
- **no neighbor ipv6-address route-policy route-policy-name { export | import }**

Parameter

Parameter	Description	Value
ipv4-address	Specifies a neighbor IPv4 address.	The value is in dotted decimal notation, for example, <i>A.B.C.D</i> , in which <i>A</i> to <i>D</i> are decimal digits ranging from 0 to 255.

Parameter	Description	Value
ipv6-address	Specifies a neighbor IPv6 address.	The address contains 128 bits and is a string of 16-bit hexadecimal digits separated by a colon (:).
export import	Specifies route update information applied to notification/learning.	-
route-policy-name	Specifies a route policy name.	-

Default Value

NA

View

BGP-ipv4 address family configuration view, BGP-ipv6 address family configuration view, BGP-VPNv4 address family view, BGP-VPNv6 address family view, BGP-VPN IPv4 address family configuration view, and BGP configuration view

Usage Guidelines

NA

Example

Set a Route-Policy for the route from the peer or a route advertised to the peer.

```
Switch(config-bgp)#neighbor 1.2.3.1 route-policy rfhn1 export
Switch(config-bgp)#
```

5.6.63 network

Function

The **network** command sets the local network route published by a BGP, that is, add a route in the local routing table to a BGP routing table in static mode and publish it to the peer.

The **no network** command deletes the configuration.

Format

BGP configuration view, BGP-ipv4 address family configuration view, BGP-VPN IPv4 address family configuration view, bgp-af-ipv4-mcast configuration view, and bgp-af-ipv4-vpn-mcast configuration view

- **network** *network-address network-mask*
- **no network** *network-ipv4-address network-mask*

BGP configuration view, BGP-ipv6 address family configuration view, and BGP-VPN IPv6 address family configuration view

- **no network** *network-ipv6-address mask-length*
- **network** *network-ipv6-address mask-length*

Parameter

Parameter	Description	Value
network-address network-ipv4-address network-ipv6-address	Specifies an IPv4 or IPv6 network address published by BGP.	-
network-mask	Specifies a subnet mask (applicable to IPv4 networks).	Specifies the mask of an IP address. If no mask is specified, the class address is used.
mask-length	Specifies a mask length (applicable to IPv6 networks).	The value is an integer ranging from 0 to 128.

Default Value

NA

View

BGP configuration view, BGP-ipv4 address family configuration view, BGP-VPN IPv4 address family configuration view, bgp-af-ipv4-mcast configuration view, bgp-af-ipv4-vpn-mcast configuration view, BGP-ipv6 address family configuration view, and BGP-VPN IPv6 address family configuration view

Usage Guidelines

NA

Example

Set the local network route published by a BGP.

```
Switch(config-bgp-af-ipv4)#network 10.18.2.105 255.255.255.0
Switch(config-bgp-af-ipv4)#
```

5.6.64 router bgp

Function

The **router bgp** command enables BGP.

The **no router bgp** command disables BGP.

Format

- **router bgp**
- **router bgp** *as-value*
- **router bgp** *string*
- **no router bgp**

Parameter

Parameter	Description	Value
as-value	Specifies an AS ID range.	The value is an integer ranging from 1 to 65535.
string	Specifies a 4-byte AS ID range.	The value is an integer ranging from <1-65535>.<0-65535>, such as 1.2.

Default Value

NA

View

Global configuration view

Usage Guidelines

When an AS ID is set for this router, you can run this command to directly enter the BGP view.

Example

Enable or disable BGP.

```
Switch(config)#router bgp 100
Switch(config-bgp)#
Switch(config)#no router bgp
Switch(config)#
```

5.6.65 router-id**Function**

The **router-id** command sets an ID for a switch.

The **no router-id** command deletes the configured ID.

Format

- **router-id** *router-id*
- **no router-id**

Parameter

Parameter	Description	Value
router-id	Specifies a router ID.	The value is in dotted decimal notation, for example, <i>A.B.C.D</i> , in which <i>A</i> to <i>D</i> are decimal digits ranging from 0 to 255.

Default Value

NA

View

BGP configuration view

Usage Guidelines

When BGP is enabled, a route ID is generated. If no route ID is configured, the system uses the maximum loop address. If no loop address is available, the system uses the maximum IP address. Each ID can only identify one switch in an AS.

Example

Set an ID for the switch.

```
Switch(config-bgp)#router-id 10.10.10.10
Switch(config-bgp)#
Switch(config-bgp)#no router-id
Switch(config-bgp)#
```

5.6.66 reset bgp**Function**

The **reset bgp** command resets all BGP connections.

Format

- **reset bgp**
- **reset bgp statistics**
- **reset bgp system-route**

Parameter

NA

Default Value

NA

View

Global configuration view

Usage Guidelines

NA

Example

Reset all BGP connections.

```
Switch(config)#reset bgp
Switch(config)#
```

5.6.67 snmp-trap {enable|disable}**Function**

The **snmp-trap {enable|disable}** command enables or disables the BGP trap notification function.

Format

snmp-trap { enable | disable }

Parameter

Parameter	Description	Value
enable	Enables the BGP trap notification function.	-
disable	Disables the BGP trap notification function.	-

Default Value

By default, the BGP trap notification function is disabled.

View

BGP configuration view

Usage Guidelines

NA

Example

Enable the SNMP alarm reporting function for BGP.

```
Switch(config-bgp)#snmp-trap enable
Switch(config-bgp)#
```

5.6.68 synchronization {enable|disable}

Function

The **synchronization {enable|disable}** command enables or disables the synchronization function.

Format

synchronization { enable | disable }

Parameter

Parameter	Description	Value
enable	Enables the synchronization function.	-
disable	Disable	-

Default Value

NA

View

BGP configuration view

Usage Guidelines

NA

Example

Enable the synchronization function.

```
Switch(config-bgp)#synchronization enable
Switch(config-bgp)#
Switch(config-bgp)#synchronization disable
Switch(config-bgp)#
```

5.6.69 update-size

Function

The **update-size** command sets the maximum bytes for a BGP update message.

Format

update-size { max-bytes | default }

Parameter

Parameter	Description	Value
max-bytes	Specifies the maximum bytes for	The value is an integer ranging from 128 to

Parameter	Description	Value
	an update message.	4096.
default	Specifies the default value.	1400

Default Value

1400

View

BGP configuration view

Usage Guidelines

NA

Example

Set the maximum bytes for a BGP update message.

```
Switch(config-bgp)#update-size 200
```

```
Switch(config-bgp)#
```

5.6.70 auto-summary {enable|disable}

Function

The **auto-summary {enable|disable}** command enables or disables the BGP automatic aggregation function.

Format

auto-summary { enable | disable }

Parameter

Parameter	Description	Value
enable	Enables the BGP automatic aggregation function.	-
disable	Disables the BGP automatic aggregation function.	-

Default Value

NA

View

BGP configuration view

Usage Guidelines

NA

Example

Enable the BGP automatic aggregation function.

```
Switch(config-bgp)#auto-summary enable
Switch(config-bgp)#
```

5.6.71 neighbor preference**Function**

The **neighbor preference** command sets the peer preference value.

Format

- **neighbor** *ipv4-address* **preference** { *value* | **default** }
- **neighbor** *ipv6-address* **preference** { *value* | **default** }

Parameter

Parameter	Description	Value
ipv4-address	Specifies a neighbor IPv4 address.	The value is in dotted decimal notation, for example, <i>A.B.C.D</i> , in which <i>A</i> to <i>D</i> are decimal digits ranging from 0 to 255.
ipv6-address	Specifies a neighbor IPv6 address.	-
value	Specifies a peer preference value.	The value is an integer ranging from 0 to 65535.

Default Value

NA

View

BGP configuration view, BGP IPv4 address family configuration view, BGP IPv6 address family configuration view, BGP IPv4 VPN address family configuration view, BGP IPv6 VPN address family configuration view

Usage Guidelines

NA

Example

Set the peer preference value.

```
Switch(config-bgp)#neighbor 10.1.1.1 preference 10
Switch(config-bgp)#
```

5.6.72 neighbor next-hop-local

Function

The **neighbor next-hop-local** command sets the local IP address as the next hop when a route is notified to the IBGP peer (group).

The **no neighbor next-hop-local** command deletes the configuration.

Format

- **neighbor** *ipv4-address* **next-hop-local**
- **neighbor** *ipv6-address* **next-hop-local**
- **no neighbor** *ipv4-address* **next-hop-local**
- **no neighbor** *ipv6-address* **next-hop-local**

Parameter

Parameter	Description	Value
ipv4-address	Specifies a neighbor IPv4 address.	The value is in dotted decimal notation, for example, <i>A.B.C.D</i> , in which <i>A</i> to <i>D</i> are decimal digits ranging from 0 to 255.
ipv6-address	Specifies a neighbor IPv6 address.	-

Default Value

NA

View

BGP configuration view

Usage Guidelines

NA

Example

Set the local IP address as the next hop when a route is notified to the IBGP peer (group).

```
Switch(config-bgp)#neighbor 10.1.1.1 next-hop-local
Switch(config-bgp)#
```

5.6.73 default local-preference

Function

The **default local-preference** command sets the default BGP local priority.

Format

default local-preference { *value* | **default** }

Parameter

Parameter	Description	Value
value	Specifies a BGP local priority. A larger value indicates a higher priority.	The value is an integer ranging from 1 to 4294967295.
default	Specifies the default BGP local priority.	100

Default Value

NA

View

BGP IPv4 address family configuration view, BGP IPv6 address family configuration view, BGP IPv4 VPN address family configuration view, BGP IPv6 VPN address family configuration view, BGP EVPN address family configuration view

Usage Guidelines

NA

Example

Set the default BGP local priority.

```
Switch(config-bgp-af-ipv4)#default local-preference 150
Switch(config-bgp-af-ipv4)#
```

5.6.74 evpn-family

Function

The **evpn-family** command enters the BGP-EVPN address family view.

Format

evpn-family

Default Value

NA

View

BGP configuration view

Usage Guidelines

NA

Example

Enter the BGP-EVPN address family view.

```
Switch(config-bgp)#evpn-family
Switch(config-bgp-af-evpn)#
```

5.6.75 show ip bgp evpn route**Function**

The **show ip bgp evpn route** command displays information about the EVPN route maintained by BGP.

Format

- **show ip bgp evpn route**
- **show ip bgp evpn route { mac-ip | prefix | tunnel }**
- **show ip bgp evpn route arp ip-address**
- **show ip bgp evpn route count**
- **show ip bgp evpn route mac mac-address**
- **show ip bgp evpn route nd ipv6-address**
- **show ip bgp evpn route prefix ip-address**
- **show ip bgp evpn route prefix ipv6-address**
- **show ip bgp evpn route tunnel ip-address tunnel-vni**
- **show ip bgp evpn route tunnel ipv6-address tunnel-vni**
- **show ip bgp evpn route { arp | nd } peer peer-ip-address l2vni l2-vni l3vni l3-vni**
- **show ip bgp evpn route { arp | nd } peer peer-ipv6-address l2vni l2-vni l3vni l3-vni**
- **show ip bgp evpn route { arp | nd | prefix } peer peer-ip-address l3vni l3-vni**
- **show ip bgp evpn route { arp | nd | prefix } peer peer-ipv6-address l3vni l3-vni**
- **show ip bgp evpn route { mac | arp | nd } peer peer-ip-address l2vni l2-vni**
- **show ip bgp evpn route { mac | arp | nd } peer peer-ipv6-address l2vni l2-vni**

- **show ip bgp evpn route { mac | arp | nd | prefix | tunnel } peer peer-ip-address**
- **show ip bgp evpn route { mac | arp | nd | prefix | tunnel } peer peer-ipv6-address**

Parameter

Parameter	Description	Value
mac-ip	Specifies a MAC/IP route.	-
prefix	Specifies a route with the prefix IP.	-
tunnel	Specifies a Mcast label tunnel route.	-
ip-address	Specifies an IP address in the static ARP entry.	The value is in dotted decimal notation.
ipv6-address	Specifies an IPv6 address.	The address contains 128 bits and is a string of 16-bit hexadecimal digits separated by a colon (:).
mac-address	Specifies a MAC address.	The format is AA:BB:CC:DD:EE:FF, where A to F are hexadecimal digits.
tunnel-vni	Specifies a tunnel VNI.	The value is an integer ranging from 1 to 16777215.
peer-ip-address	Specifies a peer IPv4 address.	The value is in dotted decimal notation.
l2-vni	Specifies a Layer-2 VNI.	The value is an integer ranging from 1 to 16777215.
l3-vni	Specifies a Layer-3 VNI.	The value is an integer ranging from 1 to 16777215.
peer-ipv6-address	Specifies a peer IPv6 address.	The address contains 128 bits and is a string of 16-bit hexadecimal digits separated by a colon (:).

Default Value

NA

View

Common user view

Usage Guidelines

To enable dynamic VXLAN tunneling and MAC entry learning, you need to set a BGP neighbor for NVE and enable the EVPN address family function.

Example

Display the EVPN route.

```
Switch>show ip bgp evpn route
```

Summary of Route

mac 0

arp 0

nd 0

tnl 0

prefix 0

```
Switch>
```

5.7 ISIS Configuration Commands

5.7.1 area-authentication-mode

Function

The **area-authentication-mode** command sets an ISIS area to authenticate the received Level-1 route information packet (LSP and SNP) in the specified mode and password or adds the authentication information to the Level-1 packet to be sent.

Format

- **area-authentication-mode { all-send-only | default }**
- **area-authentication-mode snp-packet { authentication-avoid | send-only }**

Parameter

Parameter	Description	Value
all-send-only	Encapsulates the authentication information to the generated LSP and SNP packets but does not check the received LSP and SNP packets.	-
authentication-avoid	Neither encapsulates the authentication information to the generated SNP packets nor checks the received SNP packets. Only encapsulates the authentication information to the generated LSP packets and checks the received LSP packets.	-
send-only	Encapsulates the authentication information to the generated LSP and SNP packets. Check only the received LSP packets, but do not check the received SNP packets.	-

Default Value

NA

View

ISIS configuration view

Usage Guidelines

This command is only applicable to Level-1 or Level-1-2 routers.

Example

Set an ISIS area to authenticate received Level-1 route information packets in send-only mode and password.

```
Switch(config-isis-1)#area-authentication-mode all-send-only
Switch(config-isis-1)#
```

5.7.2 area-password

Function

The **area-password** command sets an authentication password for an ISIS area.

The **no area-password** command cancels the authentication password configured for an ISIS area.

Format

- **area-password** { **simple** | **md5** } { **cipher** | **plain** } *PASSWORD*
- **area-password** { **simple** | **md5** } *PASSWORD*
- **no area-password**

Parameter

Parameter	Description	Value
PASSWORD	Specifies a password.	The value is a string consisting of 1 to 16 characters.
cipher plain	Displays the password in cipher text or plain text.	-

Default Value

NA

View

ISIS configuration view

Usage Guidelines

You can run this command for all routers in an area to prevent an unauthenticated route with intruded error route information from entering the link state database. This command is applicable to Level 1 routers.

Example

Set an authentication password for an ISIS area.

```
Switch(config-isis-1)#area-password simple 11
Switch(config-isis-1)
```

5.7.3 cost-style**Function**

The **cost-style** command sets the cost style.

Format

**cost-style { narrow | wide | compatible | narrow-compatible | wide-compatible | default }
{ level-1 | level-2 }**

Parameter

Parameter	Description	Value
narrow	Specifies a narrow style (TLV=2/128/130).	-
wide	Specifies a wide style (TLV=22/135).	-
compatible	Receives and sends routes with the cost style of both narrow and wide.	-
narrow-compatible	Receives routes with the cost style of both narrow and wide, but sends only routes with the cost style of narrow.	-
wide-compatible	Receives routes with the cost style of both narrow and wide, but sends only routes with the cost style of narrow.	-
default	Specifies the default value.	Receives routes with the cost style of both narrow and wide, but sends only routes with the cost style of narrow.

Default Value

The system receives routes with the cost style of both narrow and wide, but sends only routes with the cost style of narrow.

View

ISIS configuration view

Usage Guidelines

NA

Example

Set the cost style.

```
Switch(config-isis-1)#cost-style narrow level-1
Switch(config-isis-1)#
```

5.7.4 debug isis**Function**

The **debug isis** command debugs the ISIS information.

The **no debug isis** command cancels debugging the ISIS information.

Format

- **debug isis { all | hello | csnp | psnp | lsp | pdu | interface | adj | route4 | route6 | restart | sync | leak | tlv | spf | memory | sysmsg | sys | frr | bfd | te | alarm | timer | redist4 | redist6 | snpdetail | cmd | error | update | sr | routemsg }**
- **no debug isis { all | hello | csnp | psnp | lsp | pdu | interface | adj | route4 | route6 | restart | sync | leak | tlv | spf | memory | sysmsg | sys | frr | bfd | te | alarm | timer | redist4 | redist6 | snpdetail | cmd | error | update | sr | routemsg }**

Parameter

Parameter	Description	Value
all	Displays all the preceding information.	-
hello	Debugs Hello packet information.	-
csnp	Debugs CSNP packet information.	-
psnp	Debugs PSNP information.	-
lsp	Debugs LSP information.	-
pdu	Debugs PDU information.	-
interface	Displays interface information.	-
adj	Debugs neighbor information.	-
route4	Specifies IPv4 route information.	-
route6	Specifies IPv6 route information.	-
restart	Debugs restart information.	-
sync	Displays debugging information about synchronization.	-
leak	Debugs route leakage information.	-
tlv	Debugs TLV operation information.	-
spf	Debugs route calculation information.	-
memory	Debugs memory operation information.	-
sysmsg	Debugs system kernel information.	-

Parameter	Description	Value
all	Displays all the preceding information.	-
hello	Debugs Hello packet information.	-
csnp	Debugs CSNP packet information.	-
psnp	Debugs PSNP information.	-
lsp	Debugs LSP information.	-
pdu	Debugs PDU information.	-
interface	Displays interface information.	-
adj	Debugs neighbor information.	-
route4	Specifies IPv4 route information.	-
route6	Specifies IPv6 route information.	-
restart	Debugs restart information.	-
sync	Displays debugging information about synchronization.	-
sys	Debugs system information.	-
frr	Debugs FRR information.	-
bfd	Debugs BFD information.	-
te	Debugs TE information.	-
alarm	Alarms	-
timer	Debugs timer timeout information.	-
redist4	Debugs V4 redistribution information.	-
redist6	Debugs V6 redistribution information.	-
snpdetail	Debugs SNP details.	-
cmd	Debugs CMD information.	-
error	Debugs all error information.	-
update	Debugs update information.	-
sr	Debugs the summary.	-
routemsg	Debugs the route message.	-

Default Value

NA

View

Privileged user view

Usage Guidelines

You can run this command to debug the ISIS information.

Example

Debug the ISIS information.

```
Switch>debug isis all
```

```
Switch>
```

5.7.5 default-route-originate

Function

The **domain-authentication-mode** command generates a default route for an ISIS router.

Format

- **default-route-originate { none | level-1 | level-2 | level-1-2 }**
- **default-route-originate ipv6 { none | level-1 | level-2 | level-1-2 }**

Parameter

NA

Default Value

NA

View

ISIS configuration view

Usage Guidelines

This command is only applicable to Level-1 or Level-2 routers.

Example

Generate a default route for an ISIS router.

```
Switch(config-isis-1)#default-route-originate level-1
Switch(config-isis-1)#
```

5.7.6 domain-authentication-mode

Function

The **domain-authentication-mode** command sets an ISIS area to authenticate the received Level-2 route information packet (LSP and SNP) in the specified mode and password.

Format

- **domain-authentication-mode { all-send-only | default }**
- **domain-authentication-mode snp-packet { authentication-avoid | send-only }**

Parameter

Parameter	Description	Value
all-send-only	Encapsulates the authentication information to the generated LSP and SNP packets but does not check the received LSP and SNP packets.	-
authentication-avoid	Neither encapsulates the authentication information to the generated SNP packets nor checks the received SNP packets. Only encapsulates the authentication information to the generated LSP packets and checks the received LSP packets.	-
send-only	Encapsulates the authentication information to the generated LSP and SNP packets. Check only the received LSP packets, but do not check the received SNP packets.	-

Default Value

NA

View

ISIS configuration view

Usage Guidelines

This command is only applicable to Level-2 or Level-1-2 routers.

Example

Set an ISIS area to authenticate received Level-2 route information packets in the specified mode and password.

```
Switch(config-isis-1)#domain-authentication-mode all-send-only
Switch(config-isis-1)#
```

5.7.7 domain-password

Function

The **domain-password** command sets an authentication password for an ISIS route.

The **no domain-password** command cancels the authentication password configured for an ISIS route.

Format

- **domain-password** { **simple** | **md5** } *PASSWORD*
- **domain-password** { **simple** | **md5** } { **cipher** | **plain** } *PASSWORD*
- **no domain-password**

Parameter

Parameter	Description	Value
PASSWORD	Specifies a password.	The value is a character string.

Default Value

NA

View

ISIS configuration view

Usage Guidelines

You can run this command for all routers in an area to prevent an unauthenticated route with intruded error route information from entering the link state database. This command is applicable to Level 2 routers.

Example

```
Switch(config-isis-1)#domain-password simple 11
Switch(config-isis-1)#
```

5.7.8 filter-policy import route-policy

Function

The **filter-policy import route-policy** command sets a filter policy when adding an ISIS route to an IP routing table.

The **no filter-policy import route-policy** command cancels the configured filter policy.

Format

- **filter-policy import route-policy** *policy-name*
- **no filter-policy import route-policy**

Parameter

Parameter	Description	Value
policy-name	Specifies the name of a route filter policy.	The value is a character string.

Default Value

By default, no filter policy is configured.

View

ISIS configuration view

Usage Guidelines

NA

Example

Set a filter policy when adding an ISIS route to an IP routing table.

```
Switch(config-isis-1)#filter-policy import route-policy policy1
Switch(config-isis-1)#
```

5.7.9 frr {enable|disable}

Function

The **frr {enable|disable}** command enables or disables the FRR function.

Format

frr { enable | disable }

Parameter

Parameter	Description	Value
enable	Enables the FRR function.	-
disable	Disables the FRR function.	-

Default Value

Disable

View

ISIS configuration view

Usage Guidelines

NA

Example

Enable the FRR function.

```
Switch(config-isis-1)#frr enable
Switch(config-isis-1)#
```

5.7.10 frr noloop

Function

The **frr noloop {enable|disable}** command enables or disables the no-loop FRR function.

Format

frr noloop { enable | disable }

Parameter

Parameter	Description	Value
enable	Enables the no-loop FRR function.	-
disable	Disables the no-loop FRR function.	-

Default Value

Disable

View

ISIS configuration view

Usage Guidelines

NA

Example

Enable the no-loop FRR function.

```
Switch(config-isis-1)#frr noloop enable
Switch(config-isis-1)#
```

5.7.11 graceful-restart {enable|disable}

Function

The **graceful-restart {enable|disable}** command enables or disables the ISIS graceful restart function.

Format

- **graceful-restart enable**
- **graceful-restart disable**

Parameter

Parameter	Description	Value
enable	Enables the ISIS graceful restart function.	-
disable	Disables the ISIS graceful restart function.	-

Default Value

NA

View

ISIS configuration view

Usage Guidelines

NA

Example

Enable the ISIS graceful restart function.

```
Switch(config-router-isis)#graceful-restart enable
Switch(config-router-isis)#
```

5.7.12 hostname**Function**The **hostname** command sets a name for an ISIS host.The **no hostname** command deletes an ISIS host name.**Format**

- **hostname** *hostname*
- **no hostname**

Parameter

Parameter	Description	Value
hostname	Specifies an ISIS host name.	The value is a string of 1-30 bytes.

Default Value

NA

View

ISIS configuration view

Usage Guidelines

NA

Example

Set the ISIS host name to Switchisis.

```
Switch(config-router-isis)#hostname Switchisis
```



```
Switch(config-router-isis)#
```

5.7.13 ignore-lsp-errors

Function

The **ignore-lsp-errors** command sets whether to check the checksum of the received LSP packets.

The **no ignore-lsp-errors** command disables this function.

Format

- **ignore-lsp-errors** { **level-1** | **level-2** }
- **no ignore-lsp-errors** { **level-1** | **level-2** }

Parameter

NA

Default Value

Disable

View

ISIS configuration view

Usage Guidelines

If you enable a router to ignore received ISIS link state packets with incorrect checksum, run this command not to report the error packets.

Example

Set whether to check the checksum of the received LSP packets.

```
Switch(config-isis-1)#ignore-lsp-errors level-1
Switch(config-isis-1)#
```

5.7.14 ip router isis

Function

The **ip router isis** command enables an ISIS route process on an interface.

The **no ip router isis** command cancels the process.

Format

- **ip router isis** [*instance-id*]

- **no ip router isis**

Parameter

Parameter	Description	Value
instance-id	Specifies an ISIS instance ID.	The value is an integer ranging from 1 to 65535.

Default Value

NA

View

VLANIF configuration view, loopback interface configuration view, Ethernet routing interface configuration view, BD interface configuration view

Usage Guidelines

You can run this command to enable this function on an interface. In wired networks, the interface must have an IP address and the interface route process name must be the same as the route process name. If the route process name of the specified interface is not available, leave this field blank. If multiple areas are specified, this field cannot be blank. If only one process is specified, this field can be blank.

Example

Enable the ISIS route process for an instance with ID 10.

```
Switch(config-vlanif-100)#ip router isis 10
Switch(config-vlanif-100)#
```

5.7.15 ipv6 preference**Function**

The **ipv6 preference** command sets the priority of the IPv6 route generated by the ISIS protocol.

Format

ipv6 preference { *value* | **default** }

Parameter

Parameter	Description	Value
value	Specifies a protocol priority.	The value is an integer ranging from 1 to 255. A smaller value indicates a higher priority.
default	Specifies the default protocol priority.	50

Default Value

50

View

ISIS configuration view

Usage Guidelines

One router may have multiple dynamic routing protocols, and route sharing and selection exist. The system sets a priority for each routing protocol. When multiple routing protocols discover routes to the same destination address, the protocol with a higher priority prevails.

Example

Set the router ID for ISIS.

```
Switch(config-isis-1)#ipv6 precedence 10
Switch(config-isis-1)#
```

5.7.16 ipv6 router isis**Function**

The **ipv6 router isis** command enables an ISIS route process on an interface. The **no ipv6 router isis** command cancels the process.

Format

- **ipv6 router isis** [*instance-id*]
- **no ipv6 router isis**

Parameter

Parameter	Description	Value
instance-id	Specifies an ISIS instance ID.	The value is an integer ranging from 1 to 65535.

Default Value

NA

View

VLANIF configuration view, loopback interface configuration view, Ethernet routing interface configuration view, BD interface configuration view

Usage Guidelines

NA

Example

Enable an ISIS route process on the instance IPV6.

```
Switch(config-vlanif-2)#ipv6 router isis
Switch(config-vlanif-2)#
```

5.7.17 isis bfd {enable|disable}

Function

The **isis bfd {enable|disable}** command enables or disables BFD for an ISIS interface to create BFD session with default parameters.

Format

isis bfd { enable | disable }

Parameter

Parameter	Description	Value
enable	Enables BFD for an ISIS interface to create BFD session with default parameters.	-
disable	Disables BFD for an ISIS interface to create BFD session with default parameters.	-

Default Value

Disable

View

VLANIF configuration view, loopback interface configuration view, Ethernet routing interface configuration view, BD interface configuration view

Usage Guidelines

If BFD is not enabled globally, you can configure BFD parameters for the interface but cannot create an BFD session. The BFD priority configured by an interface is higher than that configured by a process. If BFD is enabled for an interface, a BFD session is created based on the above BFD parameters of the interface.

Example

Enable the BFD feature of the interface VLAN1.

```
Switch(config-vlanif-1)#isis bfd enable
```

```
Switch(config-vlanif-1)#
```

5.7.18 isis circuit-ext-domain

Function

The **isis circuit-ext-domain** command suppresses ISIS protocol data units that do not transmit the internal domains through the specified connection.

The **no isis circuit-ext-domain** command cancels the configuration.

Format

- **isis circuit-ext-domain**
- **no isis circuit-ext-domain**

Parameter

NA

Default Value

Suppression is not configured by default.

View

VLANIF configuration view, loopback interface configuration view, Ethernet routing interface configuration view, BD interface configuration view

Usage Guidelines

NA

Example

Suppress ISIS protocol data units that do not transmit the internal domains through the specified connection.

```
Switch(config-vlanif-100)#isis circuit-ext-domain
Switch(config-vlanif-100)#
```

5.7.19 isis circuit-level

Function

The **isis circui-level** command sets the circuit level. The **no isis circui-level** command restores the default state level-1-2.

Format

- **isis circuit-level { level-1 | level-2 | level-1-2 }**
- **no isis circuit-level**

Parameter

NA

Default Value

The circuit level is level-1-2.

View

VLANIF configuration view, loopback interface configuration view, Ethernet routing interface configuration view, BD interface configuration view

Usage Guidelines

The circuit level does not need to be configured generally. You can run this command to set the circuit level to save the bandwidth.

Example

Set the circuit level to level-2.

```
Switch(config-vlanif-100)#isis circuit-level level-2
Switch(config-vlanif-100)#
```

5.7.20 isis circuit-type**Function**

The **isis circuit-type** command sets the ISIS link type.

Format

isis circuit-type { broadcast | ppp }

Parameter

Parameter	Description	Value
broadcast	Specifies a broadcast type.	-
ppp	Specifies a PPP type.	-

Default Value

broadcast

View

VLANIF configuration view, loopback interface configuration view, Ethernet routing interface configuration view, BD interface configuration view

Usage Guidelines

NA

Example

Set the ISIS link type to PPP.

```
Switch(config-vlanif-100)# isis circuit-type ppp
Switch(config-vlanif-100)#
```

5.7.21 isis csnp-interval

Function

The **isis csnp-interval** command sets the sending interval of CSNP packets of a specified layer.

The **no isis csnp-interval** command restores the default value.

Format

- **isis csnp-interval** { **level-1** | **level-2** | **ppp** } *interval-value*
- **no isis csnp-interval** { **level-1** | **level-2** | **ppp** }

Parameter

Parameter	Description	Value
interval-value	Specifies an interval for sending CSNP data units.	The value is an integer ranging from 1 to 600, in seconds.
ppp	Specifies a PPP type.	-

Default Value

10

View

VLANIF configuration view, loopback interface configuration view, Ethernet routing interface configuration view, BD interface configuration view

Usage Guidelines

CSNP indicates a PDU with a complete serial number. The CSNP packets are sent through the specified router to keep synchronization with the database. This function is not applicable to serial

P2P interfaces. If a WAN can serve as a multi-access network grid, it can be used for WAN connection.

Example

```
Switch(config-vlanif-2)#isis csnp-interval level-1 20
Switch(config-vlanif-2)#
```

5.7.22 isis default-metric

Function

The **isis default-metric** command sets the metric value for the interface. The **no isis default-metric** command restores the default value.

Format

- **isis default-metric { level-1 | level-2 | ppp } metric-value**
- **no isis default- metric { level-1 | level-2 | ppp }**

Parameter

Parameter	Description	Value
metric-value	Specifies a metric value for the specified link interface.	The value is an integer ranging from 0 to 63.
default	Specifies the default metric value for the specified link interface.	10
ppp	Specifies a PPP type.	-

Default Value

10

View

VLANIF configuration view, loopback interface configuration view, Ethernet routing interface configuration view, BD interface configuration view

Usage Guidelines

You can run this command to set a metric value for an interface of a level-1 or level-2 router.

Example

Set the interface metric value to 20.

```
Switch(config-vlanif-2)#isis default-metric level-1 20
Switch(config-vlanif-2)#
```


5.7.23 isis fast-sense neighbor

Function

The **isis fast-sense neighbor** command sets the fast neighbor sensing time.

The **no isis fast-sense neighbor** command cancels the configuration.

Format

- **isis fast-sense neighbor { level-1 | level-2 | ppp } value**
- **no isis fast-sense neighbor { level-1 | level-2 | ppp }**

Parameter

Parameter	Description	Value
value	Specifies a sending interval for hello packets, in milliseconds.	The value is an integer ranging from 200 to 3000.

Default Value

NA

View

VLANIF configuration view, loopback interface configuration view, Ethernet routing interface configuration view, BD interface configuration view

Usage Guidelines

When ISIS BFD is not configured, you can run this command to reduce the time for detecting the neighbor state and accelerate link state convergence, but the interface accelerates sending neighbor packets, increasing the device load.

Example

Set the fast neighbor sensing time.

```
Switch(config-vlanif-2)#isis fast-sense neighbor level-1 200
Switch(config-vlanif-2)#
```

5.7.24 isis graceful-restart

Function

The **isis graceful-restart** command enables the ISIS graceful restart function.

Format

isis graceful-restart

Parameter

NA

Default Value

NA

View

ISIS configuration view

Usage Guidelines

NA

Example

Enable the ISIS graceful restart function.

```
Switch(config-isis-1)#isis graceful-restart
```

```
Switch(config-isis-1)#
```

5.7.25 isis hello padding**Function**

The **isis hello padding** command fills an ISIS hello packet size to MTU of a specified interface in a broadcast network.

The **no isis hello padding** command cancels the configuration.

Format

- **isis hello padding**
- **no isis hello padding**

Parameter

NA

Default Value

NA

View

VLANIF configuration view, loopback interface configuration view, Ethernet routing interface configuration view, BD interface configuration view

Usage Guidelines

You can run this command to fill an ISIS hello packet size to MTU of a specified interface in a broadcast network.

Example

Set to fill an ISIS hello packet size to MTU.

```
Switch(config-vlanif-100)#isis hello padding
Switch(config-vlanif-100)#
```

5.7.26 isis hello-interval

Function

The **isis hello-interval** command sets the interval of sending ISIS hello packets.

The **no isis hello-interval** command restores the default value.

Format

- **isis hello-interval** { **level-1** | **level-2** | **ppp** } *interval-value*
- **no isis hello-interval** { **level-1** | **level-2** | **ppp** }

Parameter

Parameter	Description	Value
interval-value	Specifies an ISIS handshake interval.	The value is an integer ranging from 3 to 255, in seconds.
default	Specifies the default interval of sending hello packets.	10 seconds
ppp	Specifies a PPP type.	-

Default Value

10

View

VLANIF configuration view, loopback interface configuration view, Ethernet routing interface configuration view, BD interface configuration view

Usage Guidelines

You can run this command to set the hello packet sending interval for Level 1 or Level 2 routers.

Example

Set the interval of sending ISIS hello packets.

```
Switch(config-vlanif-2)#isis hello-interval level-1 4
Switch(config-vlanif-2)#
```

5.7.27 isis hello-multiplier

Function

The **isis hello-multiplier** command sets the multiplier of ISIS hello packet retention interval.

The **no isis hello- multiplier** command restores the default value.

Format

- **isis hello-multiplier** { **level-1** | **level-2** | **ppp** } *multiple-value*
- **no isis hello- multiplier** { **level-1** | **level-2** | **ppp** }

Parameter

Parameter	Description	Value
multiple-value	Specifies the multiplier of hello packet retention interval.	The value is an integer ranging from 2 to 100.
default	Specifies the default multiplier of hello packet retention interval.	3
ppp	Specifies a PPP type.	-

Default Value

3

View

VLANIF configuration view, loopback interface configuration view, Ethernet routing interface configuration view, BD interface configuration view

Usage Guidelines

You can run this command to set the multiplier of hello packet retention interval, that is, how many ISIS hello packets from the neighbor must be discarded by the router before the router declares that its neighbor is not reachable.

Example

Set the multiplier of ISIS hello packet retention interval.

```
Switch(config-vlanif-2)#isis hello-multiplier level-1 20
Switch(config-vlanif-2)#
```

5.7.28 isis ipv6 bfd {enable|disable}

Function

The **isis ipv6 bfd {enable|disable}** command enables or disables the feature for a VLAN interface.

Format

isis ipv6 bfd { enable | disable }

Parameter

Parameter	Description	Value
enable	Enables the BFD feature. After the BFD feature is enabled, the switch can quickly detect ISIS neighbor disconnection.	-
disable	Disables the BFD feature.	-

Default Value

NA

View

VLANIF configuration view, loopback interface configuration view, Ethernet routing interface configuration view, BD interface configuration view

Usage Guidelines

NA

Example

Enable the BFD feature.

```
Switch(config-vlanif-3)#isis ipv6 bfd enable
Switch(config-vlanif-3)#
```

5.7.29 isis mesh-group

Function

The **isis mesh-group** command sets a mesh group and group ID for the ISIS interface or sets the state of the mesh group to **Blocked**.

The **no isis mesh-group** command cancels the configuration.

Format

- **isis mesh-group** *group-value*

- **isis mesh-group blocked**
- **no isis mesh-group**

Parameter

Parameter	Description	Value
group-value	Specifies the error metric value of an ISIS interface.	The value is an integer ranging from 1 to 65535.

Default Value

By default, the mesh group is not configured.

View

VLANIF configuration view, loopback interface configuration view, Ethernet routing interface configuration view, BD interface configuration view

Usage Guidelines

NA

Example

Set a mesh group for the ISIS interface and specify the group ID to 100.

```
Switch(config-vlanif-100)#isis mesh group 100
Switch(config-vlanif-100)#
```

5.7.30 isis passive-interface**Function**

The **isis passive-interface** command sets the interface mode to passive to avoid packet sending.

The **no isis passive-interface** command cancels the configuration.

Format

- **isis passive-interface**
- **no isis passive-interface**

Parameter

NA

Default Value

NA

View

VLANIF configuration view, loopback interface configuration view, Ethernet routing interface configuration view, BD interface configuration view

Usage Guidelines

NA

Example

Set the interface mode to passive to avoid packet sending.

```
Switch(config-vlanif-100)#isis passive-interface
Switch(config-vlanif-100)#
```

5.7.31 isis password**Function**

The **isis password** command sets an authentication password for the interface.

The **no isis password** command cancels the configured authentication password.

Format

- **isis password** { **simple** | **md5** } *PASSWORD* { **level-1** | **level-2** | **ppp** }
- **isis password** { **simple** | **md5** } { **cipher** | **plain** } *PASSWORD* { **level-1** | **level-2** | **ppp** }
- **no isis password** { **level-1** | **level-2** | **ppp** }

Parameter

Parameter	Description	Value
PASSWORD	Specifies a password.	-
ppp	Specifies a PPP type.	-

Default Value

No. You must set an authentication password for Level-1 | level-2| ppp.

View

VLANIF configuration view, loopback interface configuration view, Ethernet routing interface configuration view, BD interface configuration view

Usage Guidelines

You can run this command to prevent generating a neighbor relationship between an unauthenticated router and the specified router, to prevent the network from attacks. Level 1 routers can serve only as site routers, and Level 2 routers can serve only as area routers.

Example

Set an authentication password for the interface.

```
Switch(config-vlanif-2)#isis password simple 222 level-1
Switch(config-vlanif-2)#
```

5.7.32 isis priority

Function

The **isis priority** command sets the priority of a specified router.

The **no isis priority** command restores the default value.

Format

- **isis priority** { **level-1** | **level-2** } *priority-value*
- **no isis priority** { **level-1** | **level-2** }

Parameter

Parameter	Description	Value
priority-value	Specifies the priority value range of a router.	The value is an integer ranging from 0 to 127.

Default Value

64

View

VLANIF configuration view, loopback interface configuration view, Ethernet routing interface configuration view, BD interface configuration view

Usage Guidelines

You can run this command to set the priority of a specified router to specify which router in a LAN as the specified router or intermediate system. A router with a high priority or priority 0 can serve as the specified router or intermediate system. When the priority is the same, the router with a larger MAC address (System ID) serves as the specified router or intermediate system.

Example

Set the priority of a specified router.

```
Switch(config-vlanif-100)#isis priority level-1 20
Switch(config-vlanif-100)#
```

5.7.33 isis psnp-interval

Function

The **isis psnp-interval** command sets the sending interval of PSNP packets of a specified layer.

The **no isis psnp-interval** command restores the default value.

Format

- **isis psnp-interval** { **level-1** | **level-2** | **ppp** } *interval-value*
- **no isis psnp-interval** { **level-1** | **level-2** | **ppp** }

Parameter

Parameter	Description	Value
interval-value	Specifies the sending interval of ISIS PSNP packets.	The value is an integer ranging from 1 to 120, in seconds.
ppp	Specifies a PPP type.	-

Default Value

2

View

VLANIF configuration view, loopback interface configuration view, Ethernet routing interface configuration view, BD interface configuration view

Usage Guidelines

NA

Example

Set the sending interval of PSNP packets of a specified layer.

```
Switch(config-vlanif-2)#isis psnp-interval level-1 20
Switch(config-vlanif-2)#
```

5.7.34 isis three-way-handshake

Function

The **isis three-way-handshake** command sets the ISIS three-way handshake function for a VLAN interface.

The **no isis three-way-handshake** command cancels the configuration.

Format

- **isis three-way-handshake**
- **no isis three-way-handshake**

Parameter

NA

Default Value

NA

View

VLANIF configuration view, loopback interface configuration view, Ethernet routing interface configuration view, BD interface configuration view

Usage Guidelines

NA

Example

Set the ISIS three-way handshake function for a VLAN interface.

```
Switch(config-vlanif-100)#isis three-way-handshake
Switch(config-vlanif-100)#
```

5.7.35 isis wide-metric

Function

The **isis wide-metric** command sets the outbound cost style.

The **no isis wide-metric** command cancels the configured outbound cost style.

Format

- **isis wide-metric { level-1 | level-2 | ppp } metric**
- **no isis wide-metric { level-1 | level-2 | ppp }**

Parameter

Parameter	Description	Value

Parameter	Description	Value
metric	Specifies an outbound cost style.	The value is an integer ranging from 0 to 16777215.
ppp	Specifies a PPP type.	-

Default Value

10

View

VLANIF configuration view, loopback interface configuration view, Ethernet routing interface configuration view, BD interface configuration view

Usage Guidelines

NA

Example

Set the outbound cost style.

```
Switch(config-vlanif-1)#isis wide-metric level-1 100
Switch(config-vlanif-1)#
```

5.7.36 is-type**Function**

The **is-type** command sets the router level.

Format

is-type { level-1 | level-1-2 | level-2 }

Parameter

NA

Default Value

Level-1-2 (site and area routers)

View

ISIS configuration view

Usage Guidelines

You can run this command to set the router level, better the router type. In pure CLNS scenarios, use level-1 routers. In pure IP scenarios, use level-2-only routers.

Example

Set the router level to level-1.

```
Switch(config-isis-1)#is-type level-1
Switch(config-isis-1)#
```

5.7.37 lsp-generation max-interval**Function**

The **lsp-generation max-interval** command sets the delay for a specified ISIS process to generate LSP packets.

Format

lsp-generation max-interval { *max-interval* | **default** } **init-interval** { *int-interval* | **default** } **incr-interval** { *incr-interval* | **default** } { **level-1** | **level-2** }

Parameter

Parameter	Description	Value
max-interval	Specifies the maximum delay for a specified ISIS process to generate LSP packets with the same LSP ID.	The value is an integer ranging from 1 to 120, in seconds. The default value is 2.
int-interval	Specifies the delay for generating the first LSP packet.	The value is an integer ranging from 1 to 60000, in milliseconds. By default, this delay time is not set.
incr-interval	Specifies the incremental delay for generating two LSP packets with the same LSP ID.	The value is an integer ranging from 1 to 60000, in milliseconds. By default, this delay time is not set.
level-1	Specifies the delay for a level-1 router to generate Level-1 LSP packets. If no level is configured, specify the delay for generating both Level-1 and Level-2 LSP packets.	-
level-2	Specifies the delay for a level-2 router to generate Level-2 LSP packets. If no level is configured, specify the delay for generating both Level-1 and Level-2 LSP packets.	-

Default Value

The default value of Max-interval is 2.

View

ISIS configuration view

Usage Guidelines

If the delay for generating LSP packets is too long, changes to the local route cannot be notified to the neighbor in time, slowing the network convergence.

Example

Set the maximum delay for a specified ISIS process to generate LSP packets to 80s.

```
Switch(config-isis-1)#lsp-generation max-interval 80 init-interval default incr-interval default level1
Switch(config-isis-1)#
```

5.7.38 lsp-refresh-interval**Function**

The **lsp-refresh-interval** command sets the refresh interval of link state packets for a router.

The **no lsp-refresh-interval** command restores the default value.

Format

- **lsp-refresh-interval** *interval-value*
- **no lsp-refresh-interval**

Parameter

Parameter	Description	Value
interval-value	Specifies the refresh interval of link state packets for a router.	The value is an integer ranging from 1 to 65235, in seconds.

Default Value

900

View

ISIS configuration view

Usage Guidelines

You can run this command to set the refresh interval of link state packets for a router. The value must be smaller than the maximum life time of the link state packets.

Example

Set the refresh interval of link state packets for a router to 1000s.

```
Switch(config-router-isis)#lsp-refresh-interval 1000
Switch(config-router-isis)#
```

5.7.39 maximum load-balancing

Function

The **maximum load-balancing** command sets the maximum number of ECMP routes for load balancing.

Format

maximum load-balancing { *load-balancing-number* | **default** }

Parameter

Parameter	Description	Value
load-balancing-number	Specifies the maximum number of ECMP routes for load balancing.	The value is an integer ranging from 1 to 16.
default	Specifies the default maximum number of ECMP routes for load balancing.	16

Default Value

16

View

ISIS configuration view

Usage Guidelines

NA

Example

Set the maximum number of ECMP routes for load balancing.

```
Switch(config-router-isis)#maximum load-balancing 2
Switch(config-router-isis)#
```

5.7.40 max-lsp-lifetime

Function

The **max-lsp-lifetime** command sets the maximum life time of a link state packet of a router in a database when the link state packet is not refreshed.

The **no max-lsp-lifetime** command restores the default value.

Format

- **max-lsp-lifetime** *lifetime*

- **no max-lsp-lifetime**

Parameter

Parameter	Description	Value
lifetime	Specifies the maximum life time of a link state packet of a router in a database when the link state packet is not refreshed.	The value is an integer ranging from 350 to 65535, in seconds.

Default Value

1200

View

ISIS configuration view

Usage Guidelines

You can run this command to set the maximum life time of a link state packet of a router in a database when the link state packet is not refreshed. The refresh interval of the link state packet must be smaller than its maximum life time.

Example

Set the maximum life time of a link state packet of a router in a database when the link state packet is not refreshed to 2000s.

```
Switch(config-router-isis)#max-lsp-lifetime 2000
Switch(config-router-isis)#
```

5.7.41 net**Function**

The **net** command sets an ISIS network entity title for a route process.

The **no net** command cancels the configuration.

Format

- **net** *network-entity-title*
- **no net** *network-entity-title*

Parameter

Parameter	Description	Value
network-entity-title	Specifies a network entity title (address or name).	-

Default Value

NA

View

ISIS configuration view

Usage Guidelines

You can run this command to set one to three ISIS network entity titles for a route process. The network entity title must contain 8 to 20 bytes (8 and 20 are inclusive), and the last byte n-selector must be zero. The six bytes before the last byte n-selector indicate the system ID (with a fixed length). All bytes before the system ID indicate the area ID. When multiple network entity titles are configured, the system IDs must be the same and one area has multiple area IDs to facilitate area merging or division.

Example

Set an ISIS network entity for a router.

```
Switch(config)#router isis 1
Switch(config-isis-1)#net 47.004d.0000.0c11.00
```

5.7.42 redistribute**Function**

The **redistribute** command sets an ISIS interface to redistribute the routes learned by a direct port or static route or other routing protocols.

The **no redistribute** command cancels redistribution.

Format

- **redistribute** { **connect** | **static** | **rip** | **ospf** | **bgp** | **isis** }
- **redistribute** { **connect** | **static** | **rip** | **ospf** | **bgp** | **isis** } { **level-1** | **level-2** | **level-1-2** }
- **redistribute** { **connect** | **static** | **rip** | **ospf** | **bgp** | **isis** } { **level-1** | **level-2** | **level-1-2** } *route-policy policy-name*
- **redistribute** { **connect** | **static** | **rip** | **ospf** | **bgp** | **isis** } *route-policy policy-name*
- **redistribute** { **connect** | **static** | **rip** | **ospf** | **bgp** | **isis** } **cost** { *cost-value* | **default** }
- **redistribute** { **connect** | **static** | **rip** | **ospf** | **bgp** | **isis** } **cost** { *cost-value* | **default** } { **level-1** | **level-2** | **level-1-2** }

- **redistribute { connect | static | rip | ospf | bgp | isis } cost { cost-value | default } { level-1 | level-2 | level-1-2 } route-policy policy-name**
- **redistribute { connect | static | rip | ospf | bgp | isis } cost { cost-value | default } route-policy policy-name**
- **redistribute { connect | static | rip | ospf | bgp | isis } inherit-cost**
- **redistribute { connect | static | rip | ospf | bgp | isis } inherit-cost { level-1 | level-2 | level-1-2 }**
- **redistribute { connect | static | rip | ospf | bgp | isis } inherit-cost { level-1 | level-2 | level-1-2 } route-policy policy-name**
- **redistribute { connect | static | rip | ospf | bgp | isis } inherit-cost route-policy policy-name**
- **redistribute { connect | static | rip | ospf | bgp | isis } route-policy policy-name**
- **redistribute { rip | ospf | isis } process-id**
- **redistribute { rip | ospf | isis } process-id { level-1 | level-2 | level-1-2 }**
- **redistribute { rip | ospf | isis } process-id { level-1 | level-2 | level-1-2 } route-policy policy-name**
- **redistribute { rip | ospf | isis } process-id cost { cost-value | default }**
- **redistribute { rip | ospf | isis } process-id cost { cost-value | default } { level-1 | level-2 | level-1-2 }**
- **redistribute { rip | ospf | isis } process-id cost { cost-value | default } { level-1 | level-2 | level-1-2 } route-policy policy-name**
- **redistribute { rip | ospf | isis } process-id cost { cost-value | default } route-policy policy-name**
- **redistribute { rip | ospf | isis } process-id inherit-cost**
- **redistribute { rip | ospf | isis } process-id inherit-cost { level-1 | level-2 | level-1-2 }**
- **redistribute { rip | ospf | isis } process-id inherit-cost { level-1 | level-2 | level-1-2 } route-policy policy-name**
- **redistribute { rip | ospf | isis } process-id inherit-cost route-policy policy-name**
- **redistribute { rip | ospf | isis } process-id route-policy policy-name**
- **redistribute ipv6 { connect | static | rip | ospf | bgp | isis }**

- **redistribute ipv6 { connect | static | rip | ospf | bgp | isis } { level-1 | level-2 | level-1-2 }**
- **redistribute ipv6 { connect | static | rip | ospf | bgp | isis } { level-1 | level-2 | level-1-2 } route-policy *policy-name***
- **redistribute ipv6 { connect | static | rip | ospf | bgp | isis } cost { *cost-value* | default }**
- **redistribute ipv6 { connect | static | rip | ospf | bgp | isis } cost { *cost-value* | default } { level-1 | level-2 | level-1-2 }**
- **redistribute ipv6 { connect | static | rip | ospf | bgp | isis } inherit-cost**
- **redistribute ipv6 { connect | static | rip | ospf | bgp | isis } inherit-cost { level-1 | level-2 | level-1-2 }**
- **redistribute ipv6 { connect | static | rip | ospf | bgp | isis } route-policy *policy-name***
- **redistribute ipv6 { rip | ospf | isis } *process-id* { level-1 | level-2 | level-1-2 }**
- **redistribute ipv6 { rip | ospf | isis } *process-id* { level-1 | level-2 | level-1-2 } route-policy *policy-name***
- **redistribute ipv6 { rip | ospf | isis } *process-id* cost { *cost-value* | default }**
- **redistribute ipv6 { rip | ospf | isis } *process-id* cost { *cost-value* | default } { level-1 | level-2 | level-1-2 }**
- **redistribute ipv6 { rip | ospf | isis } *process-id* inherit-cost**
- **redistribute ipv6 { rip | ospf | isis } *process-id* inherit-cost { level-1 | level-2 | level-1-2 }**
- **redistribute ipv6 { rip | ospf | isis } *process-id* route-policy *policy-name***
- **no redistribute { connect | static | rip | ospf | bgp | isis }**
- **no redistribute { rip | ospf | isis } *process-id***
- **no redistribute { connect | static | rip | ospf | bgp | isis } route-policy**
- **no redistribute { rip | ospf | isis } *process-id* route-policy**
- **no redistribute ipv6 { connect | static | rip | ospf | bgp | isis }**
- **no redistribute ipv6 { connect | static | rip | ospf | bgp | isis } route-policy**
- **no redistribute ipv6 { rip | ospf | isis } *process-id***
- **no redistribute ipv6 { rip | ospf | isis } *process-id* route-policy**

Parameter

Parameter	Description	Value
policy-name	Specifies the name of a routing policy.	The value is a string consisting of up to 32 bytes.
process-id	Specifies a routing protocol process ID.	The value is an integer ranging from 1 to 65535.
cost-value	Specifies a cost value.	The value is an integer ranging from 0 to 4261412864.

Default Value

NA

View

ISIS routing configuration view

Usage Guidelines

By default, the ISIS routing protocol does not send any non-ISIS route information. To enable OSPF to send such information, you must enable ISIS route redistribution.

You can run this command to enable ISIS to notify the routes learned from the directly connected port to a neighbor router.

Example

Enable ISIS to redistribute the routes learned from the directly connected port.

```
Switch(config-isis-1)#redistribute connect level-1
Switch(config-isis-1)#
```

5.7.43 redistribute level-2 to level-1

Function

The **redistribute level-2 to level-1** command redirects a level 2 route to level 1.

The **no redistribute level-2 to level-1** command cancels the configuration.

Format

- **redistribute level-2 to level-1**
- **no redistribute level-2 to level-1**

Parameter

NA

Default Value

NA

View

ISIS routing configuration view

Usage Guidelines

NA

Example

Redirect a level 2 route to level 1.

```
Switch(config-isis-1)#redistribute level-2 to level-1
Switch(config-isis-1)#
```

5.7.44 router isis**Function**

The **router isis** command enables the ISIS routing protocol and specifies the ISIS route process.

The **no router isis** command disables the ISIS routing protocol.

Format

- **router isis**
- **router isis** *isis-instance-id*
- **router isis vpn-instance** *name*
- **router isis** *isis-instance-id* **vpn-instance** *name*
- **no router isis**
- **no router isis** *isis-instance-id*
- **no router isis all**

Parameter

Parameter	Description	Value
isis-instance-id	Specifies an ISIS instance ID.	The value is an integer ranging from 1 to 65535.
name	Specifies a VPN instance name.	The value is a string of no more than 64 characters.

Default Value

NA

View

Global configuration view

Usage Guidelines

You can run this command to enable the ISIS routing protocol and specify the ISIS route process. Only one process can be started.

Example

Enter the router ISIS view.

```
Switch(config)#router isis 10
Switch(config-isis-10)#
```

5.7.45 router-id**Function**

The **router-id** command sets the ISIS router ID.

The **no router-id** command deletes the ISIS router ID.

Format

- **router-id** *ipv4-address* { **level-1** | **level-2** }
- **no router-id** { **level-1** | **level-2** }

Parameter

Parameter	Description	Value
ipv4-address	Specifies the IPv4 address of an interface.	The value is in dotted decimal notation.

Default Value

NA

View

ISIS configuration view

Usage Guidelines

NA

Example

Set the router ID for ISIS.

```
Switch(config-isis-1)#router-id 10.1.1.1 level-1
Switch(config-isis-1)#
```

5.7.46 set-overload-bit

Function

The **set-overload-bit** command sets a router in SPF calculation so that other routers do not use this router as a hop.

The **set-overload-bit on-startup** command sets the overload flag bit for non-pseudo node LSP.

The **no set-overload-bit** command cancels the configuration.

Format

- **set-overload-bit**
- **set-overload-bit on-startup** *timeout*
- **no set-overload-bit**

Parameter

Parameter	Description	Value
timeout	Specifies the timeout duration of the overload flag bit after the system is started.	The value is an integer ranging from 5 to 86400, in seconds.

Default Value

NA

View

ISIS configuration view

Usage Guidelines

Generally, you can only set the overload bit when the router is abnormal. For example, a router has insufficient storage and the link state database is incomplete, making the routing table incomplete or incorrect. In this case, you can set an overload bit in its LSP packets to notify other routers to ignore this router during SPF calculation until this router's problem is fixed. However, other routers in this ISIS area may find no path that can pass this router. But routers with IP and CLNS prefixes directly connected to this router can still be pinged. If you want to connect a router to an ISIS network but do not want any traffic to pass this router, you can run this command. The following is an application example:

- One test router in a lab is connected to a mature network.

- One router serves as the LSP transmission router (for example, in an NBMA network, combined with the characteristic of a network group).
- One router is a collection of virtual circuits for network management. In this case, the NMS must be in a network that is directly connected to a router configured with an overload bit.

Example

Set a router to be not the hop.

```
Switch(config-router-isis)#set-overload-bit
Switch(config-router-isis)#
```

5.7.47 preference

Function

The **preference** command sets the priority of the ISIS protocol.

Format

preference *priority*

Parameter

Parameter	Description	Value
priority	Specifies the priority of an OSPF route.	The value is an integer ranging from 1 to 255.

Default Value

50

View

ISIS configuration view

Usage Guidelines

NA

Example

Set the priority of the OSPF route.

```
Switch(config-ospf-1)# preference 10
Switch(config-ospf-1)#
```

5.7.48 reset isis

Function

The **reset isis** command resets a single or all ISIS instances.

Format

- **reset isis**
- **reset isis** *isis-instance*

Parameter

Parameter	Description	Value
Isis-instance	Specifies an ISIS instance ID.	The value is an integer ranging from 1 to 65535.

Default Value

NA

View

Privileged user view, global configuration view

Usage Guidelines

NA

Example

Reset all ISIS instances.

```
Switch(config)#reset isis
Switch(config)#
```

5.7.49 show ip isis

Function

The **show ip isis** command displays information on a single or all ISIS instances.

Format

- **show ip isis**
- **show ip isis** *instance-id*

Parameter

Parameter	Description	Value
instance-id	Specifies an ISIS instance ID.	The value is an integer ranging from 1 to

Parameter	Description	Value
		65535.

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

View information on all ISIS instances.

```

Switch# show ip isis

Protocol Information for IS-IS(1)
Max LSP Lifetime           : 1200(s)
LSP-refresh-interval       : 900(s)
LSP MTU                     : 1492bytes
SPF Max-interval           : 5(s)
SPF Init-interval          : 50(ms)
SPF Incr-interval          : 200(ms)
L1 Overload-bit            : no
L2 Overload-bit            : no
L1 Overload-bit On-startup : 600(s)
L2 Overload-bit On-startup : 600(s)
L1 LSP-gen Max-interval    : 2(s)
L2 Lsp-gen Max-interval    : 2(s)
Area Auth-type             : none
Area Auth-mode             : N/A
Domain Auth-type           : none
Domain Auth-mode           : N/A
Frr                        : disable
Frr Noloop Enable          : disable
Level-1 Cost Type          : narrow
Level-2 Cost Type          : wide
TE Level-1                 : disable
TE Level-1 Router ID       : 0.0.0.0
TE Level-2                 : disable
TE Level-2 Router ID       : 0.0.0.0

```

```

Protocol Information for IS-IS(2)
Max LSP Lifetime          : 1200(s)
LSP-refresh-interval      : 900(s)
LSP MTU                   : 1492bytes
SPF Max-interval          : 5(s)
SPF Init-interval         : 50(ms)
SPF Incr-interval         : 200(ms)
L1 Overload-bit           : no
L2 Overload-bit           : no
L1 Overload-bit On-startup : 600(s)
L2 Overload-bit On-startup : 600(s)
L1 LSP-gen Max-interval   : 2(s)
L2 Lsp-gen Max-interval   : 2(s)
Area Auth-type            : none
Area Auth-mode            : N/A
Domain Auth-type          : none
Domain Auth-mode          : N/A
Frr                       : disable
Frr Noloop Enable         : disable
Level-1 Cost Type         : narrow
Level-2 Cost Type         : wide
TE Level-1                : disable
TE Level-1 Router ID      : 0.0.0.0
TE Level-2                : disable
TE Level-2 Router ID      : 0.0.0.0
Switch#

```

5.7.50 show {ip|ipv6} isis bfd session

Function

The **show {ip|ipv6} isis bfd session** command displays information on an ISIS BFD session.

Format

show { ip | ipv6 } isis bfd session

Parameter

NA

Default Value

NA

View

Common user view

Usage Guidelines

You can run this command only after a BFD session is created.

Example

View information on an ISIS BFD session.

```
Switch>show ip isis bfd session
```

Num	Interface	Type	ID	BFD State	Peer Address	Local Address
1	100ge1/1/1	L2	0010.9400.003c	unbind	192.168.2.2	192.168.2.1
2	100ge1/1/1.1	L2	0010.9400.003f	unbind	192.168.4.2	192.168.4.1

```
Switch#
```

5.7.51 show ip isis config

Function

The **show ip isis config** command displays the basic ISIS configuration information.

Format

show ip isis config

Parameter

NA

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

Display the basic ISIS configuration information.

```
Switch>show ip isis config
```

```
Version                               :ISIS_VB3.00.10.07
```

```
!
```

```
router isis 1
```

```

net 10.0000.1000.0000.0002.00
is-type level-2
cost-style wide level-2
router isis 2 vpn-instance fiber1
net 10.0001.0000.0000.0002.00
is-type level-2
cost-style wide level-2
interface 100gigaethernet 1/1/1
ip router isis 1
interface 100gigaethernet 1/1/1.1
ip router isis 2
ipv6 router isis 2
Switch#

```

5.7.52 show ip isis database

Function

The **show ip isis database** command displays the link state database.

The **show ip isis database {level-1|level-2}** command displays information on an ISIS database of a specified level.

Format

- **show ip isis database**
- **show ip isis database { level-1 | level-2 } instance-id**

Parameter

Parameter	Description	Value
instance-id	Specifies an ISIS instance ID.	The value is an integer ranging from 1 to 65535.

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

Display the link state database.

```
Switch# show ip isis database
```

Database Information for IS-IS(1)

Level-2 Link State Database

The total number of ip isis 1 database is: 73

#	ID	Level	Seq	Checksum	Lifetime	Length	ATT/P/OL
1	0010.9400.003c.00-00	2	108	28053	1159	1460	0/0/0
2	0010.9400.003c.00-01	2	108	19704	1159	1467	0/0/0
3	0010.9400.003c.00-02	2	108	12172	1159	1467	0/0/0
4	0010.9400.003c.00-03	2	108	47225	1159	1467	0/0/0
5	0010.9400.003c.00-04	2	108	35103	1159	1467	0/0/0
6	0010.9400.003c.00-05	2	108	9721	1159	1467	0/0/0
7	0010.9400.003c.00-06	2	108	58289	1159	1467	0/0/0
8	0010.9400.003c.00-07	2	108	37242	1159	1467	0/0/0
9	0010.9400.003c.00-08	2	108	15940	1159	1467	0/0/0
10	0010.9400.003c.00-09	2	108	65018	1159	1467	0/0/0
11	0010.9400.003c.00-0a	2	108	39126	1159	1467	0/0/0
12	0010.9400.003c.00-0b	2	108	27259	1159	1467	0/0/0
13	0010.9400.003c.00-0c	2	108	62057	1159	1467	0/0/0
14	0010.9400.003c.00-0d	2	108	55035	1159	1467	0/0/0
15	0010.9400.003c.00-0e	2	108	19963	1159	1467	0/0/0
16	0010.9400.003c.00-0f	2	108	13961	1160	1467	0/0/0
17	0010.9400.003c.00-10	2	108	46209	1156	1467	0/0/0
18	0010.9400.003c.00-11	2	108	36892	1156	1467	0/0/0
19	0010.9400.003c.00-12	2	108	8450	1156	1467	0/0/0
20	0010.9400.003c.00-13	2	108	60078	1156	1467	0/0/0
21	0010.9400.003c.00-14	2	108	36226	1156	1467	0/0/0
22	0010.9400.003c.00-15	2	108	17729	1156	1467	0/0/0
23	0010.9400.003c.00-16	2	108	63747	1157	1467	0/0/0
24	0010.9400.003c.00-17	2	108	40915	1157	1467	0/0/0
25	0010.9400.003c.00-18	2	108	26243	1157	1467	0/0/0
26	0010.9400.003c.00-19	2	108	63846	1157	1467	0/0/0
27	0010.9400.003c.00-1a	2	108	53764	1157	1467	0/0/0
28	0010.9400.003c.00-1b	2	108	21752	1157	1467	0/0/0
29	0010.9400.003c.00-1c	2	108	15750	1157	1467	0/0/0
30	0010.9400.003c.00-1d	2	108	45193	1157	1467	0/0/0
31	0010.9400.003c.00-1e	2	108	38681	1157	1467	0/0/0
32	0010.9400.003c.00-1f	2	108	7434	1157	1467	0/0/0
33	0010.9400.003c.00-20	2	108	61867	1157	1467	0/0/0
34	0010.9400.003c.00-21	2	108	35210	1157	1467	0/0/0

35	0010.9400.003c.00-22	2	108	19518	1157	1467	0/0/0
36	0010.9400.003c.00-23	2	108	62731	1157	1467	0/0/0
37	0010.9400.003c.00-24	2	108	42704	1157	1467	0/0/0
38	0010.9400.003c.00-25	2	108	25227	1157	1467	0/0/0
39	0010.9400.003c.00-26	2	108	355	1157	1467	0/0/0
40	0010.9400.003c.00-27	2	108	52748	1156	1467	0/0/0
41	0010.9400.003c.00-28	2	108	23541	1156	1467	0/0/0
42	0010.9400.003c.00-29	2	108	15244	1157	1467	0/0/0
43	0010.9400.003c.00-2a	2	108	16871	1157	1465	0/0/0
44	0010.9400.003c.00-2b	2	108	43270	1157	1463	0/0/0
45	0010.9400.003c.00-2c	2	108	45500	1157	1463	0/0/0
46	0010.9400.003c.00-2d	2	108	59460	1157	1463	0/0/0
47	0010.9400.003c.00-2e	2	108	6100	1156	1463	0/0/0
48	0010.9400.003c.00-2f	2	108	2465	1156	1463	0/0/0
49	0010.9400.003c.00-30	2	108	16425	1156	1463	0/0/0
50	0010.9400.003c.00-31	2	108	30640	1156	1463	0/0/0
51	0010.9400.003c.00-32	2	108	28025	1156	1463	0/0/0
52	0010.9400.003c.00-33	2	108	38670	1156	1463	0/0/0
53	0010.9400.003c.00-34	2	108	52885	1156	1463	0/0/0
54	0010.9400.003c.00-35	2	108	55880	1156	1463	0/0/0
55	0010.9400.003c.00-36	2	108	61170	1156	1463	0/0/0
56	0010.9400.003c.00-37	2	108	9850	1156	1463	0/0/0
57	0010.9400.003c.00-38	2	108	18455	1156	1463	0/0/0
58	0010.9400.003c.00-39	2	108	18135	1156	1463	0/0/0
59	0010.9400.003c.00-3a	2	108	32095	1156	1463	0/0/0
60	0010.9400.003c.00-3b	2	108	46310	1156	1463	0/0/0
61	0010.9400.003c.00-3c	2	108	40635	1156	1463	0/0/0
62	0010.9400.003c.00-3d	2	108	54340	1156	1463	0/0/0
63	0010.9400.003c.00-3e	2	108	3275	1156	1463	0/0/0
64	0010.9400.003c.00-3f	2	108	3210	1156	1463	0/0/0
65	0010.9400.003c.00-40	2	108	11305	1156	1463	0/0/0
66	0010.9400.003c.00-41	2	108	25520	1156	1463	0/0/0
67	0010.9400.003c.00-42	2	108	31065	1156	1463	0/0/0
68	0010.9400.003c.00-43	2	108	33550	1156	1463	0/0/0
69	0010.9400.003c.00-44	2	108	47765	1156	1463	0/0/0
70	0010.9400.003c.00-45	2	108	58920	1156	1463	0/0/0
71	0010.9400.003c.00-46	2	108	22765	1156	253	0/0/0
72	1000.0000.0002.00-00	2	2	51926	325	66	0/0/0
73	1000.0000.0002.01-00	2	1	35391	325	51	0/0/0

Database Information for IS-IS(2)

Level-2 Link State Database

The total number of ip isis 2 database is: 73

#	ID	Level	Seq	Checksum	Lifetime	Length	ATT/P/OL
74	0000.0000.0002.00-00	2	2	54359	325	100	0/0/0
75	0000.0000.0002.01-00	2	1	34145	325	51	0/0/0
76	0010.9400.003f.00-00	2	5167	57952	1094	1460	0/0/0
77	0010.9400.003f.00-01	2	5167	29432	1094	1467	0/0/0
78	0010.9400.003f.00-02	2	5167	21900	1094	1467	0/0/0
79	0010.9400.003f.00-03	2	5167	56953	1094	1467	0/0/0
80	0010.9400.003f.00-04	2	5167	44831	1093	1467	0/0/0
81	0010.9400.003f.00-05	2	5167	19449	1093	1467	0/0/0
82	0010.9400.003f.00-06	2	5167	2737	1093	1467	0/0/0
83	0010.9400.003f.00-07	2	5167	46970	1093	1467	0/0/0
84	0010.9400.003f.00-08	2	5167	25668	1093	1467	0/0/0
85	0010.9400.003f.00-09	2	5167	9466	1093	1467	0/0/0
86	0010.9400.003f.00-0a	2	5167	48854	1094	1467	0/0/0
87	0010.9400.003f.00-0b	2	5167	36987	1094	1467	0/0/0
88	0010.9400.003f.00-0c	2	5167	6505	1094	1467	0/0/0
89	0010.9400.003f.00-0d	2	5167	64763	1094	1467	0/0/0
90	0010.9400.003f.00-0e	2	5167	29691	1094	1467	0/0/0
91	0010.9400.003f.00-0f	2	5167	23689	1093	1467	0/0/0
92	0010.9400.003f.00-10	2	5167	55937	1093	1467	0/0/0
93	0010.9400.003f.00-11	2	5167	46620	1093	1467	0/0/0
94	0010.9400.003f.00-12	2	5167	18178	1093	1467	0/0/0
95	0010.9400.003f.00-13	2	5167	4526	1093	1467	0/0/0
96	0010.9400.003f.00-14	2	5167	45954	1093	1467	0/0/0
97	0010.9400.003f.00-15	2	5167	27457	1093	1467	0/0/0
98	0010.9400.003f.00-16	2	5167	8195	1093	1467	0/0/0
99	0010.9400.003f.00-17	2	5167	50643	1093	1467	0/0/0
100	0010.9400.003f.00-18	2	5167	35971	1093	1467	0/0/0
101	0010.9400.003f.00-19	2	5167	8294	1093	1467	0/0/0
102	0010.9400.003f.00-1a	2	5167	63492	1094	1467	0/0/0
103	0010.9400.003f.00-1b	2	5167	31480	1093	1467	0/0/0
104	0010.9400.003f.00-1c	2	5167	25478	1093	1467	0/0/0
105	0010.9400.003f.00-1d	2	5167	54921	1093	1467	0/0/0
106	0010.9400.003f.00-1e	2	5167	48409	1093	1467	0/0/0
107	0010.9400.003f.00-1f	2	5167	17162	1093	1467	0/0/0
108	0010.9400.003f.00-20	2	5167	6315	1093	1467	0/0/0
109	0010.9400.003f.00-21	2	5167	44938	1093	1467	0/0/0
110	0010.9400.003f.00-22	2	5167	29246	1093	1467	0/0/0
111	0010.9400.003f.00-23	2	5167	7179	1092	1467	0/0/0
112	0010.9400.003f.00-24	2	5167	52432	1092	1467	0/0/0
113	0010.9400.003f.00-25	2	5167	34955	1092	1467	0/0/0
114	0010.9400.003f.00-26	2	5167	10083	1092	1467	0/0/0

115	0010.9400.003f.00-27	2	5167	62476	1092	1467	0/0/0
116	0010.9400.003f.00-28	2	5167	33269	1092	1467	0/0/0
117	0010.9400.003f.00-29	2	5167	24972	1092	1467	0/0/0
118	0010.9400.003f.00-2a	2	5167	26599	1092	1465	0/0/0
119	0010.9400.003f.00-2b	2	5167	52998	1092	1463	0/0/0
120	0010.9400.003f.00-2c	2	5167	55228	1092	1463	0/0/0
121	0010.9400.003f.00-2d	2	5167	3908	1092	1463	0/0/0
122	0010.9400.003f.00-2e	2	5167	15828	1092	1463	0/0/0
123	0010.9400.003f.00-2f	2	5167	12193	1092	1463	0/0/0
124	0010.9400.003f.00-30	2	5167	26153	1092	1463	0/0/0
125	0010.9400.003f.00-31	2	5167	40368	1092	1463	0/0/0
126	0010.9400.003f.00-32	2	5167	37753	1092	1463	0/0/0
127	0010.9400.003f.00-33	2	5167	48398	1092	1463	0/0/0
128	0010.9400.003f.00-34	2	5167	62613	1092	1463	0/0/0
129	0010.9400.003f.00-35	2	5167	328	1092	1463	0/0/0
130	0010.9400.003f.00-36	2	5167	5618	1092	1463	0/0/0
131	0010.9400.003f.00-37	2	5167	19578	1092	1463	0/0/0
132	0010.9400.003f.00-38	2	5167	28183	1092	1463	0/0/0
133	0010.9400.003f.00-39	2	5167	27863	1092	1463	0/0/0
134	0010.9400.003f.00-3a	2	5167	41823	1092	1463	0/0/0
135	0010.9400.003f.00-3b	2	5167	56038	1092	1463	0/0/0
136	0010.9400.003f.00-3c	2	5167	50363	1092	1463	0/0/0
137	0010.9400.003f.00-3d	2	5167	64068	1092	1463	0/0/0
138	0010.9400.003f.00-3e	2	5167	13003	1092	1463	0/0/0
139	0010.9400.003f.00-3f	2	5167	12938	1092	1463	0/0/0
140	0010.9400.003f.00-40	2	5167	21033	1092	1463	0/0/0
141	0010.9400.003f.00-41	2	5167	35248	1092	1463	0/0/0
142	0010.9400.003f.00-42	2	5167	40793	1092	1463	0/0/0
143	0010.9400.003f.00-43	2	5167	43278	1092	1463	0/0/0
144	0010.9400.003f.00-44	2	5167	57493	1092	1463	0/0/0
145	0010.9400.003f.00-45	2	5167	3368	1092	1463	0/0/0
146	0010.9400.003f.00-46	2	5167	32493	1092	253	0/0/0

Display information on an ISIS database of a specified level.

Switch>show ip isis database level-2 1							
Database Information for IS-IS(1)							
Level-2 Link State Database							
The total number of ip isis 1 database is: 73							
#	ID	Level	Seq	Checksum	Lifetime	Length	ATT/P/OL
1	0010.9400.003c.00-00	2	108	28053	970	1460	0/0/0
2	0010.9400.003c.00-01	2	108	19704	970	1467	0/0/0

3	0010.9400.003c.00-02	2	108	12172	970	1467	0/0/0
4	0010.9400.003c.00-03	2	108	47225	970	1467	0/0/0
5	0010.9400.003c.00-04	2	108	35103	970	1467	0/0/0
6	0010.9400.003c.00-05	2	108	9721	970	1467	0/0/0
7	0010.9400.003c.00-06	2	108	58289	970	1467	0/0/0
8	0010.9400.003c.00-07	2	108	37242	970	1467	0/0/0
9	0010.9400.003c.00-08	2	108	15940	970	1467	0/0/0
10	0010.9400.003c.00-09	2	108	65018	970	1467	0/0/0
11	0010.9400.003c.00-0a	2	108	39126	970	1467	0/0/0
12	0010.9400.003c.00-0b	2	108	27259	970	1467	0/0/0
13	0010.9400.003c.00-0c	2	108	62057	970	1467	0/0/0
14	0010.9400.003c.00-0d	2	108	55035	970	1467	0/0/0
15	0010.9400.003c.00-0e	2	108	19963	970	1467	0/0/0
16	0010.9400.003c.00-0f	2	108	13961	970	1467	0/0/0
17	0010.9400.003c.00-10	2	108	46209	968	1467	0/0/0
18	0010.9400.003c.00-11	2	108	36892	968	1467	0/0/0
19	0010.9400.003c.00-12	2	108	8450	968	1467	0/0/0
20	0010.9400.003c.00-13	2	108	60078	968	1467	0/0/0
21	0010.9400.003c.00-14	2	108	36226	968	1467	0/0/0
22	0010.9400.003c.00-15	2	108	17729	968	1467	0/0/0
23	0010.9400.003c.00-16	2	108	63747	968	1467	0/0/0
24	0010.9400.003c.00-17	2	108	40915	968	1467	0/0/0
25	0010.9400.003c.00-18	2	108	26243	968	1467	0/0/0
26	0010.9400.003c.00-19	2	108	63846	968	1467	0/0/0
27	0010.9400.003c.00-1a	2	108	53764	968	1467	0/0/0
28	0010.9400.003c.00-1b	2	108	21752	968	1467	0/0/0
29	0010.9400.003c.00-1c	2	108	15750	968	1467	0/0/0
30	0010.9400.003c.00-1d	2	108	45193	968	1467	0/0/0
31	0010.9400.003c.00-1e	2	108	38681	968	1467	0/0/0
32	0010.9400.003c.00-1f	2	108	7434	968	1467	0/0/0
33	0010.9400.003c.00-20	2	108	61867	968	1467	0/0/0
34	0010.9400.003c.00-21	2	108	35210	968	1467	0/0/0
35	0010.9400.003c.00-22	2	108	19518	968	1467	0/0/0
36	0010.9400.003c.00-23	2	108	62731	968	1467	0/0/0
37	0010.9400.003c.00-24	2	108	42704	968	1467	0/0/0
38	0010.9400.003c.00-25	2	108	25227	968	1467	0/0/0
39	0010.9400.003c.00-26	2	108	355	968	1467	0/0/0
40	0010.9400.003c.00-27	2	108	52748	968	1467	0/0/0
41	0010.9400.003c.00-28	2	108	23541	968	1467	0/0/0
42	0010.9400.003c.00-29	2	108	15244	968	1467	0/0/0
43	0010.9400.003c.00-2a	2	108	16871	968	1465	0/0/0
44	0010.9400.003c.00-2b	2	108	43270	968	1463	0/0/0
45	0010.9400.003c.00-2c	2	108	45500	968	1463	0/0/0

46	0010.9400.003c.00-2d	2	108	59460	968	1463	0/0/0
47	0010.9400.003c.00-2e	2	108	6100	967	1463	0/0/0
48	0010.9400.003c.00-2f	2	108	2465	967	1463	0/0/0
49	0010.9400.003c.00-30	2	108	16425	967	1463	0/0/0
50	0010.9400.003c.00-31	2	108	30640	967	1463	0/0/0
51	0010.9400.003c.00-32	2	108	28025	967	1463	0/0/0
52	0010.9400.003c.00-33	2	108	38670	967	1463	0/0/0
53	0010.9400.003c.00-34	2	108	52885	967	1463	0/0/0
54	0010.9400.003c.00-35	2	108	55880	967	1463	0/0/0
55	0010.9400.003c.00-36	2	108	61170	967	1463	0/0/0
56	0010.9400.003c.00-37	2	108	9850	967	1463	0/0/0
57	0010.9400.003c.00-38	2	108	18455	968	1463	0/0/0
58	0010.9400.003c.00-39	2	108	18135	968	1463	0/0/0
59	0010.9400.003c.00-3a	2	108	32095	968	1463	0/0/0
60	0010.9400.003c.00-3b	2	108	46310	968	1463	0/0/0
61	0010.9400.003c.00-3c	2	108	40635	968	1463	0/0/0
62	0010.9400.003c.00-3d	2	108	54340	968	1463	0/0/0
63	0010.9400.003c.00-3e	2	108	3275	967	1463	0/0/0
64	0010.9400.003c.00-3f	2	108	3210	967	1463	0/0/0
65	0010.9400.003c.00-40	2	108	11305	967	1463	0/0/0
66	0010.9400.003c.00-41	2	108	25520	967	1463	0/0/0
67	0010.9400.003c.00-42	2	108	31065	967	1463	0/0/0
68	0010.9400.003c.00-43	2	108	33550	968	1463	0/0/0
69	0010.9400.003c.00-44	2	108	47765	968	1463	0/0/0
70	0010.9400.003c.00-45	2	108	58920	968	1463	0/0/0
71	0010.9400.003c.00-46	2	108	22765	968	253	0/0/0
72	1000.0000.0002.00-00	2	3	51415	1045	66	0/0/0
73	1000.0000.0002.01-00	2	2	34880	1045	51	0/0/0

Switch#

5.7.53 show ip isis database count

Function

The **show ip isis database count** command displays statistics on an ISIS database.

Format

show ip isis database count

Parameter

NA

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

View statistics on an ISIS database.

Switch>show ip isis database count

L1 Database Count :0

L2 Database Count :146

Switch#

5.7.54 show ip isis database verbose**Function**The **show ip isis database verbose** command displays details of a link state database.**Format**

- **show ip isis database verbose**
- **show ip isis database verbose *lsp-index***

Parameter

Parameter	Description	Value
<i>lsp-index</i>	Specifies an LSP index.	The value is an integer ranging from 1 to 65535.

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

Display details of a link state database.

```
Switch>show ip isis database verbose
```

Database Information for IS-IS(1)

Level-2 Link State Database

LSPID	LSP-LEVEL	LSPSeqNum	Checksum	LifetimeRemain	Length
ATT/P/OL					
0010.9400.003c.00-00	2	108	28053	809	1460
0/0/0					
tlv#1 =(1, 4):					
area:3-- 00. 00. 01.					
tlv#2 =(129, 1):					
proto:cc.					
tlv#3 =(137, 9):					
name:Spirent-1					
tlv#4 =(132, 4):					
ifip:192.168.2.2					
tlv#5 =(22, 23):					
ext-isnbr:10.00.00.00.00.02.01,cost 1					
stlv_len=12:					
stlv#1 =(6, 4):					
localIP = 192.168.2.2					
stlv#2 =(8, 4):					
remoteIP = 192.168.2.1					
tlv#6 =(2, 12):					
isnbr:C=1/128/128/128,10.00.00.00.00.02.01					
tlv#7 =(128, 96):					
internal-ip-reach:c=1,down=0, 12.20.249.0/24					
internal-ip-reach:c=1,down=0, 12.20.248.0/24					
internal-ip-reach:c=1,down=0, 12.20.247.0/24					
internal-ip-reach:c=1,down=0, 12.20.246.0/24					
internal-ip-reach:c=1,down=0, 12.20.245.0/24					
internal-ip-reach:c=1,down=0, 12.20.244.0/24					
internal-ip-reach:c=1,down=0, 12.20.243.0/24					
internal-ip-reach:c=1,down=0, 12.20.242.0/24					

```
tlv#8 =(128, 252):
internal-ip-reach:c=1,down=0, 12.20.241.0/24
internal-ip-reach:c=1,down=0, 12.20.240.0/24
internal-ip-reach:c=1,down=0, 12.20.239.0/24
internal-ip-reach:c=1,down=0, 12.20.238.0/24
internal-ip-reach:c=1,down=0, 12.20.237.0/24
internal-ip-reach:c=1,down=0, 12.20.236.0/24
internal-ip-reach:c=1,down=0, 12.20.235.0/24
internal-ip-reach:c=1,down=0, 12.20.234.0/24
internal-ip-reach:c=1,down=0, 12.20.233.0/24
internal-ip-reach:c=1,down=0, 12.20.232.0/24
internal-ip-reach:c=1,down=0, 12.20.231.0/24
internal-ip-reach:c=1,down=0, 12.20.230.0/24
internal-ip-reach:c=1,down=0, 12.20.229.0/24
internal-ip-reach:c=1,down=0, 12.20.228.0/24
internal-ip-reach:c=1,down=0, 12.20.227.0/24
internal-ip-reach:c=1,down=0, 12.20.226.0/24
internal-ip-reach:c=1,down=0, 12.20.225.0/24
internal-ip-reach:c=1,down=0, 12.20.224.0/24
internal-ip-reach:c=1,down=0, 12.20.223.0/24
internal-ip-reach:c=1,down=0, 12.20.222.0/24
internal-ip-reach:c=1,down=0, 12.20.221.0/24
```

```
tlv#9 =(128, 252):
internal-ip-reach:c=1,down=0, 12.20.220.0/24
internal-ip-reach:c=1,down=0, 12.20.219.0/24
internal-ip-reach:c=1,down=0, 12.20.218.0/24
internal-ip-reach:c=1,down=0, 12.20.217.0/24
internal-ip-reach:c=1,down=0, 12.20.216.0/24
internal-ip-reach:c=1,down=0, 12.20.215.0/24
internal-ip-reach:c=1,down=0, 12.20.214.0/24
internal-ip-reach:c=1,down=0, 12.20.213.0/24
internal-ip-reach:c=1,down=0, 12.20.212.0/24
internal-ip-reach:c=1,down=0, 12.20.211.0/24
internal-ip-reach:c=1,down=0, 12.20.210.0/24
internal-ip-reach:c=1,down=0, 12.20.209.0/24
internal-ip-reach:c=1,down=0, 12.20.208.0/24
internal-ip-reach:c=1,down=0, 12.20.207.0/24
internal-ip-reach:c=1,down=0, 12.20.206.0/24
internal-ip-reach:c=1,down=0, 12.20.205.0/24
internal-ip-reach:c=1,down=0, 12.20.204.0/24
internal-ip-reach:c=1,down=0, 12.20.203.0/24
internal-ip-reach:c=1,down=0, 12.20.202.0/24
```

```
internal-ip-reach:c=1,down=0, 12.20.201.0/24
internal-ip-reach:c=1,down=0, 12.20.200.0/24
```

```
tlv#10=(128, 252):
```

```
internal-ip-reach:c=1,down=0, 12.20.199.0/24
internal-ip-reach:c=1,down=0, 12.20.198.0/24
internal-ip-reach:c=1,down=0, 12.20.197.0/24
internal-ip-reach:c=1,down=0, 12.20.196.0/24
internal-ip-reach:c=1,down=0, 12.20.195.0/24
internal-ip-reach:c=1,down=0, 12.20.194.0/24
internal-ip-reach:c=1,down=0, 12.20.193.0/24
internal-ip-reach:c=1,down=0, 12.20.192.0/24
internal-ip-reach:c=1,down=0, 12.20.191.0/24
internal-ip-reach:c=1,down=0, 12.20.190.0/24
internal-ip-reach:c=1,down=0, 12.20.189.0/24
internal-ip-reach:c=1,down=0, 12.20.188.0/24
internal-ip-reach:c=1,down=0, 12.20.187.0/24
internal-ip-reach:c=1,down=0, 12.20.186.0/24
internal-ip-reach:c=1,down=0, 12.20.185.0/24
internal-ip-reach:c=1,down=0, 12.20.184.0/24
internal-ip-reach:c=1,down=0, 12.20.183.0/24
internal-ip-reach:c=1,down=0, 12.20.182.0/24
internal-ip-reach:c=1,down=0, 12.20.181.0/24
internal-ip-reach:c=1,down=0, 12.20.180.0/24
internal-ip-reach:c=1,down=0, 12.20.179.0/24
```

```
tlv#11=(128, 252):
```

```
internal-ip-reach:c=1,down=0, 12.20.178.0/24
internal-ip-reach:c=1,down=0, 12.20.177.0/24
internal-ip-reach:c=1,down=0, 12.20.176.0/24
internal-ip-reach:c=1,down=0, 12.20.175.0/24
internal-ip-reach:c=1,down=0, 12.20.174.0/24
internal-ip-reach:c=1,down=0, 12.20.173.0/24
internal-ip-reach:c=1,down=0, 12.20.172.0/24
internal-ip-reach:c=1,down=0, 12.20.171.0/24
internal-ip-reach:c=1,down=0, 12.20.170.0/24
internal-ip-reach:c=1,down=0, 12.20.169.0/24
internal-ip-reach:c=1,down=0, 12.20.168.0/24
internal-ip-reach:c=1,down=0, 12.20.167.0/24
internal-ip-reach:c=1,down=0, 12.20.166.0/24
internal-ip-reach:c=1,down=0, 12.20.165.0/24
internal-ip-reach:c=1,down=0, 12.20.164.0/24
internal-ip-reach:c=1,down=0, 12.20.163.0/24
```

```

internal-ip-reach:c=1,down=0, 12.20.162.0/24
internal-ip-reach:c=1,down=0, 12.20.161.0/24
internal-ip-reach:c=1,down=0, 12.20.160.0/24
internal-ip-reach:c=1,down=0, 12.20.159.0/24
internal-ip-reach:c=1,down=0, 12.20.158.0/24

```

```

tlv#12=(128, 252):

```

```

internal-ip-reach:c=1,down=0, 12.20.157.0/24
internal-ip-reach:c=1,down=0, 12.20.156.0/24
internal-ip-reach:c=1,down=0, 12.20.155.0/24
internal-ip-reach:c=1,down=0, 12.20.154.0/24
internal-ip-reach:c=1,down=0, 12.20.153.0/24
internal-ip-reach:c=1,down=0, 12.20.152.0/24
internal-ip-reach:c=1,down=0, 12.20.151.0/24
internal-ip-reach:c=1,down=0, 12.20.150.0/24
internal-ip-reach:c=1,down=0, 12.20.149.0/24
internal-ip-reach:c=1,down=0, 12.20.148.0/24
internal-ip-reach:c=1,down=0, 12.20.147.0/24
internal-ip-reach:c=1,down=0, 12.20.146.0/24
internal-ip-reach:c=1,down=0, 12.20.145.0/24
internal-ip-reach:c=1,down=0, 12.20.144.0/24
internal-ip-reach:c=1,down=0, 12.20.143.0/24
internal-ip-reach:c=1,down=0, 12.20.142.0/24
internal-ip-reach:c=1,down=0, 12.20.141.0/24
internal-ip-reach:c=1,down=0, 12.20.140.0/24
internal-ip-reach:c=1,down=0, 12.20.139.0/24
internal-ip-reach:c=1,down=0, 12.20.138.0/24
internal-ip-reach:c=1,down=0, 12.20.137.0/24

```

```

0010.9400.003c.00-01      2          108          19704      804          1467      0/0/0

```

```

tlv#1 =(128, 168):

```

```

internal-ip-reach:c=1,down=0, 12.21.112.0/24
internal-ip-reach:c=1,down=0, 12.21.111.0/24
internal-ip-reach:c=1,down=0, 12.21.110.0/24
internal-ip-reach:c=1,down=0, 12.21.109.0/24
internal-ip-reach:c=1,down=0, 12.21.108.0/24
internal-ip-reach:c=1,down=0, 12.21.107.0/24
internal-ip-reach:c=1,down=0, 12.21.106.0/24
internal-ip-reach:c=1,down=0, 12.21.105.0/24
internal-ip-reach:c=1,down=0, 12.21.104.0/24
internal-ip-reach:c=1,down=0, 12.21.103.0/24
internal-ip-reach:c=1,down=0, 12.21.102.0/24
internal-ip-reach:c=1,down=0, 12.21.101.0/24

```

```
internal-ip-reach:c=1,down=0, 12.21.100.0/24
internal-ip-reach:c=1,down=0, 12.21.99.0/24
```

```
tlv#2 =(128, 252):
```

```
internal-ip-reach:c=1,down=0, 12.21.98.0/24
internal-ip-reach:c=1,down=0, 12.21.97.0/24
internal-ip-reach:c=1,down=0, 12.21.96.0/24
internal-ip-reach:c=1,down=0, 12.21.95.0/24
internal-ip-reach:c=1,down=0, 12.21.94.0/24
internal-ip-reach:c=1,down=0, 12.21.93.0/24
internal-ip-reach:c=1,down=0, 12.21.92.0/24
internal-ip-reach:c=1,down=0, 12.21.91.0/24
internal-ip-reach:c=1,down=0, 12.21.90.0/24
internal-ip-reach:c=1,down=0, 12.21.89.0/24
internal-ip-reach:c=1,down=0, 12.21.88.0/24
internal-ip-reach:c=1,down=0, 12.21.87.0/24
internal-ip-reach:c=1,down=0, 12.21.86.0/24
internal-ip-reach:c=1,down=0, 12.21.85.0/24
internal-ip-reach:c=1,down=0, 12.21.84.0/24
internal-ip-reach:c=1,down=0, 12.21.83.0/24
internal-ip-reach:c=1,down=0, 12.21.82.0/24
internal-ip-reach:c=1,down=0, 12.21.81.0/24
internal-ip-reach:c=1,down=0, 12.21.80.0/24
internal-ip-reach:c=1,down=0, 12.21.79.0/24
internal-ip-reach:c=1,down=0, 12.21.78.0/24
```

```
tlv#3 =(128, 252):
```

```
internal-ip-reach:c=1,down=0, 12.21.77.0/24
internal-ip-reach:c=1,down=0, 12.21.76.0/24
internal-ip-reach:c=1,down=0, 12.21.75.0/24
internal-ip-reach:c=1,down=0, 12.21.74.0/24
internal-ip-reach:c=1,down=0, 12.21.73.0/24
internal-ip-reach:c=1,down=0, 12.21.72.0/24
internal-ip-reach:c=1,down=0, 12.21.71.0/24
internal-ip-reach:c=1,down=0, 12.21.70.0/24
internal-ip-reach:c=1,down=0, 12.21.69.0/24
internal-ip-reach:c=1,down=0, 12.21.68.0/24
internal-ip-reach:c=1,down=0, 12.21.67.0/24
internal-ip-reach:c=1,down=0, 12.21.66.0/24
internal-ip-reach:c=1,down=0, 12.21.65.0/24
internal-ip-reach:c=1,down=0, 12.21.64.0/24
internal-ip-reach:c=1,down=0, 12.21.63.0/24
internal-ip-reach:c=1,down=0, 12.21.62.0/24
```



```
internal-ip-reach:c=1,down=0, 12.21.61.0/24
internal-ip-reach:c=1,down=0, 12.21.60.0/24
internal-ip-reach:c=1,down=0, 12.21.59.0/24
internal-ip-reach:c=1,down=0, 12.21.58.0/24
internal-ip-reach:c=1,down=0, 12.21.57.0/24
```

tlv#4 =(128, 252):

```
internal-ip-reach:c=1,down=0, 12.21.56.0/24
internal-ip-reach:c=1,down=0, 12.21.55.0/24
internal-ip-reach:c=1,down=0, 12.21.54.0/24
internal-ip-reach:c=1,down=0, 12.21.53.0/24
internal-ip-reach:c=1,down=0, 12.21.52.0/24
internal-ip-reach:c=1,down=0, 12.21.51.0/24
internal-ip-reach:c=1,down=0, 12.21.50.0/24
internal-ip-reach:c=1,down=0, 12.21.49.0/24
internal-ip-reach:c=1,down=0, 12.21.48.0/24
internal-ip-reach:c=1,down=0, 12.21.47.0/24
internal-ip-reach:c=1,down=0, 12.21.46.0/24
internal-ip-reach:c=1,down=0, 12.21.45.0/24
internal-ip-reach:c=1,down=0, 12.21.44.0/24
internal-ip-reach:c=1,down=0, 12.21.43.0/24
internal-ip-reach:c=1,down=0, 12.21.42.0/24
internal-ip-reach:c=1,down=0, 12.21.41.0/24
internal-ip-reach:c=1,down=0, 12.21.40.0/24
internal-ip-reach:c=1,down=0, 12.21.39.0/24
internal-ip-reach:c=1,down=0, 12.21.38.0/24
internal-ip-reach:c=1,down=0, 12.21.37.0/24
internal-ip-reach:c=1,down=0, 12.21.36.0/24
```

tlv#5 =(128, 252):

```
internal-ip-reach:c=1,down=0, 12.21.35.0/24
internal-ip-reach:c=1,down=0, 12.21.34.0/24
internal-ip-reach:c=1,down=0, 12.21.33.0/24
internal-ip-reach:c=1,down=0, 12.21.32.0/24
internal-ip-reach:c=1,down=0, 12.21.31.0/24
internal-ip-reach:c=1,down=0, 12.21.30.0/24
internal-ip-reach:c=1,down=0, 12.21.29.0/24
internal-ip-reach:c=1,down=0, 12.21.28.0/24
internal-ip-reach:c=1,down=0, 12.21.27.0/24
internal-ip-reach:c=1,down=0, 12.21.26.0/24
internal-ip-reach:c=1,down=0, 12.21.25.0/24
internal-ip-reach:c=1,down=0, 12.21.24.0/24
internal-ip-reach:c=1,down=0, 12.21.23.0/24
```

```

internal-ip-reach:c=1,down=0, 12.21.22.0/24
internal-ip-reach:c=1,down=0, 12.21.21.0/24
internal-ip-reach:c=1,down=0, 12.21.20.0/24
internal-ip-reach:c=1,down=0, 12.21.19.0/24
internal-ip-reach:c=1,down=0, 12.21.18.0/24
internal-ip-reach:c=1,down=0, 12.21.17.0/24
internal-ip-reach:c=1,down=0, 12.21.16.0/24
internal-ip-reach:c=1,down=0, 12.21.15.0/24

```

tlv#6 =(128, 252):

```

internal-ip-reach:c=1,down=0, 12.21.14.0/24
internal-ip-reach:c=1,down=0, 12.21.13.0/24
internal-ip-reach:c=1,down=0, 12.21.12.0/24
internal-ip-reach:c=1,down=0, 12.21.11.0/24
internal-ip-reach:c=1,down=0, 12.21.10.0/24
internal-ip-reach:c=1,down=0, 12.21.9.0/24
internal-ip-reach:c=1,down=0, 12.21.8.0/24
internal-ip-reach:c=1,down=0, 12.21.7.0/24
internal-ip-reach:c=1,down=0, 12.21.6.0/24
internal-ip-reach:c=1,down=0, 12.21.5.0/24
internal-ip-reach:c=1,down=0, 12.21.4.0/24
internal-ip-reach:c=1,down=0, 12.21.3.0/24
internal-ip-reach:c=1,down=0, 12.21.2.0/24
internal-ip-reach:c=1,down=0, 12.21.1.0/24
internal-ip-reach:c=1,down=0, 12.21.0.0/24
internal-ip-reach:c=1,down=0, 12.20.255.0/24
internal-ip-reach:c=1,down=0, 12.20.254.0/24
internal-ip-reach:c=1,down=0, 12.20.253.0/24
internal-ip-reach:c=1,down=0, 12.20.252.0/24
internal-ip-reach:c=1,down=0, 12.20.251.0/24
internal-ip-reach:c=1,down=0, 12.20.250.0/24

```

```

0010.9400.003c.00-02      2          108          12172      803          1467      0/0/0

```

tlv#1 =(128, 168):

```

internal-ip-reach:c=1,down=0, 12.21.231.0/24
internal-ip-reach:c=1,down=0, 12.21.230.0/24
internal-ip-reach:c=1,down=0, 12.21.229.0/24
internal-ip-reach:c=1,down=0, 12.21.228.0/24
internal-ip-reach:c=1,down=0, 12.21.227.0/24
internal-ip-reach:c=1,down=0, 12.21.226.0/24
internal-ip-reach:c=1,down=0, 12.21.225.0/24
internal-ip-reach:c=1,down=0, 12.21.224.0/24
internal-ip-reach:c=1,down=0, 12.21.223.0/24

```

```
internal-ip-reach:c=1,down=0, 12.21.222.0/24
internal-ip-reach:c=1,down=0, 12.21.221.0/24
internal-ip-reach:c=1,down=0, 12.21.220.0/24
internal-ip-reach:c=1,down=0, 12.21.219.0/24
internal-ip-reach:c=1,down=0, 12.21.218.0/24
```

tlv#2 =(128, 252):

```
internal-ip-reach:c=1,down=0, 12.21.217.0/24
internal-ip-reach:c=1,down=0, 12.21.216.0/24
internal-ip-reach:c=1,down=0, 12.21.215.0/24
internal-ip-reach:c=1,down=0, 12.21.214.0/24
internal-ip-reach:c=1,down=0, 12.21.213.0/24
internal-ip-reach:c=1,down=0, 12.21.212.0/24
internal-ip-reach:c=1,down=0, 12.21.211.0/24
internal-ip-reach:c=1,down=0, 12.21.210.0/24
internal-ip-reach:c=1,down=0, 12.21.209.0/24
internal-ip-reach:c=1,down=0, 12.21.208.0/24
internal-ip-reach:c=1,down=0, 12.21.207.0/24
internal-ip-reach:c=1,down=0, 12.21.206.0/24
internal-ip-reach:c=1,down=0, 12.21.205.0/24
internal-ip-reach:c=1,down=0, 12.21.204.0/24
internal-ip-reach:c=1,down=0, 12.21.203.0/24
internal-ip-reach:c=1,down=0, 12.21.202.0/24
internal-ip-reach:c=1,down=0, 12.21.201.0/24
internal-ip-reach:c=1,down=0, 12.21.200.0/24
internal-ip-reach:c=1,down=0, 12.21.199.0/24
internal-ip-reach:c=1,down=0, 12.21.198.0/24
internal-ip-reach:c=1,down=0, 12.21.197.0/24
```

tlv#3 =(128, 252):

```
internal-ip-reach:c=1,down=0, 12.21.196.0/24
internal-ip-reach:c=1,down=0, 12.21.195.0/24
internal-ip-reach:c=1,down=0, 12.21.194.0/24
internal-ip-reach:c=1,down=0, 12.21.193.0/24
internal-ip-reach:c=1,down=0, 12.21.192.0/24
internal-ip-reach:c=1,down=0, 12.21.191.0/24
internal-ip-reach:c=1,down=0, 12.21.190.0/24
internal-ip-reach:c=1,down=0, 12.21.189.0/24
internal-ip-reach:c=1,down=0, 12.21.188.0/24
internal-ip-reach:c=1,down=0, 12.21.187.0/24
internal-ip-reach:c=1,down=0, 12.21.186.0/24
internal-ip-reach:c=1,down=0, 12.21.185.0/24
internal-ip-reach:c=1,down=0, 12.21.184.0/24
```

```
internal-ip-reach:c=1,down=0, 12.21.183.0/24
internal-ip-reach:c=1,down=0, 12.21.182.0/24
internal-ip-reach:c=1,down=0, 12.21.181.0/24
internal-ip-reach:c=1,down=0, 12.21.180.0/24
internal-ip-reach:c=1,down=0, 12.21.179.0/24
internal-ip-reach:c=1,down=0, 12.21.178.0/24
internal-ip-reach:c=1,down=0, 12.21.177.0/24
internal-ip-reach:c=1,down=0, 12.21.176.0/24
```

tlv#4 =(128, 252):

```
internal-ip-reach:c=1,down=0, 12.21.175.0/24
internal-ip-reach:c=1,down=0, 12.21.174.0/24
internal-ip-reach:c=1,down=0, 12.21.173.0/24
internal-ip-reach:c=1,down=0, 12.21.172.0/24
internal-ip-reach:c=1,down=0, 12.21.171.0/24
internal-ip-reach:c=1,down=0, 12.21.170.0/24
internal-ip-reach:c=1,down=0, 12.21.169.0/24
internal-ip-reach:c=1,down=0, 12.21.168.0/24
internal-ip-reach:c=1,down=0, 12.21.167.0/24
internal-ip-reach:c=1,down=0, 12.21.166.0/24
internal-ip-reach:c=1,down=0, 12.21.165.0/24
internal-ip-reach:c=1,down=0, 12.21.164.0/24
internal-ip-reach:c=1,down=0, 12.21.163.0/24
internal-ip-reach:c=1,down=0, 12.21.162.0/24
internal-ip-reach:c=1,down=0, 12.21.161.0/24
internal-ip-reach:c=1,down=0, 12.21.160.0/24
internal-ip-reach:c=1,down=0, 12.21.159.0/24
internal-ip-reach:c=1,down=0, 12.21.158.0/24
internal-ip-reach:c=1,down=0, 12.21.157.0/24
internal-ip-reach:c=1,down=0, 12.21.156.0/24
internal-ip-reach:c=1,down=0, 12.21.155.0/24
```

tlv#5 =(128, 252):

```
internal-ip-reach:c=1,down=0, 12.21.154.0/24
internal-ip-reach:c=1,down=0, 12.21.153.0/24
internal-ip-reach:c=1,down=0, 12.21.152.0/24
internal-ip-reach:c=1,down=0, 12.21.151.0/24
internal-ip-reach:c=1,down=0, 12.21.150.0/24
internal-ip-reach:c=1,down=0, 12.21.149.0/24
internal-ip-reach:c=1,down=0, 12.21.148.0/24
internal-ip-reach:c=1,down=0, 12.21.147.0/24
internal-ip-reach:c=1,down=0, 12.21.146.0/24
internal-ip-reach:c=1,down=0, 12.21.145.0/24
```

```

internal-ip-reach:c=1,down=0, 12.21.144.0/24
internal-ip-reach:c=1,down=0, 12.21.143.0/24
internal-ip-reach:c=1,down=0, 12.21.142.0/24
internal-ip-reach:c=1,down=0, 12.21.141.0/24
internal-ip-reach:c=1,down=0, 12.21.140.0/24
internal-ip-reach:c=1,down=0, 12.21.139.0/24
internal-ip-reach:c=1,down=0, 12.21.138.0/24
internal-ip-reach:c=1,down=0, 12.21.137.0/24
internal-ip-reach:c=1,down=0, 12.21.136.0/24
internal-ip-reach:c=1,down=0, 12.21.135.0/24
internal-ip-reach:c=1,down=0, 12.21.134.0/24

```

tlv#6 =(128, 252):

```

internal-ip-reach:c=1,down=0, 12.21.133.0/24
internal-ip-reach:c=1,down=0, 12.21.132.0/24
internal-ip-reach:c=1,down=0, 12.21.131.0/24
internal-ip-reach:c=1,down=0, 12.21.130.0/24
internal-ip-reach:c=1,down=0, 12.21.129.0/24
internal-ip-reach:c=1,down=0, 12.21.128.0/24
internal-ip-reach:c=1,down=0, 12.21.127.0/24
internal-ip-reach:c=1,down=0, 12.21.126.0/24
internal-ip-reach:c=1,down=0, 12.21.125.0/24
internal-ip-reach:c=1,down=0, 12.21.124.0/24
internal-ip-reach:c=1,down=0, 12.21.123.0/24
internal-ip-reach:c=1,down=0, 12.21.122.0/24
internal-ip-reach:c=1,down=0, 12.21.121.0/24
internal-ip-reach:c=1,down=0, 12.21.120.0/24
internal-ip-reach:c=1,down=0, 12.21.119.0/24
internal-ip-reach:c=1,down=0, 12.21.118.0/24
internal-ip-reach:c=1,down=0, 12.21.117.0/24
internal-ip-reach:c=1,down=0, 12.21.116.0/24
internal-ip-reach:c=1,down=0, 12.21.115.0/24
internal-ip-reach:c=1,down=0, 12.21.114.0/24
internal-ip-reach:c=1,down=0, 12.21.113.0/24

```

```

0010.9400.003c.00-03      2          108          47225      802          1467      0/0/0

```

tlv#1 =(128, 168):

```

internal-ip-reach:c=1,down=0, 12.22.94.0/24
internal-ip-reach:c=1,down=0, 12.22.93.0/24
internal-ip-reach:c=1,down=0, 12.22.92.0/24
internal-ip-reach:c=1,down=0, 12.22.91.0/24
internal-ip-reach:c=1,down=0, 12.22.90.0/24
internal-ip-reach:c=1,down=0, 12.22.89.0/24

```

```
internal-ip-reach:c=1,down=0, 12.22.88.0/24
internal-ip-reach:c=1,down=0, 12.22.87.0/24
internal-ip-reach:c=1,down=0, 12.22.86.0/24
internal-ip-reach:c=1,down=0, 12.22.85.0/24
internal-ip-reach:c=1,down=0, 12.22.84.0/24
internal-ip-reach:c=1,down=0, 12.22.83.0/24
internal-ip-reach:c=1,down=0, 12.22.82.0/24
internal-ip-reach:c=1,down=0, 12.22.81.0/24
```

tlv#2 =(128, 252):

```
internal-ip-reach:c=1,down=0, 12.22.80.0/24
internal-ip-reach:c=1,down=0, 12.22.79.0/24
internal-ip-reach:c=1,down=0, 12.22.78.0/24
internal-ip-reach:c=1,down=0, 12.22.77.0/24
internal-ip-reach:c=1,down=0, 12.22.76.0/24
internal-ip-reach:c=1,down=0, 12.22.75.0/24
internal-ip-reach:c=1,down=0, 12.22.74.0/24
internal-ip-reach:c=1,down=0, 12.22.73.0/24
internal-ip-reach:c=1,down=0, 12.22.72.0/24
internal-ip-reach:c=1,down=0, 12.22.71.0/24
internal-ip-reach:c=1,down=0, 12.22.70.0/24
internal-ip-reach:c=1,down=0, 12.22.69.0/24
internal-ip-reach:c=1,down=0, 12.22.68.0/24
internal-ip-reach:c=1,down=0, 12.22.67.0/24
internal-ip-reach:c=1,down=0, 12.22.66.0/24
internal-ip-reach:c=1,down=0, 12.22.65.0/24
internal-ip-reach:c=1,down=0, 12.22.64.0/24
internal-ip-reach:c=1,down=0, 12.22.63.0/24
internal-ip-reach:c=1,down=0, 12.22.62.0/24
internal-ip-reach:c=1,down=0, 12.22.61.0/24
internal-ip-reach:c=1,down=0, 12.22.60.0/24
```

tlv#3 =(128, 252):

```
internal-ip-reach:c=1,down=0, 12.22.59.0/24
internal-ip-reach:c=1,down=0, 12.22.58.0/24
internal-ip-reach:c=1,down=0, 12.22.57.0/24
internal-ip-reach:c=1,down=0, 12.22.56.0/24
internal-ip-reach:c=1,down=0, 12.22.55.0/24
internal-ip-reach:c=1,down=0, 12.22.54.0/24
internal-ip-reach:c=1,down=0, 12.22.53.0/24
internal-ip-reach:c=1,down=0, 12.22.52.0/24
internal-ip-reach:c=1,down=0, 12.22.51.0/24
internal-ip-reach:c=1,down=0, 12.22.50.0/24
```

```
internal-ip-reach:c=1,down=0, 12.22.49.0/24
internal-ip-reach:c=1,down=0, 12.22.48.0/24
internal-ip-reach:c=1,down=0, 12.22.47.0/24
internal-ip-reach:c=1,down=0, 12.22.46.0/24
internal-ip-reach:c=1,down=0, 12.22.45.0/24
internal-ip-reach:c=1,down=0, 12.22.44.0/24
internal-ip-reach:c=1,down=0, 12.22.43.0/24
internal-ip-reach:c=1,down=0, 12.22.42.0/24
internal-ip-reach:c=1,down=0, 12.22.41.0/24
internal-ip-reach:c=1,down=0, 12.22.40.0/24
internal-ip-reach:c=1,down=0, 12.22.39.0/24
```

tlv#4 =(128, 252):

```
internal-ip-reach:c=1,down=0, 12.22.38.0/24
internal-ip-reach:c=1,down=0, 12.22.37.0/24
internal-ip-reach:c=1,down=0, 12.22.36.0/24
internal-ip-reach:c=1,down=0, 12.22.35.0/24
internal-ip-reach:c=1,down=0, 12.22.34.0/24
internal-ip-reach:c=1,down=0, 12.22.33.0/24
internal-ip-reach:c=1,down=0, 12.22.32.0/24
internal-ip-reach:c=1,down=0, 12.22.31.0/24
internal-ip-reach:c=1,down=0, 12.22.30.0/24
internal-ip-reach:c=1,down=0, 12.22.29.0/24
internal-ip-reach:c=1,down=0, 12.22.28.0/24
internal-ip-reach:c=1,down=0, 12.22.27.0/24
internal-ip-reach:c=1,down=0, 12.22.26.0/24
internal-ip-reach:c=1,down=0, 12.22.25.0/24
internal-ip-reach:c=1,down=0, 12.22.24.0/24
internal-ip-reach:c=1,down=0, 12.22.23.0/24
internal-ip-reach:c=1,down=0, 12.22.22.0/24
internal-ip-reach:c=1,down=0, 12.22.21.0/24
internal-ip-reach:c=1,down=0, 12.22.20.0/24
internal-ip-reach:c=1,down=0, 12.22.19.0/24
internal-ip-reach:c=1,down=0, 12.22.18.0/24
```

tlv#5 =(128, 252):

```
internal-ip-reach:c=1,down=0, 12.22.17.0/24
internal-ip-reach:c=1,down=0, 12.22.16.0/24
internal-ip-reach:c=1,down=0, 12.22.15.0/24
internal-ip-reach:c=1,down=0, 12.22.14.0/24
internal-ip-reach:c=1,down=0, 12.22.13.0/24
internal-ip-reach:c=1,down=0, 12.22.12.0/24
internal-ip-reach:c=1,down=0, 12.22.11.0/24
```

```

internal-ip-reach:c=1,down=0, 12.22.10.0/24
internal-ip-reach:c=1,down=0, 12.22.9.0/24
internal-ip-reach:c=1,down=0, 12.22.8.0/24
internal-ip-reach:c=1,down=0, 12.22.7.0/24
internal-ip-reach:c=1,down=0, 12.22.6.0/24
internal-ip-reach:c=1,down=0, 12.22.5.0/24
internal-ip-reach:c=1,down=0, 12.22.4.0/24
internal-ip-reach:c=1,down=0, 12.22.3.0/24
internal-ip-reach:c=1,down=0, 12.22.2.0/24
internal-ip-reach:c=1,down=0, 12.22.1.0/24
internal-ip-reach:c=1,down=0, 12.22.0.0/24
internal-ip-reach:c=1,down=0, 12.21.255.0/24
internal-ip-reach:c=1,down=0, 12.21.254.0/24
internal-ip-reach:c=1,down=0, 12.21.253.0/24

```

tlv#6 =(128, 252):

```

internal-ip-reach:c=1,down=0, 12.21.252.0/24
internal-ip-reach:c=1,down=0, 12.21.251.0/24
internal-ip-reach:c=1,down=0, 12.21.250.0/24
internal-ip-reach:c=1,down=0, 12.21.249.0/24
internal-ip-reach:c=1,down=0, 12.21.248.0/24
internal-ip-reach:c=1,down=0, 12.21.247.0/24
internal-ip-reach:c=1,down=0, 12.21.246.0/24
internal-ip-reach:c=1,down=0, 12.21.245.0/24
internal-ip-reach:c=1,down=0, 12.21.244.0/24
internal-ip-reach:c=1,down=0, 12.21.243.0/24
internal-ip-reach:c=1,down=0, 12.21.242.0/24
internal-ip-reach:c=1,down=0, 12.21.241.0/24
internal-ip-reach:c=1,down=0, 12.21.240.0/24
internal-ip-reach:c=1,down=0, 12.21.239.0/24
internal-ip-reach:c=1,down=0, 12.21.238.0/24
internal-ip-reach:c=1,down=0, 12.21.237.0/24
internal-ip-reach:c=1,down=0, 12.21.236.0/24
internal-ip-reach:c=1,down=0, 12.21.235.0/24
internal-ip-reach:c=1,down=0, 12.21.234.0/24
internal-ip-reach:c=1,down=0, 12.21.233.0/24
internal-ip-reach:c=1,down=0, 12.21.232.0/24

```

```

0010.9400.003c.00-04      2          108          35103      801          1467      0/0/0

```

tlv#1 =(128, 168):

```

internal-ip-reach:c=1,down=0, 12.22.213.0/24
internal-ip-reach:c=1,down=0, 12.22.212.0/24
internal-ip-reach:c=1,down=0, 12.22.211.0/24

```



```
internal-ip-reach:c=1,down=0, 12.22.210.0/24
internal-ip-reach:c=1,down=0, 12.22.209.0/24
internal-ip-reach:c=1,down=0, 12.22.208.0/24
internal-ip-reach:c=1,down=0, 12.22.207.0/24
internal-ip-reach:c=1,down=0, 12.22.206.0/24
internal-ip-reach:c=1,down=0, 12.22.205.0/24
internal-ip-reach:c=1,down=0, 12.22.204.0/24
internal-ip-reach:c=1,down=0, 12.22.203.0/24
internal-ip-reach:c=1,down=0, 12.22.202.0/24
internal-ip-reach:c=1,down=0, 12.22.201.0/24
internal-ip-reach:c=1,down=0, 12.22.200.0/24
```

tlv#2 =(128, 252):

```
internal-ip-reach:c=1,down=0, 12.22.199.0/24
internal-ip-reach:c=1,down=0, 12.22.198.0/24
internal-ip-reach:c=1,down=0, 12.22.197.0/24
internal-ip-reach:c=1,down=0, 12.22.196.0/24
internal-ip-reach:c=1,down=0, 12.22.195.0/24
internal-ip-reach:c=1,down=0, 12.22.194.0/24
internal-ip-reach:c=1,down=0, 12.22.193.0/24
internal-ip-reach:c=1,down=0, 12.22.192.0/24
internal-ip-reach:c=1,down=0, 12.22.191.0/24
internal-ip-reach:c=1,down=0, 12.22.190.0/24
internal-ip-reach:c=1,down=0, 12.22.189.0/24
internal-ip-reach:c=1,down=0, 12.22.188.0/24
internal-ip-reach:c=1,down=0, 12.22.187.0/24
internal-ip-reach:c=1,down=0, 12.22.186.0/24
internal-ip-reach:c=1,down=0, 12.22.185.0/24
internal-ip-reach:c=1,down=0, 12.22.184.0/24
internal-ip-reach:c=1,down=0, 12.22.183.0/24
internal-ip-reach:c=1,down=0, 12.22.182.0/24
internal-ip-reach:c=1,down=0, 12.22.181.0/24
internal-ip-reach:c=1,down=0, 12.22.180.0/24
internal-ip-reach:c=1,down=0, 12.22.179.0/24
```

tlv#3 =(128, 252):

```
internal-ip-reach:c=1,down=0, 12.22.178.0/24
internal-ip-reach:c=1,down=0, 12.22.177.0/24
internal-ip-reach:c=1,down=0, 12.22.176.0/24
internal-ip-reach:c=1,down=0, 12.22.175.0/24
internal-ip-reach:c=1,down=0, 12.22.174.0/24
internal-ip-reach:c=1,down=0, 12.22.173.0/24
internal-ip-reach:c=1,down=0, 12.22.172.0/24
```

```
internal-ip-reach:c=1,down=0, 12.22.171.0/24
internal-ip-reach:c=1,down=0, 12.22.170.0/24
internal-ip-reach:c=1,down=0, 12.22.169.0/24
internal-ip-reach:c=1,down=0, 12.22.168.0/24
internal-ip-reach:c=1,down=0, 12.22.167.0/24
internal-ip-reach:c=1,down=0, 12.22.166.0/24
internal-ip-reach:c=1,down=0, 12.22.165.0/24
internal-ip-reach:c=1,down=0, 12.22.164.0/24
internal-ip-reach:c=1,down=0, 12.22.163.0/24
internal-ip-reach:c=1,down=0, 12.22.162.0/24
internal-ip-reach:c=1,down=0, 12.22.161.0/24
internal-ip-reach:c=1,down=0, 12.22.160.0/24
internal-ip-reach:c=1,down=0, 12.22.159.0/24
internal-ip-reach:c=1,down=0, 12.22.158.0/24
```

tlv#4 =(128, 252):

```
internal-ip-reach:c=1,down=0, 12.22.157.0/24
internal-ip-reach:c=1,down=0, 12.22.156.0/24
internal-ip-reach:c=1,down=0, 12.22.155.0/24
internal-ip-reach:c=1,down=0, 12.22.154.0/24
internal-ip-reach:c=1,down=0, 12.22.153.0/24
internal-ip-reach:c=1,down=0, 12.22.152.0/24
internal-ip-reach:c=1,down=0, 12.22.151.0/24
internal-ip-reach:c=1,down=0, 12.22.150.0/24
internal-ip-reach:c=1,down=0, 12.22.149.0/24
internal-ip-reach:c=1,down=0, 12.22.148.0/24
internal-ip-reach:c=1,down=0, 12.22.147.0/24
internal-ip-reach:c=1,down=0, 12.22.146.0/24
internal-ip-reach:c=1,down=0, 12.22.145.0/24
internal-ip-reach:c=1,down=0, 12.22.144.0/24
internal-ip-reach:c=1,down=0, 12.22.143.0/24
internal-ip-reach:c=1,down=0, 12.22.142.0/24
internal-ip-reach:c=1,down=0, 12.22.141.0/24
internal-ip-reach:c=1,down=0, 12.22.140.0/24
internal-ip-reach:c=1,down=0, 12.22.139.0/24
internal-ip-reach:c=1,down=0, 12.22.138.0/24
internal-ip-reach:c=1,down=0, 12.22.137.0/24
```

tlv#5 =(128, 252):

```
internal-ip-reach:c=1,down=0, 12.22.136.0/24
internal-ip-reach:c=1,down=0, 12.22.135.0/24
internal-ip-reach:c=1,down=0, 12.22.134.0/24
internal-ip-reach:c=1,down=0, 12.22.133.0/24
```

```
internal-ip-reach:c=1,down=0, 12.22.132.0/24
internal-ip-reach:c=1,down=0, 12.22.131.0/24
internal-ip-reach:c=1,down=0, 12.22.130.0/24
internal-ip-reach:c=1,down=0, 12.22.129.0/24
internal-ip-reach:c=1,down=0, 12.22.128.0/24
internal-ip-reach:c=1,down=0, 12.22.127.0/24
internal-ip-reach:c=1,down=0, 12.22.126.0/24
internal-ip-reach:c=1,down=0, 12.22.125.0/24
internal-ip-reach:c=1,down=0, 12.22.124.0/24
internal-ip-reach:c=1,down=0, 12.22.123.0/24
internal-ip-reach:c=1,down=0, 12.22.122.0/24
internal-ip-reach:c=1,down=0, 12.22.121.0/24
internal-ip-reach:c=1,down=0, 12.22.120.0/24
internal-ip-reach:c=1,down=0, 12.22.119.0/24
internal-ip-reach:c=1,down=0, 12.22.118.0/24
internal-ip-reach:c=1,down=0, 12.22.117.0/24
internal-ip-reach:c=1,down=0, 12.22.116.0/24

internal-ip-reach:c=1,down=0, 12.22.115.0/24
internal-ip-reach:c=1,down=0, 12.22.114.0/24
internal-ip-reach:c=1,down=0, 12.22.113.0/24
internal-ip-reach:c=1,down=0, 12.22.112.0/24
internal-ip-reach:c=1,down=0, 12.22.111.0/24
internal-ip-reach:c=1,down=0, 12.22.110.0/24
internal-ip-reach:c=1,down=0, 12.22.109.0/24
internal-ip-reach:c=1,down=0, 12.22.108.0/24
internal-ip-reach:c=1,down=0, 12.22.107.0/24
internal-ip-reach:c=1,down=0, 12.22.106.0/24
internal-ip-reach:c=1,down=0, 12.22.105.0/24
internal-ip-reach:c=1,down=0, 12.22.104.0/24
internal-ip-reach:c=1,down=0, 12.22.103.0/24
internal-ip-reach:c=1,down=0, 12.22.102.0/24
internal-ip-reach:c=1,down=0, 12.22.101.0/24
internal-ip-reach:c=1,down=0, 12.22.100.0/24
internal-ip-reach:c=1,down=0, 12.22.99.0/24
internal-ip-reach:c=1,down=0, 12.22.98.0/24
internal-ip-reach:c=1,down=0, 12.22.97.0/24
internal-ip-reach:c=1,down=0, 12.22.96.0/24
internal-ip-reach:c=1,down=0, 12.22.95.0/24Switch#
```

5.7.55 show ip isis event-log

Function

The **show ip isis event-log** command displays logs of an ISIS internal event.

Format

show ip isis event-log

Parameter

NA

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

View logs of an ISIS internal event.

```
Switch>show ip isis event-log
ISIS Internal Event Log
2018/04/09 10:50:00(205ms)(isis-1) spf-request level up
2018/04/09 10:50:00(206ms)(isis-1) route calculate,time=0,L1/L2/V4/V6=0/0/0/0
2018/04/09 10:50:00(206ms)(isis-1) route calculate,time=0,L1/L2/V4/V6=0/0/0/0
2018/04/09 10:50:00(206ms)(isis-1) route calculate,time=0,L1/L2/V4/V6=0/0/0/0
2018/04/09 10:50:00(206ms)(isis-1) route calculate,time=0,L1/L2/V4/V6=0/0/0/0
2018/04/09 10:50:00(206ms)(isis-1) route calculate,time=0,L1/L2/V4/V6=0/0/0/0
2018/04/09 10:50:00(208ms)(isis-2) spf-request level up
2018/04/09 10:50:00(208ms)(isis-2) route calculate,time=0,L1/L2/V4/V6=0/0/0/0
2018/04/09 10:50:00(208ms)(isis-2) route calculate,time=0,L1/L2/V4/V6=0/0/0/0
2018/04/09 10:50:00(208ms)(isis-2) route calculate,time=0,L1/L2/V4/V6=0/0/0/0
2018/04/09 10:50:00(209ms)(isis-2) route calculate,time=0,L1/L2/V4/V6=0/0/0/0
2018/04/09 10:50:00(209ms)(isis-2) route calculate,time=0,L1/L2/V4/V6=0/0/0/0
2018/04/09 10:50:01(502ms)(isis-2) spf-request wait lsp rebuild
2018/04/09 10:50:01(502ms)(isis-1) spf-request wait lsp rebuild
2018/04/09 10:50:02(42ms)(isis-1) 100GigaEthernet1/1/1-CID-2 l2 adj 0010.9400.003c down
2018/04/09 10:50:02(42ms)(isis-2) 100GigaEthernet1/1/1.1-CID-1 l2 adj 0010.9400.003f down
2018/04/09 10:50:02(92ms)(isis-1) rebuild l2 lsp 1000.0000.0002.00.00,seq 1,len 53
```

```

2018/04/09 10:50:03(43ms)(isis-2) spf-request wait lsp rebuild
2018/04/09 10:50:04(293ms)(isis-1) route calculate,time=0,L1/L2/V4/V6=0/1/1/0
2018/04/09 10:50:04(783ms)(isis-2) rebuild l2 lsp 0000.0000.0002.00.00,seq 1,len 87
2018/04/09 10:50:05(885ms)(isis-2) route calculate,time=0,L1/L2/V4/V6=0/1/1/1
2018/04/09 10:50:13(801ms)(isis-2) 100GigaEthernet1/1/1.1-CID-1 l2 adj 0010.9400.003f up
2018/04/09 10:50:13(801ms)(isis-2) spf-request create lsp
2018/04/09 10:50:14(179ms)(isis-1) 100GigaEthernet1/1/1-CID-2 l2 adj 0010.9400.003c up
2018/04/09 10:50:14(179ms)(isis-1) spf-request create lsp
2018/04/09 10:50:14(800ms)(isis-2) spf-request wait lsp rebuild
2018/04/09 10:50:15(170ms)(isis-1) spf-request wait lsp rebuild
2018/04/09 10:50:15(800ms)(isis-2) rebuild l2 lsp 0000.0000.0002.00.00,seq 2,len 100
2018/04/09 10:50:15(800ms)(isis-2) rebuild l2 lsp 0000.0000.0002.01.00,seq 1,len 51
2018/04/09 10:50:16(171ms)(isis-1) rebuild l2 lsp 1000.0000.0002.00.00,seq 2,len 66
2018/04/09 10:50:16(171ms)(isis-1) rebuild l2 lsp 1000.0000.0002.01.00,seq 1,len 51
2018/04/09 10:50:16(2ms)(isis-2) route calculate,time=0,L1/L2/V4/V6=0/2/1/1
2018/04/09 10:50:17(373ms)(isis-1) route calculate,time=0,L1/L2/V4/V6=0/2/1/0
2018/04/09 10:50:24(763ms)(isis-2) spf-request create lsp
2018/04/09 10:50:24(763ms)(isis-2) rx changed l2 lsp 0010.9400.003f.00.00,seq 5166,len 1460
Switch>

```

5.7.56 show {ip|ipv6} isis frr route

Function

The **show {ip|ipv6} isis frr route** displays the ISIS FRR route.

Format

- **show { ip | ipv6 } isis frr route**
- **show { ip | ipv6 } isis frr route { level-1 | level-2 }**
- **show { ip | ipv6 } isis frr route vpn-instance *name***

Parameter

Parameter	Description	Value
level-1	Specifies the route of a level-1 ISIS.	-
level-2	Specifies the route of a level-2 ISIS.	-
name	Specifies the name of an ISIS multi-instance process of a VPN.	The value is a character string.

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

View the ISIS FRR route.

```
Switch>show ip isis frr route
Total number of IP frr route is :4
level      dest                nexthop          mac              cost
Level-1    1.1.1.0/24          1.2.2.4          0000:00a0:000a   35
Level-1    2.2.2.0/24          1.2.2.4          0000:00a0:000a   35
Level-1    2.2.3.0/24          1.2.2.4          0000:00a0:000a   35
Level-1    5.5.5.0/24          1.2.2.4          0000:00a0:000a   25

Switch(config)#
```

5.7.57 show ip isis hostname

Function

The **show ip isis hostname** command displays mapping of the ISIS dynamic host.

Format

show ip isis hostname

Parameter

NA

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

Display mapping of the ISIS dynamic host.

```
Switch>show ip isis hostname
Switch#
```

5.7.58 show ip isis import-route

Function

The **show ip isis import-route** command displays the ISIS route redistribution information.

Format

show ip isis import-route

Parameter

NA

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

Display the ISIS route redistribution information.

```
Switch>show ip isis import-route
Switch>
```

5.7.59 show ip isis interface

Function

The **show ip isis interface** command displays information or details of the interface enabled with ISIS.

Format

- **show ip isis interface**
- **show ip isis interface verbose** [*if-name*]

Parameter

Parameter	Description	Value
if-name	Name	The value is a character string.

Default Value

NA

View

Common user view

Usage Guidelines

If the authentication type is nonAuth, password is not displayed in the ISIS interface information.

Example

View the ISIS interface information.

```
Switch>show ip isis interface
```

```
Interface information for IS-IS(1)
```

```
The total number of isis(1) interface is:1
```

Interface	CircID	Adminstate	Type	Level	MeshEnable	SmallHello
vlan-11	1	on	broadcast	L1-2	inactive	false

```
Switch(config)#
```

View details of the ISIS interface.

```
Switch>show ip isis interface verbose
```

```
Interface information for IS-IS(1)
```

Interface	CircID	Adminstate	Type	Level	MeshEnable	SmallHello
vlan-2	1	on	ptToPt	L1-2	Set	False

```

Ip isis state           :enabled
Ipv6 isis state         :disabled
Ext-domain              :enabled
Passive interface       :yes
Three-way-handshake     :enabled
Bfd state               :enabled
Mesh group              :65535
Level-1 metric          :63
Level-1 wide metric     :16777215
Level-1 priority        :127
Level-1 hello multiplier :100
Level-1 hello time      :255s
Level-1 DIS hello time  :1s
Level-1 flood interval  :30s

```



```

Level-1 LSP retransmit interval :2s
Level-1 CSNP interval          :600s
Level-1 PSNP interval          :120s
Level-1 adjacency number       :0
Level-1 level id               :0001.0002.0003
Level-1 DIS id                 :0000.0000.0000.00
Level-1 auth type              :md5
Level-1 auth key               :9df3cc012575c84c
Level-2 metric                 :0
Level-2 wide metric            :0
Level-2 priority               :0
Level-2 hello multiplier       :2
Level-2 hello time             :3s
Level-2 DIS hello time        :1s
Level-2 flood interval         :30s
Level-2 LSP retransmit interval :2s
Level-2 CSNP interval          :1s
Level-2 PSNP interval          :1s
Level-2 adjacency number       :0
Level-2 level id               :0001.0002.0003
Level-2 DIS id                 :0000.0000.0000.00
Level-2 auth type              :simple
Level-2 auth key               :9df3cc012575c84c
Switch(config)#

```

5.7.60 show ip isis lsp-log

Function

The **show ip isis lsp-log** command displays SPF calculation logs of an ISIS instance.

Format

show ip isis lsp-log

Parameter

NA

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

View SPF calculation logs of an ISIS instance.

```
Switch>show ip isis lsp-log
Switch#
```

5.7.61 show ip isis lsp-option**Function**

The **show ip isis lsp-option** command displays LSP local options of an ISIS instance.

Format

show ip isis lsp-option

Parameter

NA

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

View LSP local options of an ISIS instance.

```
Local LSP Option of IS-IS(1)
```

```
Level-2
```

```
option#1:t=1,l=4,lsp=0.0,orig=0,tlvstate=2,tlvlen=6
```

```
area:3--10 00 00
```

option#2:t=22,l=74,lsp=0.0,orig=0,tlvstate=2,tlvlen=76

ext-isnbr:10.00.00.00.00.02.02,cost 10

stlv_len=63:

stlv#1 =(3, 4):

admingroup = 0

stlv#2 =(6, 4):

loacalIP = 192.168.2.1

stlv#3 =(9, 4):

maxBW = 0

stlv#4 =(10, 4):

maxRsveBW = 0

stlv#5 =(11, 32):

unRsveBW[0][0] = 0

unRsveBW[0][1] = 0

unRsveBW[0][2] = 0

unRsveBW[0][3] = 0

unRsveBW[0][4] = 0

unRsveBW[0][5] = 0

unRsveBW[0][6] = 0

unRsveBW[0][7] = 0

stlv#6 =(18, 3):

eCost = 0

option#3:t=22,l=11,lsp=2.0,orig=0,tlvstate=2,tlvlen=24

ext-isnbr:00.10.94.00.00.3c.00,cost 0

option#4:t=22,l=11,lsp=2.0,orig=0,tlvstate=2,tlvlen=24

ext-isnbr:10.00.00.00.00.02.00,cost 0

option#5:t=129,l=2,lsp=0.0,orig=0,tlvstate=2,tlvlen=4

proto:cc.8e.

option#6:t=132,l=4,lsp=0.0,orig=0,tlvstate=2,tlvlen=6

ifip:192.168.2.1

option#7:t=135,l=8,lsp=0.0,orig=1,tlvstate=2,tlvlen=10

te-ipreach: c=10, down=0,192.168.2.0./24

option#8:t=232,l=16,lsp=0.0,orig=0,tlvstate=2,tlvlen=18

ifip6:2000::1

option#9:t=236,l=14,lsp=0.0,orig=1,tlvstate=2,tlvlen=16

ip6reach:c=10,f=0,2000::/64

Local LSP Option of IS-IS(2)

Level-2

option#1:t=1,l=4,lsp=0.0,orig=0,tlvstate=2,tlvlen=6

area:3--10 00 01

option#2:t=22,l=11,lsp=0.0,orig=0,tlvstate=2,tlvlen=13

ext-isnbr:00.00.00.00.00.02.01,cost 10

option#3:t=22,l=11,lsp=1.0,orig=0,tlvstate=2,tlvlen=24

ext-isnbr:00.00.00.00.00.02.00,cost 0

option#4:t=22,l=11,lsp=1.0,orig=0,tlvstate=2,tlvlen=24

ext-isnbr:00.10.94.00.00.3f.00,cost 0

option#5:t=129,l=2,lsp=0.0,orig=0,tlvstate=2,tlvlen=4

proto:cc.8e.

option#6:t=132,l=4,lsp=0.0,orig=0,tlvstate=2,tlvlen=6

ifip:192.168.4.1

option#7:t=135,l=8,lsp=0.0,orig=1,tlvstate=2,tlvlen=10

te-ipreach: c=10, down=0,192.168.4.0./24

option#8:t=232,l=16,lsp=0.0,orig=0,tlvstate=2,tlvlen=18

ifip6:1000:1:192:4::1

option#9:t=236,l=14,lsp=0.0,orig=1,tlvstate=2,tlvlen=16

ip6reach:c=10,f=0,1000:1:192:4::/64

5.7.62 show ip isis neighbor

Function

The **show ip isis neighbor** command displays information on an ISIS neighbor.

Format

- **show ip isis neighbor**
- **show ip isis neighbor verbose**

Parameter

NA

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

View the ISIS neighbor information.

```
Switch# show ip isis neighbor
                               Neighbor information for IS-IS(1)
The total number of isis(1) neighbor is:2
Interface   Level      ID          MAC          Priority   HoldTime   UpTime      Name
vlan-1111   L1      0020.0200.2002  0004.6790.ffff   64    19    0 days 0:00:20    ---
vlan-1111   L2      0020.0200.2002  0004.6790.ffff   64    29    0 days 0:00:19    ---
Switch#
```

View details of an ISIS neighbor.

```
Switch# show ip isis neighbors verbose
Neighbor information for IS-IS(1)
Neighbor sequence      : 1
Interface              : vlan-20
Level                  : L2
System ID              : 0002.0002.0002
State                  : up
Support protocol       : iso,ip
Area                   : 47
```

```

Ip/Ipv6           : 192.1.2.100
System type       : L1L2IntermediateSystem
3way state        : up
Life time         : 30s
Life time remain  : 8s
Extend cid        : 0

Neighbor sequence : 2
Interface         : vlan-20
Level            : L1
System ID         : 0002.0002.0002
State            : up
Support protocol  : iso,ip
Area             : 47
Ip/Ipv6          : 192.1.2.100
System type       : L1L2IntermediateSystem
3way state        : up
Life time         : 30s
Life time remain  : 8s
Extend cid        : 0

```

Switch#

5.7.63 show {ip|ipv6} isis route

Function

The **show {ip|ipv6} isis route** command displays the ISIS route information.

Format

- **show { ip | ipv6 } isis route**
- **show { ip | ipv6 } isis route *dst-ip-address***
- **show { ip | ipv6 } isis route { *level-1* | *level-2* }**
- **show { ip | ipv6 } isis route all**
- **show { ip | ipv6 } isis route *vpn-instance name***

Parameter

Parameter	Description	Value
level-1	Specifies the route of a level-1 ISIS.	-
level-2	Specifies the route of a level-2 ISIS.	-
name	Specifies the name of an ISIS multi-instance	The value is a character string.

Parameter	Description	Value
	process of a VPN.	
dst-ip-address	Specifies a destination IPv4 or IPv6 address.	The value is in dotted decimal notation. In this case, a 128-bit IP address is divided into 8 groups separated by a colon (:). 16 bits of each group are indicated by four hexadecimal characters (0 to 9 and A to F). Every "X" represents a group of hexadecimal digits.

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

Display the ISIS route information.

Switch>show ip isis route				
Total number of IP route is :1				
level	dest	nexthop	mac	cost
Level-1	192.1.1.0/24	192.1.1.100	e005:c56e:cdaf	20
Switch>show ip isis route all				
Total number of IP route is :9				
level	dest	nexthop	mac	cost
Level-1	1.1.1.0/24	1.1.1.2	0000:00b8:0001	10
Level-1	1.1.1.0/24	1.2.2.4	0000:00a0:000a	35
Level-1	1.2.2.0/24	1.2.2.4	0000:00a0:000a	10
Level-1	2.2.2.0/24	1.1.1.2	0000:00b8:0001	10
Level-1	2.2.2.0/24	1.2.2.4	0000:00a0:000a	35
Level-1	2.2.3.0/24	1.1.1.2	0000:00b8:0001	10
Level-1	2.2.3.0/24	1.2.2.4	0000:00a0:000a	35
Level-1	5.5.5.0/24	1.2.2.4	0000:00a0:000a	10
Level-1	5.5.5.0/24	1.2.2.4	0000:00a0:000a	25
Switch#				

5.7.64 show ip isis spf-log

Function

The **show ip isis spf-log** command displays SPF calculation logs of an ISIS instance.

Format

show ip isis spf-log

Parameter

NA

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

View SPF calculation logs of an ISIS instance.

Switch>show ip isis spf-log							
SPF Log of IS-IS(1)							
date	period	L1Node	L2Node	calls	v4Route	v6Route	reason
2018/04/09 11:35:59	0	0	2	0	0		level up
0000.0000.0000.00.00							
2018/04/09 11:36:17	0	0	2	0	0		create lsp
0000.0000.0000.00.01							
2018/04/09 11:40:59	0	0	1	0	0		periodic spf
0000.0000.0000.00.01							
2018/04/09 11:43:42	1	0	1	0	0		delete lspf
0000.0000.0000.00.01							
2018/04/09 11:43:42	0	0	1	0	0		delete lspf
0000.0000.0000.00.01							
2018/04/09 11:43:42	0	0	3	0	0		fast spfspf
0000.0000.0000.00.01							
2018/04/09 11:43:45	0	1	1	13	0	1	rebuild lspf
1000.0000.0002.00.01							

2018/04/09 11:43:53 0	0	1	2	0	1	delete lspff	
1000.0000.0002.00.01							
2018/04/09 11:43:53 0	0	0	2	0	0	delete lspff	
1000.0000.0002.00.01							
2018/04/09 11:43:54 0	0	0	7	0	0	delete lspff	
1000.0000.0002.00.00							
2018/04/09 11:43:58 0	0	1	6	0	1	rebuild lspf	
1000.0000.0002.00.00							
2018/04/09 11:44:13 0	0	1	1	1	1	rebuild lspf	
1000.0000.0002.00.00							
2018/04/09 11:44:19 0	0	1	1	1	1	add adj ifip	
1000.0000.0002.00.00							
2018/04/09 11:44:29 0	0	2	4	1	1	rebuild lspf	
1000.0000.0002.02.00							
2018/04/09 11:44:52 106	0	3	71	5001	1	create lsppp	
0010.9400.003c.00.46							
2018/04/09 11:45:59 9	0	3	1	5001	1	periodic spf	
0010.9400.003c.00.46							
SPF Log of IS-IS(2)							
date	period	L1Node	L2Node	calls	v4Route	v6Route	reason
2018/04/09 10:50:00 0	0	0	2	0	0		level up spf
0000.0000.0000.00.00							
2018/04/09 10:50:00 0	0	0	0	0	0		level up spf
0000.0000.0000.00.00							
2018/04/09 10:50:00 0	0	0	0	0	0		level up spf
0000.0000.0000.00.00							
2018/04/09 10:50:00 0	0	0	7	0	0		delete lspff
0000.0000.0002.00.00							
2018/04/09 10:50:00 0	0	0	4	0	0		delete lspff
0000.0000.0002.00.00							
2018/04/09 10:50:05 0	0	1	8	1	1		rebuild lspf
0000.0000.0002.00.00							
2018/04/09 10:50:16 0	0	2	4	1	1		rebuild lspf
0000.0000.0002.01.00							
2018/04/09 10:50:32 98	0	3	71	5001	1		create lsppp
0010.9400.003f.00.46							
2018/04/09 10:55:01 8	0	3	1	5001	1		periodic spf
0010.9400.003f.00.46							
2018/04/09 11:00:01 8	0	3	1	5001	1		periodic spf
0010.9400.003f.00.46							
2018/04/09 11:05:01 8	0	3	1	5001	1		periodic spf

```

0010.9400.003f.00.46
  2018/04/09 11:10:01 8      0      3      1      5001      1      periodic spf
0010.9400.003f.00.46
  2018/04/09 11:15:01 8      0      3      1      5001      1      periodic spf
0010.9400.003f.00.46
  2018/04/09 11:20:01 8      0      3      1      5001      1      periodic spf
0010.9400.003f.00.46
  2018/04/09 11:25:01 8      0      3      1      5001      1      periodic spf
0010.9400.003f.00.46
  2018/04/09 11:30:01 9      0      3      1      5001      1      periodic spf
0010.9400.003f.00.46
  2018/04/09 11:35:01 8      0      3      1      5001      1      periodic spf
0010.9400.003f.00.46
  2018/04/09 11:35:50 8      0      3      5      5001      1      rebuild lspf
0000.0000.0002.00.00
  2018/04/09 11:40:01 9      0      3      1      5001      1      periodic spf
0000.0000.0002.00.00
  2018/04/09 11:45:01 8      0      3      1      5001      1      periodic spf
0000.0000.0002.00.00
Switch>

```

5.7.65 show ip isis spf-tree

Function

The **show ip isis spf-tree** command displays the SPF tree topology.

Format

show ip isis spf-tree

Parameter

NA

Default Value

NA

View

Common user view

Usage Guidelines

The generated SPF tree can be used for route calculation only when the SPF state is complete and I-SPF calculation is completed.

Example

View the SPF tree topology.

```
Switch>show ip isis spf-tree
```

SPF-tree information for IS-IS(1)

Topo	Level	ID	C-NHop2Dest	C-NHop2Root	C-2MNHop	C-2NHop	Role	Nexthop	CID
0	1	1357.affd.1111.00-00	N/A	N/A	N/A	0	Main	N/A	N/A
0	1	1357.affd.1111.01-00	N/A	N/A	N/A	10	Main	0000.0000.0000	1
0	1	1357.affd.1111.02-00	N/A	N/A	N/A	10	Main	0000.0000.0000	2
0	1	1357.affd.2222.00-00	N/A	N/A	N/A	10	Main	1357.affd.2222	2
							1357.affd.2222	1	
0	2	1357.affd.1111.00-00	N/A	N/A	N/A	0	Main	N/A	N/A
0	2	1357.affd.1111.01-00	N/A	N/A	N/A	10	Main	0000.0000.0000	1
0	2	1357.affd.1111.02-00	N/A	N/A	N/A	10	Main	0000.0000.0000	2
0	2	1357.affd.2222.00-00	N/A	N/A	N/A	10	Main	1357.affd.2222	2
							1357.affd.2222	1	

```
Switch#
```

5.7.66 show ip isis statistic**Function**

The **show ip isis statistic** command displays statistics on an ISIS instance, an ISIS interface, an ISIS memory, or ISIS route update.

Format

- **show ip isis statistic**
- **show ip isis statistic interface**
- **show ip isis statistic memory**
- **show ip isis statistic route-update**

Parameter

NA

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

Display ISIS statistics.

```
Switch(config-vlanif-1)#show ip isis statistic
```

Statistic information for IS-IS(1)

Level-1 Statistic

ID Field Length Mismatches	:0
Auth Type Fails	:0
Auth Fails	:0
Corrupt LSPs	:0
LSP Errors	:0
LSP Database Overloads	:0
Own LSP Purges	:0
SeqNum Skips	:0
Attmpt To Exceed Max SeqNums	:0
Manual Address DropFromAreas	:0
SPF Runs	:11

Level-2 Statistic

ID Field Length Mismatches	:0
Auth Type Fails	:0
Auth Fails	:0
Corrupt LSPs	:0
LSP Errors	:0
LSP Database Overloads	:0
Own LSP Purges	:0
SeqNum Skips	:0
Attmpt To Exceed Max SeqNums	:0
Manual Address DropFromAreas	:0
SPF Runs	:3

```
Switch(config-vlanif-1)#
```

```
Switch>show ip isis statistic interface
```

Statistic information for IS-IS(1)

Interface vlan 2 Statistic

Level-1 ID Field Length Mismatches	:0
Level-1 Auth Type Fails	:0

```

Level-1 Auth Fails :0
Level-1 MaxAreaAddr Mismatches :0
Level-1 Rejected Adjacencies :0
Level-1 Adjacency Changes :0
Level-1 Init Fails :0
Level-1 Designated IS Changes :0
Level-1 Out Hellos :111
Level-1 Out LSPs :0
Level-1 Out CSNPs :0
Level-1 Out PSNPs :0
Level-1 Out Unknown Packets :0
Level-2 ID Field Length Mismatches :0
Level-2 Auth Type Fails :0
Level-2 Auth Fails :0
Level-2 MaxAreaAddr Mismatches :0
Level-2 Rejected Adjacencies :0
Level-2 Adjacency Changes :0
Level-2 Init Fails :0
Level-2 Designated IS Changes :0

```

Interface vlan 3 Statistic

```

Level-1 ID Field Length Mismatches :0
Level-1 Auth Type Fails :0
Level-1 Auth Fails :0
Level-1 MaxAreaAddr Mismatches :0
Level-1 Rejected Adjacencies :0
Level-1 Adjacency Changes :0
Level-1 Init Fails :0
Level-1 Designated IS Changes :0
Level-2 ID Field Length Mismatches :0
Level-2 Auth Type Fails :0
Level-2 Auth Fails :0
Level-2 MaxAreaAddr Mismatches :0
Level-2 Rejected Adjacencies :0
Level-2 Adjacency Changes :0
Level-2 Init Fails :0
Level-2 Designated IS Changes :0

```

Switch#

5.7.67 show ip isis virtual-system

Function

The **show ip isis virtual-system** command displays information on an ISIS virtual system.

Format

show ip isis virtual-system

Parameter

NA

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

View information on an ISIS virtual system.

```
Switch>show ip isis virtual-system
  Instance  System ID          Index
  1         1111.1111.1111      1
Switch#
```

5.7.68 snmp-trap**Function**

The **snmp-trap** command enables or disables the SNMP alarm reporting function for CFM.

Format

snmp-trap { enable | disable }

Parameter

Parameter	Description	Value
enable	Enables the SNMP alarm reporting function for CFM.	-
disable	Disables the SNMP alarm reporting function for CFM.	-

Default Value

By default, the SNMP alarm reporting function is disabled for CFM.

View

ISIS configuration view

Usage Guidelines

NA

Example

Enable the SNMP trap function of CFM.

```
Switch(config-isis-1)#snmp-trap enable
Switch(config-isis-1)#
```

5.7.69 summary-address**Function**

The **summary-address** command enables address summary/aggregation.

The **no summary-address** command disables address summary.

Format

- **summary-address** (A.B.C.D) (A.B.C.D) { **level-1** | **level-2** }
- **summary-address** (A.B.C.D) (A.B.C.D) **metric** { *metric-value* | **default** } { **level-1** | **level-2** }
- **no summary-address** (A.B.C.D) (A.B.C.D) { **level-1** | **level-2** }

Parameter

Parameter	Description	Value
A.B.C.D	Specifies the IP address for summary.	The value is in dotted decimal notation, for example, A.B.C.D, in which A to D are decimal digits ranging from 0 to 255.
metric-value	Specifies the metric value of addresses to be summarized.	The value is an integer ranging from 0 to 63.
default	Specifies the default metric value of addresses to be summarized.	0

Default Value

By default, route aggregation is not performed.

View

ISIS configuration view

Usage Guidelines

You can run this command for address summary/aggregation. Addresses in multiple groups of a specified level and routes obtained by other routing protocols can be summarized. The metric value for notifying the aggregated route is the smallest one among that of all routes.

Example

Enable address summary/aggregation.

```
Switch(config-isis-1)#summary-address 10.2.3.1 255.255.255.0
Switch(config-isis-1)#
```

5.7.70 summary-prefix

Function

The **summary-prefix** command enables ISIS to generate an IPv6 aggregated route.

The **no summary-prefix** command disables the aggregation.

Format

- **summary-prefix** (*X:X::X:X/M*) { **level-1** | **level-2** }
- **summary-prefix** (*X:X::X:X/M*) **metric** { *metric-value* | **default** } { **level-1** | **level-2** }
- **no summary-address** (*X:X::X:X/M*) { **level-1** | **level-2** }

Parameter

Parameter	Description	Value
X:X::X:X/M	Specifies an IPv6 address and its mask to be summarized.	-
metric-value	Specifies the metric value of addresses to be summarized.	The value is an integer ranging from 0 to 63.
default	Specifies the default metric value of addresses to be summarized.	0

Default Value

By default, route aggregation is not performed.

View

ISIS configuration view

Usage Guidelines

You can run this command for address summary/aggregation. Addresses in multiple groups of a specified level and routes obtained by other routing protocols can be summarized. The metric value for notifying the aggregated route is the smallest one among that of all routes.

Example

Enable ISIS to generate an aggregated route 2000::/32.

```
Switch(config-isis-1)#summary-prefix 2000::/32 level-1
Switch(config-isis-1)#
```

5.7.71 timer spf max-interval init-interval incr-interval

Function

The **timer spf** command sets the adjustment parameter of the SPF calculation intelligent timer.

Format

timer spf max-interval { *max-interval* | **default** } **init-interval** { *init-interval* | **default** } **incr-interval** { *incr-interval* | **default** }

Parameter

Parameter	Description	Value
max-interval	Specifies the maximum delay of the SPF calculation timer.	The value is an integer ranging from 5 to 120.
init-interval	Specifies the initial delay of the SPF calculation timer.	The value is an integer ranging from 1 to 60000.
incr-interval	Specifies the incremental delay of the SPF calculation timer for repeated schedule.	The value is an integer ranging from 1 to 60000.

Default Value

The default value of above parameters is 5, 50, and 200 respectively.

View

ISIS configuration view

Usage Guidelines

NA

Example

Set the maximum delay of the SPF calculation timer to 20.

```
Switch(config-isis-1)#timer spf max-interval 20 init-interval default incr-interval default
```

```
Switch(config-isis-1)#
```

5.7.72 traffic-engineer

Function

The **traffic-engineer** command enables the traffic engineer function for ISIS.

Format

traffic-engineer { **enable** | **disable** } { **level-1** | **level-2** }

Parameter

NA

Default Value

NA

View

ISIS configuration view

Usage Guidelines

NA

Example

Enable the traffic engineer function for ISIS.

```
Switch(config-router-isis)#traffic-engineer enable level-1
Switch(config-router-isis)#
```

5.7.73 virtual-system

Function

The **virtual-system** command sets the ISIS virtual system ID.

The **no virtual-system** command deletes the ID of a virtual system.

Format

- **virtual-system** *sys-id*
- **no virtual-system** *sys-id*

Parameter

Parameter	Description	Value

Parameter	Description	Value
sys-id	Specifies the virtual system ID of an ISIS process.	The value contains up to 6 bytes and is in the format of XXXX.XXXX.XXXX.

Default Value

By default, no virtual system ID is set for the ISIS process.

View

ISIS configuration view

Usage Guidelines

Same as the ordinary ID, the virtual ID must also be unique in the routing domain.

Example

Set the virtual system ID of an ISIS process.

```
Switch(config-isis-1)#virtual-system 1111.1111.1111
Switch(config-isis-1)#
```

5.8 Routing Policy Configuration Commands

5.8.1 apply as-path

Function

The **apply as-path** command sets an action in the routing policy to change the AS Path property of a BGP route.

Format

- **apply as-path** *as-path-number1* { **additive** | **overwrite** | **delete** }
- **apply as-path** *as-path-number1 as-path-number2* { **additive** | **overwrite** | **delete** }
- **apply as-path** *as-path-number1 as-path-number2 as-path-number3* { **additive** | **overwrite** | **delete** }
- **apply as-path** *as-path-number1 as-path-number2 as-path-number3 as-path-number4* { **additive** | **overwrite** | **delete** }
- **apply as-path** *as-path-number1 as-path-number2 as-path-number3 as-path-number4 as-path-number5* { **additive** | **overwrite** | **delete** }

- **apply as-path** *as-path-number1 as-path-number2 as-path-number3 as-path-number4 as-path-number5 as-path-number6* { **additive** | **overwrite** | **delete** }
- **apply as-path** *as-path-number1 as-path-number2 as-path-number3 as-path-number4 as-path-number5 as-path-number6 as-path-number7* { **additive** | **overwrite** | **delete** }
- **apply as-path** *as-path-number1 as-path-number2 as-path-number3 as-path-number4 as-path-number5 as-path-number6 as-path-number7 as-path-number8* { **additive** | **overwrite** | **delete** }
- **apply as-path** *as-path-number1 as-path-number2 as-path-number3 as-path-number4 as-path-number5 as-path-number6 as-path-number7 as-path-number8 as-path-number9* { **additive** | **overwrite** | **delete** }
- **apply as-path** *as-path-number1 as-path-number2 as-path-number3 as-path-number4 as-path-number5 as-path-number6 as-path-number7 as-path-number8 as-path-number9 as-path-number10* { **additive** | **overwrite** | **delete** }
- **apply as-path none overwrite**
- **no apply as-path**

Parameter

Parameter	Description	Value
as-path-number1 as-path-number2 as-path-number3 as-path-number4 as-path-number5 as-path-number6 as-path-number7 as-path-number8 as-path-number9 as-path-number10	Specifies the dotted AS number to be replaced or added. You can specify up to 10 AS numbers in one command at a time.	The value is an integer ranging from 1 to 65535.
additive	Adds the specified AS number to the original AS_Path list.	-
overwrite	Uses the specified AS number to overwrite the original AS_Path list.	-
delete	Deletes specified AS numbers from the original AS_Path list.	-
none overwrite	Clears the original AS_Path list.	-

Default Value

By default, the routing policy is not configured with any action to change the AS_Path property of a BGP route.

View

Routing policy configuration view

Usage Guidelines

NA

Example

Set the action to add the specified AS number 100 to the original AS Path list.

```
Switch(config)#route-policy fhn permit node 12
Switch(config-route-policy)#apply as-path 100 additive
Switch(config-route-policy)#
```

5.8.2 apply cost

Function

The **apply cost** command sets the route cost in the routing information.

The **no apply cost** command restores the route cost to the default value.

Format

- **apply cost** *cost-value*
- **apply cost** { **plus** | **minus** } *cost-value*
- **no apply cost**

Parameter

Parameter	Description	Value
cost-value	Specifies a route cost value.	The value is an integer ranging from 0 to 4294967295.
plus	Specifies an increased cost value.	-
minus	Specifies a decreased cost value.	-

Default Value

By default, no route cost is configured.

View

Routing policy configuration view

Usage Guidelines

NA

Example

Set the route cost in the routing information to 200.

```
Switch(config)#route-policy fhn permit node 12
Switch(config-route-policy)#apply cost 200
Switch(config-route-policy)#
```

5.8.3 apply cost-type**Function**

The **apply cost-type** command sets the route cost type in the routing information.

The **no apply cost-type** command cancels the route cost type setting.

Format

- **apply cost-type { type-1 | type-2 }**
- **no apply cost-type**

Parameter

Parameter	Description	Value
type-1	Indicates that the route is set to OSPF external Type-1.	-
type-2	Indicates that the route is set to OSPF external Type-2.	-

Default Value

By default, the route cost type is not configured.

View

Routing policy configuration view

Usage Guidelines

NA

Example

Set the route cost type to OSPF external Type-1.

```
Switch(config)#route-policy fhn permit node 12
```

```
Switch(config-route-policy)#apply cost-type type-1
Switch(config-route-policy)#
```

5.8.4 apply local-preference

Function

The **apply local-preference** command sets the local priority of a BGP route.

The **no apply local-preference** command cancels the configuration.

Format

- **apply local-preference** *local-priority*
- **no apply local-preference**

Parameter

Parameter	Description	Value
local-priority	Specifies the local priority of a BGP route.	The value is an integer ranging from 0 to 4294967295.

Default Value

By default, no local priority is specified for the BGP route.

View

Routing policy configuration view

Usage Guidelines

NA

Example

Set the local priority of a BGP route to 150.

```
Switch(config)#route-policy fhn permit node 12
Switch(config-route-policy)#apply local-preference 150
Switch(config-route-policy)#
```

5.8.5 apply isis

Function

The **apply isis** command sets an action in the routing policy to change the level of routes imported to the ISIS protocol.

Format

- **apply isis { level-1 | level-2 | level-1-2 }**
- **no apply isis**

Parameter

Parameter	Description	Value
level-1	Specifies the level of ISIS routes to Level-1.	-
level-2	Specifies the level of ISIS routes to Level-2.	-
level-1-2	Specifies the level of ISIS routes to Level-1-2.	-

Default Value

By default, no action is set in the routing policy to change the level of routes imported to the ISIS protocol.

View

Routing policy configuration view

Usage Guidelines

NA

Example

Set the level of routes imported to the ISIS protocol to level-1.

```
Switch(config)#route-policy fhn permit node 12
Switch(config-route-policy)#apply isis level-1
Switch(config-route-policy)#
```

5.8.6 apply origin

Function

The **apply origin** command sets the source of the BGP route information.

The **no apply origin** command cancels the configuration.

Format

- **apply origin { igp | incomplete }**
- **apply origin egp *as-number***
- **no apply origin**

Parameter

Parameter	Description	Value

Parameter	Description	Value
igp	Specifies internal routes as the BGP route information source.	-
incomplete	Specifies unknown routes as the BGP route information source.	-
egp	Specifies external routes as the BGP route information source.	-
as-number	Specifies the AS number of a BGP external route.	The value is an integer ranging from 1 to 65535.

Default Value

By default, no source is specified for the BGP route information.

View

Routing policy configuration view

Usage Guidelines

NA

Example

Set the route source to incomplete.

```
Switch(config)#route-policy fhn permit node 12
Switch(config-route-policy)#apply origin incomplete
Switch(config-route-policy)#
```

5.8.7 apply ospf

Function

The **apply ospf** command sets the OSPF translation mode.

The **no apply ospf** command cancels the setting.

Format

- **apply ospf { translate | not-translate }**
- **no apply ospf**

Parameter

Parameter	Description	Value
translate	Indicates that OSPF works in translation mode.	-
not-translate	Indicates that OSPF works in non-translation	-

Parameter	Description	Value
	mode.	

Default Value

By default, the OSPF translation mode is not configured.

View

Routing policy configuration view

Usage Guidelines

NA

Example

Configure the OSPF translation mode.

```
Switch(config)#route-policy fhn permit node 12
Switch(config-route-policy)#apply ospf translate
Switch(config-route-policy)#
```

5.8.8 apply preferred-value**Function**

The **apply preferred-value** command sets the preferred value of a BGP route.

The **no apply preferred-value** command cancels the configuration.

Format

- **apply preferred-value** *preferred-value*
- **no apply preferred-value**

Parameter

Parameter	Description	Value
preferred-value	Specifies the preferred value of a BGP route.	The value is an integer ranging from 0 to 65535.

Default Value

By default, no preferred value is specified for the BGP route.

View

Routing policy configuration view

Usage Guidelines

NA

Example

Set the preferred value of a BGP route to 100.

```
Switch(config)#route-policy fhn permit node 12
Switch(config-route-policy)#apply preferred-value 100
Switch(config-route-policy)#
```

5.8.9 apply tag

Function

The **apply tag** command sets the tag in the routing information.

The **no apply tag** command cancels the tag in the routing information.

Format

- **apply tag** *tag-value*
- **no apply tag**

Parameter

Parameter	Description	Value
tag-value	Specifies the tag in routing information.	The value is an integer ranging from 0 to 4294967295.

Default Value

By default, the routing information tag is not configured.

View

Routing policy configuration view

Usage Guidelines

For RIP protocol, the maximum value of the routing tag field is 65535.

Example

Set the tag in the routing information to 200.

```
Switch(config)#route-policy fhn permit node 12
Switch(config-route-policy)#apply tag 200
Switch(config-route-policy)#
```

5.8.10 debug route-policy

Function

The **debug route-policy** command enables routing policy debugging.

The **no debug route-policy** command disables routing policy debugging.

Format

- **debug route-policy { error | map | config | all }**
- **no debug route-policy { error | map | config | all }**

Parameter

Parameter	Description	Value
error	Indicates the error information generated during routing policy configuration.	-
map	Indicates the mapping entries generated during routing policy configuration.	-
config	Indicates the configuration generated during routing policy matching.	-
all	Indicates all the preceding information.	-

Default Value

By default, routing policy debugging is disabled.

View

Privileged user view

Usage Guidelines

You can use this command to maintain and debug routing policies, and therefore facilitating problem locating.

Example

Enable routing policy debugging and display error information generated for the routing policy.

```
Switch#debug route-policy error
Switch#
```

5.8.11 match aspath

Function

The **match aspath** command sets a match rule based on the AS path filter.

The **no match aspath** command deletes the configured rule.

Format

- **match aspath** *name*
- **no match aspath**

Parameter

Parameter	Description	Value
name	Specifies the ID of an AS path filter.	The value is a string consisting of 1 to 31 characters, without spaces. The value is case sensitive.

Default Value

By default, no match rule based on a process number is not configured.

View

Routing policy configuration view

Usage Guidelines

This command is only applicable to the BGP protocol. To make the match rule take effect, you must run **ip as-path-filter** to define an AS path filter.

Example

Define a route policy named **test**, in which a match rule is defined for the AS path filter 2 referred by the node 10.

```
Switch(config)#route-policy test permit node 10
Switch(config-route-policy)#match aspath a
Switch(config-route-policy)#
```

5.8.12 match community-filter

Function

The **match community-filter** command sets a match rule for a community filter.

The **no match community-filter** command deletes the specified community filter.

Format

- **match community-filter** *community-filter*
- **no match community-filter**

Parameter

Parameter	Description	Value
community-filter	Specifies the ID of a community filter.	The value is an integer ranging from 1 to 99.

Default Value

By default, no community filter is set in the system.

View

Routing policy configuration view

Usage Guidelines

NA

Example

Set the match rule of a community filter to 10.

```
Switch(config)#route-policy fln permit node 12
Switch(config-route-policy)#match community-filter 10
Switch(config-route-policy)#
```

5.8.13 match extcommunity-filter rt**Function**

The **match extcommunity-filter rt** command sets a match rule based on an extension community filter.

The **no match extcommunity-filter rt** command deletes the configured match rule.

Format

- **match extcommunity-filter rt** *extcommunity-filter*
- **no match extcommunity-filter rt** *extcommunity-filter*

Parameter

Parameter	Description	Value
extcommunity-filter	Specifies the ID of an extension community filter.	The value is an integer ranging from 1 to 99.

Default Value

NA

View

Routing policy configuration view

Usage Guidelines

NA

Example

Set the ID of the extension community filter to 10.

```
Switch(config-route-policy)# match extcommunity-filter rt 10
Switch(config-route-policy)#
```

5.8.14 match process**Function**

The **match process** command sets a match rule based on a process number.

The **no match process** command cancels the configuration.

Format

- **match process** *process-number*
- **no match process**

Parameter

Parameter	Description	Value
process-number	Specifies a protocol process ID.	The value is a string consisting of 0 to 2048 characters, without spaces. The value is case sensitive.

Default Value

By default, no match rule is configured based on the protocol process ID filter.

View

Routing policy configuration view

Usage Guidelines

This command is used together with the RIP/OSPF/ISIS/BGP route redistribution policy configuration commands. When a protocol has multiple instances, you can configure a filter rule to reserve only one instance.

Example

Configure a filter rule based on a process ID.

```
Switch(config)#route-policy test permit node 10
Switch(config-route-policy)#match process 100
Switch(config-route-policy)#
```

5.8.15 match cost

Function

The **match cost** command sets a match rule based on the route cost.

The **no match cost** command cancels a match rule based on the route cost.

Format

- **match cost** *cost-value*
- **no match cost**

Parameter

Parameter	Description	Value
cost-value	Specifies a route cost value.	The value is an integer ranging from 0 to 4294967295.

Default Value

By default, the match rule based on the route cost is not configured.

View

Routing policy configuration view

Usage Guidelines

NA

Example

Configure the routing information matching route cost 10.

```
Switch(config)#route-policy fhn permit node 12
Switch(config-route-policy)#match cost 10
Switch(config-route-policy)#
```

5.8.16 match ip filter-list

Function

The **match ip filter-list** command sets the IPv4-based filter rule for matching the destination network segment.

The **no match ip filter-list** command cancels the IPv4-based filter rule for matching the destination network segment.

The **match ip {next-hop|route-source} filter-list** command sets the IPv4-based filter rule for matching the next hop address or source address advertised by the route.

The **no match ip {next-hop|route-source} filter-list** command cancels the IPv4-based filter rule for matching the next hop address or source address advertised by the route.

Format

- **match ip filter-list** *ipv4-filter-list-number*
- **no match ip filter-list**
- **match ip { next-hop | route-source } filter-list** *ipv4-filter-list-number*
- **no match ip { next-hop | route-source } filter-list**

Parameter

Parameter	Description	Value
ipv4-filter-list-number	Specifies an IPv4-based filter number.	The value is an integer ranging from 1001 to 2000.
next-hop	Indicates matching the next hop address of the route.	-
route-source	Indicates matching the source address advertised by the route.	-

Default Value

By default, the match rule based on any filter is not configured.

View

Routing policy configuration view

Usage Guidelines

Before using this command, you must run the **filter rule-number ip ipv4-address/M any** command.

The configuration of ipv4-address/M varies with application requirements.

Application	Value
Matching the destination network segment	ipv4-address: specifies the destination network segment. M: specifies the mask length.

Application	Value
Matching the next-hop address or source address advertising the route	Ipv4-address: specifies the next-hop IP address or source IP address advertising the route. M: 32 (IPv4)

Example

Configure an IPv4-based filter match rule.

```
Switch(config)#route-policy fhn permit node 12
Switch(config-route-policy)#match ip filter-list 1002
Switch(config-route-policy)#
```

5.8.17 match ip-prefix**Function**

The **match ip-prefix** command sets a match rule based on the IP address prefix list.

The **no match ip-prefix** command cancels a match rule based on the IP address prefix list.

Format

- **match ip-prefix** *prefix-name*
- **no match ip-prefix**

Parameter

Parameter	Description	Value
prefix-name	Specifies the name of an IP address prefix list.	The value is a character string.

Default Value

By default, no match rule based on an IPv4 address prefix list is configured.

View

Routing policy configuration view

Usage Guidelines

NA

Example

Configure a match rule based on an IPv4 address prefix list.

```
Switch>show ip prefix-list
ip prefix-list : tes
```

```

index: 11      permit 2.2.0.0/16
Switch#configure
    %Enter configuration commands.End with Ctrl+Z or command "quit" & "end"
Switch(config)#route-policy fhn permit node 12
Switch(config-route-policy)#match ip-prefix tes
Switch(config-route-policy)#

```

5.8.18 match ip {next-hop|route-source} ip-prefix

Function

The **match ip {next-hop|route-source} ip-prefix** command sets a match rule based on the IP prefix list.

The **no match ip {next-hop|route-source} ip-prefix** command deletes the configured match rule.

Format

- **match ip { next-hop | route-source } ip-prefix** *prefix-name*
- **no match ip { next-hop | route-source } ip-prefix**

Parameter

Parameter	Description	Value
next-hop	Indicates matching the next hop address of the route.	-
route-source	Indicates matching the source address advertised by the route.	-
prefix-name	Specifies the name of an IP address prefix list.	The value is a character string.

Default Value

By default, no match rule based on an IPv4 address prefix list is configured.

View

Routing policy configuration view

Usage Guidelines

NA

Example

Configure a match rule based on IP information.

```
Switch>show ip prefix-list
```

```

ip prefix-list : tes
  index: 11      permit 2.2.0.0/16
Switch#configure
  %Enter configuration commands.End with Ctrl+Z or command "quit" & "end"
Switch(config)#route-policy fhn permit node 12
Switch(config-route-policy)#match ip next-hop ip-prefix tes
Switch(config-route-policy)#

```

5.8.19 match ipv6 filter-list

Function

The **match ipv6 filter-list** command sets the IPv6-based filter rule for matching the destination network segment.

The **no match ipv6 filter-list** command cancels the IPv6-based filter rule for matching the destination network segment.

The **match ipv6 {next-hop|route-source} filter-list** command sets the IPv6-based filter rule for matching the next hop address or source address advertised by the route.

The **no match ipv6 {next-hop|route-source} filter-list** command cancels the IPv6-based filter rule for matching the next hop address or source address advertised by the route.

Format

- **match ipv6 filter-list** *ipv6-filter-list-number*
- **no match ipv6 filter-list**
- **match ipv6 { next-hop | route-source } filter-list** *ipv6-filter-list-number*
- **no match ipv6 { next-hop | route-source } filter-list**

Parameter

Parameter	Description	Value
ipv6-filter-list-number	Specifies an IPv6-based filter number.	The value is an integer ranging from 3001 to 4000.
next-hop	Indicates matching the next hop address of the route.	-
route-source	Indicates matching the source address advertised by the route.	-

Default Value

By default, the match rule based on any filter is not configured.

View

Routing policy configuration view

Usage Guidelines

NA

Example

Configure an IPv6-based filter match rule.

```
Switch(config-route-policy)#match ipv6 filter-list 1002
Switch(config-route-policy)#
```

5.8.20 match ipv6 {address|next-hop|route-source} prefix-list**Function**

The **match ipv6 {address|next-hop|route-source} prefix-list** command sets an IPv6-based match rule.

The **no match ipv6 {address|next-hop|route-source} prefix-list** command cancels an IPv6-based match rule.

Format

- **match ipv6 { address | next-hop | route-source } prefix-list *prefix-name***
- **no match ipv6 { address | next-hop | route-source } prefix-list**

Parameter

Parameter	Description	Value
address	Indicates matching the destination address of the IPv6 route.	-
next-hop	Indicates matching the next hop address of the route.	-
route-source	Indicates matching the source address advertised by the route.	-
prefix-name	Specifies the name of an IP address prefix list.	The value is a character string.

Default Value

By default, no match rule based on an IPv6 address prefix list is configured.

View

Routing policy configuration view

Usage Guidelines

Before using this command, you must configure an IP address prefix list.

Example

Set an IPv6-based match rule.

```
Switch(config)#route-policy me permit node 1
Switch(config-route-policy)#match ipv6 address prefix-list test
Switch(config-route-policy)#
```

5.8.21 match route-type

Function

The **match route-type** command sets a match rule based on the route type.

The **no match route-type** command cancels a match rule based on the route type.

Format

- **match route-type { internal | external-type1 | external-type2 | external-type1or2 | nssa-external-type1 | nssa-external-type2 | nssa-external-type1or2 }**
- **no match route-type { internal | external-type1 | external-type2 | external-type1or2 | nssa-external-type1 | nssa-external-type2 | nssa-external-type1or2 }**

Parameter

Parameter	Description	Value
internal	Indicates internal routes, including inter-area or intra-area OSPF routes.	-
external-type1	Indicates external routes of OSPF Type1.	-
external-type2	Indicates external routes of OSPF Type2.	-
external-type1or2	Indicates external OSPF routes.	-
nssa-external-type1	Indicates external routes of OSPF NSSA Type1.	-
nssa-external-type2	Indicates external routes of OSPF NSSA Type2.	-
nssa-external-type1or2	Indicates external routes of OSPF NSSA.	-

Default Value

By default, the match rule based on the route type is not configured.

View

Routing policy configuration view

Usage Guidelines

For the same routing policy node, if multiple match route-type clauses are configured and the clauses are in an "Or" relation, the apply clause action is implemented when any clause is matched.

Example

Configure a rule for matching external routes of OSPF Type1.

```
Switch(config)#route-policy fhn permit node 12
Switch(config-route-policy)#match route-type external-type1
Switch(config-route-policy)#
```

5.8.22 match tag

Function

The **match tag** command sets a match rule based on the route tag.

The **no match tag** command cancels a match rule based on the route tag.

Format

- **match tag** *tag-value*
- **no match tag**

Parameter

Parameter	Description	Value
tag-value	Specifies a tag value.	The value is an integer ranging from 0 to 4294967295.

Default Value

By default, the match rule based on the route tag is not configured.

View

Routing policy configuration view

Usage Guidelines

For RIP protocol, the maximum value of the routing tag field is 65535.

Example

Configure OSPF routing information matching route tag 8.

```
Switch(config)#route-policy fhn permit node 12
Switch(config-route-policy)#match tag 8
```



```
Switch(config-route-policy)#
```

5.8.23 route-policy

Function

The route-policy command creates a routing policy and enters the Route-Policy view.

The no route-policy command deletes a created routing policy. If node-number is not carried, all routing policy nodes in the routing policy are deleted. If node-number is carried, a specified routing policy node in the routing policy is deleted.

Format

- **route-policy** *policy-name* { **permit** | **deny** } **node** *node-number*
- **no route-policy** *policy-name*
- **no route-policy** *policy-name* **node** *node-number*

Parameter

Parameter	Description	Value
policy-name	Specifies a routing policy name. It uniquely identifies a routing policy.	The value is a string of 1 to 20 characters.
permit	Sets the routing policy match mode to permit.	-
deny	Sets the routing policy match mode to deny. In this mode, the apply clause is not executed.	-
node-number	Specifies the node number of a routing policy.	The value is an integer ranging from 0 to 65535.

Default Value

By default, no routing policy is created.

View

Global configuration view

Usage Guidelines

One routing policy consists of multiple routing policy nodes (node-number).

Multiple nodes in a routing policy are in an "Or" filter relation. That is, on condition that routing information passes the filter by one node, it can pass all nodes in the routing policy, and match test is not implemented on other routing policy nodes. If routing information does not pass the filter by any node, it cannot pass the routing policy.

If one routing policy defines more than one routing policy node, the smaller the node-number, the higher the priority, and the earlier the match test is performed.

One node-number can contain multiple match and apply clauses.

The match clause defines the match condition for a routing policy node. The apply clause defines the route behavior for filtering. The match clauses are in an "And" filter relation. That is, a route is considered to pass the filter of a routing policy node unless it matches all match clauses of this routing policy node.

In permit mode, the match mode of a specified node is permit. If a route matches all match clauses of a routing policy node, the route passes the test and is processed with a series of specified actions in the apply clause. Otherwise, the route must attend the test of a next routing policy node.

In deny mode, the match mode of a specified node is deny, and the apply clause is not executed. If a route matches all match clauses of a routing policy node, the route fails the test and cannot attend the test of the next routing policy node. Otherwise, the route continues to be tested by the next node.

Example

Configure policy fhn with node-number 12 and match mode permit. Enter the routing policy view.

```
Switch(config)#route-policy fhn permit node 12
Switch(config-route-policy)#
```

5.8.24 show route-policy config

Function

The **show route-policy config** command displays the routing policy configuration.

Format

show route-policy config

Parameter

NA

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

Display the routing policy configuration.

```
Switch>show route-policy config
!
route-policy 1 permit node 1
  match ip filter-list 1003
route-policy 2 deny node 10
Switch>
```

5.8.25 show route-policy information**Function**The **show route-policy information** command displays global routing policy information.**Format****show route-policy information****Parameter**

NA

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

Display global routing policy information.

```
Switch>show route-policy information
Version ROUTEPOLICY_VB3.00.10.00
routepolicy global structure size 856
RouteSocket=132
Memory Statistics
Configuration Params:
List:100
```

```

Rule:1000
Community List:1000
Community Rule:1000
ExCommunity List:1000
ExCommunity Rule:1000

```

```
Total Allocate memory:1156800 Bytes
```

Detailed Memory Operation

Index	Add	Fail	Free	Current	Size	Description
0	2	0	0	2	128	Map List
1	2	0	0	2	672	Map Rule
2	0	0	0	0	72	Community List
3	0	0	0	0	160	Community Rule
4	0	0	0	0	72	ExCommunity List
5	0	0	0	0	168	ExCommunity Rule

```
Switch>
```

5.8.26 show route-policy

Function

The **show route-policy** command displays the routing information.

Format

- **show route-policy** *policy-name*
- **show route-policy** *policy-name* **node** *node-number*

Parameter

Parameter	Description	Value
policy-name	Specifies a routing policy name.	The value is a character string.
node-number	Specifies the node number of a routing policy.	The value is an integer ranging from 0 to 65535.

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

Display configuration of a routing policy named fhn.

```
Switch>show route-policy fhn
policyName:fhn
  type:permit  node:1
  match ip filter-list 3000
  match route-type external-type1
  match cost 234545
  apply isis level-1
  type:permit  node:12
  match ip filter-list 1002
  match ip next-hop filter-list 3000
  match ip route-source filter-list 3000
  match route-type internal
  match route-type external-type1or2
Switch>
```

Display configuration of a routing policy named fhn and node 12 under the policy.

```
Switch>show route-policy fhn node 12
route-policy fhn permit node 12
  match ip filter-list 1002
  match ip next-hop filter-list 3000
  match ip route-source filter-list 3000
  match route-type internal
  match route-type external-type1or2
  match route-type isis_level1
  match route-type isis_level2
  match route-type nssa-external-type1or2
  match cost 16777215
  match tag 4294967295
  apply cost 16777215
  apply cost-type type-2
  apply isis level-1-2
  apply tag 4294967295
Switch>
```

5.8.27 as-path-filter**Function**

The **as-path-filter** command creates an AS path filter.

The **no as-path-filter** command cancels the function.

Format

- **as-path-filter** *listname* { **deny** | **permit** } *expression*
- **as-path-filter** *listname* **index** *index* { **deny** | **permit** } *expression*
- **no as-path-filter** *listname*
- **no as-path-filter** *listname* **index** *index*

Parameter

Parameter	Description	Value
listname	Specifies the name of an AS path filter.	The value is a string consisting of 1 to 31 characters.
deny	Specifies the match mode of the AS path filter to deny.	-
permit	Specifies the match mode of the AS path filter to permit.	-
Index	Specifies the match rule ID of the filter.	The value is an integer ranging from 1 to 65535.

Default Value

By default, the routing information tag is not configured.

View

Global configuration view

Usage Guidelines

NA

Example

Create an AS path filter numbered 1 to deny routes of which AS_PATH starting from 20.

```
Switch(config)#as-path-filter 1 deny 20
Switch(config)#
```

5.8.28 show as-path-filter**Function**

The **show as-path-filter** command displays the configuration of an AS path filter.

Format

- **show as-path-filter**

- **show as-path-filter config**
- **show as-path-filter information**
- **show as-path-filter** *list-name*

Parameter

Parameter	Description	Value
list-name	Specifies the name of an AS path filter.	The value is a string consisting of 1 to 32 characters.

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

Display the configuration of the AS path filter.

```
Switch>show as-path-filter
As path filter name: aaa
    index: 10      deny      allow
Switch>
```

5.8.29 debug as-path-filter

Function

The **debug as-path-filter** command enables debugging the routing policy.

The **no debug as-path-filter** command disables debugging the routing policy.

Format

- **debug as-path-filter { config | match | error | all }**
- **no debug as-path-filter { config | match | error | all }**

Parameter

Parameter	Description	Value
config	Debugs configuration information	-

Parameter	Description	Value
match	Debugs filter information.	-
error	Debugs error information.	-
all	Displays all the preceding information.	-

Default Value

NA

View

Privileged user view

Usage Guidelines

NA

Example

Enable debugging the routing policy.

```
Switch#debug as-path-filter config
Switch#
```

5.9 Policy-based Route Configuration Commands

5.9.1 apply ip-address next-hop

Function

The **apply ip-address next-hop** command sets the next hop for a packet.

The **no apply ip-address next-hop** command cancels the next hop for a packet.

Format

- **apply ip-address next-hop** *ip-address*
- **apply ip-address next-hop** *ip-address* **vpn-instance** *name*
- **no apply ip-address next-hop**

Parameter

Parameter	Description	Value
ip-address	Specifies the IP address of a VLAN interface.	The value is in dotted decimal notation.

Parameter	Description	Value
name	Specifies a VPN instance name.	The value contains up to 64 characters.

Default Value

By default, no next hop is set for the packet.

View

Policy-based route configuration view

Usage Guidelines

NA

Example

Cancel the next hop for a packet.

```
Switch(config-policy-route)#no apply ip-address next hop
Switch(config-policy-route)#
```

5.9.2 apply ipv6-address next-hop

Function

The **apply ipv6-address next-hop** command sets the next hop for a packet.

The **no apply ipv6-address next-hop** command cancels the next hop for a packet.

Format

- **apply ipv6-address next-hop** *ipv6-address*
- **apply ipv6-address next-hop** *ipv6-address vpn-instance name*
- **no apply ipv6-address next-hop**

Parameter

Parameter	Description	Value
ipv6-address	Specifies the IPv6 address of an interface.	-
name	Specifies a VPN instance name.	The value contains up to 64 characters.

Default Value

By default, no next hop is set for the packet.

View

Policy-based route configuration view

Usage Guidelines

NA

Example

Cancel the next hop for a packet.

```
Switch(config-policy-route)#no apply ipv6-address next hop
Switch(config-policy-route)#
```

5.9.3 apply ip-precedence

Function

The **apply ip-precedence** command sets the priority of an IP packet.

The **no apply ip-precedence** command cancels the priority of an IP packet.

Format

- **apply ip-precedence** *precedence-value*
- **no apply ip-precedence**

Parameter

Parameter	Description	Value
precedence-value	Specifies the priority of an IP packet.	The value is an integer ranging from 1 to 7.

Default Value

By default, no priority is set for the IP packet.

View

Policy-based route configuration view

Usage Guidelines

NA

Example

Set the priority of an IP packet.

```
Switch(config-policy-route)#apply ip-precedence 2
Switch(config-policy-route)#
```

5.9.4 apply output-interface

Function

The **apply output-interface** command sets the outbound interface for a packet.

The **no apply output-interface** command cancels the outbound interface for a packet.

Format

- **apply output-interface** { **ethernet** | **xgigaethernet** | **10gigaethernet** | **25gigaethernet** | **40gigaethernet** | **100gigaethernet** } *interface-number*
- **no apply output-interface**

Parameter

Parameter	Description	Value
interface-number	Specifies an Ethernet interface number.	The value is an integer in the range of <1-1>/<0-1>/<1-48> (For reference only. The

Default Value

By default, no outbound interface is set for the packet.

View

Policy-based route configuration view

Usage Guidelines

NA

Example

Cancel the outbound interface for a packet.

```
Switch(config-policy-route)#no apply output-interface
Switch(config-policy-route)#
```

5.9.5 if-match acl

Function

The **if-match acl** command sets an ACL match rule.

The **no if-match acl** command cancels an ACL match rule.

Format

- **if-match acl** *acl-number*

- **no if-match acl**

Parameter

Parameter	Description	Value
acl-number	Specifies the ID of an IPv4 ACL.	The value is an integer ranging from 1001 to 4000.

Default Value

By default, no ACL match rule is configured.

View

Policy-based route configuration view

Usage Guidelines

NA

Example

Set an ACL match rule.

```
Switch(config-policy-route)#if-match acl 1002
Switch(config-policy-route)#
```

5.9.6 policy-based-route

Function

The **policy-based-route** command creates a policy-based route.

The **no policy-based-route** command deletes the created policy-based route. If node-number is not specified, all nodes of the policy-based route are deleted. If node-number is specified, the specified node of the policy-based route is deleted.

Format

- **policy-based-route** *policy-name* { **permit** | **deny** } **node** *node-number*
- **no policy-based-route** *policy-name*
- **no policy-based-route** *policy-name* **node** *node-number*

Parameter

Parameter	Description	Value
policy-name	Specifies the name of a policy-based route. It	The value contains up to 16 characters.

Parameter	Description	Value
	uniquely identifies a policy-based route.	
permit	Sets the policy-based route match mode to permit.	-
deny	Sets the policy-based route match mode to deny. In this mode, the apply clause is not executed.	-
node-number	Specifies the number of nodes of the policy-based route.	The value is an integer ranging from 1 to 10.

Default Value

By default, no policy-based route is created.

View

Global configuration view

Usage Guidelines

One policy-based route consists of multiple policy-based route nodes (node-number).

Multiple nodes in a policy-based route are in an "Or" filter relation. That is, on condition that routing information passes the filter by one node, it can pass all nodes in the policy-based route, and match test is not implemented on other policy-based route nodes. If routing information does not pass the filter by any node, it cannot pass the policy-based route.

If one policy-based route has more than one node, match test is performed first on the node with a smaller node-number. Each node should have at least one node in permit match mode.

One node-number can contain multiple if-match and apply clauses.

The if-match clause defines the match condition for a policy-based route node. The apply clause defines the route behavior for filtering.

In permit mode, the match mode of a specified node is permit. If a route matches all if-match clauses of a policy-based route node, the route passes the test and is processed with a series of specified actions in the apply clause. Otherwise, the route must attend the test of a next policy-based route node.

In deny mode, the match mode of a specified node is deny, and the apply clause is not executed. If a route matches all if-match clauses of a policy-based route node, the route fails the test and cannot attend the test of the next policy-based route node. Otherwise, the route continues to be tested by the next node.

Example

Create a policy-based route.

```
Switch(config)#policy-based-route abc deny node 2
Switch(config)#
```

5.9.7 ip policy-based-route

Function

The **ip policy-based-route** command applies a policy-based route to a physical port.

The **ip policy-based-route** command cancels a policy-based route applied to a physical port.

Format

- **ip policy-based-route** *policy-name*
- **no ip policy-based-route**

Parameter

Parameter	Description	Value
policy-name	Specifies the name of a policy-based route. It uniquely identifies a policy-based route.	The value contains up to 16 characters.

Default Value

NA

View

Ethernet bridge interface configuration view, Ethernet routing interface configuration view, Eth-trunk interface configuration view

Usage Guidelines

One interface can have only one policy-based route

Example

Cancel a policy-based route applied to a physical port.

```
Switch(config-10ge1/0/1)#no ip policy-based route
Switch(config-10ge1/0/1)#
```

5.9.8 show ip policy-based-route

Function

The **show ip policy-based-route** command displays information on all policy-based routes.

Format

- **show ip policy-based-route**
- **show ip policy-based-route** *policy-name*

Parameter

Parameter	Description	Value
policy-name	Specifies the name of a policy-based route. It uniquely identifies a policy-based route.	The value contains up to 16 characters.

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

Display information on all policy-based routes.

```
Switch>show ip policy-based-route
policy-based-route : 1
Node 1 : permit
apply ip-address next-hop 1.1.1.2
Switch>
```

5.9.9 apply load-balance next-hop**Function**

The **apply load-balance ip-address next-hop** command configures the next hop IP address for redirection.

Format**apply load-balance ip-address next-hop** *next-hop-address***Parameter**

Parameter	Description	Value
next-hop-address	Specifies the next-hop IP address	The value is in dotted decimal notation, such as

Parameter	Description	Value
	for redirection.	A.B.C.D, where each of A to D is a decimal number ranging from 0 to 255.

Default Value

NA

View

Global configuration view

Usage Guidelines

You can configure **next-hop-address** to specify up to 4 next hops.

Configuring multiple next hops can redirect and forward packets according to the load balancing mode of equal-cost routes, that is, forward the incoming packets that match the conditions to the specified multiple outgoing interfaces according to the load balancing mode. If all the configured next hops are unavailable, the device forwards the packet based on the original destination address.

During the direction to multiple next-hop IP addresses, if the outbound interface of a next hop suddenly becomes down or the route is suddenly changed, the device rapidly switches the link to the outbound interface corresponding to an available next hop. According to the order in which the IP addresses are configured, the one configured first has the highest priority.

Example

Configure the next-hop IP addresses for redirection to 10.1.1.1, 50.1.1.2, and 30.1.1.1.

```
Switch(config)# filter-list 1001
Switch (configure-filter-ipv4-1001)# filter 1 udp any 1000 any any
Switch(configure-filter-ipv4-1001)# filter 1 action permit
Switch(configure-filter-ipv4-1001)# policy-based-route PBR1 permit node 1
Switch(config-policy-based-route-PBR1-1)# if-match acl 1001
Switch(config-policy-based-route-PBR1-1)#apply load-balance ip-address next-hop 10.1.1.1 50.1.1.2 30.1.1.1
Switch(config-policy-based-route-PBR1-1)#
```

5.9.10 show ip policy-based-route config

Function

The **show ip policy-based-route config** command displays configuration of all policy-based routes.

Format

show ip policy-based-route config

Parameter

NA

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

Display configuration of all policy-based routes.

```
Switch>show ip policy-based-route config
!
policy-based-route 1 permit node 1
  apply ip-address next-hop 1.1.1.2
Switch>
```

5.9.11 debug policy-based-route**Function**

The **debug policy-based-route** command enables debugging of a policy-based route.

The **no debug policy-based-route** command disables debugging of a policy-based route.

Format

- **debug policy-based-route { hw | pkt | config | all }**
- **no debug policy-based-route { hw | pkt | config | all }**

Parameter

Parameter	Description	Value
hw	Indicates the hardware information generated in the policy-based route.	-
pkt	Indicates the ping packet information sent by the policy-based route.	-
config	Indicates the debugging information for internal running.	-

Parameter	Description	Value
all	Indicates all the preceding information.	-

Default Value

By default, the debugging function is disabled.

View

Privileged user view

Usage Guidelines

You can run this command to maintain and debug policy-based routes for troubleshooting convenience.

Example

Enable debugging of a policy-based route.

```
Switch#debug policy-based-route hw
Switch#
```

5.10 Hwroute Configuration Commands

5.10.1 debug hwroute

Function

The **debug hwroute** command enables hardware debugging for a route.

The **no debug hwroute** command disables hardware debugging for a route.

Format

- **debug hwroute { arp | route | tunnel | ilm | l2vpn | evpn | l3vpn | rtm | all }**
- **no debug hwroute { arp | route | tunnel | ilm | l2vpn | evpn | l3vpn | rtm | all }**

Parameter

Parameter	Description	Value
arp	Debugs ARP information.	-
route	Debugs route information.	-
tunnel	Debugs tunnel information.	-
ilm	Debugs ILM information.	-
l2vpn	Debugs I2VPN information.	-

Parameter	Description	Value
evpn	Debugs EVPN information.	-
l3vpn	Debugs I3VPN information.	-
rtm	Debugs RTM information.	-
all	Displays all the preceding information.	-

Default Value

Disable

View

Privileged user view

Usage Guidelines

NA

Example

Enable debugging of all hardware information for a route.

```
Switch#debug hwroute all
Switch#
```

5.10.2 show hwroute ecmp-group**Function**

The **show hwroute ecmp-group** command displays the ECMP group information on an HwRoute module.

Format

- **show hwroute ecmp-group**
- **show hwroute ecmp-group6**

Parameter

NA

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

View the ECMP group information on an HwRoute module.

```
Switch>show hwroute ecmp-group
Switch>
```

5.10.3 show hwroute statistic**Function**

The **show hwroute statistic rtm** command displays statistics on route messages received by an HwRoute module.

The **show hwroute statistic route** command displays statistics on route messages of an HwRoute module.

Format

- **show hwroute statistic rtm**
- **show hwroute statistic route { v4 | v6 | all }**

Parameter

Parameter	Description	Value
rtm	Specifies received route information.	-
v4	Specifies IPv4 route information.	-
v6	Specifies IPv6 route information.	-
all	Specifies all route information.	-

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

View statistics on route messages of an HwRoute module.

```
Switch# show hwroute statistic route all
```

ROUTE4 ADD INFORMATION:			
rtAddCnt:	3541358	rtAddParamErrCnt:	0
rtAddDestAddCnt:			
3541358	rtAddNoDestMemErrCnt:	0	
rtAddSwDelCnt:	0	rtAddNoArpDelCnt:	0
rtAddVpnAddRtReadyAddCnt:	0	rtAddVpnAddRtClearCnt:	0
rtAddNoCancelCnt:	0	rtAddPppCnt:	0
rtAddNoSameMetricReadyDelCnt:	0	rtAddNoSameMetricCnt:	0
rtAddNhopAddCnt:	3541358	rtAddnhopBigCnt:	0
rtAddMplsProtoExistCnt:	0	rtAddRedupErrCnt:	0
rtAddTunCnt:	0	rtAddNormalCnt:	3539493
rtAddNoNhopMemErrCnt:	0	rtAddNoEndCnt:	0
rtAddPendAddCnt:	1865	rtAddReadyDelCnt:	0
3539493	rtAddL2vpnPublicAddCnt:	0	rtAddNormalReadyAddCnt:
ROUTE4 DEL INFORMATION:			
rtDelCnt:	3535356	rtDelParamErrCnt:	0
rtDelDestDelCnt:			0
rtDelNoNexthopEntryErrCnt:	0		
rtDelSwAddCnt:	0	rtDelRtdelCnt:	3535356
rtDelMplsRtdelCnt:			0
rtDelNoDestEntryErrCnt:	0		
rtDelAgainCnt:	0	rtDelNoSucessCnt:	0
rtDelRealRtdelCnt:			3535356
rtDelMplsFrrRtdelCnt:	0		
rtDelCardupCnt:	0	rtDelVpnInAddCnt:	0
rtDelNoSucPublicVpn6DelCnt:	0	rtDelNoSucFrrDelCnt:	0
rtDelNhopsCnt:	0	rtDelReadyDelCnt:	0
rtDelNoSucSwDelCnt:			0
rtDelNoSucPendDelCnt:	0		
rtDelTunCnt:	0	rtDelNormalCnt:	3535356
rtDelVpnSuccessCnt:			0
rtDelNoSucPublic4DelCnt:	0		
rtDelReadyAddCnt:	3535356	rtDelMplsdelCnt:	0
rtDelNoSucPublic6DelCnt:			0
rtDelNoSucPublicVpn4DelCnt:	0		
ROUTE4 UPDATE INFORMATION:			
updatePendDelCnt:	0	updateReadyDelCnt:	7076714
updateSwVpnDelCnt:			0
updateSwRouteDelCnt:	3535356		
updateSendMsgCnt:	443210	updateNoArpAddCnt:	0
hwUpdateAddOldCnt:			0
hwUpdateAddSwDelCnt:	0		
InsertAddNhopCnt:	3541358	InsertDelNhopCnt:	3535356
InsertNoopNhopCnt:			0
InsertBackupNhopCnt:	0		
hwRouteA1Cnt:	0	hwRouteA2Cnt:	0
hwRouteA3Cnt:			0
hwRouteA6Cnt:	3541358		
hwRouteD1Cnt:	0	hwRouteD2Cnt:	0
hwRouteD3Cnt:			0
hwRouteD6Cnt:	3535356		
setRouteDelFlagCnt:	0	hwCardupVpnCnt:	0
updateBackUpToDelCnt:			0
InsertRtTunnelFlagCnt:	0		
hwUpdateAddNewCnt:	0	ecmpUpdataAddCnt:	0
ecmpUpdataDelCnt:			0

```

InsertPosTunnelFlagCnt:      0
  cardUpRtToBackCnt:    0      hwUpdateRouteSwDelCnt: 0      hwUpdateRouteDstDelCnt:      0

  ROUTE6 ADD INFORMATION:
    rt6AddCnt:          492626 rt6AddParamErrCnt:    0      rt6AddDestAddCnt:
492626 rt6AddNoDestMemErrCnt:      0
    rt6AddSwDelCnt:      0      rt6AddNoArpDelCnt:    0      rt6AddVpnAddRtClearCnt:      0
rt6AddVpnAddRtReadyAddCnt:    0
    rtAddPppCnt:          0      rt6AddV4NhopCnt:      0      rtAddNoSameMetricCnt:      0
rtAddNoSameMetricReadyDelCnt: 0
    rtAddNhopAddCnt:      492626 rtAddRedupErrCnt:    0      rt6AddSwDelReadyDelCnt:      0
rtAddL2vpnPublicAddCnt:      0
    rtAddTunCnt:          0      rtAddNormalCnt:      492626 rtAddNoEndCnt:      0
rtAddNoNhopMemErrCnt:      0
    rtAddPendAddCnt:      0      rtAddReadyDelCnt:    0      rtAddNormalReadyAddCnt:
492626
  ROUTE6 DEL INFORMATION:
    rt6DelCnt:          490120 rt6DelParamErrCnt:    0      rt6DelDestDelCnt:      0
rt6DelNoNexthopEntryErrCnt:    0
    rt6DelSwAddCnt:      0      rt6DelAgainCnt:      0      rt6DelNoSuccessCnt:      0
rt6DelMplsFrrRtdelCnt:      0
    rt6DelCardupCnt:      0      rt6DelVpnInAddCnt:    0      rt6DelNoDestEntryErrCnt:    0
rt6DelNoSucPublicVpn6DelCnt: 0
    rt6DelNhopsCnt:      0      rt6DelReadyDelCnt:    0      rt6DelNoSucSwDelCnt:      0
rt6DelNoSucPendDelCnt:      0
    rt6DelTunCnt:          0      rt6DelNormalCnt:      490120 rt6DelVpnSuccessCnt:      0
rt6DelNoSucPublic4DelCnt:    0
    rt6DelPrivateRefCnt: 0      rt6DelL2vpnRefCnt:    0      rt6DelReadyAddCnt:      490120
rt6DelNoSucPublic6DelCnt:    0
    rt6DelNoSucPublicVpn4DelCnt: 0
  ROUTE6 UPDATE INFORMATION:
    updatePend6DelCnt:    0      updateReady6DelCnt: 982746 updateSwVpn6DelCnt:      0
updateSwRoute6DelCnt:      490120
    hwRoute6A1Cnt:      492626 hwRoute6A2Cnt:      0      hwRoute6A3Cnt:      0
hwRoute6A4Cnt:      0
    hwRoute6D1Cnt:      490120 hwRoute6D3Cnt:      0      hwRoute6D4Cnt:      0
updateBackUp6ToDelCnt:      0
    hwUpdateAdd6OldCnt:    0      hwUpdateAdd6NewCnt:    0      hwUpdateAdd6SwDelCnt:
0      hwUpdate6DelEcmpNhopDelCnt:    0
    ecmp6UpdataDelCnt:    0      ecmp6UpdataAdd6Cnt:    0      hwUpdate6DelEcmpDstDelCnt:    0
hwUpdate6DelEcmpDstDelCnt:    0
    hwCardupVpn6Cnt:      0      hwUpdate6DelNhopDelCnt: 0      hwUpdate6DelDstDelCnt:
0

```

```
Switch#
```

5.10.4 show hwroute hardware

Function

The **show hwroute hardware** command displays the hardware route information on an HwRoute module.

Format

- **show hwroute hardware arp**
- **show hwroute hardware ilm**
- **show hwroute hardware nd**
- **show hwroute hardware route4**
- **show hwroute hardware route6**
- **show hwroute hardware route4 pend**
- **show hwroute hardware route6 pend**

Parameter

Parameter	Description	Value
arp	Specifies ARP information.	-
ilm	Specifies ILM information.	-
nd	Specifies ND information.	-
route4	Specifies hardware route information.	-
route6	Specifies an IPv6 route.	-

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

View the hardware route information on an HwRoute module.

```

Switch>show hwroute hardware arp
ARP Table: Total:3      hard:1
  Next-Hop      Port      MAC      Out-Port      Status
  10.1.3.2      vlan300  0010:9400:0003  10ge1/0/48    1
Switch#
Switch>show hwroute hardware nd
ND6 Table: Total:8      hard:2      abnormal:0
  Next-Hop      Port      MAC      Out-Port      Status
  1000:300::2    vlan300  0010:9400:0004  10ge1/0/48    1
  fe80::1        vlan300  0010:9400:0004  10ge1/0/48    1
Switch#

```

5.10.5 show hwroute nexthop

Function

The **show hwroute nexthop** command displays the next hop route information on an HwRoute module

Format

- **show hwroute nexthop** *route-id*
- **show hwroute nexthop6** *route-id*

Parameter

Parameter	Description	Value
route-id	Specifies a route ID.	The value is an integer ranging from 0 to 4294967295.

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

View the next hop route information on an HwRoute module.

```
Switch>show hwroute nexthop 1
```



```
Switch>
```

Chapter 6 QoS Commands

This chapter introduces the commands for configuring QoS functions on the Switch, including traffic policing, traffic shaping, queue scheduling, and congestion control.

6.1 Diffserv Configuration Commands

6.1.1 debug diffserv

Function

The **debug diffserv** command enables DiffServ debugging.

The **no debug diffserv** command disables DiffServ debugging.

Format

- **debug diffserv**
- **no debug diffserv**

Parameter

NA

Default Value

By default, DiffServ debugging is disabled.

View

Privileged user view

Usage Guidelines

NA

Example

Enable DiffServ debugging.

Switch#debug diffserv

Switch#

Related Commands

NA

6.1.2 diffserv domain

Function

The **diffserv domain** command creates a DiffServ domain and displays its configuration view.

The **no diffserv domain** command deletes a DiffServ domain.

Format

- **diffserv domain** *name*
- **no diffserv domain** *name*

Parameter

Parameter	Description	Value
name	Specifies a DiffServ domain name.	The value is a string of 1 to 32 characters without spaces and can be none .

Default Value

NA

View

Global configuration view

Usage Guidelines

You can only modify mappings of the default domain but cannot delete it.

Example

```
Switch(config)#diffserv domain 123
Switch(config-dsdomain-123)#
```

6.1.3 8021p-inbound

Function

The **8021p-inbound** command configures the mappings between 802.1p priorities of ingress VLAN packets and per hop behaviors (PHBs) in a DiffServ domain and marks the color of packets.

The **8021p-inbound default** command restores the default mappings.

Format

- **8021p-inbound** *priority* **default**
- **8021p-inbound** *priority* **phb** { **be** | **af1** | **af2** | **af3** | **af4** | **ef** | **cs6** | **cs7** }

- **8021p-inbound priority phb** { **be** | **af1** | **af2** | **af3** | **af4** | **ef** | **cs6** | **cs7** } { **green** | **yellow** | **red** }
- **8021p-inbound default**

Parameter

Parameter	Description	Value
priority	Specifies the 802.1p priority of VLAN packets.	The value is an integer ranging from 0 to 7. The larger the value, the higher the priority.
be af1 af2 af3 af4 ef cs6 cs7	Specifies the PHB, namely, BE, AF1 to AF4, EF, CS6, or CS7. The PHBs correspond to queues 0 to 7 on an interface.	-
green yellow red	Marks packets in green, yellow, or red.	-

Default Value

By default, the mappings between 802.1p priorities, PHBs, and colors of ingress VLAN packets in a DiffServ domain are as follows.

802.1p Priority	PHB	Color
0	BE	green
1	AF1	green
2	AF2	green
3	AF3	green
4	AF4	green
5	EF	green
6	CS6	green
7	CS7	green

By default, the mappings between DSCP priorities, PHBs, and colors of ingress IP messages in a DiffServ domain are as follows.

DSCP	PHB	Color	DSCP	PHB	Color
0	BE	green	32	AF4	green
1	BE	green	33	BE	green
2	BE	green	34	AF4	green
3	BE	green	35	BE	green
4	BE	green	36	AF4	yellow
5	BE	green	37	BE	green
6	BE	green	38	AF4	red
7	BE	green	39	BE	green
8	AF1	green	40	EF	green
9	BE	green	41	BE	green

DSCP	PHB	Color	DSCP	PHB	Color
10	AF1	green	42	BE	green
11	BE	green	43	BE	green
12	AF1	yellow	44	BE	green
13	BE	green	45	BE	green
14	AF1	red	46	EF	green
15	BE	green	47	BE	green
16	AF2	green	48	CS6	green
17	BE	green	49	BE	green
18	AF2	green	50	BE	green
19	BE	green	51	BE	green
20	AF2	yellow	52	BE	green
21	BE	green	53	BE	green
22	AF2	red	54	BE	green
23	BE	green	55	BE	green
24	AF3	green	56	CS7	green
25	BE	green	57	BE	green
26	AF3	green	58	BE	green
27	BE	green	59	BE	green
28	AF3	yellow	60	BE	green
29	BE	green	61	BE	green
30	AF3	red	62	BE	green
31	BE	green	63	BE	green

View

DiffServ domain configuration view

Usage Guidelines

You can bind a DiffServ domain to the inbound interface of packets so that the system can map the priorities of packets from the upstream device to certain PHBs and colors based on mappings configured in the DiffServ domain.

Example

```
Switch(config-dsdomain-domain-1)#8021p-inbound 1 phb be
Switch(config-dsdomain-domain-1)#
```

6.1.4 8021p-outbound

Function

The **8021p-outbound** command configures the mappings from per hop behaviors (PHBs) and colors of egress VLAN packets to 802.1p priorities in a DiffServ domain.

The **8021p-outbound default** command restores the default mappings.

Format

- **8021p-outbound { be | af1 | af2 | af3 | af4 | ef | cs6 | cs7 } { green | yellow | red } default**
- **8021p-outbound { be | af1 | af2 | af3 | af4 | ef | cs6 | cs7 } { green | yellow | red } map *priority***
- **8021p-outbound default**

Parameter

Parameter	Description	Value
priority	Specifies the 802.1p priority of VLAN packets.	The value is an integer ranging from 0 to 7. The larger the value, the higher the priority.
be af1 af2 af3 af4 ef cs6 cs7	Specifies the PHB, namely, BE, AF1 to AF4, EF, CS6, or CS7. The PHBs correspond to queues 0 to 7 on an interface.	-
green yellow red	Marks packets in green, yellow, or red.	-

Default Value

By default, the mappings between PHBs, colors, and 802.1p priorities of egress VLAN packets in a DiffServ domain are as follows.

PHB	Color	802.1p Priority
BE	green	0
BE	yellow	0
BE	red	0
AF1	green	1
AF1	yellow	1
AF1	red	1
AF2	green	2
AF2	yellow	2
AF2	red	2
AF3	green	3
AF3	yellow	3
AF3	red	3
AF4	green	4
AF4	yellow	4
AF4	red	4

PHB	Color	802.1p Priority
EF	green	5
EF	yellow	5
EF	red	5
CS6	green	6
CS6	yellow	6
CS6	red	6
CS7	green	7
CS7	yellow	7
CS7	red	7

By default, the mappings between PHBs, colors, and DSCP priorities of egress IP messages in a DiffServ domain are as follows.

PHB	Color	802.1p Priority
BE	green	0
BE	yellow	0
BE	red	0
AF1	green	10
AF1	yellow	12
AF1	red	14
AF2	green	18
AF2	yellow	20
AF2	red	22
AF3	green	26
AF3	yellow	28
AF3	red	30
AF4	green	34
AF4	yellow	36
AF4	red	38
EF	green	46
EF	yellow	46
EF	red	46
CS6	green	48
CS6	yellow	48
CS6	red	48
CS7	green	56
CS7	yellow	56
CS7	red	56

View

DiffServ domain configuration view

Usage Guidelines

You can bind a DiffServ domain to the outbound interface of packets so that the system can map the PHBs and colors of packets sent to the downstream device to certain priorities based on mappings configured in the DiffServ domain.

Example

```
Switch(config-dsdomain-domain-1)#8021p-outbound be green map 1
Switch(config-dsdomain-domain-1)#
```

6.1.5 ip-dscp-inbound

Function

The **ip-dscp-inbound** command configures the mappings between DSCP priorities of ingress IP packets and per hop behaviors (PHBs) in a DiffServ domain and marks the color of packets.

The **ip-dscp-inbound default** command restores the default mappings.

Format

- **ip-dscp-inbound priority default**
- **ip-dscp-inbound priority phb { be | af1 | af2 | af3 | af4 | ef | cs6 | cs7 }**
- **ip-dscp-inbound priority phb { be | af1 | af2 | af3 | af4 | ef | cs6 | cs7 } { green | yellow | red }**
- **ip-dscp-inbound default**

Parameter

Parameter	Description	Value
priority	Specifies the DSCP priority of packets.	The value is an integer ranging from 0 to 63.
be af1 af2 af3 af4 ef cs6 cs7	Specifies the PHB, namely, BE, AF1 to AF4, EF, CS6, or CS7. The PHBs correspond to queues 0 to 7 on an interface.	-
green yellow red	Marks packets in green, yellow, or red.	-

Default Value

By default, the mappings between DSCP priorities, PHBs, and colors of ingress IP messages in a DiffServ domain are as follows.

DSCP	PHB	Color	DSCP	PHB	Color
0	BE	green	32	AF4	green

DSCP	PHB	Color	DSCP	PHB	Color
1	BE	green	33	BE	green
2	BE	green	34	AF4	green
3	BE	green	35	BE	green
4	BE	green	36	AF4	yellow
5	BE	green	37	BE	green
6	BE	green	38	AF4	red
7	BE	green	39	BE	green
8	AF1	green	40	EF	green
9	BE	green	41	BE	green
10	AF1	green	42	BE	green
11	BE	green	43	BE	green
12	AF1	yellow	44	BE	green
13	BE	green	45	BE	green
14	AF1	red	46	EF	green
15	BE	green	47	BE	green
16	AF2	green	48	CS6	green
17	BE	green	49	BE	green
18	AF2	green	50	BE	green
19	BE	green	51	BE	green
20	AF2	yellow	52	BE	green
21	BE	green	53	BE	green
22	AF2	red	54	BE	green
23	BE	green	55	BE	green
24	AF3	green	56	CS7	green
25	BE	green	57	BE	green
26	AF3	green	58	BE	green
27	BE	green	59	BE	green
28	AF3	yellow	60	BE	green
29	BE	green	61	BE	green
30	AF3	red	62	BE	green
31	BE	green	63	BE	green

View

DiffServ domain configuration view

Usage Guidelines

When QoS scheduling is required for IP messages carrying DSCP priorities from the upstream device, you can use this command to set the mappings from DSCP priorities to PHBs and colors in a DiffServ domain. After the DiffServ domain is bound to the inbound interface of messages, the

switch sends messages to corresponding queues on the interface based on the PHBs to implement congestion management. After a drop profile is configured, the system can implement congestion avoidance based on message colors.

Example

```
Switch(config-dsdomain-domain-1)# ip-dscp-inbound 1 phb be
Switch(config-dsdomain-domain-1)#
```

6.1.6 ip-dscp-outbound

Function

The **ip-dscp-outbound** command configures the mappings from per hop behaviors (PHBs) and colors of egress IP messages to DSCP priorities in a DiffServ domain.

The **ip-dscp-outbound default** command restores the default mappings.

Format

- **ip-dscp-outbound { be | af1 | af2 | af3 | af4 | ef | cs6 | cs7 } { green | yellow | red } default**
- **ip-dscp-outbound { be | af1 | af2 | af3 | af4 | ef | cs6 | cs7 } { green | yellow | red } map *priority***
- **ip-dscp-outbound default**

Parameter

Parameter	Description	Value
priority	Specifies the DSCP priority of IP messages.	The value is an integer ranging from 0 to 63.
be af1 af2 af3 af4 ef cs6 cs7	Specifies the PHB, namely, BE, AF1 to AF4, EF, CS6, or CS7. The PHBs correspond to queues 0 to 7 on an interface.	-
green yellow red	Marks packets in green, yellow, or red.	-

Default Value

NA

View

DiffServ domain configuration view

Usage Guidelines

You can use this command to configure mappings from PHBs and colors to DSCP priorities on a DiffServ domain for IP messages after QoS scheduling. After the DiffServ domain is bound to the

outbound interface of messages, the downstream device can perform message scheduling based on the DSCP priority.

Example

```
Switch(config-dsdomain-domain-1)# ip-dscp-outbound be green default
Switch(config-dsdomain-domain-1)#
```

6.1.7 show diffserv domain

Function

The **show diffserv domain** command displays DiffServ domain configuration.

Format

- **show diffserv domain**
- **show diffserv domain config**
- **show diffserv domain** *name*
- **show diffserv domain interface**
- **show diffserv domain interface** { **ethernet** | **xgigaethernet** | **10gigaethernet** | **25gigaethernet** | **40gigaethernet** | **100gigaethernet** } *interface-number*
- **show diffserv domain interface eth-trunk** *trunk-number*

Parameter

Parameter	Description	Value
interface-number	Specifies an interface number.	The value is an integer in the range of <1-1>/<0-1>/<1-48> (For reference only. The specific value range depends on the slot number and card type).
trunk-number	Specifies an aggregation port number.	The value is an integer ranging from 1 to 128.
name	Specifies a DiffServ domain name.	The value is a string of 1 to 32 characters without spaces and can be none .

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

Display DiffServ domain configuration.

```
Switch>show diffserv domain
Total number:8   Used number:1
Index    DS name
0        default
Switch#
```

6.1.8 trust 8021p**Function**

The **trust 8021p** command specifies the type of the priority to be mapped in packets in the interface configuration view.

Format**trust 8021p { inner | outer }****Parameter**

Parameter	Description	Value
Inner outer	Maps the 802.1p priority in the inner or outer tag of packets.	-

Default Value

NA

View

Ethernet bridge interface configuration view, Ethernet routing interface configuration view, Trunk interface configuration view

Usage Guidelines

The new DSCP and 8021p configuration overwrites the existing one. By default, both 8021p and DSCP are not trusted.

Example

Set to map the 802.1p priority in the inner tag of packets.

```
Switch(config-10ge1/0/1)#trust 8021p inner
Switch(config-10ge1/0/1)#
```

Set to map the 802.1p priority in the outer tag of packets.

```
Switch(config-10ge1/0/1)#trust 8021p outer
Switch(config-10ge1/0/1)#
```

6.1.9 trust dscp

Function

The **trust dscp** command specifies the type of the priority to be mapped in DSCP packets.

Format

trust dscp

Parameter

NA

Default Value

NA

View

Ethernet bridge interface configuration view, Ethernet routing interface configuration view, Trunk interface configuration view

Usage Guidelines

The new DSCP and 8021p configuration overwrites the existing one. By default, both 8021p and DSCP are not trusted.

Example

Specify the type of the priority to be mapped in DSCP packets.

```
Switch(config-10ge1/0/1)#trust dscp
Switch(config-10ge1/0/1)#
```

6.1.10 trust none

Function

The **trust none** command cancels the type of the priority to be mapped in packets.

Format

trust none

Parameter

NA

Default Value

NA

View

Ethernet bridge interface configuration view, Ethernet routing interface configuration view, Trunk interface configuration view

Usage Guidelines

NA

Example

Cancel the type of the priority to be mapped in packets.

```
Switch(config-10ge1/0/1)#trust none
Switch(config-10ge1/0/1)#
```

6.1.11 qos phb marking 8021p**Function**

The **qos phb marking 8021p** command enables or disables mapping outbound PHB packets to 802.1p packets.

Format

qos phb marking 8021p { enable | disable | default }

Parameter

Parameter	Description	Value
enable	Enables mapping outbound PHB packets to 802.1p packets.	-
disable	Disables mapping outbound PHB packets to 802.1p packets.	-
default	Enables mapping outbound PHB packets to 802.1p packets.	enable

Default Value

Enables the synchronization function.

View

Ethernet bridge interface configuration view, Ethernet routing interface configuration view, Trunk interface configuration view

Usage Guidelines

NA

Example

Disable mapping outbound PHB packets to 802.1p packets.

```
Switch(config-10ge1/0/1)#qos phb marking 8021p disable
Switch(config-10ge1/0/1)#
```

6.1.12 qos phb marking dscp**Function**

The **qos phb marking dscp** command enables or disables mapping outbound PHB packets to DSCP values.

Format

qos phb marking dscp { enable | disable | default }

Parameter

Parameter	Description	Value
enable	Enables mapping outbound PHB packets to DSCP values.	-
disable	Disables mapping outbound PHB packets to DSCP values.	-
default	Disables mapping outbound PHB packets to DSCP values.	disable

Default Value

Disable

View

Ethernet bridge interface configuration view, Ethernet routing interface configuration view, Trunk interface configuration view

Usage Guidelines

NA

Example

Enable mapping outbound PHB packets to DSCP values.

```
Switch(config-10ge1/0/1)#qos phb marking dscp enable
Switch(config-10ge1/0/1)#
```

6.1.13 trust dffserv**Function**

The **trust diffserv** command binds a DiffServ domain to an interface. Then, the system maps the priority of packets passing through this interface based on the mapping relationship of the DiffServ domain.

Format

trust diffserv domain { *NAME* | **default** }

Parameter

Parameter	Description	Value
NAME	Specifies a DiffServ domain name.	The value is a string consisting of 1 to 32 characters, without spaces.
default	Specifies the default DiffServ domain, of which the mapping relationship cannot be modified.	-

Default Value

NA

View

Ethernet bridge interface configuration view, Ethernet routing interface configuration view, Trunk interface configuration view

Usage Guidelines

NA

Example

Bind a DiffServ domain.

```
Switch(config-10ge1/0/1)#trust diffserv domain default
Switch(config-10ge1/0/1)#
```

6.2 Traffic Policing and Traffic Shaping Configuration Commands

6.2.1 counter

Function

The **counter** command sets a counter.

The **no counter** command cancels the configuration.

Format

- **counter** *counter-number* { **packet** | **byte** | **all** } **sort** { **green** | **red** | **greenred** | **greenyellow** | **redyellow** | **total** }
- **no counter** *counter-number*

Parameter

Parameter	Description	Value
counter-number	Indicates the counter number.	The value is an integer ranging from 1 to 1024.
packet byte all	Indicates the packet type and byte type of the counter.	-
green red greenred greenyellow redyellow total	Specifies a counter state display type, including green, red, green/red, green/yellow, red/yellow, and all.	-

Default Value

NA

View

Global configuration view

Usage Guidelines

NA

Example

Set a counter.

```
Switch(config)#counter 100 packet sort green
Switch(config)#
```

6.2.2 debug cos**Function**The **debug cos** command enables CoS debugging.The **no debug cos** command disables CoS debugging.**Format**

- **debug cos**
- **no debug cos**

Parameter

NA

Default Value

NA

View

Privileged user view

Usage Guidelines

NA

Example

Enable/Disable CoS debugging.

```
Switch#debug cos
Switch#
Switch#no debug cos
Switch#
```

6.2.3 meter**Function**

The **meter** command specifies the CIR, CBS, PIR, EBS, and PBS rate limiting rule through the meter.

The **no meter** command cancels the configuration.

Format

- **meter** *meter-number* **cir** *cir-number* **cbs** *cbs-number* **ebs** *ebs-number*
- **meter** *meter-number* **cir** *cir-number* **cbs** *cbs-number* **ebs** *ebs-number* { **aware** | **blind** }
- **meter** *meter-number* **cir** *cir-number* **cbs** *cbs-number* **pbs** *pbs-number* **pir** *pir-number*
- **meter** *meter-number* **cir** *cir-number* **cbs** *cbs-number* **pbs** *pbs-number* **pir** *pir-number* { **aware** | **blind** }
- **no meter** *meter-number*

Parameter

Parameter	Description	Value
meter-number	Specifies a meter number.	The value is an integer ranging from 1 to 256.
cir-number	Specifies a CIR number.	The value is an integer ranging from 64 to 4294967295.

Parameter	Description	Value
cbs-number	Specifies a CBS number.	The value is an integer ranging from 10000 to 4294967295.
ebs-number	Specifies an EBS number.	The value is an integer ranging from 10000 to 4294967295.
pbs-number	Specifies a PBS number.	The value is an integer ranging from 10000 to 4294967295.
pir-number	Specifies a PIR number.	The value is an integer ranging from 64 to 4294967295.
aware	Indicates the action to respond to the configured rate limiting rule and specified rule.	-
blind	Indicates the action not to respond to the configured rate limiting rule and specified rule.	-

Default Value

NA

View

Global configuration view

Usage Guidelines

You can use this command to configure the QoS CAR template (CIR, CBS, PIR, and PBS), applied in the inbound or outbound interface. After the QoS CAR applies to the physical interface or Eth-Trunk interface, the system limits the rate of all upstream packets transmitted over the physical interface or Eth-Trunk interface.

The priority of QoS CAR applied to the interface is higher than the QoS CAR of the VLAN. If the QoS CAR is enabled for both interface and VLAN, the QoS CAR of the interface shall prevail.

The *cir-value* specifies the committed information rate (CIR) that ensures a mean rate of packets passing through an interface.

The value is an integer ranging from 64 to 4294967295, in kbit/s.

The *cbs-value* specifies the size of the committed burst traffic that can pass through an interface.

The value is an integer ranging from 10000 to 4294967295, in bytes.

The *pir-value* specifies the peak data rate. The value is an integer ranging from 64 to 4294967295, in kbit/s. The *pir-value* must be equal to or larger than *cir-value*. By default, *pir-value* is equal to

cir-value. If the pir-value is equal to cir-value, the pbs-value is 0 bytes by default. Otherwise, pbs-value is 125 times the pir-value by default.

The pbs-value specifies the size of the peak burst. The value is an integer ranging from 10000 to 4294967295, in bytes. The pbs-value must be equal to or larger than cbs-value.

Traffic-based traffic policing enables a switch to limit the rate of traffic in compliance with the traffic classification rules. By policing the traffic rate, the switch discards traffic beyond the rate limiting, so that traffic entering the switch is limited within a reasonable range, thereby protecting network resources and carrier's interests. The traffic-based traffic policing adopts the dual leaky bucket algorithm.

You can specify the rate limiting rule using the meter, including the CIR, CBS, PIR, and PBS, specify the traffic type through the ACL, and associate the traffic type with the meter. You can enable the ACL at a physical interface (including Trunk) or VLAN interface.

The Switch supports two types of traffic shaping, namely, port shaping and port queue shaping. You can select the traffic shaping mode according to actual requirements. When both traffic shaping modes co-exist, ensure that the CIR of port shaping is equal to or larger than the sum of CIR of port queue shaping. Otherwise, traffic shaping is abnormal (for example, traffic in a queue with a lower priority preempts for bandwidth for traffic in a queue with a higher priority).

Example

Specify the CIR, CBS, PIR, EBS, and PBS rate limiting rule using a meter.

```
Switch(config)#meter 100 cir 100 cbs 20000 ebs 20000 aware
Switch(config)#
```

6.2.4 reset counter filter-list filter

Function

The **reset counter filter-list** command resets the filter counter of an ACL.

Format

- **reset counter filter-list** *acl-number* **filter** *filter-number* **port** { **ethernet** | **xgigaethernet** | **10gigaethernet** | **25gigaethernet** | **40gigaethernet** | **100gigaethernet** } *interface-number* { **in** | **out** }
- **reset counter filter-list** *acl-number* **filter** *filter-number* **port eth-trunk** *trunk-number* { **in** | **out** }
- **reset counter filter-list** *acl-number* **filter** *filter-number* { **in** | **out** }

- **reset counter filter-list** *acl-number* **filter** *filter-number* **vlan** *vlan-id* { **in** | **out** }

Parameter

Parameter	Description	Value
acl-number	Specifies an ACL number.	The value is an integer ranging from 1 to 4000.
filter-number	Specifies a filter number.	The value is an integer ranging from 1 to 2048.
in out	Indicates that the ACL takes effect in the inbound or outbound direction of a port.	-
trunk-number	Specifies an aggregation port number.	The value is an integer ranging from 1 to 128.
vlan-id	Specifies a VLAN ID.	The value is an integer ranging from 1 to 4094.
interface-number	Specifies an Ethernet interface number.	The value is an integer in the range of <1-1>/<0-1>/<1-48> (For reference only. The specific value range depends on the slot number and card type).

Default Value

NA

View

Global configuration view

Usage Guidelines

NA

Example

Reset the counter of filter 1 in ACL 100 in the inbound direction of interface xgigaethernet 1/0/1.

```
Switch(config)#reset counter filter-list 100 filter 1 port xgigaethernet 1/0/1 in
Switch(config)#
```

6.2.5 show counter

Function

The **show counter** command displays counter information and configuration information.

Format

- **show counter**
- **show counter config**

Parameter

NA

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

Display counter information.

```
Switch>show counter
  Version is COUNTER_VB3.00.00.00
  The total number of counter is :0
Switch>
```

6.2.6 show meter**Function**

The **show meter** command displays rate limiting configuration of the meter, including the CIR, CBS, PIR, EBS, and PBS.

Format**show meter****Parameter**

NA

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

Display meter configuration.

```
Switch>show meter
  ID   CIR   PIR   CBS   EBS   PBS   Mode  Ref-Cnt Status
  ---  ---  ---  ---  ---  ---  ---  ---  ---
   1   100   -    1000000 10000000- aware 0      Valid
Switch>
```

6.2.7 show meter config

Function

The **show meter config** command displays rate limiting configuration of the meter, including the CIR, CBS, PIR, EBS, and PBS.

Format

show meter config

Parameter

NA

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

Display meter configuration.

```
Switch>show meter config
meter 1 cir 10 cbs 20000 ebs 100000 blind
Switch>
```

6.2.8 traffic-car include-interframe

Function

The **traffic-car include-interframe** command enables or disables including IFG and lead code of a packet in calculation of traffic policing and interface rate limit.

Format

traffic-car include-interframe { enable | disable }

Parameter

Parameter	Description	Value
enable	Enables including IFG and lead code of a packet in calculation of traffic policing and interface rate limit.	-
disable	Disables including IFG and lead code of a packet in calculation of traffic policing and interface rate limit.	-

Default Value

NA

View

Global configuration view

Usage Guidelines

NA

Example

Display meter configuration.

```
Switch(config)#traffic-car include-interframe enable
Switch(config)#
```

6.3 Queue Scheduling and Congestion Control Configuration Commands

6.3.1 cos queue weight

Function

The **cos queue weight** command sets the weight of a port queue.

Format

- **cos queue** *queue-number* **weight** *weight*
- **cos queue** *queue-list* **weight** *weight*

Parameter

Parameter	Description	Value

Parameter	Description	Value
queue-number	Specifies a queue number.	The value is an integer ranging from 0 to 7.
weight	Specifies a queue weight.	The value is an integer ranging from 0 to 7.
queue-list	Specifies a queue sequence.	The value is a string of integers, for example 1, 2, with each integer ranging from 0 to 7.

Default Value

If the value is set to the default value SP using the **cos scheduling** command, the switch does not have the default weight entry. If the value is set to WRR using the **cos scheduling** command, the default number of weight entries is 1.

View

Ethernet bridge interface configuration view, Ethernet routing interface configuration view, Peerlink interface configuration view

Usage Guidelines

You must run **cos queue weight** and **cos scheduling algorithm** together (**sp+wrr** or **wrr**). If **scheduling algorithm** is set to **SP**, **cos queue weight** cannot be configured. See cos scheduling.

Example

Set the weight of a port queue.

```
Switch#config
  %Enter configuration commands.End with Ctrl+Z or command "quit" & "end"
Switch(config)#interface xgigaethernet 1/0/1
Switch(config-10ge1/0/1)#cos queue 1 weight 1
Switch(config-10ge1/0/1)#
```

6.3.2 cos queue priority

Function

The **cos queue priority** command configures the priority of a specified port queue.

Format

cos queue *queue-index* **priority** *priority-value*

Parameter

Parameter	Description	Value
queue-index	Specifies a queue index.	The value is an integer ranging from 0 to 7.
priority-value	Specifies a priority.	The value is an integer ranging from 0 to 7.

Default Value

The default value is 1.

View

Ethernet bridge interface configuration view, Ethernet routing interface configuration view

Usage Guidelines

This command is valid only for devices supporting the interface mode.

Example

Configure the priority of a specified port queue.

```
Switch(config)#interface 10gigaethernet 1/0/1
Switch(config-10ge1/0/1)#cos queue 0 priority 7
Switch(config-10ge1/0/1)#
```

6.3.3 cos scheduling**Function**

The **cos scheduling** command sets the scheduling mode for queues on an interface.

Format

- **cos scheduling { sp | rr | wrr | drr }**
- **cos scheduling { sp+rr | sp+wrr | sp+drr } queue-list**

Parameter

Parameter	Description	Value
sp	Indicates the Strict Priority (SP) scheduling mode.	-
rr	Indicates the Round Robin (RR) scheduling mode.	-
wrr	Indicates the Weighted Round Robin (WRR) scheduling mode.	-
drr	Indicates the Deficit Round Robin (DRR) scheduling mode.	-
queue-list	Specifies a queue sequence.	The value is a string of integers, for example 1, 2, with each integer ranging from 0 to 7.

Default Value

The default mode is SP.

View

Ethernet bridge interface configuration view, Ethernet routing interface configuration view, Peerlink interface configuration view

Usage Guidelines

When a network encounters intermittent congestion, congestion management is required if the delay-sensitive services require higher QoS quality than the non-delay-sensitive services. Congestion management is generally implemented using queue scheduling technology. The Switch supports the following queue scheduling technologies:

SP queue scheduling

WRR queue scheduling

DRR queue scheduling

SP + WRR queue scheduling

SP + DRR queue scheduling

The Switch supports eight queues on each interface. These queues can use different queue scheduling algorithms. During queue scheduling, the switch schedules the SP queues first. Multiple SP queues are scheduled based on the priority from high to low. After scheduling of SP queues is complete, the system starts weighted round robin scheduling for WRR or DRR queues.

Before configuring queue shaping on an interface, set the scheduling mode to WRR or DRR for the specified queues. Otherwise, the queue shaping function will not take effect.

Example

Configure the scheduling mode for queues on an interface.

```
Switch(config-10ge1/0/1)#cos scheduling sp
Switch(config-10ge1/0/1)#
```

6.3.4 cos queue {min-bandwidth|max-bandwidth}**Function**

The **cos queue {min-bandwidth|max-bandwidth}** command sets the maximum bandwidth for queues.

Format

- **cos queue** { *queue-index* | *queue-list* } { **min-bandwidth** | **max-bandwidth** } { **kbps** | **mbps** | **gbps** } *bandwidth-value*

- **no cos queue *queue-index* bandwidth**
- **no cos queue *queue-list* bandwidth**

Parameter

Parameter	Description	Value
queue-index	Specifies a queue number.	The value is an integer ranging from 0 to 7.
queue-list	Specifies a queue sequence.	The value is a string of integers, for example 1, 2, with each integer ranging from 0 to 7.
bandwidth-value	Specifies the bandwidth in the granularity of Kbps, Mbps, and Gbps.	When the unit is Mbit/s, the bandwidth value ranges from 1 to 10000. When the unit is Gbit/s, the bandwidth value ranges from 1 to 10. When the unit is kbit/s, the bandwidth value ranges from 1 to 10000000.

Default Value

NA

View

Ethernet bridge interface configuration view, Ethernet routing interface configuration view, Peerlink interface configuration view

Usage Guidelines

NA

Example

Set the minimum bandwidth of queue 0 on interface xgigaethernet 1/0/1 to 64 kbit/s.

```
Switch(config-10ge1/0/1)#cos queue 0 min-bandwidth kbps 4
Switch(config-10ge1/0/1)#
```

6.3.5 show cos interface

Function

The **show cos interface** command displays the CoS configuration on an interface.

Format

- **show cos interface**
- **show cos interface { ethernet | xgigaethernet | 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet } interface-number**

Parameter

Parameter	Description	Value
interface-number	Specifies an interface number.	The value is an integer in the range of <1-1>/<0-1>/<1-48> (For reference only. The specific value range depends on the slot number and card type).

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

View the CoS configuration on an interface.

```
Switch>show cos interface
'BW' means 'Bandwidth'
'bps' means 'bits per second'
```

Interface	Queue	Max-BW(bps)	Min-BW(bps)	Weight
10ge1/0/1	0	0M	0M	N/A
10ge1/0/1	1	0M	0M	N/A
10ge1/0/1	2	0M	0M	N/A
10ge1/0/1	3	0M	0M	N/A
10ge1/0/1	4	0M	0M	N/A
10ge1/0/1	5	0M	0M	N/A
10ge1/0/1	6	0M	0M	N/A
10ge1/0/1	7	0M	0M	N/A
10ge1/0/2	0	0M	0M	N/A
10ge1/0/2	1	0M	0M	N/A
10ge1/0/2	2	0M	0M	N/A
10ge1/0/2	3	0M	0M	N/A
10ge1/0/2	4	0M	0M	N/A
10ge1/0/2	5	0M	0M	N/A
10ge1/0/2	6	0M	0M	N/A
10ge1/0/2	7	0M	0M	N/A
10ge1/0/3	0	0M	0M	N/A
10ge1/0/3	1	0M	0M	N/A
10ge1/0/3	2	0M	0M	N/A

```
Switch>
```

6.3.6 show cos config

Function

The **show cos config** command displays the CoS configuration.

Format

show cos config

Parameter

NA

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

View the CoS configuration.

```
Switch> show cos config
!
interface 10gigaethernet 1/0/1
  cos scheduling wrr
Switch>
```

6.3.7 show drop-profile

Function

The **show drop-profile** command displays summary information about all WRED drop profiles on the switch.

The **show drop-profile** *drop-profile-name* command displays configuration of a specified WRED drop profile.

The **show drop-profile all** command displays detailed information about all WRED drop profiles on the switch.

Format

show drop-profile**show drop-profile** *drop-profile-name***show drop-profile all****Parameter**

Parameter	Description	Value
drop-profile-name	Specifies the name of a WRED drop profile.	The value is a string consisting of up to 32 bytes.

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

Display summary information about all WRED drop profiles on the switch.

Switch(config-10ge1/0/40)#show drop-profile	
Index	Drop profile name
0	default
1	fhn
2	1
Total:64	Used:3
Switch(config-10ge1/0/40)#	

6.3.8 show wred config**Function**The **show wred config** command displays all WRED configuration on an interface or a VLAN.**Format****show wred config****Parameter**

NA

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

Display all WRED configuration on interface xge1/0/40.

```

Switch(config-10ge1/0/40)#show wred config
  drop-profile fhn
  drop-profile 1
  color red low-threshold 20 high-threshold 40 discard-percent 40

interface xgigaethernet 1/0/40
  qos wred fhn

interface xgigaethernet 1/0/40
  qos queue 2 wred fhn
Switch(config-10ge1/0/40)#

```

6.3.9 debug wred**Function**The **debug wred** command enables WRED debugging.The **no debug wred** command disables WRED debugging.**Format****debug wred****no debug wred****Parameter**

NA

Default Value

NA

View

Privileged user view

Usage Guidelines

NA

Example

Enable WRED debugging.

```
Switch#debug wred
Switch#
```

6.3.10 drop-profile

Function

The **drop-profile** command creates a WRED drop profile and displays its configuration view or directly displays the configuration view of an existing drop profile.

The **no drop-profile** command deletes a specified WRED drop profile.

Format

drop-profile { *drop-profile-name* | **default** }

no drop-profile *drop-profile-name*

Parameter

Parameter	Description	Value
drop-profile-name	Specifies the name of a WRED drop profile.	The value is a string consisting of up to 32 bytes.

Default Value

NA

View

Global configuration view

Usage Guidelines

A WRED drop profile specifies WRED parameters for packets of different priorities in interface queues, to implement congestion avoidance for the interface or interface queue to which the WRED drop profile is bound.

Example

Create WRED drop profile fhn.

```
Switch(config)#drop-profile fhn
Switch(config-drop-fhn)#
```

6.3.11 qos ecn

Function

The **qos ecn** command enables the ECN function globally.

The **no qos ecn** command disables the ECN function globally.

Format

qos ecn *name*

no qos ecn

Parameter

Parameter	Description	Value
name	Specifies the name of a drop profile.	The value is a string consisting of up to 32 bytes.

Default Value

By default, ECN is not enabled globally.

View

Ethernet bridge configuration view, Ethernet route configuration view, Ethernet bridge GRP configuration view, Ethernet route GRP configuration view

Usage Guidelines

NA

Example

Enable ECN globally.

```
Switch(config-10ge1/0/1)#qos ecn fhn
Switch(config-10ge1/0/1)#
```

6.3.12 qos wred

Function

The **qos wred** command applies a WRED drop profile to an interface.

The **no qos wred** command deletes a WRED drop profile applied to an interface.

Format

qos wred *name*

no qos wred

Parameter

Parameter	Description	Value
name	Specifies the name of a WRED drop profile.	The value is a string consisting of up to 32 bytes.

Default Value

By default, no WRED drop profile is applied to the interface.

View

Interface configuration view (Ethernet), interface group configuration view

Usage Guidelines

Before running this command, you must run drop-profile to create a WRED drop profile.

Example

Apply a WRED drop profile to an interface.

```
Switch(config-10ge1/0/40)#qos wred fhj
Switch(config-10ge1/0/40)#
```

6.3.13 qos queue wred**Function**

The **qos queue wred** command applies a WRED drop profile to an interface queue.

The **no qos queue wred** command deletes a WRED drop profile applied to an interface queue.

Format

qos queue *queue-index* **wred** *name*

no qos queue *queue-index* **wred**

Parameter

Parameter	Description	Value
queue-index	Specifies a queue index.	The value is an integer ranging from 0 to 7.
name	Specifies the name of a WRED drop profile	The value is a string consisting of up to

Parameter	Description	Value
	to be bound.	32 bytes.

Default Value

By default, no WRED drop profile is applied to the interface queue.

View

Interface configuration view (Ethernet), interface group configuration view

Usage Guidelines

Before running this command, you must run drop-profile to create a WRED drop profile.

Example

Apply a WRED drop profile to an interface queue.

```
Switch(config-10ge1/0/40)#qos queue 2 wred fhv
Switch(config-10ge1/0/40)#
```

6.3.14 qos queue ecn

Function

The **qos queue ecn** command enables the Explicit Congestion Notification (ECN) function for the specified queue and configures the drop threshold percentage and maximum drop probability through the specified bound drop profile.

The **no qos queue ecn** command disables the ECN function for the specified queue

Format

qos queue *queue-index* **ecn** *name*

no qos queue *queue-index* **ecn**

Parameter

Parameter	Description	Value
queue-index	Specifies a queue index.	The value is an integer ranging from 0 to 7.
name	Specifies the name of a drop profile.	The value is a string consisting of up to 32 bytes.

Default Value

By default, ECN is not enabled for any queue.

View

Ethernet bridge configuration view, Ethernet route configuration view, Ethernet bridge GRP configuration view, Ethernet route GRP configuration view

Usage Guidelines

NA

Example

Disable ECN for the specified queue.

```
Switch(config-10ge1/0/1)#no qos queue 2 ecn
Switch(config-10ge1/0/1)#
```

6.3.15 ecn low-limit low-limit high-limit discard-percent**Function**

The **ecn low-limit low-limit high-limit discard-percent** command sets the Explicit Congestion Notification (ECN) parameters, including the absolute drop threshold, discard threshold percentage, and maximum discard probability.

Format

ecn low-limit { *low-limit* | **default** } **high-limit** { *high-limit* | **default** } **discard-percent** { *discard-percent* | **default** }

Parameter

Parameter	Description	Value
low-limit	Specifies the lower WRED drop threshold. When the percentage of the packet length against the queue length reaches this threshold, the system starts to drop packets.	The value is an integer ranging from 1 to 100. The default value is 100.
high-limit	Specifies the upper WRED drop threshold. When the percentage of the packet length against the queue length reaches this threshold, the system drops all newly received packets.	The value is an integer ranging from 1 to 100. The default value is 100.
discard-percent	Specifies the maximum WRED drop probability.	The value is an integer ranging from 1 to 100. The default value is 100.

Default Value

NA

View

Drop-profile configuration view

Usage Guidelines

When both upstream and downstream devices support ECN, after the drop threshold and maximum drop probability are configured, the system sets the packet ECN field to CE when the lower drop threshold is reached, so that the downstream device can detect network congestion based on the value of the packet ECN domain and notify the upstream device. After receiving the notification, the upstream device reduces the packet sending rate to avoid increasing congestion.

Example

Set ECN parameters.

```
Switch(config-drop-1)#ecn low-limit 20 high-limit 40 discard-percent 20
Switch(config-drop-1)#
```

6.3.16 qos ecn {enable|disable}**Function**

The **qos ecn {enable|disable}** command enables or disables ECN.

Format

qos ecn { enable | disable }

Parameter

Parameter	Description	Value
enable	Enables ECN.	-
disable	Disables ECN.	-

Default Value

Disable

View

Drop-profile configuration view

Usage Guidelines

When both upstream and downstream devices support ECN, the downstream device can detect network congestion based on the value of the packet ECN domain and notify the upstream device. After receiving the notification, the upstream device reduces the packet sending rate to avoid increasing congestion.

Example

Enable ECN.

```
Switch(config-drop-1)#qos ecn enable
Switch(config-drop-1)#
```

6.3.17 reset cos statistics**Function**

The **reset cos statistics** command resets the CoS statistics.

Format

- **reset cos statistics all**
- **reset cos statistics interface { ethernet | xgigaethernet | 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet } interface-number**

Parameter

Parameter	Description	Value
interface-number	Specifies an interface number.	The value is an integer in the range of <1-1>/<0-1>/<1-48> (For reference only. The specific value range depends on the slot number and card type).

Default Value

NA

View

Global configuration view

Usage Guidelines

NA

Example

Reset the CoS statistics.

```
Switch(config)#reset cos statistics all
Switch(config)#
```

6.3.18 show cos statistics**Function**

The **show cos statistics** command displays the CoS statistics.

Format

- **show cos statistics all**
- **show cos statistics interface { ethernet | xgigaethernet | 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet } interface-number**

Parameter

Parameter	Description	Value
interface-number	Specifies an Ethernet interface number.	The value is an integer in the range of <1-1>/<0-1>/<1-48> (For reference only. The specific value range depends on the slot number and card type).

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

Display the CoS statistics.

Switch>show cos statistics interface 25gigaethernet 1/0/1				
Interface	Queue	Passed-Packets(H/L)	Passed-Bytes(H/L)	Dropped-Packets(H/L)
Dropped-Bytes(H/L)				
25ge1/0/1	0	0/0	0/0	0/0
25ge1/0/1	1	0/0	0/0	0/0
25ge1/0/1	2	0/0	0/0	0/0
25ge1/0/1	3	0/0	0/0	0/0
25ge1/0/1	4	0/0	0/0	0/0
25ge1/0/1	5	0/0	0/0	0/0


```
0/0
 25ge1/0/1      6      0/0      0/0      0/0
0/0
 25ge1/0/1      7      0/0      0/0      0/0
0/0
Switch>
```

Chapter 7 Multicast Commands

This chapter introduces the commands for configuring multicast services on the Switch, including IGMP Snooping, IGMP, and MLD Snooping.

7.1 IGMP Snooping Configuration Commands

7.1.1 debug igmpsnoop

Function

The **debug igmpsnoop** command enables IGMP snooping debugging.

The **no debug igmpsnoop** command disables IGMP snooping debugging.

Format

- **debug igmpsnoop { rx | tx | report | query | leave | group | uplink | mvlan | interface | message | sync | hw | error | control | all }**
- **no debug igmpsnoop { rx | tx | report | query | leave | group | uplink | mvlan | interface | message | sync | hw | error | control | all }**

Parameter

NA

Default Value

By default, IGMP snooping debugging is disabled.

View

Privileged user view

Usage Guidelines

NA

Example

Enable IGMP snooping debugging.

```
Switch#debug igmpsnoop all
Switch#
```

7.1.2 hwmc mac-ip-check {enable|disable}

Function

The **hwmc mac-ip-check {enable|disable}** command enables or disables consistency check between the multicast destination MAC address and destination IP address.

Format

hwmc mac-ip-check { enable | disable }

Parameter

Parameter	Description	Value
enable	Enables consistency check between the multicast destination MAC address and destination IP address.	-
disable	Disables consistency check between the multicast destination MAC address and destination IP address.	-

Default Value

By default, the consistency check between the multicast destination MAC address and destination IP address is enabled.

View

Global configuration view

Usage Guidelines

During IP multicasting, the lower 23 bits of the IP address are mapped to the lower 23 bits of the MAC address. After check is enabled, if the mapping between the destination MAC and IP addresses of the multicast packet does not meet the above rule, the packet is discarded.

Example

Disable consistency check between the multicast destination MAC address and destination IP address.

```
Switch(config)#hwmc mac-ip-check disable
Switch(config)#
```

7.1.3 igmp-snooping {enable|disable}

Function

The **igmp-snooping {enable|disable}** command enables or disables IGMP snooping on an interface.

Format

igmp-snooping { enable | disable }**Parameter**

Parameter	Description	Value
enable	Enables IGMP snooping.	-
disable	Disables IGMP snooping.	-

Default Value

Disable

View

Interface configuration view (Trunk), Ethernet bridge interface configuration view, Ethernet routing interface configuration view, GRP bridge interface configuration view, and GRP routing interface configuration view

Usage Guidelines

Before using this command, run the **igmp-snooping start** command in the global configuration view.

Example

Enable IGMP snooping.

```
Switch(config)#interface xgigaethernet 1/0/1
Switch(config-10ge1/0/1)#igmp-snooping enable
Switch(config-10ge1/0/1)#
```

7.1.4 igmp-snooping ctrlmode {enable|disable}**Function**

The **igmp-snooping ctrlmode {enable|disable}** command configures controllable multicast on an interface.

Format

igmp-snooping ctrlmode { enable | disable }

Parameter

Parameter	Description	Value
enable	Enables controllable multicast on the interface.	-
disable	Disables controllable multicast on the interface.	-

Default Value

Disable

View

Interface configuration view (Trunk), Ethernet bridge interface configuration view, Ethernet routing interface configuration view, GRP bridge interface configuration view, and GRP routing interface configuration view

Usage Guidelines

Before using this command, run the `igmp-snooping {enable|disable}` command to enable the multicast snooping of the interface.

Example

Enable controllable multicast on an interface.

```
Switch(config-10ge1/0/1)#igmp-snooping enable
Switch(config-10ge1/0/1)#igmp-snooping ctrlmode enable
Switch(config-10ge1/0/1)#
```

7.1.5 igmp-snooping fast-leave

Function

The **igmp-snooping fast-leave** command enables or disables the fast leave function on an interface.

Format

igmp-snooping fast-leave { enable | disable }

Parameter

Parameter	Description	Value
enable	Enables the fast leave function.	-
disable	Disables the fast leave function.	-

Default Value

NA

View

Interface configuration view (Trunk), Ethernet bridge interface configuration view, Ethernet routing interface configuration view

Usage Guidelines

After the fast leave function is enabled on an interface, the Switch will delete the interface from the forwarding entry of a multicast group immediately after receiving an IGMP Leave packet for this group from a host. When only one user host is connected to the interface, the fast leave mechanism enables the switch to release bandwidth resources in a timely manner.

Before using this command, run the **igmp-snooping start** and **igmp-snooping enable** commands in the global configuration view and interface configuration view respectively.



Caution

You can configure the fast leave function only when each multicast group member interface in a VLAN is connected to only one receiver host. If an interface is connected to multiple receiver hosts, fast leave will interrupt multicast data transmission to other receiver hosts.

Example

Enable the fast leave function.

```
Switch(config-10ge1/0/1)#igmp-snooping fast-leave enable
Switch(config-10ge1/0/1)#
```

7.1.6 igmp-snooping fast-switch

Function

The **igmp-snooping fast-switch** command enables or disables fast switchover when the STP snooping changes.

Format

igmp-snooping fast-switch { enable | disable }

Parameter

Parameter	Description	Value
enable	Enables fast switchover when the STP snooping changes.	-
disable	Disables fast switchover when the STP snooping changes.	-

Default Value

NA

View

MVLAN configuration view

Usage Guidelines

NA

Example

```
# Enable fast switchover when the STP snooping changes.
```

```
Switch(config-igmpsnoop-mvlan100)#igmp-snooping fast-switch enable
Switch(config-igmpsnoop-mvlan100)#
```

7.1.7 igmp-snooping fast-switch query {enable|disable}**Function**

The **igmp-snooping fast-switch query {enable|disable}** command enables or disables sending the general query function when fast switchover is triggered due to changes of the STP snooping.

Format

igmp-snooping fast-switch query { enable | disable }

Parameter

Parameter	Description	Value
enable	Enables sending the general query function when fast switchover is triggered due to changes of the STP snooping.	-
disable	Disables sending the general query function when fast switchover is triggered due to changes of the STP snooping.	-

Default Value

NA

View

MVLAN configuration view

Usage Guidelines

NA

Example

```
# Enable sending the general query function when fast switchover is triggered due to changes of the STP snooping.
```

```
Switch(config)#igmp-snooping fast-switch query enable
Switch (config)#
```

7.1.8 igmp-snooping group-address mvlan

Function

The **igmp-snooping group-address mvlan** command creates a pre-joined group.

The **no igmp-snooping group-address mvlan** command deletes a pre-joined group.

Format

- **igmp-snooping group-address** *group-address* **mvlan** *vlan-id*
- **no igmp-snooping group-address** *group-address* **mvlan** *vlan-id*

Parameter

Parameter	Description	Value
group-address	Specifies a multicast IP address.	The value is in dotted decimal notation, for example, <i>A.B.C.D</i> , in which <i>A</i> to <i>D</i> are decimal digits ranging from 0 to 255.
vlan-id	Specifies a VLAN entry.	The value is an integer ranging from 1 to 4094.

Default Value

NA

View

Global configuration view

Usage Guidelines

NA

Example

Create a pre-joined group.

```
Switch(config)#igmp-snooping group-address 225.0.0.1 mvlan 100
Switch(config)#
```

7.1.9 igmp-snooping max-response-time

Function

The **igmp-snooping max-response-time** command sets the global maximum response time for IGMP snooping General Query packets.

Format

igmp-snooping max-response-time { *max-response-time* | **default** }

Parameter

Parameter	Description	Value
max-response-time	Specifies the maximum response time.	The value is an integer ranging from 1 to 25, in seconds.
default	Specifies the default value.	10 seconds

Default Value

10 seconds

View

Global configuration view, MVLAN configuration view

Usage Guidelines

The maximum response time provides the following functions:

Controls the deadline for hosts to send Membership Report Packets. Enables hosts to rapidly respond to Query packets and avoids traffic congestion due to a large number of Report packets sent by many hosts simultaneously.

Adjusts the aging time of member interfaces. When the Switch receives an IGMP Report packet from a host, it sets the aging time of the corresponding group member interface to: IGMP robustness count x General query interval + Maximum response time. This command sets the maximum response time used in the formula. The IGMP robustness count is configured using the `igmp-snooping query-duplicate-suppress {enable|disable}` command. The general query interval is configured using the `igmp-snooping proxy-uplink-port` command.

Before using this command, run the **igmp-snooping start** command in the global configuration view.



Caution

The value of **max-response-time** must be smaller than that of **query-interval**.

Example

```
# Configure the global maximum response time for IGMP snooping General Query packets.
```

```
Switch(config)#igmp-snooping max-response-time 10
Switch(config)#
```

7.1.10 igmp-snooping multicast user-vlan

Function

The **igmp-snooping multicast user-vlan** command specifies user VLANs for multicast replication.

The **no igmp-snooping multicast user-vlan** command deletes user VLANs for multicast replication.

Format

- **igmp-snooping multicast user-vlan** *vlan-list*
- **no igmp-snooping multicast user-vlan** *vlan-list*
- **no igmp-snooping multicast user-vlan all**

Parameter

Parameter	Description	Value
vlan-list	Specifies a VLAN list.	The value is an integer ranging from 1 to 4094.

Default Value

NA

View

MVLAN configuration view

Usage Guidelines

Before using this command, run the **igmp-snooping start** command in the global configuration view.

Example

Configure user VLANs for multicast replication.

```
Switch(config-igmpsnoop-mvlan100)#igmp-snooping multicast user-vlan 100
Switch(config-igmpsnoop-mvlan100)#
```

7.1.11 igmp-snooping multicast-vlan

Function

The **igmp-snooping multicast-vlan** command enables or disables the multicast replication function.

Format

igmp-snooping multicast-vlan { enable | disable }

Parameter

Parameter	Description	Value
enable	Enables the multicast replication function.	-
disable	Disables the multicast replication function.	-

Default Value

NA

View

MVLAN configuration view

Usage Guidelines

Before using this command, run the **igmp-snooping start** command in the global configuration view.

Example

Enable the multicast replication function.

```
Switch(config-igmpsnoop-mvlan100)#igmp-snooping multicast-vlan enable
Switch(config-igmpsnoop-mvlan100)#
```

7.1.12 igmp-snooping mvlan

Function

The **igmp-snooping mvlan** command creates a multicast VLAN (MVLAN) and displays the MVLAN configuration view.

The **no igmp-snooping mvlan** command deletes a multicast VLAN.

Format

- **igmp-snooping mvlan** *vlan-id*
- **no igmp-snooping mvlan** *vlan-id*

Parameter

Parameter	Description	Value
vlan-id	Specifies a VLAN entry.	The value is an integer ranging from 1 to 4094.

Default Value

NA

View

Global configuration view

Usage Guidelines

Before using this command, run the **igmp-snooping start** command in the global configuration view.

Example

Create an MVLAN and display the MVLAN configuration view.

```
Switch(config)#igmp-snooping mvlan 100
Switch(config-igmpsnoop-mvlan100)#
```

7.1.13 igmp-snooping mvlan uplink-port**Function**

The **igmp-snooping mvlan uplink-port** command creates an uplink interface of an MVLAN.

The **no igmp-snooping mvlan uplink-port** command deletes an uplink interface of an MVLAN.

Format

- **igmp-snooping mvlan** *vlan-id* **uplink-port**
- **no igmp-snooping mvlan** *vlan-id* **uplink-port**

Parameter

Parameter	Description	Value
vlan-id	Specifies a VLAN entry.	The value is an integer ranging from 1 to 4094.

Default Value

NA

View

Interface configuration view (Trunk), Ethernet bridge interface configuration view, Ethernet routing interface configuration view

Usage Guidelines

Before using this command, run the **igmp-snooping enable** command in the interface configuration view.

Example

Create an uplink interface of an MVLAN.

```
Switch(config-10ge5/0/1)#igmp-snooping enable
Switch(config-10ge5/0/1)#igmp-snooping mvlan 100 uplink-port
Switch(config-10ge5/0/1)#show
```

7.1.14 igmp-snooping forwarding-mode {ip|mac}

Function

The **igmp-snooping forwarding-mode {ip|mac}** command sets the multicast data forwarding mode.

Format

- **igmp-snooping forwarding-mode ip**
- **igmp-snooping forwarding-mode mac**

Parameter

Parameter	Description	Value
ip	Forwards multicast data according to the IP address.	-
mac	Forwards multicast data according to MAC address.	-

Default Value

NA

View

MVLAN configuration view

Usage Guidelines

Before using this command, run the **igmp-snooping start** command in the global configuration view.

Example

Set the multicast data forwarding mode.

```
Switch(config-igmpsnoop-mvlan2)#igmp-snooping forwarding-mode ip
Switch(config-igmpsnoop-mvlan2)#
```

7.1.15 igmp-snooping group-policy filter-list

Function

The **igmp-snooping group-policy filter-list** command sets a multicast policy for a MVLAN.

The **no igmp-snooping group-policy** command cancels the configuration.

Format

- **igmp-snooping group-policy filter-list** *acl-number*
- **igmp-snooping group-policy filter-list** *acl-number version version-list*
- **no igmp-snooping group-policy**

Parameter

Parameter	Description	Value
acl-number	Specifies the ACL number bound with a multicast policy.	The value is an integer ranging from 1001 to 2000.
version-list	Specifies the list of applicable multicast snooping protocol versions.	The value is an integer ranging from 1 to 3. The version list can be in a format similar to 1-3.

Default Value

NA

View

Interface configuration view (Trunk), Ethernet bridge interface configuration view, Ethernet routing interface configuration view, GRP bridge interface configuration view, GRP routing interface configuration view, and IGMP Snooping MVLAN configuration view

Usage Guidelines

NA

Example

Configure a multicast policy within the multicast VLAN.

```
Switch(config-igmpsnoop-mvlan1)#igmp-snooping group-policy filter-list 1001 version 1-3
Switch(config-igmpsnoop-mvlan1)#
```

7.1.16 igmp-snooping querier {enable|disable}**Function**

The **igmp-snooping querier {enable|disable}** command enables or disables the querier function on a VLAN.

Format

igmp-snooping querier { enable | disable }

Parameter

Parameter	Description	Value
enable	Enables the querier function on a VLAN.	-
disable	Disables the querier function on a VLAN.	-

Default Value

NA

View

MVLAN configuration view

Usage Guidelines

Before using this command, run the **igmp-snooping start** command in the global configuration view.

Example

Enable the querier function on a VLAN.

```
Switch(config-igmpsnoop-mvlan2)#igmp-snooping querier enable
Switch(config-igmpsnoop-mvlan2)#
```

7.1.17 igmp-snooping proxy-ip

Function

The **igmp-snooping proxy ip** command configures a multicast proxy IP address.

The **no igmp-snooping proxy ip** command deletes the configured multicast proxy IP address.

Format

- **igmp-snooping proxy-ip** *ip-address*
- **no igmp-snooping proxy-ip**

Parameter

Parameter	Description	Value
ip-address	Specifies a destination IP address.	The value is in dotted decimal notation, for example, <i>A.B.C.D</i> , in which <i>A</i> to <i>D</i> are decimal digits ranging from 0 to 255.

Default Value

NA

View

MVLAN configuration view

Usage Guidelines

Before using this command, run the **igmp-snooping start** command in the global configuration view.

Example

Configure a multicast proxy IP address.

```
Switch(config-igmpsnoop-mvlan100)#igmp-snooping proxy-ip 2.2.2.2
Switch(config-igmpsnoop-mvlan100)#
```

7.1.18 igmp-snooping proxy-uplink-port

Function

The **igmp-snooping proxy-uplink-port {enable|disable}** command enables or disables sending IGMP query packets to an interface.

Format

igmp-snooping proxy-uplink-port { enable | disable }

Parameter

Parameter	Description	Value
enable	Enables sending IGMP query packets to an interface.	-
disable	Disables sending IGMP query packets to an interface.	-

Default Value

NA

View

MVLAN configuration view

Usage Guidelines

NA

Example

Enable sending IGMP query packets to an interface.

```
Switch(config-igmpsnoop-mvlan100)#igmp-snooping proxy-uplink-port enable
Switch(config-igmpsnoop-mvlan100)#
```


7.1.19 igmp-snooping query-interval

Function

The **igmp-snooping query-interval** command sets the global general query interval for IGMP snooping.

Format

igmp-snooping query-interval { *query-interval* | **default** }

Parameter

Parameter	Description	Value
query-interval	Specifies a query interval.	The value is an integer ranging from 10 to 65535.
default	Specifies the default value.	60 seconds

Default Value

60 seconds

View

Global configuration view

Usage Guidelines

The general query interval can be used to:

It is used to configure the interval for sending IGMP general query messages. If the querier function is enabled in a VLAN, you can use this command to set the general query interval. The switch then periodically sends General Query messages to maintain group memberships on interfaces in the VLAN. The smaller the general query interval, the more sensitive the querier will be, but the more resources will be consumed on the switch.

Adjust the aging time of member interfaces. When the switch receives an IGMP Report packet from a host, the switch sets the aging time of the corresponding group member interface to: IGMP robustness variable x General query interval + Maximum response time. This command sets the general query interval used in the formula. The IGMP robustness count is configured using the **igmp-snooping query-duplicate-suppress {enable|disable}** command. The maximum response time is configured using the **igmp-snooping max-response-time** command.

Before using this command, run the **igmp-snooping start** command in the global configuration view.

Example

```
# Set the global IGMP snooping general query interval.
```

```
Switch(config)#igmp-snooping query-interval 20
Switch(config)#
```

7.1.20 igmp-snooping report-suppress

Function

The **igmp-snooping report-suppress** command enables or disables the multicast report proxy function.

Format

igmp-snooping report-suppress { enable | disable }

Parameter

Parameter	Description	Value
enable	Enables the multicast report proxy function.	-
disable	Disables the multicast report proxy function.	-

Default Value

Disable

View

MVLAN configuration view

Usage Guidelines

After you configure this command, the switch sends a Report or a Leave packet to the upstream device only when the first member joins the multicast group or the last member leaves the multicast group.

Before using this command, run the **igmp-snooping start** command in the global configuration view.

Example

Enable the multicast report proxy function.

```
Switch(config-igmpsnoop-mvlan100)#igmp-snooping report-suppress enable
Switch(config-igmpsnoop-mvlan100)#
```

7.1.21 igmp-snooping require-router-alert

Function

The **igmp-snooping require-router-alert** command configures the Router-Alert checking function of a multicast VLAN.

Format

igmp-snooping require-router-alert { enable | disable }

Parameter

Parameter	Description	Value
enable	Enables the Router-Alert checking function for the multicast VLAN.	-
disable	Disables the Router-Alert checking function for the multicast VLAN.	-

Default Value

Disable

View

MVLAN configuration view

Usage Guidelines

NA

Example

Enable the Router-Alert checking function for the multicast VLAN.

```
Switch(config-igmpsnoop-mvlan1)#igmp-snooping require-router-alert enable
Switch(config-igmpsnoop-mvlan1)#
```

7.1.22 igmp-snooping query-duplicate-suppress {enable|disable}

Function

The **igmp-snooping query-duplicate-suppress {enable|disable}** command enables or disables the query packet duplication suppression function.

Format

igmp-snooping query-duplicate-suppress { enable | disable }

Parameter

Parameter	Description	Value
enable	Enables the query packet duplication suppression function.	-
disable	Disables the query packet duplication suppression function.	-

Default Value

NA

View

Interface configuration view (Trunk), Ethernet bridge interface configuration view, Ethernet routing interface configuration view

Usage Guidelines

NA

Example

Enable the query packet duplication suppression function.

```
Switch(config-10ge1/0/1)#igmp-snooping enable
Switch(config-10ge1/0/1)#igmp-snooping query-duplicate-suppress enable
Switch(config-10ge1/0/1)#
```

7.1.23 igmp-snooping robust-count**Function**

The **igmp-snooping robust-count** command sets the robustness count, that is, the number of Group-specific Query packets sent by the querier.

Format

igmp-snooping robust-count { *robust-count* | **default** }

Parameter

Parameter	Description	Value
robust-count	Specifies the number of sending a specific query packet. It indicates the IGMP robustness count of the current VLAN.	The value is an integer ranging from 2 to 5.
default	Specifies the default value.	2

Default Value

2

View

Global configuration view

Usage Guidelines

The IGMP robustness count can be used to:

Configure the number of Group-specific Query packets sent by the querier to avoid packet loss. When the Switch receives an IGMP Leave packet for a group on a host, it sends a specified number of Group-specific Query packets to check whether this group has other members. The number of Group-specific Query packets is specified by the robustness count. The interval for sending Group-specific Query packets is configured using the `igmp-snooping lastmember-queryinterval` command.

Adjust the aging time of member interfaces. When the Switch receives an IGMP Report packet from a host, it sets the aging time of the corresponding group member interface to: IGMP robustness count x General query interval + Maximum response time. This command sets the robustness count used in the formula. The general query interval is configured using the `igmp-snooping query-interval` command. The maximum response time is configured using the `igmp-snooping max-response-time` command.

Before using this command, run the **igmp-snooping start** command in the global configuration view.

If you repeatedly run this command in the same configuration view, the new configuration will overwrite the old configuration.

Example

Set the number of Group-specific Query packets.

```
Switch(config)#igmp-snooping robust-count 2
Switch(config)#
```

7.1.24 igmp-snooping router-aging-time

Function

The **igmp-snooping router-aging time** command sets the global aging time for router interfaces.

Format

igmp-snooping router-aging-time { *router-aging-time* | **default** }

Parameter

Parameter	Description	Value
router-aging-time	Specifies the aging time of router interfaces.	The value is an integer ranging from 1 to 1000, in seconds.
default	Specifies the default value.	180 seconds

Default Value

180 seconds

View

Global configuration view

Usage Guidelines

When a dynamic router interface receives an IGMP Query packet or PIM Hello packet, the Switch resets the aging timer of the router interface.

By default:

When a dynamic router interface receives an IGMP Query packet, the Switch resets the aging timer of the router interface to 400 seconds.

When the interface receives a PIM Hello packet and the Holdtime value carried in the packet is greater than the remaining aging time of the router interface, the Switch resets the aging timer of the router interface to the Holdtime value. If the Holdtime value is smaller than the remaining aging time, the switch does not reset the aging timer of the router interface.

Before using this command, run the **igmp-snooping start** command in the global configuration view.



Caution

If you repeatedly run this command in the same configuration view, the new configuration will overwrite the old configuration.

Example

Configure the global aging time of router interfaces.

```
Switch(config)#igmp-snooping router-aging-time 2
Switch(config)#
```

7.1.25 igmp-snooping send-query source-address

Function

The **igmp-snooping send-query source-address** command sets the source IP address of a query packet in snooping mode.

Format

- **igmp-snooping send-query source-address *src-address***
- **igmp-snooping send-query source-address default**

Parameter

Parameter	Description	Value
src-address	Specifies a source IP address for the packet.	The value is in dotted decimal notation.
default	Specifies the default value.	The default IP address is 192.168.0.1.

Default Value

The default IP address is 192.168.0.1.

View

MVLAN configuration view

Usage Guidelines

NA

Example

Set the source IP address of a query packet in snooping mode.

```
Switch(config-igmpsnoop-mvlan100)#igmp-snooping send-query source-address 123.11.11.10
Switch(config-igmpsnoop-mvlan100)#
```

7.1.26 igmp-snooping lastmember-querynumber

Function

The **igmp-snooping lastmember-querynumber** command sets the number of group-specific queries globally.

Format

igmp-snooping lastmember-querynumber { *query-number* | **default** }

Parameter

Parameter	Description	Value
query-number	Specifies the number of group-specific queries.	The value is an integer ranging from 2 to 5.
default	Specifies the default value.	2

Default Value

2

View

MVLAN configuration view

Usage Guidelines

Before using this command, run the **igmp-snooping start** command in the global configuration view.

Example

Set the number of group-specific queries.

```
Switch(config-igmpsnoop-mvlan100)#igmp-snooping lastmember-querynumber 5
Switch(config-igmpsnoop-mvlan100)#
```

7.1.27 igmp-snooping lastmember-queryinterval**Function**

The **igmp-snooping lastmember-queryinterval** command sets the global group-specific query interval.

Format

igmp-snooping lastmember-queryinterval { *query-interval* | **default** }

Parameter

Parameter	Description	Value
query-interval	Specifies a group-specific query interval.	The value is an integer ranging from 1 to 5, in seconds.
default	Specifies the default value.	1

Default Value

1

View

Global configuration view, MVLAN configuration view

Usage Guidelines

Before using this command, run the **igmp-snooping start** command in the global configuration view.

Example

Set the global group-specific query interval.

```
Switch(config)#igmp-snooping lastmember-queryinterval 2
Switch(config)#
```

7.1.28 igmp-snooping {start|stop}

Function

The **igmp-snooping {start|stop}** command enables or disables the IGMP snooping protocol globally.

Format

igmp-snooping { start | stop }

Parameter

Parameter	Description	Value
start	Enables the IGMP snooping protocol.	-
stop	Disables the IGMP snooping protocol.	-

Default Value

Disable

View

Global configuration view

Usage Guidelines

NA

Example

Enable the IGMP snooping protocol globally.

```
Switch(config)#igmp-snooping start
Switch(config)#
```

7.1.29 igmp-snooping 8021p priority

Function

The **igmp-snooping 8021p priority** command set the 802.1p priority for the IGMP snooping protocol.

Format

igmp-snooping 8021p priority { value | default }**Parameter**

Parameter	Description	Value
value	Specifies a 802.1p priority.	The value is an integer ranging from 0 to 7.
default	Specifies the default priority.	-

Default Value

NA

View

MVLAN configuration view

Usage Guidelines

Before using this command, run the **igmp-snooping start** command in the global configuration view.

Example

Set the 802.1p priority to 5.

```
Switch(config-igmpsnoop-mvlan100)# igmp-snooping 8021p priority 5
```

```
Switch(config-igmpsnoop-mvlan100)#
```

7.1.30 igmp-snooping group-limit**Function**

The **igmp-snooping group-limit** command sets the maximum number of multicast groups on an interface.

The **igmp-snooping group-limit action** command sets the action when the number of multicast groups on an interface exceeds the limit.

Format

- **igmp-snooping group-limit** *group-limit-value*
- **igmp-snooping group-limit** *group-limit-value* **action** { **delay** | **replace** }
- **no igmp-snooping group-limit**

Parameter

Parameter	Description	Value
group-limit-value	Specifies the maximum number of multicast	The value is an integer ranging from

Parameter	Description	Value
	groups on an interface.	1 to 2048.
delay	Drops packets when the limit is exceeded.	-
replace	Replace	-

Default Value

NA

View

Interface configuration view (Trunk), Ethernet bridge interface configuration view, Ethernet routing interface configuration view

Usage Guidelines

Before running this command, you must enable the multicast snooping function using the `igmp-snooping {enable|disable}` command.

Example

Set the maximum number of multicast groups on the interface to 2.

```
Switch(config-10ge1/0/1)#igmp-snooping group-limit 2
Switch(config-10ge1/0/1)#
```

7.1.31 igmp-snooping static-group group-address mvlan

Function

The **igmp-snooping static-group group-address mvlan** command configures or deletes a static multicast group on an interface when no multicast service is running.

Format

- **igmp-snooping static-group group-address** *group-address* **mvlan** *vlan-id*
- **igmp-snooping static-group group-address** *group-address* **mvlan** *vlan-id* **user-vlan** *vlan-id*
- **igmp-snooping static-group group-address** *group-address* **source-address** *source-address* **mvlan** *vlan-id*
- **no igmp-snooping static-group**
- **no igmp-snooping static-group group-address** *group-address* **mvlan** *vlan-id*
- **no igmp-snooping static-group group-address** *group-address* **mvlan** *vlan-id* **user-vlan** *vlan-id*

- **no igmp-snooping static-group group-address** *group-address* **source-address** *source-address* **mvlan** *vlan-id*
- **no igmp-snooping static-group mvlan** *vlan-list*

Parameter

Parameter	Description	Value
group-address	Specifies a multicast IP address.	The value ranges from 224.0.0.0 to 239.255.255.255.
source-address	Specifies a source IP address.	The value is in dotted decimal notation.
vlan-id	Specifies a VLAN entry.	The value is an integer ranging from 1 to 4094.
vlan-list	Specifies a VLAN list.	The value is an integer ranging from 1 to 4094.

Default Value

NA

View

Interface configuration view (Trunk), Ethernet bridge interface configuration view, Ethernet routing interface configuration view

Usage Guidelines

NA

Example

Set a static multicast group on an interface.

```
Switch(config-10ge1/0/1)#igmp-snooping static-group group-address 224.0.0.1 mvlan 100
Switch(config-10ge1/0/1)#
```

7.1.32 igmp-snooping static-group group-address mvlan user-vlan

Function

The **igmp-snooping static-group group-address mvlan user-vlan** command configures static user VLANs for multicast replication.

The **no igmp-snooping static-group group-address mvlan user-vlan** command deletes specified or all static user VLANs for multicast replication.

Format

- **igmp-snooping static-group group-address** *group-address* **mvlan** *vlan-id* **user-vlan** *vlan-list*

- **no igmp-snooping static-group group-address group-address mvlan vlan-id user-vlan vlan-list**
- **no igmp-snooping static-group group-address group-address mvlan vlan-id user-vlan all**

Parameter

Parameter	Description	Value
group-address	Specifies a multicast IP address.	The value is in dotted decimal notation, for example, <i>A.B.C.D</i> , in which <i>A</i> to <i>D</i> are decimal digits ranging from 0 to 255.
vlan-id	Specifies a multicast VLAN to which the user wants to join.	The value is an integer ranging from 1 to 4094.
vlan-list	Specifies a list of static user VLANs.	The value is an integer ranging from 1 to 4094.

Default Value

NA

View

Interface configuration view (Trunk), Ethernet bridge interface configuration view, Ethernet routing interface configuration view

Usage Guidelines

NA

Example

Set a user static VLAN.

```
Switch(config-10ge1/0/1)#igmp-snooping static-group group-address 224.1.1.1 mvlan 100 user-vlan 1000
Switch(config-10ge1/0/1)#
```

7.1.33 igmp-snooping uplink-port

Function

The **igmp-snooping uplink-port** command sets an uplink interface for IGMP snooping.

The **no igmp-snooping uplink-port** command deletes an uplink interface for IGMP snooping.

Format

- **igmp-snooping uplink-port { ethernet | xgigaethernet | 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet } interface-number**

- **igmp-snooping uplink-port eth-trunk** *trunk-number*
- **no igmp-snooping uplink-port { ethernet | xgigaethernet | 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet }** *interface-number*
- **no igmp-snooping uplink-port eth-trunk** *trunk-number*

Parameter

Parameter	Description	Value
interface-number	Specifies the number of an Ethernet port.	The value is an integer in the range of <1-1>/<0-1>/<1-48> (For reference only. The specific value range depends on the slot number and card type).
trunk-number	Specifies the number of a Trunk interface.	The value is an integer ranging from 1 to 128.

Default Value

NA

View

MVLAN configuration view

Usage Guidelines

NA

Example

Set an uplink interface for IGMP snooping.

```
Switch(config-igmpsnoop-mvlan100)#igmp-snooping uplink-port xgigaethernet 1/0/1
Switch(config-igmpsnoop-mvlan100)#
```

7.1.34 igmp-snooping uplink-port drop-report**Function**

The **igmp-snooping uplink-port drop-report {enable|disable}** command enables or disables multicast entry learning prohibition on an uplink interface.

Format**igmp-snooping uplink-port drop-report {enable|disable }****Parameter**

Parameter	Description	Value
enable	Enables multicast entry learning	-

Parameter	Description	Value
	prohibition on an uplink interface.	
disable	Disables multicast entry learning prohibition on an uplink interface.	-

Default Value

NA

View

MVLAN configuration view

Usage Guidelines

NA

Example

Enable multicast entry learning prohibition on an uplink interface.

```
Switch(config-igmpsnoop-mvlan100)#igmp-snooping uplink-port drop-report enable
Switch(config-igmpsnoop-mvlan100)#
```

7.1.35 igmp-snooping uplink-port-limit

Function

The **igmp-snooping uplink-port-limit** command limits the uplink interface number.

Format

igmp-snooping uplink-port-limit { *uplink-port-limit* | **default** }

Parameter

Parameter	Description	Value
uplink-port-limit	Specifies the number of an uplink interface.	The value is an integer ranging from 1 to 256.
default	Specifies the default value.	1

Default Value

1

View

MVLAN configuration view

Usage Guidelines

NA

Example

Set the limit of uplink interface number to 100.

```
Switch(config-igmpsnoop-mvlan100)#igmp-snooping uplink-port-limit 100
Switch(config-igmpsnoop-mvlan100)#
```

7.1.36 igmp-snooping version

Function

The **igmp-snooping version** command sets the IGMP snooping version.

Format

igmp-snooping version { v1 | v2 | v3 }

Parameter

Parameter	Description	Value
v1	Indicates IGMP snooping version 1.	-
v2	Indicates IGMP snooping version 2.	-
v3	Indicates IGMP snooping version 3.	-

Default Value

The default multicast version is V2.

View

MVLAN configuration view

Usage Guidelines

When the version is V3, you must run the **igmp-snooping forwarding-mode ip** command first.

Example

Set the IGMP snooping version.

```
Switch(config-igmpsnoop-mvlan100)#igmp-snooping version v1
Switch(config-igmpsnoop-mvlan100)#
```

7.1.37 igmp-snooping workmode

Function

The **igmp-snooping workmode** command sets the IGMP snooping working mode.

Format

igmp-snooping workmode { igmp-snooping | igmp-proxy }

Parameter

Parameter	Description	Value
igmp-snooping	Indicates the IGMP-snooping mode.	-
igmp-proxy	Indicates the IGMP-proxy mode.	-

Default Value

NA

View

MVLAN configuration view

Usage Guidelines

NA

Example

Configure the IGMP snooping working mode.

```
Switch(config-igmpsnoop-mvlan100)#igmp-snooping workmode igmp-snooping
Switch(config-igmpsnoop-mvlan100)#
```

7.1.38 igmp-snooping drop**Function**

The **igmp-snooping drop** command configures the type of IGMP packet to be dropped on the interface

Format

- **igmp-snooping drop { report | query | both }**
- **no igmp-snooping drop**

Parameter

Parameter	Description	Value
Report	Indicates the IGMP snooping report mode.	-
query	Indicates the IGMP snooping query mode.	-

Default Value

NA

View

Interface configuration view (Trunk), Ethernet bridge interface configuration view, Ethernet routing interface configuration view

Usage Guidelines

Before running this command, you must enable IGMP snooping using the `igmp-snooping {enable|disable}` command.

Example

Configure to drop the IGMP packets of the report type on the interface.

```
Switch(config-10ge1/0/40)#igmp-snooping drop report
Switch(config-10ge1/0/40)#
```

7.1.39 reset igmp-snooping group**Function**

The **reset igmp-snooping group** command resets the dynamic multicast table for IGMP snooping.

Format

reset igmp-snooping group

Parameter

NA

Default Value

NA

View

Global configuration view

Usage Guidelines

NA

Example

Reset the dynamic multicast table for IGMP snooping.

```
Switch(config)#reset igmp-snooping group
Switch(config)#
```

7.1.40 reset igmp-snooping statistic

Function

The **reset igmp-snooping statistic** command clears IGMP-snooping statistics.

Format

reset igmp-snooping statistic

Parameter

NA

Default Value

NA

View

Global configuration view

Usage Guidelines

NA

Example

Clear IGMP-snooping statistics.

```
Switch(config)#igmp-snooping start
Switch(config)#reset igmp-snooping statistic
Switch(config)#
```

7.1.41 show igmp-snooping

Function

The **show igmp-snooping** command displays the global IGMP snooping configuration.

Format

show igmp-snooping

Parameter

NA

Default Value

NA

View

Common user view

Usage Guidelines

This command displays the following information: IGMP snooping status (enabled or disabled), number of query packets, global general query interval, global aging time, and line card synchronization status.

Example

Display global IGMP snooping configuration.

```
Switch>show igmp-snooping
  Version                      : IGMP Snooping_VB3.03.00.00
Switch>
```

7.1.42 show igmp-snooping config

Function

The **show igmp-snooping config** command displays the IGMP snooping configuration.

Format

show igmp-snooping config

Parameter

NA

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

View the IGMP snooping configuration.

```
Switch> show igmp-snooping config
  igmp-snooping start
  igmp-snooping mvlan 1

Interface ge-1/0/1
```

```

igmp-snooping enable
igmp-snooping mvlan 1 uplink-port
Switch>

```

7.1.43 show igmp-snooping egress-port

Function

The **show igmp-snooping egress-port** command displays the configuration of IGMP snooping egress interfaces.

Format

show igmp-snooping egress-port

Parameter

NA

Default Value

NA

View

Common user view

Usage Guidelines

This command displays the following information: group address of the outbound interface, multicast VLAN ID, interface type, and interface number.

Example

Display the configuration of IGMP snooping outbound interfaces.

```

Switch>show igmp-snooping egress-port
Total Entry(s) : 0

Switch>

```

7.1.44 show igmp-snooping egress-port interface

Function

The **show igmp-snooping egress-port interface** command displays the forwarding entries of an interface in static groups.

Format

- **show igmp-snooping egress-port interface { ethernet | xgigaethernet | 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet } interface-number**
- **show igmp-snooping egress-port interface eth-trunk trunk-number**

Parameter

Parameter	Description	Value
interface-number	Specifies an Ethernet interface number.	The value is an integer in the range of <1-1>/<0-1>/<1-48> (For reference only. The specific value range depends on the slot number and card type).
trunk-number	Specifies the number of a Trunk interface.	The value is an integer ranging from 1 to 128.

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

View the forwarding entries of an interface in static groups.

```
Switch>show igmp-snooping egress-port interface gigaethernet 1/01
Group Address : 225.1.1.1
MVlan: 100
Interface: ge-1/01
Type: static
Expires: 00:00:00
OutVlan: 5-10
Switch>
```

7.1.45 show igmp-snooping egress-port mvlan

Function

The **show igmp-snooping egress-port mvlan** command displays the forwarding entries of a multicast VLAN in static groups.

Format

show igmp-snooping egress-port mvlan mvlan-id

Parameter

Parameter	Description	Value
mvlan-id	Specify a multicast VLAN ID.	The value is an integer ranging from 1 to 4094.

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

Display the forwarding entries of multicast VLAN100 in static groups.

```
Switch>show igmp-snooping egress-port mvlan 100
Group Address: 225.1.1.1
MVlan: 100
Interface: ge-1/0/1
Type: static
Expires: 00:00:00
OutVlan: 5-10
Switch>
```

7.1.46 show igmp-snooping group**Function**

The **show igmp-snooping group** command displays configuration of a multicast group in IGMP snooping mode.

Format

show igmp-snooping group

Parameter

NA

Default Value

NA

View

Common user view

Usage Guidelines

This command displays the following information: group address, multicast VLAN ID, and member interfaces added to multicast groups.

Example

Display configuration of IGMP snooping groups.

```
Switch>show igmp-snooping group
      Total Entry(s) : 0
Switch>
```

7.1.47 show igmp-snooping interface**Function**

The **show igmp-snooping interface** command displays the configuration of a multicast interface in IGMP snooping mode.

Format

show igmp-snooping interface

Parameter

NA

Default Value

NA

View

Common user view

Usage Guidelines

This command displays the following information: multicast interface type, IGMP snooping information, fast leave function status, and controllable multicast information (ctrlmode).

Example

Display the configuration of IGMP snooping interfaces.

```
Switch>show igmp-snooping interface
      Interface      Igmp-Snooping  Fastleave
```



```

    ge-1/0/1      enable      disable
Switch>

```

7.1.48 show igmp-snooping mvlan

Function

The **show igmp-snooping mvlan** command displays IGMP snooping MVLAN configuration.

Format

show igmp-snooping mvlan

Parameter

NA

Default Value

NA

View

Common user view

Usage Guidelines

This command displays the following information: multicast VLAN working mode, multicast VLAN ID, IGMP snooping version, log proxy function status, and user VLANs.

Example

Display IGMP snooping MVLAN configuration.

```

Switch>show igmp-snooping mvlan
MVLAN : 1
  Work Mode : snooping
  Version : v2
  Report Suppress : disable
  Leave Suppress : disable
  Forwarding Mode : ip
  Max Response Time : 10
  Require Router Alert : disable
  Querier : disable
  Proxy Ip : 0.0.0.0
  Multicast Vlan : disable
  SSM Mapping : disable
  Lastmember Query Interval : 1
  Lastmember Query Number : 2

```

```
Switch>
```

7.1.49 show igmp-snooping source-address

Function

The **show igmp-snooping source-address** command displays the multicast source address configuration in IGMP snooping mode.

Format

show igmp-snooping source-address

Parameter

NA

Default Value

NA

View

Common user view

Usage Guidelines

This command displays the following information: multicast source address, multicast VLAN ID, interface type, and port type.

Example

Display configuration of IGMP snooping source addresses.

```
Switch>show igmp-snooping source-address
Total Entry(s) : 0
Switch>
```

7.1.50 show igmp-snooping uplinkport

Function

The **show igmp-snooping uplinkport** command displays the configuration of IGMP snooping uplink interfaces.

Format

show igmp-snooping uplinkport

Parameter

NA

Default Value

NA

View

Common user view

Usage Guidelines

This command displays the following information: uplink interfaces, multicast VLAN ID, and port type.

Example

Display the configuration of IGMP snooping uplink interfaces.

```
Switch> show igmp-snooping uplinkport
  Mvlan   UplinkPort   Expires   Type
  1        10ge-1/0/1   ---       static
Switch>
```

7.1.51 show igmp-snooping statistic**Function**

The **show igmp-snooping statistic** command displays the IGMP-snooping statistics.

Format

- **show igmp-snooping statistic**
- **show igmp-snooping statistic interface**
- **show igmp-snooping statistic interface { ethernet | xgigaethernet | 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet } interface-number**
- **show igmp-snooping statistic interface eth-trunk trunk-number**

Parameter

Parameter	Description	Value
interface-number	Specifies an Ethernet interface number.	The value is an integer in the range of <1-1>/<0-1>/<1-48> (For reference only. The specific value range depends on the slot number and card type).
trunk-number	Specifies the number of a	The value is an integer ranging from 1 to 128.

Parameter	Description	Value
	Trunk interface.	

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

Display the configuration of IGMP snooping uplink interfaces.

```

Switch>show igmp-snooping statistic
Receive packet number    : 0
Receive report v1 number: 0
Receive report v2 number: 0
Receive report v3 number: 0
Receive query number     : 0
Receive leave number     : 0

Send packet number       : 0
Send report v1 number    : 0
Send report v2 number    : 0
Send report v3 number    : 0
Send query number        : 0
Send leave number        : 0

Switch>

```

7.2 IGMP Configuration Commands

7.2.1 clear igmp-control config

FunctionThe **clear igmp-control config** command clears the controllable multicast configuration.**Format****clear igmp-control config****Parameter**

NA

Default Value

NA

View

Global configuration view

Usage Guidelines

NA

Example

Clear the controllable multicast configuration.

```
Switch(config)#clear igmp-control config
Switch(config)#
```

7.2.2 debug igmp

Function

The **debug igmp** command enables IGMP debugging.

The **no debug igmp** command disables IGMP debugging.

Format

- **debug igmp { send | receive | protocol | device | event | timer | all }**
- **debug igmp { send | receive | protocol | device | event | timer | all } vpn-instance *name***
- **no debug igmp { send | receive | protocol | device | event | timer | all }**
- **no debug igmp { send | receive | protocol | device | event | timer | all } vpn-instance *name***
- **no debug igmp vpn-instance**

Parameter

Parameter	Description	Value
send	Indicates debugging information about the sent IGMP packets.	-
receive	Indicates debugging information about the received IGMP packets.	-
protocol	Indicates debugging information about the IGMP protocol.	-
device	Indicates debugging information about the	-

Parameter	Description	Value
	IGMP devices.	
event	Indicates debugging information about the IGMP events.	
timer	Indicates debugging information about the IGMP timers.	-
all	Indicates all debugging information about the IGMP protocol.	-
name	Specifies a VPN instance name.	The value is a character string.

Default Value

By default, IGMP debugging is disabled.

View

Privileged user view

Usage Guidelines

You can use this command to view information about the IGMP process and IGMP packets sent and received. This command is used to maintain and debug the IGMP function of the switch.

Example

Enable IGMP debugging.

```
Switch#debug igmp all
Switch#
```

7.2.3 general-query

Function

The **general-query** command sets a specified VLAN interface or an Ethernet interface to send General Query messages.

Format

- **general-query** *vlan* *vlan-id*
- **general-query** { **ethernet** | **xgigaethernet** | **10gigaethernet** | **25gigaethernet** | **40gigaethernet** | **100gigaethernet** } *interface-number*

Parameter

Parameter	Description	Value
vlan-id	Specifies the VLAN in which General Query	The value is an integer ranging from 1

Parameter	Description	Value
	messages are sent.	to 4094.
interface-number	Specifies the ID of the Ethernet interface through which General Query messages are sent.	The value is an integer in the range of <1-1>/<0-1>/<1-48> (For reference only. The specific value range depends on the slot number and card type).

Default Value

By default, an interface does not send General Query messages.

View

IGMP configuration view, IGMP VPN configuration view

Usage Guidelines

You can run this command to set a VLAN interface to send General Query messages in the IGMP configuration view.

Example

Configure VLANIF 100 to send General Query messages.

```
Switch(config-igmp)#general-query vlan 100
Switch(config-igmp)#
```

7.2.4 igmp {enable|disable}

Function

The **igmp enable** command enables IGMP on an interface.

The **igmp disable** command disables IGMP on an interface.

Format

igmp { enable | disable }

Parameter

Parameter	Description	Value
enable	Enables IGMP on an interface.	-
disable	Disables IGMP on an interface.	-

Default Value

By default, IGMP is not enabled for the interface.

View

VLANIF configuration view, Ethernet routing interface configuration view

Usage Guidelines



Caution

When configuring IGMP in the VLANIF configuration view, make sure that the corresponding VLAN has been configured with an IP address. Otherwise, IGMP configuration fails.

Before enabling IGMP on an interface, enable IGMP in the instance to which the interface belongs. Otherwise, IGMP cannot be enabled on this interface.

Example

Enable IGMP on an interface.

```
Switch(config)#interface vlan 100
Switch(config-vlanif-100)#igmp enable
Switch(config-vlanif-100)#
```

7.2.5 igmp {start|stop}

Function

The **igmp {start|stop}** command enables or disables IGMP globally.

Format

igmp { start | stop }

Parameter

Parameter	Description	Value
start	Enables the IGMP function.	-
stop	Disables the IGMP function.	-

Default Value

By default, IGMP is disabled globally.

View

Global configuration view

Usage Guidelines

This command must be used before all the other IGMP configuration commands. Other configuration takes effect only after the IGMP is enabled globally.

Example

Enable or disable IGMP globally.

```
Switch(config)#igmp start
Switch(config)#

Switch(config)#igmp stop
Switch(config)#
```

7.2.6 igmp fast-leave**Function**

The **igmp fast-leave enable** command enables IGMP fast leave on an interface.

The **igmp fast-leave disable** command disables IGMP fast leave on an interface.

Format

igmp fast-leave { enable | disable }

Parameter

Parameter	Description	Value
enable	Enables IGMP fast leave on an interface.	-
disable	Disables IGMP fast leave on an interface.	-

Default Value

By default, IGMP fast leave is disabled on an interface.

View

VLANIF configuration view, Ethernet routing interface configuration view

Usage Guidelines

When a group member leaves the multicast group, the host sends an IGMP Leave packet. If IGMP fast leave is enabled on an interface, the switch will delete the multicast forwarding entry of the interface immediately after receiving an IGMP Leave packet. This function conserves bandwidth and system resources, and enables fast switching of service traffic.

After IGMP fast leave is disabled, the IGMP querier does not send a Leave packet to the upstream device after receiving an IGMP Leave packet from a host. Instead, it sends IGMP Group-Specific Query or Source-Specific Query packets.

Example

Enable IGMP fast leave on an interface.

```
Switch(config-vlanif-100)#igmp fast-leave enable
Switch(config-vlanif-100)#
```

7.2.7 igmp general-query

Function

The **igmp general-query** command configures an interface to send General Query messages.

Format

igmp general-query

Parameter

NA

Default Value

By default, an interface does not send General Query messages.

View

VLANIF configuration view, Ethernet routing interface configuration view

Usage Guidelines

This function has similar function as the **general-query vlan** command.

The IGMP querier periodically sends General Query messages to every connected subnet to determine whether any group members exist and check which subnets have no group member.

Example

Configure VLANIF 100 to send General Query messages.

```
Switch(config-vlanif-100)#igmp general-query
Switch(config-vlanif-100)#
```

7.2.8 igmp group-policy filter-list

Function

The **igmp group-policy filter-list** command configures an IGMP group filter on an interface to limit the range of multicast groups that the interface can join.

The **no igmp group-policy** command deletes the IGMP group filter on an interface.

Format

- **igmp group-policy filter-list *acl-number***
- **igmp group-policy filter-list *acl-number* **version** *version-list***
- **no igmp group-policy**

Parameter

Parameter	Description	Value
acl-number	Specifies an ACL number.	The value is an integer ranging from 1001 to 2000, indicating an IPv4 ACL.
version-list	1: Limits the scope of multicast groups for IGMPv1 hosts to join. 2: Limits the scope of multicast groups for IGMPv2 hosts to join. 3: Limits the scope of multicast groups for IGMPv3 hosts to join.	The value is an integer ranging from 1 to 3. The version list can be in a format similar to 1-3.

Default Value

By default, no filter is configured on an interface, and hosts can join any multicast groups.

View

VLANIF configuration view, Ethernet routing interface configuration view

Usage Guidelines

Before using this command, configure the ACL you want to reference to limit the range of multicast groups that hosts connected to the interface can join.

If you do not specify any IGMP version in the command, the ACL applies to IGMPv1, IGMPv2, and IGMPv3 hosts.

Example

Configure ACL 1001 to allow hosts to accept messages from multicast group 225.1.1.1. Configure a filter referencing this ACL on VLANIF 10 to specify that hosts connected to the interface can only join multicast group 225.1.1.1.

```
Switch(config)#filter-list 1001
Switch(configure-filter-ipv4-1001)#filter 1 ip 225.1.1.1/32 any
Switch(configure-filter-ipv4-1001)#filter 1 action permit
Switch(configure-filter-ipv4-1001)#quit
Switch(config)#interface vlan 10
Switch(config-vlanif-10)#igmp group-policy filter-list 1001
Switch(config-vlanif-10)#
```

7.2.9 igmp lastmember-queryinterval

Function

The **igmp lastmember-queryinterval** command sets the interval at which the IGMP querier sends Group-Specific Query packets after receiving an IGMP Leave packet from a host.

Format

igmp lastmember-queryinterval { *interval* | **default** }

Parameter

Parameter	Description	Value
interval	Specifies the interval at which the IGMP querier sends Group-Specific Query packets.	The value is an integer ranging from 1 to 5, in seconds.
default	Specifies the default value.	The value is dynamic and inherits the value of the igmp-snooping lastmember-queryinterval { <i>query-interval</i> default } command configured in the global configuration view.

Default Value

By default, the value is dynamic and inherits the value of the **igmp-snooping lastmember-queryinterval** { *query-interval* | **default** } command configured in the global configuration view.

View

VLANIF configuration view, Ethernet routing interface configuration view

Usage Guidelines

This command takes effect for an IGMP querier running IGMPv2 or IGMPv3. This command (valid only on the current interface) has the same function as the **lastmember-queryinterval** command in the IGMP view (globally valid for all interfaces), except for the scopes they take effect. The configuration in the interface view takes precedence over the global configuration. The configuration in the IGMP view takes effect only when no configuration is made in the interface view.

A shared network of hosts may be connected to multiple multicast switches. These switches perform an election, and the winner acts as the querier to maintain IGMP group memberships on interfaces. When the querier receives a Leave packet for a multicast group, it sends Group-Specific Query packets continuously to check whether this group has other members. If other members of the group exist on the network segment, the members must send Report packets within the maximum response

time. If the querier receives Report packets from hosts within the maximum response time, it continues maintaining the memberships of this group. Otherwise, the querier considers that the last member of the group has left and stops maintaining memberships of this group.

Example

Set the interval at which the IGMP querier sends Group-Specific Query packets to 2 seconds.

```
Switch(config-vlanif-100)#igmp lastmember-queryinterval 2
Switch(config-vlanif-100)#
```

7.2.10 igmp limit

Function

The **igmp limit** command sets the maximum number of IGMP group memberships on an interface.

Format

igmp limit *number*

Parameter

Parameter	Description	Value
number	Specifies the maximum number of IGMP entries on an interface.	The value is an integer ranging from 1 to 2048.
default	Specifies the default value.	The default value is dynamic and inherits the global configuration value.

Default Value

The default value is dynamic and inherits the global configuration value.

View

VLANIF configuration view, Ethernet routing interface configuration view

Usage Guidelines

The system no longer creates new IGMP entries when the number of existing IGMP entries reaches the configured limit. To add new multicast groups, delete unnecessary entries, change the limit value, or create static multicast groups.

Example

Set the maximum number of IGMP entries on VLANIF 100 to 200.

```
Switch(config-vlanif-100)#igmp limit 200
Switch(config-vlanif-100)#
```

7.2.11 igmp max-response-time

Function

The **igmp max-response-time** command sets the maximum response time of IGMP query packets on an interface.

Format

igmp max-response-time { *interval* | **default** }

Parameter

Parameter	Description	Value
interval	Specifies the maximum response time of IGMP query packets on an interface.	The value is an integer ranging from 1 to 25, in seconds.
default	Specifies the default value.	The value is dynamic and inherits the value of the igmp-snooping max-response-time { <i>max-response-time</i> default } command configured in the global configuration view.

Default Value

The value is dynamic and inherits the value of the **igmp-snooping query-interval** { *max-response-time* | **default** } command configured in the global configuration view.

View

VLANIF configuration view, Ethernet routing interface configuration view

Usage Guidelines

The maximum response time controls the deadline for hosts to send Membership Report Packets. It can enable host to rapidly respond to Query packets and avoid traffic congestion due to a large number of Report packets sent by many hosts simultaneously. The actual maximum response time of hosts to General Query packets is a value ranging from 0 to max-response-time.

This command (valid for the current interface only) and the **max-response-time** (valid for all interfaces) command have the same function but different applicable scope. The configuration in the interface view takes precedence over the global configuration. The configuration in the IGMP view takes effect only when no configuration is made in the interface view.

Example

Set the maximum response time of IGMP general query packets on an interface to 6s.

```
Switch(config-vlanif-100)#igmp max-response-time 6
Switch(config-vlanif-100)#
```

7.2.12 igmp require-router-alert

Function

The **igmp require-router-alert** command specifies that IGMP packets received on an interface must contain the Router-Alert option in packet headers.

The **no igmp require-router-alert** restores the default Router-Alert configuration.

Format

- **igmp require-router-alert**
- **no igmp require-router-alert**

Parameter

NA

Default Value

By default, the system does not check the Router-Alert option in IGMP packet headers on an interface. That is, the system processes all the received IGMP packets, including those not carrying the Router-Alert option.

View

VLANIF configuration view, Ethernet routing interface configuration view

Usage Guidelines

After you use this command to configure Router-Alert option check on an interface, received IGMP packets not carrying this option will be dropped on this interface. This command is applicable to IGMPv2 and IGMPv3.

This command (valid only on the current interface) has the same function as the **require-router-alert** command in the IGMP view (globally valid for all interfaces), except for the scopes they take effect. The configuration in the interface view takes precedence over the global configuration. The configuration in the IGMP view takes effect only when no configuration is made in the interface view.

Example

Configure VLANIF 100 to drop IGMP packets without the Router-Alert option.

```
Switch(config-vlanif-100)#igmp require-router-alert
Switch(config-vlanif-100)#
```

7.2.13 igmp robust-count

Function

The **igmp robust-count** command sets the IGMP querier robustness count on an interface.

Format

igmp robust-count { *robust* | **default** }

Parameter

Parameter	Description	Value
robust	Indicates the IGMP robustness variable, which is a message retransmission count to prevent the risk of network packet loss.	The value is an integer ranging from 2 to 7.
default	Specifies the default value.	The value is dynamic and inherits the value of the igmp-snooping robust-count { <i>robust-count</i> default } command configured in the global configuration view.

Default Value

The value is dynamic and inherits the value of the **igmp-snooping query-interval** { *robust-count* | **default** } command configured in the global configuration view.

View

VLANIF configuration view, Ethernet routing interface configuration view

Usage Guidelines

The IGMP querier maintains IGMP group memberships on interfaces. The robustness count affects the timeout duration of group memberships.

The group membership timeout duration is calculated using the following formula: Group membership timeout duration = IGMP general query interval x Robustness count + Maximum response time.

This command (valid only on the current interface) has the same function as the **send-router-alert** command in the IGMP view (globally valid for all interfaces), except for the scopes they take effect. The configuration in the interface view takes precedence over the global configuration. The configuration in the IGMP view takes effect only when no configuration is made in the interface view.

Example

Set the robustness count of the IGMP querier to 4 on VLANIF 100.

```
Switch(config-vlanif-100)#igmp robust-count 4
Switch(config-vlanif-100)#
```

7.2.14 igmp send-router-alert

Function

The **igmp send-router-alert** command configures an interface to send IGMP packets carrying the Router-Alert option.

The **no igmp send-router-alert** command configures an interface to send IGMP packets without the Router-Alert option.

Format

- **igmp send-router-alert**
- **no igmp send-router-alert**

Parameter

NA

Default Value

By default, IGMP packets sent from an interface carry the Router-Alert option in IP packet headers.

View

VLANIF configuration view, Ethernet routing interface configuration view

Usage Guidelines

This command (valid only on the current interface) has the same function as the **send-router-alert** command in the IGMP view (globally valid for all interfaces), except for the scopes they take effect. The configuration in the interface view takes precedence over the global configuration. The configuration in the IGMP view takes effect only when no configuration is made in the interface view.

Example

Configure VLANIF 100 to send IGMP packets carrying the Router-Alert option.

```
Switch(config-vlanif-100)#igmp send-router-alert
Switch(config-vlanif-100)#
```

7.2.15 igmp static-group egress-port

Function

The **igmp static-group egress-port** command creates an IGMP static multicast group on an interface and specifies the outbound interface.

The **no igmp static-group egress-port** command deletes the created IGMP static multicast group and specified outbound interface.

Format

- **igmp static-group** *group-address* **egress-port** { **ethernet** | **xgigaethernet** | **10gigaethernet** | **25gigaethernet** | **40gigaethernet** | **100gigaethernet** } *interface-number*
- **igmp static-group** *group-address* **egress-port** **eth-trunk** *trunk-number*
- **no igmp static-group** *group-address* **egress-port** { **ethernet** | **xgigaethernet** | **10gigaethernet** | **25gigaethernet** | **40gigaethernet** | **100gigaethernet** } *interface-number*
- **no igmp static-group** *group-address* **egress-port** **eth-trunk** *trunk-number*

Parameter

Parameter	Description	Value
group-address	Specifies a multicast group address.	The value is in decimal notation, ranging from 224.0.0.0 to 239.255.255.255.
interface-number	Specifies an Ethernet interface number.	The value is an integer in the range of <1-1>/<0-1>/<1-48> (For reference only. The specific value range depends on the slot number and card type).
trunk-number	Indicates the egress port that forwards multicast data.	The value is an integer ranging from 1 to 128.

Default Value

By default, no static multicast group is created on a port.

View

VLANIF configuration view, Ethernet routing interface configuration view

Usage Guidelines

After you use this command to create a static multicast group on a port, the IGMP entry created on the switch does not have a timer. Therefore, the switch considers that the port is always connected to group member hosts and continuously forwards multicast packets matching specified conditions to

the network segment of the port. If you do not want the switch to forward multicast data to receiver hosts connected to the port, you must manually delete the static multicast group.

Example

Create a static multicast group 224.1.1.1 on the interface VLANIF100 and specify the outbound interface to gigabitEthernet1/0/1.

```
Switch(config-vlanif-100)#igmp static-group 224.1.1.1 egress-port gigabitEthernet 1/0/1
Switch(config-vlanif-100)#
```

7.2.16 igmp static-group source egress-port

Function

The **igmp static-group source egress-port** command creates a static IGMP group and specifies the matching multicast source address and outbound interface on a port.

The **no igmp static-group source egress-port** command deletes a static IGMP group and the matching multicast source address and outbound interface on a port.

Format

- **igmp static-group** *group-address* **source** *source-address* **egress-port** { **ethernet** | **xgigabitEthernet** | **10gigabitEthernet** | **25gigabitEthernet** | **40gigabitEthernet** | **100gigabitEthernet** } *interface-number*
- **igmp static-group** *group-address* **source** *source-address* **egress-port eth-trunk** *trunk-number*
- **no igmp static-group** *group-address* **source** *source-address* **egress-port** { **ethernet** | **xgigabitEthernet** | **10gigabitEthernet** | **25gigabitEthernet** | **40gigabitEthernet** | **100gigabitEthernet** } *interface-number*
- **no igmp static-group** *group-address* **source** *source-address* **egress-port eth-trunk** *trunk-number*

Parameter

Parameter	Description	Value
group-address	Specifies a multicast group address.	The value is in decimal notation, ranging from 224.0.0.0 to 239.255.255.255.
source-address	Specifies a multicast source address.	The value is in dotted decimal notation.
interface-number	Specifies an outbound interface ID.	The value is an integer in the range of <1-1>/<0-1>/<1-48> (For reference only. The specific value range depends on the slot number)

Parameter	Description	Value
		and card type).
trunk-number	Specifies a trunk number.	The value is an integer ranging from 1 to 128.

Default Value

By default, no static multicast group is created on a port.

View

VLANIF configuration view, Ethernet routing interface configuration view

Usage Guidelines

After you use this command to create a static multicast group on a port, the IGMP entry created on the switch does not have a timer. Therefore, the switch considers that the port is always connected to group member hosts and continuously forwards multicast packets matching specified conditions to the network segment of the port. If you do not want the switch to forward multicast data to receiver hosts connected to the interface, you must manually delete the static multicast group.

Example

Create static multicast group 224.1.1.1 and specify multicast source 10.18.11.1 and outbound interface gigabitEthernet1/0/1 on VLANIF 100.

```
Switch(config-vlanif-100)#igmp static-group 224.1.1.1 source 10.18.11.1 egress-port gigabitEthernet 1/0/1
Switch(config-vlanif-100)#
```

7.2.17 igmp static-group source

Function

The **igmp static-group source** command creates a static IGMP group and specifies a matching multicast source address on a port.

The **no igmp static-group source** command deletes a static IGMP group and the matching multicast source address on a port.

Format

- **igmp static-group** *group-address* **source** *source-address*
- **no igmp static-group** *group-address* **source** *source-address*

Parameter

Parameter	Description	Value
group-address	Specifies a multicast group address.	The value is in decimal notation, ranging

Parameter	Description	Value
		from 224.0.0.0 to 239.255.255.255.
source-address	Specifies a multicast source address.	The value is in dotted decimal notation.

Default Value

By default, no static multicast group is created on a port.

View

VLANIF configuration view, Ethernet routing interface configuration view

Usage Guidelines

After you use this command to create a static multicast group on a port, the IGMP entry created on the switch does not have a timer. Therefore, the switch considers that the port is always connected to group member hosts and continuously forwards multicast packets matching specified conditions to the network segment of the port. If you do not want the switch to forward multicast data to receiver hosts connected to the interface, you must manually delete the static multicast group.

Example

Create static multicast group 224.1.1.1 and specify multicast source 10.18.11.1 on VLANIF 100.

```
Switch(config-vlanif-100)#igmp static-group 224.1.1.1 source 10.18.11.1
Switch(config-vlanif-100)#
```

7.2.18 igmp static-group

Function

The **igmp static-group** command creates a static IGMP group on a port.

The **no igmp static-group** deletes a static IGMP group on a port.

Format

- **igmp static-group** *group-address*
- **no igmp static-group** *group-address*

Parameter

Parameter	Description	Value
group-address	Specifies a multicast group address.	The value is in decimal notation, ranging from 224.0.0.0 to 239.255.255.255.

Default Value

By default, no static multicast group is created on a port.

View

VLANIF configuration view, Ethernet routing interface configuration view

Usage Guidelines

After you use this command to create a static multicast group on a port, the IGMP entry created on the switch does not have a timer. Therefore, the switch considers that the port is always connected to group member hosts and continuously forwards multicast packets matching specified conditions to the network segment of the port. If you do not want the switch to forward multicast data to receiver hosts connected to the interface, you must manually delete the static multicast group.

Example

Create static multicast group 224.1.1.1 on VLANIF 100.

```
Switch(config-vlanif-100)#igmp static-group 224.1.1.1
Switch(config-vlanif-100)#
```

7.2.19 igmp timer other-querier-present

Function

The **igmp timer other-querier-present** command sets the IGMP other querier present timer on an interface.

Format

igmp timer other-querier-present { *interval* | **default** }

Parameter

Parameter	Description	Value
interval	Specifies the other IGMP querier present timer value.	The value is an integer ranging from 10 to 65535, in seconds.
default	Specifies the default value.	The value is dynamic and inherits the value of the igmp-snooping query-interval { <i>query-interval</i> default } command configured in the global configuration view.

Default Value

The value is dynamic and inherits the value of the **igmp-snooping query-interval** { *query-interval* | **default** } command configured in the global configuration view.

View

VLANIF configuration view, Ethernet routing interface configuration view

Usage Guidelines

The querier present timer value is calculated using the following formula: IGMP other querier present timer = Robustness count x IGMP general query interval + 1/2 x Maximum response time for Query packets. If the robustness count, IGMP general query interval, and maximum response time all retain the default values, the IGMP other querier present timer is 255 seconds (default value).

This command is applicable to IGMPv2 and IGMPv3. This command (valid for the current interface only) and the **timer other-querier-present** (valid for all interfaces) command have the same function but different applicable scope. The configuration in the interface view takes precedence over the global configuration. The configuration in the IGMP view takes effect only when no configuration is made in the interface view.

**Caution**

If the other IGMP querier present timer value is smaller than the general query interval, the querier on the network will change frequently on the network. Therefore, set an appropriate value for the timer.

Example

Set the querier present timer to 100 seconds on VLANIF 100.

```
Switch(config-vlanif-100)#igmp timer other-querier-present 100
Switch(config-vlanif-100)#
```

7.2.20 igmp timer query**Function**

The **igmp timer query** command sets the sending interval of IGMP general group query messages on an interface.

Format

igmp timer query { *interval* | **default** }

Parameter

Parameter	Description	Value
interval	Specifies the sending interval of IGMP general group query messages on a device.	The value is an integer ranging from 2 to 10000, in seconds.
default	Specifies the default value.	125 seconds

Default Value

By default, the sending interval of IGMP general group query messages on an interface is 125s.

View

VLANIF configuration view, Ethernet routing interface configuration view

Usage Guidelines

This command (valid for the current interface only) and the **timer query** (valid for all interfaces) command have the same function but different applicable scope. The configuration in the interface view takes precedence over the global configuration. The configuration in the IGMP view takes effect only when no configuration is made in the interface view.

Example

Set the sending interval of IGMP general group query messages on the interface VLANIF100 to 100s.

```
Switch(config-vlanif-100)#igmp timer query 100
Switch(config-vlanif-100)#
```

7.2.21 igmp version**Function**

The **igmp version** command configures the IGMP version running on an interface.

Format

igmp version { v1 | v2 | v3 | default }

Parameter

Parameter	Description	Value
v1	Indicates IGMPv1.	-
v2	Indicates IGMPv2.	-
v3	Indicates IGMPv3.	-
default	Specifies the default value.	IGMPv2

Default Value

By default, an interface runs IGMPv2.

View

VLANIF configuration view, Ethernet routing interface configuration view

Usage Guidelines

All device interfaces in the same subnet must run the same IGMP version and cannot automatically switch between different IGMP versions.

Example

Set the IGMP version on VLANIF 100 to IGMPv1.

```
Switch(config-vlanif-100)#igmp version v1
Switch(config-vlanif-100)#
```

7.2.22 igmp

Function

The **igmp** command creates the IGMP public network instance.

The **no igmp** command deletes the IGMP public network instance.

The **igmp vpn-instance** command creates an IGMP VPN instance.

The **no igmp vpn-instance** command deletes an IGMP VPN instance.

Format

- **igmp**
- **igmp vpn-instance** *name*
- **no igmp**
- **no igmp vpn-instance** *name*

Parameter

Parameter	Description	Value
name	Specifies a VPN instance name.	The value is a string of up to 30 characters.

Default Value

NA

View

Global configuration view

Usage Guidelines

NA

Example

Create the IGMP public network instance.

```
Switch(config)#igmp
Switch(config-igmp)#
```

7.2.23 lastmember-queryinterval

Function

The **lastmember-queryinterval** command sets the global interval at which the IGMP querier sends Group-Specific Query packets after receiving an IGMP Leave packet from a host.

Format

lastmember-queryinterval { *interval* | **default** }

Parameter

Parameter	Description	Value
interval	Specifies the global interval at which the IGMP querier sends Group-Specific Query packets after receiving an IGMP Leave packet from a host.	The value is an integer ranging from 1 to 5, in seconds.
default	Specifies the default value.	1 seconds

Default Value

By default, the IGMP querier sends Group-Specific Query packets at intervals of 1 second.

View

IGMP configuration view

Usage Guidelines

This command is globally valid for all interfaces. It has the same function in the VLANIF configuration command and Ethernet routing interface configuration view (valid only on the current interface), except for the scopes they take effect. The configuration in the interface view takes precedence over the global configuration. The configuration in the IGMP view takes effect only when no configuration is made in the interface view.

This command takes effect only in the instance scope. Instance configurations are inherited when the interface of this instance is created.

Example

In the IGMP configuration view, set the interval at which the IGMP querier sends Group-Specific Query packets to 2 seconds.

```
Switch(config-igmp)#lastmember-queryinterval 2
Switch(config-igmp)#
```

7.2.24 igmp max-response-time

Function

The **igmp max-response-time** command sets the maximum response time of IGMP query packets on an interface.

Format

igmp max-response-time { *interval* | **default** }

Parameter

Parameter	Description	Value
interval	Specifies the maximum response time of IGMP query packets on an interface.	The value is an integer ranging from 1 to 25, in seconds.
default	Specifies the default value.	The default value is dynamic and inherits the global configuration value.

Default Value

By default, the maximum response time of IGMP query packets is dynamic and inherits the global configuration.

View

IGMP configuration view

Usage Guidelines

The maximum response time controls the deadline for hosts to send Membership Report Packets. It can enable host to rapidly respond to Query packets and avoid traffic congestion due to a large number of Report packets sent by many hosts simultaneously. The actual maximum response time of hosts to General Query packets is a value ranging from 0 to max-response-time.

The configuration in the interface view takes precedence over the global configuration. The configuration in the IGMP view takes effect only when no configuration is made in the interface view.

Example

Set the maximum response time of IGMP general query packets on an interface to 6s.

```
Switch(config-vlanif-100)#igmp max-response-time 6
Switch(config-vlanif-100)#
```

7.2.25 limit

Function

The **limit** command sets the maximum number of IGMP entries that can be created in the system.

Format

limit { *number* | **default** }

Parameter

Parameter	Description	Value
number	Specifies the maximum number of IGMP entries that can be created in the system.	The value is an integer ranging from 1 to 1024.
default	Specifies the default value.	1024

Default Value

By default, a maximum of 1024 IGMP entries can be created in the system.

View

IGMP configuration view

Usage Guidelines

The system no longer creates new IGMP entries when the number of existing IGMP entries reaches the configured limit. To add new multicast groups, delete unnecessary entries, change the limit value, or create static multicast groups.

This command takes effect only in the instance scope. Instance configurations are inherited when the interface of this instance is created.

Example

Set the maximum number of IGMP entries can be created in the system to 1000.

```
Switch(config-igmp)#limit 1000
```

```
Switch(config-igmp)#
```

7.2.26 max-response-time

Function

The **max-response-time** command sets the maximum response time for IGMP Query packets.

Format

max-response-time { *interval* | **default** }

Parameter

Parameter	Description	Value
interval	Specifies the maximum response time of IGMP query packets on an interface.	The value is an integer ranging from 1 to 25, in seconds.
default	Specifies the default value.	10 seconds

Default Value

By default, the maximum response time for IGMP Query packets is 10 seconds.

View

IGMP configuration view, IGMP VPN instance configuration view

Usage Guidelines

This command (valid for all interfaces) and the **igmp max-response-time** (valid for the current interface only) command in the VLANIF configuration view have the same function but different applicable scope. The configuration in the interface view takes precedence over the global configuration. The configuration in the IGMP view takes effect only when no configuration is made in the interface view.

Example

Set the maximum response time for IGMP Query packets to 15 seconds.

```
Switch(config-igmp)#max-response-time 15
Switch(config-igmp)#
```

7.2.27 no igmp group

Function

The **no igmp group** command deletes a specified VLAN interface or the dynamic IGMP entry of the specified group address on the specified Ethernet interface.

The **no igmp group all** command deletes all dynamic IGMP entries.

The **no igmp group source** command deletes a specified VLAN interface of the multicast source in the dynamic IGMP entry with the specified group on a specified Ethernet interface.

Format

- **no igmp group { ethernet | xgigaethernet | 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet } interface-number**
- **no igmp group { ethernet | xgigaethernet | 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet } interface-number group-address**
- **no igmp group { ethernet | xgigaethernet | 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet } interface-number group-address source source-address**
- **no igmp group { ethernet | xgigaethernet | 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet } interface-number group-address source source-address egress-port { ethernet | xgigaethernet | 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet } interface-number**
- **no igmp group { ethernet | xgigaethernet | 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet } interface-number group-address source source-address egress-port all**
- **no igmp group { ethernet | xgigaethernet | 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet } interface-number group-address source all**
- **no igmp group vlan vlan-id**
- **no igmp group vlan vlan-id group-address**
- **no igmp group vlan vlan-id group-address source source-address**
- **no igmp group vlan vlan-id group-address source source-address egress-port { ethernet | xgigaethernet | 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet } interface-number**
- **no igmp group vlan vlan-id group-address source source-address egress-port all**
- **no igmp group vlan vlan-id group-address source source-address egress-port eth-trunk trunk-number**
- **no igmp group vlan vlan-id group-address source all**
- **no igmp group all**

Parameter

Parameter	Description	Value
vlan-id	Specifies the ID of the VLAN to which dynamic IGMP entries belong.	The value is an integer ranging from 1 to 4094.
group-address	Specifies the group address in a dynamic IGMP entry.	The value is in decimal notation, ranging from 224.0.0.0 to 239.255.255.255.
all	Deletes all multicast sources in dynamic IGMP entries of a multicast group.	-
source-address	Specifies a multicast source address.	The value is in dotted decimal notation.
interface-number	Specifies the ID of the Ethernet interface through which General Query messages are sent.	The value is an integer in the range of <1-1>/<0-1>/<1-48> (For reference only. The specific value range depends on the slot number and card type).
trunk-number	Specifies the number of a Trunk interface.	The value is an integer ranging from 1 to 128.

Default Value

NA

View

IGMP configuration view, IGMP VPN configuration view

Usage Guidelines

This command deletes only dynamic IGMP entries and does not take effect on multicast groups.

Example

Set the multicast source 10.18.2.12 in the dynamic IGMP entry with the specified group 225.1.1.0 on the VLANIF100 interface .

```
Switch(config-igmp)#no igmp group vlan 100 255.1.1.0 source 10.18.2.12
Switch(config-igmp)#
```

Set all dynamic IGMP entries.

```
Switch(config-igmp)#no igmp group vlan 100
Switch(config-igmp)#
```

7.2.28 require-router-alert

Function

The **require-router-alert** command specifies that IGMP packets received in the system must contain the Router-Alert option in packet headers.

The **no require-router-alert** restores the default Router-Alert configuration.

Format

- **require-router-alert**
- **no require-router-alert**

Parameter

NA

Default Value

By default, the system does not check the Router-Alert option in IGMP packet headers. That is, the system processes all the received IGMP packets, including those not carrying the Router-Alert option.

View

IGMP configuration view

Usage Guidelines

After you use this command to configure Router-Alert option check, received IGMP packets not carrying this option will be dropped. This command is applicable to IGMPv2 and IGMPv3.

This command (valid for all commands) has the same function as the command in the VLANIF configuration command and Ethernet routing interface configuration view (valid only on the current interface), except for the scopes they take effect. The configuration in the interface view takes precedence over the global configuration. The configuration in the IGMP view takes effect only when no configuration is made in the interface view.

This command takes effect only in the instance scope. Instance configurations are inherited when the interface of this instance is created.

Example

Specify that IGMP packets received in the system must contain the Router-Alert option in packet headers globally.

```
Switch(config-igmp)#require-router-alert
Switch(config-igmp)#
```

7.2.29 send-router-alert**Function**

The **send-router-alert** command configures the system to send IGMP packets carrying the Router-Alert option in packet headers.

The **no send-router-alert** command configures the system to send IGMP packets without the Router-Alert option in packet headers.

Format

- **send-router-alert**
- **no send-router-alert**

Parameter

NA

Default Value

By default, IGMP packets sent from the switch carry the Router-Alert option in IP packet headers.

View

IGMP configuration view

Usage Guidelines

This command is usually used together with the **require-router-alert** command.

This command (valid for all commands) has the same function as the command in the VLANIF configuration command and Ethernet routing interface configuration view (valid only on the current interface), except for the scopes they take effect. The configuration in the interface view takes precedence over the global configuration. The configuration in the IGMP view takes effect only when no configuration is made in the interface view.

This command takes effect only in the instance scope. Instance configurations are inherited when the interface of this instance is created.

Example

Specify that IGMP packets sent by the system must contain the Router-Alert option in packet headers globally.

```
Switch(config-igmp)#send-router-alert
Switch(config-igmp)#
```

7.2.30 robust-count

Function

The **robust-count** command sets the global IGMP querier robustness count.

Format

robust-count { *robust* | **default** }

Parameter

Parameter	Description	Value
robust	Indicates the IGMP robustness variable, which is a message retransmission count to prevent the risk of network packet loss.	The value is an integer ranging from 2 to 7.
default	Specifies the default value.	2

Default Value

By default, the robustness count of the IGMP querier is 2.

View

IGMP configuration view

Usage Guidelines

The IGMP querier robustness count is used to set the following parameters:

- Number of times the querier sends General Query packets upon startup
- Number of times the querier sends Group-Specific packets after receiving a Leave packet.

This command (valid for all commands) has the same function as the command in the VLANIF configuration command and Ethernet routing interface configuration view (valid only on the current interface), except for the scopes they take effect. The configuration in the interface view takes precedence over the global configuration. The configuration in the IGMP view takes effect only when no configuration is made in the interface view.

This command takes effect only in the instance scope. Instance configurations are inherited when the interface of this instance is created.

Example

Set the global IGMP querier robustness count to 4.

```
Switch(config-igmp)#robust-count 4
Switch(config-igmp)#
```

7.2.31 show igmp config

Function

The **show igmp config** command displays the IGMP configuration.

Format

show igmp config**Parameter**

NA

Default Value

NA

View

Common user view

Usage Guidelines

You can use this command to check IGMP configuration information, including whether IGMP is enabled globally, configuration of **require-route-alert**, **send-route-alert**, and **timer query**, and IGMP configuration on VLAN interfaces.

Example

Display IGMP configuration on the switch.

```
Switch>show igmp config
!
!Igmp Configuration
  igmp start

!Interface configuration
  VID:100
  igmp enable
  igmp version v1
  igmp max-response-time 100
  igmp timer other-querier-present 100
  igmp fast-leave enable
  igmp require-router-alert
  igmp limit 100
  igmp static-group 1.1.1.1
  igmp static-group 1.1.1.1 egress-port xgigaethernet 1/0/1

Switch>
```

7.2.32 show igmp egress-port**Function**

The **show igmp egress-port** command displays information about outbound interfaces in IGMP entries.

Format

- **show igmp egress-port**
- **show igmp egress-port { static | dynamic | all }**
- **show igmp egress-port { static | dynamic | all } { ethernet | xgigaethernet | 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet } interface-number**
- **show igmp egress-port { static | dynamic | all } { ethernet | xgigaethernet | 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet } interface-number group group-address**
- **show igmp egress-port { static | dynamic | all } { ethernet | xgigaethernet | 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet } interface-number group group-address source source-address**
- **show igmp egress-port { static | dynamic | all } vlan vlan-id**
- **show igmp egress-port { static | dynamic | all } vlan vlan-id group group-address**
- **show igmp egress-port { static | dynamic | all } vlan vlan-id group group-address source source-address**

Parameter

Parameter	Description	Value
vlan-id	Specifies a VLAN ID.	The value is an integer ranging from 1 to 4094.
group-address	Specifies a multicast group address.	The value is in decimal notation, ranging from 224.0.0.0 to 239.255.255.255.
source-address	Specifies a multicast source address.	The value is in dotted decimal notation.
interface-number	Specifies the ID of the Ethernet interface through which General Query messages are sent.	The value is an integer in the range of <1-1>/<0-1>/<1-48> (For reference only. The specific value range depends on the slot number and card type).
static	Displays information about static multicast groups only.	-
dynamic	Displays information about dynamic multicast groups only.	-
all	Displays information about all multicast groups.	-

Default Value

NA

View

Common user view

Usage Guidelines

You can use this command to view information about outbound interfaces in IGMP entries, including the VLAN ID, group address, multicast source address, outbound interface number, and type (static or dynamic).

Example

Display information about outbound interfaces in IGMP entries.

```
Switch>show igmp egress-port all
Switch>
```

7.2.33 show igmp group**Function**

The **show igmp group** command displays the IGMP group information.

Format

- **show igmp group** { **static** | **dynamic** | **all** } { **ethernet** | **xgigaethernet** | **10gigaethernet** | **25gigaethernet** | **40gigaethernet** | **100gigaethernet** } *interface-number*
- **show igmp group** { **static** | **dynamic** | **all** } [**vlan** *vlan-id*]
- **show igmp group**

Parameter

Parameter	Description	Value
vlan-id	Specifies a VLAN ID.	The value is an integer ranging from 1 to 4094.
interface-number	Specifies the ID of the Ethernet interface through which General Query messages are sent.	The value is an integer in the range of <1-1>/<0-1>/<1-48> (For reference only. The specific value range depends on the slot number and card type).
static	Displays information about static multicast groups.	-
dynamic	Displays information about dynamic multicast groups.	-
all	Displays information about all	-

Parameter	Description	Value
	multicast groups.	

Default Value

NA

View

Common user view

Usage Guidelines

You can run this command to display the IGMP information, including the VLAN ID, group address, address of the member last sending the report information, and update time.

Example

View the IGMP group information.

```
Switch>show igmp group all
VLAN ID is:100
  Group Address:1.1.1.1
  Last reporter address:0.0.0.0
  Uptime:695 s
  Expiry Time:5 s
  Exclude mode expiry time:0 s
  V1 Host Timer:0 s
  V2 Host Timer:0 s
  Filter mode:include
  Group status:static
Switch>
```

7.2.34 show igmp interface

Function

The **show igmp interface** command displays IGMP information on a specified interface.

Format

- **show igmp interface**
- **show igmp interface vlan** *vlan-id*
- **show igmp interface { ethernet | xgigaethernet | 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet } interface-number**

- **show igmp interface { ethernet | xgigaethernet | 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet } interface-number.subinterface**

Parameter

Parameter	Description	Value
vlan-id	Specifies a VLAN ID.	The value is an integer ranging from 1 to 4094.
interface-number	Specifies the ID of the Ethernet interface through which General Query messages are sent.	The value is an integer in the range of <1-1>/<0-1>/<1-48> (For reference only. The specific value range depends on the slot number and card type).
subinterface	Specifies a sub-interface number.	The value is an integer ranging from 1 to 4094.

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

View information on the port gigaethernet1/0/1.

Switch>show igmp interface				
VID	Querier-address	Version	Fast-leave	Querier-remain
100	1.1.1.1	v1	enable	101
Switch>				

Display IGMP information on VLANIF 100.

Switch> show igmp interface vlan 100				
show igmp interface vlan 100				
Interface vlan100				
IGMP VPN Instance: Public				
Switch>				

7.2.35 show igmp source**Function**The **show igmp source** command displays IGMP multicast source information.**Format**

- **show igmp source**
- **show igmp source { static | dynamic | all }**
- **show igmp source { static | dynamic | all } vlan *vlan-id***
- **show igmp source { static | dynamic | all } vlan *vlan-id* group *group-address***
- **show igmp source { static | dynamic | all } { ethernet | xgigaethernet | 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet } *interface-number* group *group-address***
- **show igmp source { static | dynamic | all } { ethernet | xgigaethernet | 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet } *interface-number***

Parameter

Parameter	Description	Value
vlan-id	Specifies a VLAN ID.	The value is an integer ranging from 1 to 4094.
group-address	Specifies a multicast group address.	The value is in decimal notation, ranging from 224.0.0.0 to 239.255.255.255.
interface-number	Specifies the ID of the Ethernet interface through which General Query messages are sent.	The value is an integer in the range of <1-1>/<0-1>/<1-48> (For reference only. The specific value range depends on the slot number and card type).
static	Displays information about static multicast groups.	-
dynamic	Displays information about dynamic multicast groups.	-
all	Displays information about all multicast groups.	-

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

Display the multicast source matching group 225.1.1.1 on VLANIF 100.

```
Switch>show igmp source all
```


VID	Group-Address	Source-Address	Expiry-Time	Mode	Ingress-Port	Status
100	1.1.1.1	0.0.0.0	0	include Outband		static
Switch>						

7.2.36 show igmp vpn-instance

Function

The **show igmp vpn-instance** command displays IGMP information in a VPN instance.

Format

- **show igmp vpn-instance**
- **show igmp vpn-instance** *name*

Parameter

Parameter	Description	Value
name	Specifies a VPN instance name.	The value is a string of up to 64 characters.

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

Display IGMP information in VPN instance 1.

Switch>show igmp vpn-instance 1
IGMP VPN Instance: 1
Require-router-alert: disable
Send-router-alert: enable
Timer Query: 125 s
Robust-count: 2
Max Response Time: 10 s
Timer Other Querier Present: 255 s
Last Member Query Interval: 1 s
Limit: 2048
Current Interface Number: 0

```

Current Group Number: 0
Current Source Number: 0
Current Egress Number: 0
Switch>

```

7.2.37 show igmp

Function

The **show igmp** command displays global IGMP resource information.

Format

show igmp

Parameter

NA

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

Display global IGMP resource information.

```

Switch>show igmp
Version           :IGMP_VB3.00.00.00
Switch>s

```

7.2.38 timer other-querier-present

Function

The **timer other-querier-present** command sets the global IGMP other querier present timer.

Format

timer other-querier-present { *interval* | **default** }

Parameter

Parameter	Description	Value
interval	Specifies the other IGMP querier present timer value.	The value is an integer ranging from 10 to 65535, in seconds.
default	Specifies the default value.	255 seconds

Default Value

By default, the querier present timer is 255 seconds.

View

IGMP configuration view

Usage Guidelines

The querier present timer value is calculated using the following formula: IGMP other querier present timer = Robustness count x IGMP general query interval + 1/2 x Maximum response time for Query packets. If the robustness count, IGMP general query interval, and maximum response time all retain the default values, the IGMP other querier present timer is 255 seconds (default value).

This command is applicable to IGMPv2 and IGMPv3. This command (valid for all commands) has the same function as the **igmp timer other-querier-present** command in the VLANIF configuration command and Ethernet routing interface configuration view (valid only on the current interface), except for the scopes they take effect. The configuration in the interface view takes precedence over the global configuration. The configuration in the IGMP view takes effect only when no configuration is made in the interface view.

This command takes effect only in the instance scope. Instance configurations are inherited when the interface of this instance is created.



Caution

If the other IGMP querier present timer value is smaller than the general query interval, the querier on the network will change frequently on the network. Therefore, set an appropriate value for the timer.

Example

Set the global querier present timer to 100 seconds.

```
Switch(config-igmp)#timer other-querier-present 100
Switch(config-igmp)#
```

7.2.39 timer query

Function

The **timer query** command sets the global IGMP general query interval.

Format

timer query { *interval* | **default** }

Parameter

Parameter	Description	Value
interval	Specifies the sending interval of IGMP general group query messages on a device.	The value is an integer ranging from 1 to 65535, in seconds.
default	Specifies the default value.	125 seconds

Default Value

By default, the general query interval is 125 seconds.

View

IGMP configuration view

Usage Guidelines

This command (valid for all commands) has the same function as the **igmp timer query** command in the VLANIF configuration command and Ethernet routing interface configuration view (valid only on the current interface), except for the scopes they take effect. The configuration in the interface view takes precedence over the global configuration. The configuration in the IGMP view takes effect only when no configuration is made in the interface view.

This command takes effect only in the instance scope. Instance configurations are inherited when the interface of this instance is created.

Example

Set the global general query interval to 100 seconds.

```
Switch(config-igmp)#timer query 100
Switch(config-igmp)#
```

7.3 MLD Snooping Configuration Commands

7.3.1 debug mldsnop

Function

The **debug mldsnoop** command enables MLD Snooping debugging.

The **no debug mldsnoop** command disables MLD Snooping debugging.

Format

- **debug mldsnoop { rx | tx | report | query | leave | group | uplink | mvlan | interface | message | sync | hw | error | control | all }**
- **no debug mldsnoop { rx | tx | report | query | leave | group | uplink | mvlan | interface | message | sync | hw | error | control | all }**

Parameter

NA

Default Value

By default, the MLD Snooping debugging function is disabled.

View

Privileged user view

Usage Guidelines

NA

Example

Enable MLD Snooping debugging.

```
Switch#debug mldsnoop all
Switch#
```

7.3.2 mld-snooping {enable|disable}

Function

The **mld-snooping {enable|disable}** command enables or disables MLD Snooping.

Format

mld-snooping { enable | disable }

Parameter

Parameter	Description	Value
enable	Enables MLD Snooping on an interface.	-
disable	Disables MLD Snooping on an interface.	-

Default Value

NA

View

Ethernet bridge interface configuration view, Ethernet routing interface configuration view, interface configuration view (Trunk), GRP bridge interface configuration view, and GRP routing interface configuration view

Usage Guidelines

NA

Example

Enable MLD Snooping on an interface.

```
Switch(config-10ge1/0/1)#mld-snooping enable
Switch(config-10ge1/0/1)#
```

7.3.3 mld-snooping {start|stop}**Function**

The **mld-snooping {start|stop}** command globally enables or disables MLD Snooping.

Format

mld-snooping { start | stop }

Parameter

Parameter	Description	Value
start	Enables MLD Snooping globally.	-
stop	Disables MLD Snooping globally.	-

Default Value

By default, MLD Snooping is disabled globally.

View

Global configuration view

Usage Guidelines

NA

Example

Enable MLD Snooping globally.

```
Switch>mld-snooping start
Switch>
```

7.3.4 mld-snooping fast-leave {enable|disable}

Function

The **mld-snooping fast-leave {enable|disable}** command enables or disables the fast leave function for an MLD Snooping module on an interface.

Format

mld-snooping fast-leave { enable | disable }

Parameter

Parameter	Description	Value
enable	Enables the fast leave function on an interface.	-
disable	Disables the fast leave function on an interface.	-

Default Value

By default, the fast leave function is disabled.

View

Ethernet bridge interface configuration view, Ethernet routing interface configuration view, interface configuration view (Trunk)

Usage Guidelines

Before running this command, you must run **mld-snooping enable** to enable MLD Snooping.

Then, the switch does not send any query packets. Instead, it directly deletes the multicast forwarding entries.

Example

Enable the fast leave function for an MLD Snooping module.

```
Switch(config-10ge1/0/1)#mld-snooping enable
Switch(config-10ge1/0/1)#mld-snooping fast-leave enable
Switch(config-10ge1/0/1)#
```

7.3.5 mld-snooping fast-switch {enable|disable}

Function

The **mld-snooping fast-switch {enable|disable}** command enables or disables the fast switchover function when the STP topology changes.

Format

mld-snooping fast-switch { enable | disable }

Parameter

Parameter	Description	Value
enable	Enables the fast switchover function when the STP topology changes.	-
disable	Disables the fast switchover function when the STP topology changes.	-

Default Value

By default, the fast switchover function is disabled.

View

MLD Snooping MVLAN configuration view

Usage Guidelines

NA

Example

Enable the fast switchover function when the STP topology changes.

```
Switch(config-mldsnoop-mvlan1)#mld-snooping fast-switch enable
Switch(config-mldsnoop-mvlan1)#
```

7.3.6 mld-snooping fast-switch query {enable|disable}

Function

The **mld-snooping fast-switch query {enable|disable}** command enables or disables sending the query function when fast switchover is triggered due to changes of the STP topology.

Format

mld-snooping fast-switch query { enable | disable }

Parameter

Parameter	Description	Value
enable	Enables sending the query function when fast switchover is triggered due to changes of the STP topology.	-
disable	Disables sending the query function when fast switchover is triggered due to changes of the STP topology.	-

Default Value

Disable

View

MLD Snooping MVLAN configuration view

Usage Guidelines

NA

Example

Enable sending the query function when fast switchover is triggered due to changes of the STP topology.

```
Switch(config-mldsnoop-mvlan1)#mld-snooping fast-switch query enable
Switch(config-mldsnoop-mvlan1)#
```

7.3.7 mld-snooping forwarding-mode**Function**

The **mld-snooping forwarding-mode** command sets the multicast data forwarding mode.

Format

mld-snooping forwarding-mode { ip | mac }

Parameter

Parameter	Description	Value
ip	Forwards multicast data according to the IP address.	-
mac	Forwards multicast data according to MAC address.	-

Default Value

By default, the switch forwards multicast data according to MAC address.

View

MLD Snooping MVLAN configuration view

Usage Guidelines

NA

Example

Set the multicast data forwarding mode.

```
Switch(config-mldsnoop-mvlan1)#mld-snooping forwarding-mode ip
Switch(config-mldsnoop-mvlan1)#
```

7.3.8 mld-snooping lastmember-queryinterval

Function

The **mld-snooping lastmember-queryinterval** command sets the global group-specific query interval.

Format

mld-snooping lastmember-queryinterval { *queryinterval-value* | **default** }

Parameter

Parameter	Description	Value
queryinterval-value	Specifies a global group-specific query interval.	The value is an integer ranging from 1 to 5, in seconds.
default	Specifies the default value.	1

Default Value

1

View

Global configuration view

Usage Guidelines

NA

Example

Set the global group-specific interval to 3s.

```
Switch>mld-snooping lastmember-queryinterval 3
Switch>
```

7.3.9 mld-snooping leave-suppress {enable|disable}

Function

The **mld-snooping leave-suppress {enable|disable}** command enables or disables the multicast leave proxy function.

Format

mld-snooping leave-suppress { enable | disable }**Parameter**

Parameter	Description	Value
enable	Enables the multicast leave proxy function.	-
disable	Disables the multicast leave proxy function.	-

Default Value

NA

View

MLD Snooping MVLAN configuration view

Usage Guidelines

NA

Example

Enable the multicast leave proxy function.

```
Switch(config-mldsnoop-mvlan1)#mld-snooping leave-suppress enable
Switch(config-mldsnoop-mvlan1)#
```

7.3.10 mld-snooping max-response-time**Function**

The **mld-snooping max-response-time** command sets the global maximum response time for MLD snooping General Query packets.

Format**mld-snooping max-response-time { responsetime-value | default }****Parameter**

Parameter	Description	Value
responsetime-value	Specifies the maximum response time of MLD packets for an MLD Snooping module.	The value is an integer ranging from 1 to 25, in seconds.
default	Specifies the default value.	10 seconds

Default Value

10 seconds

View

Global configuration view, MLD Snooping MVLAN configuration view

Usage Guidelines

NA

Example

Set the global maximum response time for MLD snooping General Query packets to 20s.

```
Switch>mld-snooping max-response-time 20
Switch>
```

7.3.11 mld-snooping static-group group-address mvlan

Function

The **mld-snooping static-group group-address mvlan** command sets the MLD Snooping static group information on an interface.

The **no mld-snooping static-group group-address mvlan** command deletes the configuration of an MLD Snooping static group on an interface.

Format

- **mld-snooping static-group group-address** *group-ipv6-address* **mvlan** *vlan-id*
- **mld-snooping static-group group-address** *group-ipv6-address* **mvlan** *vlan-id* **user-vlan** *vlan-list*
- **mld-snooping static-group group-address** *group-ipv6-address* **source-address** *source-ipv6-address* **mvlan** *vlan-id*
- **no mld-snooping static-group**
- **no mld-snooping static-group group-address** *group-ipv6-address* **mvlan** *vlan-id*
- **no mld-snooping static-group group-address** *group-ipv6-address* **mvlan** *vlan-id* **user-vlan** *all*
- **no mld-snooping static-group group-address** *group-ipv6-address* **mvlan** *vlan-id* **user-vlan** *vlan-list*
- **no mld-snooping static-group group-address** *group-ipv6-address* **source-address** *source-ipv6-address* **mvlan** *vlan-id*
- **no mld-snooping static-group mvlan** *vlan-list*

Parameter

Parameter	Description	Value
group-ipv6-address	Specifies a group address.	In this format, a 128-digit IP address is divided into 8 segments. Each segment consists of 16 digits and is represented by 4 hexadecimal characters (0-9 and A-F). Segments are separated by colons (:). Every "X" represents a group of hexadecimal digits.
source-ipv6-address	Specifies a source IPv6 address.	In this format, a 128-digit IP address is divided into 8 segments. Each segment consists of 16 digits and is represented by 4 hexadecimal characters (0-9 and A-F). Segments are separated by colons (:). Every "X" represents a group of hexadecimal digits.
vlan-id	Specifies a VLAN ID.	The value is an integer ranging from 1 to 4094.
vlan-list	Specifies a VLAN list.	The value is a VLAN list, such as (2,3,5-10).

Default Value

NA

View

Ethernet bridge interface configuration view, Ethernet routing interface configuration view, interface configuration view (Trunk)

Usage Guidelines

NA

Example

Set a multicast group IP address.

```
Switch(config-10ge1/0/1)#mld-snooping static-group group-address 4000::1 mvlan 1
Switch(config-10ge1/0/1)#
```

7.3.12 mld-snooping uplink-port

Function

The **mld-snooping uplink-port** command sets an uplink interface.

The **no mld-snooping uplink-port** command deletes an uplink interface.

Format

- **mld-snooping uplink-port** { **ethernet** | **xgigaethernet** | **10gigaethernet** | **25gigaethernet** | **40gigaethernet** | **100gigaethernet** } *interface-number*
- **mld-snooping uplink-port eth-trunk** *trunk-number*
- **no mld-snooping uplink-port** { **ethernet** | **xgigaethernet** | **10gigaethernet** | **25gigaethernet** | **40gigaethernet** | **100gigaethernet** } *interface-number*
- **no mld-snooping uplink-port eth-trunk** *trunk-number*

Parameter

Parameter	Description	Value
interface-number	Specifies an Ethernet interface number.	The value is an integer in the range of <1-1>/<0-1>/<1-48> (For reference only. The specific value range depends on the slot number and card type).
trunk-number	Specifies the number of an aggregation interface.	The value is an integer ranging from 1 to 128.

Default Value

NA

View

MLD Snooping MVLAN configuration view

Usage Guidelines

NA

Example

Set the interface 1/0/1 as the uplink interface.

```
Switch(config-mldsnoop-mvlan1)#mld-snooping uplink-port gigabitEthernet 1/0/1
Switch(config-mldsnoop-mvlan1)#
```

7.3.13 mld-snooping multicast user-vlan

Function

The **mld-snooping multicast user-vlan** command sets user VLANs for multicast replication.

The **no mld-snooping multicast user-vlan** command deletes user VLANs for multicast replication.

Format

- **mld-snooping multicast user-vlan** *vlan-list*
- **no mld-snooping multicast user-vlan**

Parameter

Parameter	Description	Value
vlan-list	Specifies a VLAN list.	The value is an integer ranging from 1 to 4094.

Default Value

NA

View

MLD Snooping MVLAN configuration view

Usage Guidelines

NA

Example

Set the user VLAN for multicast replication to 200.

```
Switch(config-mldsnoop-mvlan1)#mld-snooping multicast user-vlan 200
Switch(config-mldsnoop-mvlan1)#
```

7.3.14 mld-snooping multicast-vlan**Function**The **mld-snooping multicast-vlan** command enables or disables the multicast replication function.**Format****mld-snooping multicast-vlan { enable | disable }****Parameter**

Parameter	Description	Value
enable	Enables the multicast replication function.	-
disable	Disables the multicast replication function.	-

Default Value

NA

View

MLD Snooping MVLAN configuration view

Usage Guidelines

NA

Example

Enable the multicast replication function.

```
Switch(config-mldsnoop-mvlan1)#mld-snooping multicast-vlan enable
Switch(config-mldsnoop-mvlan1)#
```

7.3.15 mld-snooping mvlan

Function

The **mld-snooping mvlan** command creates a multicast VLAN (MVLAN) and displays the MLD Snooping MVLAN configuration view.

The **no mld-snooping mvlan** command deletes the created MVLAN.

Format

- **mld-snooping mvlan** *vlan-id*
- **no mld-snooping mvlan** *vlan-id*

Parameter

Parameter	Description	Value
vlan-id	Specifies the MVLAN ID for MLD Snooping.	The value is an integer ranging from 1 to 4094.

Default Value

NA

View

Global configuration view

Usage Guidelines

NA

Example

Set the MVLAN ID to 4000.


```
Switch>mld-snooping mvlan 4000
Switch(config-mldsnoop-mvlan4000)#
```

7.3.16 mld-snooping mvlan uplink-port

Function

The **mld-snooping mvlan uplink-port** command creates an uplink interface of an MVLAN.

The **no mld-snooping mvlan uplink-port** command deletes an uplink interface of an MVLAN.

Format

- **mld-snooping mvlan *vlan-id* uplink-port**
- **no mld-snooping mvlan *vlan-id* uplink-port**

Parameter

Parameter	Description	Value
vlan-id	Specifies the MVLAN ID for MLD Snooping.	The value is an integer ranging from 1 to 4094.

Default Value

NA

View

Ethernet bridge interface configuration view, Ethernet routing interface configuration view, GRP bridge interface configuration view, GRP routing interface configuration view, and interface configuration view (Trunk)

Usage Guidelines

Before running this command, you must enable MLD Snooping for all interfaces and create an MVLAN.

Example

Create an uplink interface 10ge5/0/1 of an MVLAN.

```
Switch(config-10ge5/0/1)#mld-snooping mvlan 100 uplink-port
Switch(config-10ge5/0/1)#
```

7.3.17 mld-snooping proxy-ip

Function

The **mld-snooping proxy-ip** command sets the multicast proxy address.

The **no mld-snooping proxy-ip** command deletes the multicast proxy address.

Format

- **mld-snooping proxy-ip** *ipv6-address*
- **no mld-snooping proxy-ip**

Parameter

Description	Description	Value
ipv6-address	Specifies an IPv6 address.	In this format, a 128-digit IP address is divided into 8 segments. Each segment consists of 16 digits and is represented by 4 hexadecimal characters (0-9 and A-F). Segments are separated by colons (:). Every "X" represents a group of hexadecimal digits.

Default Value

NA

View

MLD Snooping MVLAN configuration view

Usage Guidelines

NA

Example

Set the multicast proxy address to 2001::1.

```
Switch(config-mldsnoop-mvlan1)#mld-snooping proxy-ip 2001::1
Switch(config-mldsnoop-mvlan1)#
```

7.3.18 mld-snooping group-policy

Function

The **mld-snooping group-policy filter-list** command sets a multicast policy for an MVLAN.

The **no mld-snooping group-policy** command cancels the configuration.

Format

- **mld-snooping group-policy filter-list** *acl-number*

- **mld-snooping group-policy filter-list** *acl-number version version-list*
- **no mld-snooping group-policy**

Parameter

Parameter	Description	Value
acl-number	Specifies the ACL number bound with a multicast policy.	The value is an integer ranging from 3001 to 4000.
version-list	Specifies the list of applicable multicast snooping protocol versions.	The value is an integer ranging from 1 to 2.

Default Value

NA

View

Ethernet bridge interface configuration view, Ethernet routing interface configuration view, interface configuration view (Trunk), MLD Snooping MVLAN configuration view

Usage Guidelines

NA

Example

Configure a multicast policy within the multicast VLAN.

```
Switch(config-mldsnoop-mvlan1)#mld-snooping group-policy filter-list 3001 version 1-2
Switch(config-mldsnoop-mvlan1)#
```

7.3.19 mld-snooping querier {enable|disable}**Function**

The **mld-snooping querier {enable|disable}** command enables or disables the general query function.

Format

mld-snooping querier { enable | disable }

Parameter

Parameter	Description	Value
enable	Enables the general query function.	-
disable	Disables the general query function.	-

Default Value

NA

View

MLD Snooping MVLAN configuration view

Usage Guidelines

NA

Example

Enable the general query function.

```
Switch(config-mldsnoop-mvlan1)#mld-snooping querier enable
Switch(config-mldsnoop-mvlan1)#
```

7.3.20 mld-snooping query-interval**Function**

The **mld-snooping query-interval** command sets the global general query interval for MLD Snooping.

Format**mld-snooping query-interval** { *queryinterval-value* | **default** }**Parameter**

Parameter	Description	Value
queryinterval-value	Specifies a global general query interval.	The value is an integer ranging from 10 to 65535, in seconds.
default	Specifies the default value.	60 seconds

Default Value

60 seconds

View

Global configuration view

Usage Guidelines

NA

Example

Set the global general query interval to 80s.

```
Switch>mld-snooping query-interval 80
Switch>
```

7.3.21 mld-snooping report-suppress {enable|disable}

Function

The **mld-snooping report-suppress {enable|disable}** command enables or disables the multicast report proxy function.

Format

mld-snooping report-suppress { enable | disable }

Parameter

Parameter	Description	Value
enable	Enables the multicast report proxy function.	-
disable	Disables the multicast report proxy function.	-

Default Value

NA

View

MLD Snooping MVLAN configuration view

Usage Guidelines

NA

Example

Enable the multicast report proxy function.

```
Switch(config-mldsnoop-mvlan1)#mld-snooping report-suppress enable
Switch(config-mldsnoop-mvlan1)#
```

7.3.22 mld-snooping require-router-alert

Function

The **mld-snooping require-router-alert** command sets the Router-Alert checking function of a multicast VLAN.

Format

mld-snooping require-router-alert { enable | disable }**Parameter**

Parameter	Description	Value
enable	Enables the Router-Alert checking function for the multicast VLAN.	-
disable	Disables the Router-Alert checking function for the multicast VLAN.	-

Default Value

Disable

View

MLD Snooping MVLAN configuration view

Usage Guidelines

NA

Example

Enable the Router-Alert checking function for the multicast VLAN.

```
Switch(config-mldsnoop-mvlan1)#mld-snooping require-router-alert enable
Switch(config-mldsnoop-mvlan1)#
```

7.3.23 mld-snooping robust-count**Function**

The **mld-snooping robust-count** command sets the number of Group-specific Query packets sent by the querier.

Format

mld-snooping robust-count { robust-count-num | default }

Parameter

Parameter	Description	Value
robust-count-num	Specifies the number of Group-specific Query packets sent by the querier.	The value is an integer ranging from 2 to 5.

Default Value

The default value is 2.

View

Global configuration view

Usage Guidelines

NA

Example

Set the number of Group-specific Query packets sent by the querier to 3.

```
Switch>mld-snooping robust-count 3
Switch>
```

7.3.24 mld-snooping router-aging-time**Function**

The **mld-snooping router-aging-time** command sets the global aging time for router interfaces.

Format

mld-snooping router-aging-time { *router-aging-time* | **default** }

Parameter

Description	Description	Value
router-aging-time	Specifies the aging time of router interfaces.	The value is an integer ranging from 1 to 1000, in seconds.

Default Value

The default value is 180s.

View

Global configuration view

Usage Guidelines

NA

Example

Set the global aging time of router interfaces to 200s.

```
Switch>mld-snooping router-aging-time 200
Switch>
```

7.3.25 reset mld-snooping group**Function**

The **reset mld-snooping group** command clears the MLD Snooping multicast group information.

Format

reset mld-snooping group

Parameter

NA

Default Value

NA

View

Global configuration view

Usage Guidelines

NA

Example

Clear the MLD Snooping multicast group information.

```
Switch>reset mld-snooping group
Switch>
```

7.3.26 mld-snooping uplink-port drop-report {enable|disable}

Function

The **mld-snooping uplink-port drop-report {enable|disable}** command enables or disables learning the multicast group on an uplink interface.

Format

mld-snooping uplink-port drop-report { enable | disable }

Parameter

Description	Description	Value
enable	Enables learning the multicast group on an uplink interface.	-
disable	Disables learning the multicast group on an uplink interface.	-

Default Value

NA

View

MLD Snooping MVLAN configuration view

Usage Guidelines

NA

Example

Enable learning the multicast group on an uplink interface.

```
Switch(config-mldsnoop-mvlan1)#mld-snooping uplink-port drop-report enable
Switch(config-mldsnoop-mvlan1)#
```

7.3.27 mld-snooping uplink-port-limit**Function**

The **mld-snooping uplink-port-limit** command limits the uplink interface number.

Format

mld-snooping uplink-port-limit {*uplink-port-limit* | **default**}

Parameter

Description	Description	Value
uplink-port-limit	Specifies the number of an uplink interface.	The value is an integer ranging from 1 to 256.
default	Specifies the default value.	1

Default Value

1

View

MLD Snooping MVLAN configuration view

Usage Guidelines

NA

Example

Set the limit of uplink interface number to 100.

```
Switch(config-mldsnoop-mvlan1)#mld-snooping uplink-port-limit 100
Switch(config-mldsnoop-mvlan1)#
```

7.3.28 mld-snooping version**Function**

The **mld-snooping version** command sets the version of MLD packets that MLD Snooping can process.

Format

mld-snooping version { v1 | v2 }

Parameter

NA

Default Value

NA

View

MLD Snooping MVLAN configuration view

Usage Guidelines

NA

Example

Set the version of MLD packets that MLD Snooping can process to 1.

```
Switch>mld-snooping mvlan 4000
Switch(config-mldsnoop-mvlan4000)#mld-snooping version v1
Switch(config-mldsnoop-mvlan4000)#
```

7.3.29 mld-snooping workmode

Function

The **mld-snooping workmode** command sets the MLD snooping working mode.

Format

mld-snooping workmode { mld-snooping | mld-proxy }

Parameter

Description	Description	Value
mld-snooping/mld-proxy	Indicates the MLD Snooping working mode.	-

Default Value

NA

View

MLD Snooping MVLAN configuration view

Usage Guidelines

NA

Example

Set the MLD Snooping working mode to mld-snooping.

```
Switch(config-mldsnoop-mvlan1)#mld-snooping workmode mld-snooping
Switch(config-mldsnoop-mvlan1)#
```

7.3.30 mld-snooping group-address mvlan

Function

The **mld-snooping group-address mvlan** command sets a pre-joined group.

The **no mld-snooping group-address mvlan** command deletes a pre-joined group.

Format

- **mld-snooping group-address** *group-address* **mvlan** *vlan-id*
- **no mld-snooping group-address** *group-address* **mvlan** *vlan-id*

Parameter

Description	Description	Value
group-address	Specifies a multicast IPv6 address.	The value range is FF00::/8.
vlan-id	Specifies a VLAN entry.	The value is an integer ranging from 1 to 4094.

Default Value

NA

View

Global configuration view

Usage Guidelines

NA

Example

Delete a pre-joined group.

```
Switch(config)#no mld-snooping group-address FF00:: mvlan 100
Switch(config)#
```

7.3.31 mld-snooping send-query source-address

Function

The **mld-snooping send-query source-address** command sets the source IP address of an MLD query packet.

Format

- **mld-snooping send-query source-address** *source-address*
- **mld-snooping send-query source-address default**

Parameter

Parameter	Description	Value
source-address	Specifies a multicast IPv6 address.	-

Default Value

FE80::

View

MLD Snooping MVLAN configuration view

Usage Guidelines

NA

Example

Set the source IP address of an MLD query packet.

```
Switch(config-mldsnoop-mvlan1)#mld-snooping send-query source-address 4000::1
Switch(config-mldsnoop-mvlan1)#
```

7.3.32 show mld-snooping config

Function

The **show mld-snooping config** command displays the MLD Snooping configuration.

Format

show mld-snooping config

Parameter

NA

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

Display the MLD snooping configuration file information.

```

Switch>show mld-snooping config
!
mld-snooping start
mld-snooping mvlan 10
  mld-snooping querier enable
  mld-snooping uplink-port 10gigaethernet 1/0/29
interface 10ge1/0/29
  mld-snooping enable
interface 10ge1/0/30
  mld-snooping enable
  mld-snooping fast-leave enable
interface 10ge1/0/31
  mld-snooping enable
Switch>

```

7.3.33 show mld-snooping egress-port**Function**

The **show mld-snooping egress-port** command displays information on the MLD Snooping outbound interface.

Format**show mld-snooping egress-port****Parameter**

NA

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

Display information on the MLD snooping outbound interface.

```
Switch>show mld-snooping egress-port
Total Entry(s) : 0
Switch>
```

7.3.34 show mld-snooping group

Function

The **show mld-snooping group** command displays the MLD Snooping multicast group information.

Format

show mld-snooping group

Parameter

NA

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

Display the MLD Snooping multicast group information.

```
Switch>show mld-snooping group
Total Entry(s) : 0
Switch>
```

7.3.35 show mld-snooping interface

Function

The **show mld-snooping interface** command displays the MLD Snooping multicast interface information.

Format

show mld-snooping interface

Parameter

NA

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

Display the MLD Snooping multicast interface information.

```
Switch>show mld-snooping interface
      Interface      Mld-Snooping  Fastleave
      ge-1/0/1        enable         disable
Switch>
```

7.3.36 show mld-snooping mvlan

Function

The **show mld-snooping mvlan** command displays the MLD Snooping MVLAN information.

Format

show mld-snooping mvlan

Parameter

NA

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

Display the MLD Snooping MVLAN information.

```
Switch>show mld-snooping mvlan
MVLAN : 4000
  Work Mode : snooping
  Version : v1
  Report Suppress : disable
  Leave Suppress : disable
  Forwarding mode : ip
  Querier : disable
  Proxy Ip : ---
  Multicast Vlan : disable
  Multicast User Vlan : ---
Switch>
```

7.3.37 show mld-snooping source-address

Function

The **show mld-snooping source-address** command displays the source address list of the multicast group.

Format

show mld-snooping source-address

Parameter

NA

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

View the source address list of the multicast group.

```
Switch>show mld-snooping source
Total Entry(s) : 0
Switch>
```

7.3.38 show mld-snooping uplinkport**Function**

The **show mld-snooping uplinkport** command displays the MLD Snooping multicast uplink interface information.

Format

show mld-snooping uplinkport

Parameter

NA

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

Display the MLD Snooping multicast uplink interface information.

```
Switch>show mld-snooping uplinkport
Mvlan   UplinkPort   Expires      Type
4000    ge-1/0/2     ---          static
Switch>
```

7.3.39 show mld-snooping**Function**

The **show mld-snooping** command displays the current basic parameter configurations of MLD Snooping.

Format**show mld-snooping****Parameter**

NA

Default Value

NA

View

Common user view

Usage Guidelines

Before running this command, you must run **mld-snooping start** to enable MLD Snooping.

Example

Display the current basic parameter configurations of MLD Snooping.

```
Switch>show mld-snooping
  Version                : MLDSNOOP_VB3.02.00.00
  Mld-snooping           : start
  Robustness              : 2
  Query Interval         : 60 seconds
  Query Max Response Time : 10 seconds
  Lastmember Query Interval : 1 seconds
  V2router Aging Time     : 180 seconds
Switch>
```

7.4 PIM Configuration Commands

7.4.1 ip multicast-routing

Function

The **ip multicast-routing** command enables IP multicast routing globally.

The **no ip multicast-routing** command disables IP multicast routing globally.

Format

- **ip multicast-routing**
- **no ip multicast-routing**

Parameter

NA

Default Value

By default, IP multicast routing is disabled globally.

View

Global configuration view

Usage Guidelines

This command enables IP multicast routing globally, which shall be done before PIM is used.

Example

Enable IP multicast routing in global view.

```
Switch(config)#
Switch(config)#ip multicast-routing
```

7.4.2 pim**Function**

The **pim** command creates a PIM instance.

The **no pim** command deletes a PIM instance.

Format

- **pim**
- **no pim**
- **pim vpn-instance** *NAME*
- **no pim vpn-instance** *NAME*

Parameter

Parameter	Description	Value
NAME	Instance name	Name of a created IP instance

Default Value

By default, no PIM instance is configured.

View

Global configuration view

Usage Guidelines

This command creates a PIM public network instance or VPN instance. Before creating a PIM VPN instance, you need to create a VPN instance first.

Example

Create a PIM VPN instance named aa.

```
Switch(config)# ip vpn-instance aa
Switch(config-vpn-instance-aa)#quit
Switch(config)#pim vpn-instance aa
Switch(config-pim-aa)#
```

7.4.3 anycast-rp

Function

The **anycast-rp** command sets an anycast rendezvous point (RP).

Format

- **anycast-rp** *rp-address* **local-address** *local-address*
- **anycast-rp** *rp-address* **peer** *peer-address*
- **no anycast-rp** *rp-address*
- **no anycast-rp** *rp-address* **peer** *peer-address*

Parameter

Parameter	Description	Value
rp-address	Anycast RP address	The value is in dotted decimal notation.
local-address	Local address for establishing neighbor relationships	The value is in dotted decimal notation.
peer-address	Peer address for establishing neighbor relationships	The value is in dotted decimal notation.

Default Value

By default, no anycast RP is configured.

View

Public network instance PIM view, VPN instance PIM view

Usage Guidelines

Configure the local address and peer address of the anycast RP. A loopback port is recommended.

In the traditional PIM-SM domain, each multicast group can be mapped to only one RP. However, if the network is overloaded or traffic is too concentrated, problems, such as excessive load on RPs, slow convergence of routes after RP failure, and non-optimal multicast forwarding paths, may occur.

Applying anycast RP in the PIM-SM domain enables multicast sources to register nearby and receivers to join nearby. It not only relieves the burden of a single RP, but also achieves RP backup and optimizes the forwarding path.

After using the anycast RP feature based on the PIM protocol, when the RP receives a registration message, it checks the source address of the registration message. If it is from the source DR, the registration message will be forwarded to the configured anycast RP peer, and if it is sent from the anycast RP peer, the registration message is not forwarded. This allows anycast RPs to learn source group information from each other.

Example

Set anycast RP 10.1.1.1, local address 2.2.2.2, and peer address 3.3.3.3 in public instance PIM view.

```
Switch(config-pim)#anycast-rp 10.1.1.1 local-address 2.2.2.2
Switch(config-pim)#anycast-rp 10.1.1.1 peer 3.3.3.3
```

7.4.4 c-bsr admin-scope

Function

The **c-bsr admin-scope enable** command enables the BSR administrative scope in an instance.

The **c-bsr admin-scope disable** command disables the BSR administrative scope in an instance.

Format

- **c-bsr admin-scope enable**
- **c-bsr admin-scope disable**

Parameter

NA

Default Value

By default, no BSR administrative scope is enabled in an instance.

View

PIM instance configuration view

Usage Guidelines

The device can elect a BSR only after BSR administrative scope is enabled.

Example

Enable the BRS administrative scope in the PIM public network instance.

```
Switch(config-pim)#
Switch(config-pim)#c-bsr admin-scope enable
```

7.4.5 c-bsr send-interval

Function

The **c-bsr send-interval** command sets the interval at which a C-BSR sends Bootstrap messages.

Format

- **c-bsr send-interval** *interval*
- **c-bsr send-interval default**

Parameter

Parameter	Description	Value
interval	Interval in seconds	The value is an integer ranging from 1 to 107374177.

Default Value

By default, the interval at which a C-BSR sends Bootstrap messages is 60s.

View

Public network instance PIM view, VPN instance PIM view

Usage Guidelines

When a C-BSR wins the election to become a BSR, it periodically sends Bootstraps message to the network, which carry its own IP address and RP information. The interval for sending Bootstrap messages is BSR_interval, which can be configured using the c-bsr send-interval command.

Example

Set the interval at which a C-BSR sends Bootstrap messages to 30s in the public network instance.

```
Switch(config)# ip multicast-routing
Switch(config)#pim
Switch(config-pim)#c-bsr send-interval 30
```

7.4.6 c-rp hold-time

Function

The **c-rp hold-time** command sets the holdtime on a BSR for an Advertisement message from the C-RP.

The **c-rp hold-time default** command restores the default value.

Format

- **c-rp hold-time** *interval*
- **c-rp hold-time default**

Parameter

Parameter	Description	Value
interval	Hold time, in seconds	The value is an integer ranging from 1 to 65535.

Default Value

By default, the holdtime on the BSR for an Advertisement message from the C-RP is 150 seconds.

View

Public network instance PIM view, VPN instance PIM view

Usage Guidelines

After this command is configured on a C-RP, the C-RP encapsulates the parameter in an Advertisement message and transmits it to the BSR. The BSR obtains the parameter from the message and starts the timer. If the BSR still does not receive the Advertisement message from the C-RP after the timeout period, the C-RP is considered to be currently disabled or unreachable in the network.

Example

Set the holdtime on the BSR for an Advertisement message from the C-RP to 90 seconds in the public network instance.

```
Switch(config)# ip multicast-routing
Switch(config)#pim
Switch(config-pim)#c-rp hold-time 90
```

7.4.7 c-rp send-interval

Function

The **c-rp send-interval** command sets the interval at which a C-RP sends Advertisement messages.

The **c-rp send-interval default** command restores the default value.

Format

- **c-rp send-interval** *interval*
- **c-rp send-interval default**

Parameter

Parameter	Description	Value
interval	Interval in seconds	The value is an integer ranging from 1 to 65535.

Default Value

By default, the interval at which a C-RP sends Advertisement messages is 60 seconds.

View

Public network instance PIM view, VPN instance PIM view

Usage Guidelines

All C-RPs in the PIM-SM domain send periodic unicast Advertisement messages to the same BSR. The Advertisement message carries the C-RP address, the group range served, and the C-RP priority. Therefore, this BSR is able to collect all RPs for election.

Example

Set the interval at which a C-RP sends Advertisement messages to 30 seconds in the public network instance.

```
Switch(config)# ip multicast-routing
Switch(config)#pim
Switch(config-pim)#c-rp send-interval 30
```

7.4.8 rp-address

Function

The **rp-address** command sets a static RP.

The **no rp-address** command deletes a static RP.

Format

- **rp-address** *ip-address group group-address/mask-length*

- **rp-address** *ip-address* **group** *default*
- **no rp-address** *ip-address* **group** *group-address/mask-length*
- **no rp-address** *ip-address* **group** *default*

Parameter

Parameter	Description	Value
ip-address	IP address of the static RP to be configured	The value is in dotted decimal notation.
group-address	IP address range of a group for which static RPs are suitable	The value is in dotted decimal notation.
mask-length	Specifies the mask address	The value is in dotted decimal notation.
default	Applicable to all multicast groups	224.0.0.0/4

Default

By default, no static RP is configured.

View

Public network instance PIM view, VPN instance PIM view

Usage Guidelines

When there is only one RP in the network, you can manually configure static RPs instead of using dynamic RPs. This avoids unnecessary bandwidth occupation due to frequent message interactions between the C-RP and BSR. To enable a static RP to work properly, all switches must be configured with the exact same **rp-address** command.

Example

In the public network instance, set address 10.1.1.1 as a static RP to serve the group 225.0.0.1/24.

```
Switch(config)# ip multicast-routing
Switch(config)# pim
Switch(config-pim)#rp-address 10.1.1.1 group 225.0.0.1/24
```

7.4.9 receive-check-neighbor

Function

The **receive-check-neighbor enable** command enables the system to check whether the join/prune or graft/graft ack messages are from PIM neighbors.

The **receive-check-neighbor disable** command disables the system from checking whether the messages are from PIM neighbors.

Format

- **receive-check-neighbor enable**
- **receive-check-neighbor disable**

Parameter

NA

Default Value

By default, checking whether the packets are from a PIM neighbor is enabled in an instance.

View

Public network instance PIM view, VPN instance PIM view

Usage Guidelines

Enable the switch to check whether the join/prune or graft/graft ack messages are from PIM neighbors. If this function is enabled, messages from PIM neighbors are processed, otherwise they will be discarded.

Example

Enable PIM neighbor check when receiving Join/Prune or graft/graft ack messages in the public network instance.

```
Switch(config)# ip multicast-routing
Switch(config)#pim
Switch(config-pim)#receive-check-neighbor enable
```

7.4.10 send-check-neighbor

Function

The **send-check-neighbor enable** command enables the system to check whether join/prune messages are sent to PIM neighbors.

The **send-check-neighbor disable** command disables the system from checking whether join/prune messages are sent to PIM neighbors.

Format

- **send-check-neighbor enable**

- **send-check-neighbor disable**

Parameter

NA

Default Value

By default, checking whether the packets are sent to PIM neighbors is enabled in an instance.

View

Public network instance PIM view, VPN instance PIM view

Usage Guidelines

Enable the system to check whether the Join/Prune messages are sent to PIM neighbors. If not, these messages will not be sent.

Example

Enable PIM neighbor check when sending Join/Prune messages in the public network instance.

```
Switch(config)# ip multicast-routing
Switch(config)# pim
Switch(config-pim)#send-check-neighbor enable
```

7.4.11 source-lifetime**Function**

The **source-lifetime** command specifies the timeout period of an (S,G) entry.

The **source-lifetime default** command restores the default value.

Format

- **source-lifetime** *interval*

- **source-lifetime default**

Parameter

Parameter	Description	Value
interval	Timeout period of an (S,G) entry	The value is an integer ranging from 60 to 65535, in seconds.

Default Value

By default, the timeout period of an (S,G) entry is 210s.

View

Public network instance PIM view, VPN instance PIM view

Usage Guidelines

The switch creates a timer for each (S,G) table entry. The **source-lifetime** command is used to set the timeout value of this timer. After receiving a multicast message from the source S, the switch resets the timer. If the timer times out, the (S,G) entry is considered invalid.

Example

In the public network instance, set the timeout period of an (S,G) entry to 150s.

```
Switch(config)# ip multicast-routing
Switch(config)# pim
Switch(config-pim)#source-lifetime 150
```

7.4.12 state-refresh-interval

Function

The **state-refresh-interval** command sets the interval for sending state-refresh messages for all interfaces in an instance.

Format

- **state-refresh-interval default**
- **state-refresh-interval** *interval*

Parameter

Parameter	Description	Value
interval	User defined, in seconds	The value is an integer ranging from 1 to 255.

Default Value

By default, the interval for sending state-refresh messages is 60s.

View

Public network instance PIM view, VPN instance PIM view

Usage Guidelines

This command sets the interval for sending state-refresh messages for all PIM-DM-enabled interfaces in a PIM instance.

Example

Set the interval for sending state-refresh messages to 50s in the public network instance PIM view.

```
Switch(config)# ip multicast-routing
Switch(config)#pim
Switch(config-pim)#state-refresh-interval 50
```

7.4.13 state-refresh-rate-limit

Function

The **state-refresh-rate-limit** command sets the time to wait before the switch receives the next PIM state-refresh message.

Format

- **state-refresh-rate-limit default**
- **state-refresh-rate-limit** *interval*

Parameter

Parameter	Description	Value
interval	Specifies the time to wait before the switch receives the next PIM state-refresh message.	The value is an integer ranging from 1 to 65535, in seconds.

Default Value

By default, the time to wait before the switch receives the next PIM state-refresh message is 30s in an instance.

View

Public network instance PIM view, VPN instance PIM view

Usage Guidelines

In a PIM-DM network, a switch may receive PIM state-refresh messages from multiple devices in a short period. However, some of these messages are duplicated. To avoid that, execute this command. When the switch receives the first state-refresh message, it immediately resets the related prune timer and starts the state-refresh timer, and the timeout period is the time for the device to wait to receive the next state-refresh message.

Example

Set the time to wait before receiving the next PIM state-refresh message to 45s in public instance PIM view.

```
Switch(config)# ip multicast-routing
```

```
Switch(config)#pim
Switch(config-pim)#state-refresh-rate-limit 45
```

7.4.14 state-refresh-ttl

Function

The **state-refresh-ttl** command sets the TTL value for forwarding state-refresh messages for all interfaces in an instance.

Format

- **state-refresh-ttl default**
- **state-refresh-ttl** *count*

Parameter

Parameter	Description	Value
count	Specifies the TTL value of the state-refresh message forwarded by an interface.	The value is an integer ranging from 1 to 255.

Default Value

By default, the TTL for forwarding state-refresh messages is 255.

View

Public network instance PIM view, VPN instance PIM view

Usage Guidelines

This command sets the TTL value for the PIM-DM-enabled device to forward the state-refresh messages.

Example

Set the TTL value of state-refresh messages to 100 in the public instance PIM view.

```
Switch(config)# ip multicast-routing
Switch(config)#pim
Switch(config-pim)#state-refresh-ttl 100
```

7.4.15 register probe-interval

Function

The **register probe-interval** command sets the interval for sending register-probe messages to the RP.

Format

- **register probe-interval** *interval*
- **register probe-interval default**

Parameter

Parameter	Description	Value
interval	Specifies the interval for sending register-probe messages to the RP.	The value is an integer ranging from 1 to 1799.

Default Value

By default, the interval for sending register-probe messages to the RP is 60s.

View

Public network instance PIM view, VPN instance PIM view

Usage Guidelines

When the source DR receives a Register-Stop message from the RP, the source DR stops sending register messages and enters the register suppression state. During the register suppression, the source DR sends Probe messages to notify the RP that the multicast source is still active. After the register suppression times out, the source DR resumes sending register messages.

Example

Set the interval for sending register-probe messages to the RP to 50s in public instance PIM view.

```
Switch(config)# ip multicast-routing
Switch(config)# pim
Switch(config-pim)# register probe-interval 50
```

7.4.16 register suppression-timeout**Function**

The **register suppression-timeout** command sets the timeout period during which the switch maintains the register suppression state.

The **register suppression-timeout default** command restores the default value.

Format

- **register suppression-timeout** *interval*
- **register suppression-timeout default**

Parameter

Parameter	Description	Value
interval	Specifies the timeout period during which the switch maintains the register suppression state.	The value is an integer ranging from 11 to 3600.

Default Value

By default, the switch maintains the register suppression state for 60s.

View

Public network instance PIM view, VPN instance PIM view

Usage Guidelines

When receiving a Register-Stop message related to the (S,G) entry from the RP, the source DR immediately stops sending Register messages encapsulated with multicast data. At this time, the switch enters the register suppression state.

Example

Set the timeout period during which the switch maintains the register suppression state to 90s in the public network instance PIM view.

```
Switch(config)# ip multicast-routing
Switch(config)#pim
Switch(config-pim)#register suppression-timeout 90
```

7.4.17 ip pim-sm**Function**

The **ip pim-sm** command enables PIM-SM mode on an interface.

The **no ip pim-sm** command disables PIM-SM mode on an interface.

Format

- **ip pim-sm**
- **no ip pim-sm**

Parameter

NA

Default Value

By default, PIM-SM is disabled on interfaces.

View

VLANIF configuration view, loopback interface configuration view

Usage Guidelines

When an interface is configured with an IP address, use this command to start running pim-sm on that interface (i.e., PIM packets can be sent/received and correctly processed on that interface). The prerequisite for configuring this command is to enable PIM globally, i.e., to configure **ip multicast-routing** and create a PIM instance in global view.

Example

Enable PIM-SM on vlan10.

```
Switch(config-vlanif-10)#
Switch(config-vlanif-10)#ip pim-sm
```

7.4.18 ip pim-dm

Function

The **ip pim-dm** command enables PIM-DM mode on an interface.

The **no ip pim-dm** command disables PIM-DM mode on an interface.

Format

- **ip pim-dm**
- **no ip pim-dm**

Parameter

NA

Default Value

By default, PIM-DM is disabled on interfaces.

View

VLANIF configuration view, loopback interface configuration view

Usage Guidelines

When an interface is configured with an IP address, this command is used to run **pim-dm** on that interface (i.e., PIM packets can be sent/received and correctly processed on that interface). The

prerequisite for configuring this command is to enable PIM globally, i.e., to set **ip multicast-routing** and create a PIM instance in global view.

Example

Enable PIM-DM on vlan10.

```
Switch(config-vlanif-10)#
Switch(config-vlanif-10)#ip pim-dm
```

7.4.19 ip pim bsr-boundary group

Function

The **ip pim bsr-boundary group** command sets a BSR boundary on interfaces.

The **no ip pim bsr-boundary group** command removes the BSR boundary from interfaces.

Format

- **ip pim bsr-boundary group** *group-address/mask-len*
- **ip pim bsr-boundary group default**
- **no ip pim bsr-boundary group** *group-address/mask-len*
- **no ip pim bsr-boundary group default**

Parameter

Parameter	Description	Value
group-address	Specifies the group address	The value is in dotted decimal notation.
mask-len	Specifies the address mask.	The value is in dotted decimal notation.

Default Value

By default, no BSR boundary is configured on interfaces.

View

VLANIF configuration view

Usage Guidelines

With a BSR boundary configured, the interface only receives bootstrap messages but does not send any bootstrap messages.

Example

Set the BSR boundary for group range 225.0.0.1/24 on vlan10.

```
Switch(config-vlanif-10)#
Switch(config-vlanif-10)#ip pim bsr-boundary group 225.0.0.1/24
```

7.4.20 ip pim c-bsr group

Function

The **ip pim c-bsr group** command sets an interface as a C-BSR.

The **no ip pim c-bsr group** command removes C-BSR configuration from an interface.

Format

- **ip pim c-bsr group** *group-address/mask-len*
- **ip pim c-bsr group** *group-address/mask-len hash-length len*
- **ip pim c-bsr group** *group-address/mask-len hash-length len priority priority*
- **ip pim c-bsr group default**
- **no ip pim c-bsr group** *group-address/mask-len*
- **no ip pim c-bsr group default**

Parameter

Parameter	Description	Value
group-address	Group address	The value is in dotted decimal notation.
mask-len	Group address mask range	The value is in dotted decimal notation.
len	Specifies the hash mask length for this C-BSR.	The value is an integer ranging from 0 to 32. Default: 0.
priority	Priority of C-BSR	The value is an integer ranging from 0 to 255. Default value: 0.

Default Value

By default, no C-BSR is configured on interfaces.

View

VLANIF configuration view, loopback interface configuration view

Usage Guidelines

The PIM-SM network dynamically elects RPs by means of the BSR mechanism. Elected from C-BSRs, the BSR is responsible for collecting and advertising RP information in the PIM-SM domain. All the devices in the network are able to compute the RPs corresponding to a specific multicast group based on the RPs. Because a large amount of information needs to be exchanged

between a BSR and other devices in the PIM-SM domain, a relatively large bandwidth should be provided between the C-BSRs and other devices in the PIM-SM domain.

The BSR election process is summarized as follows:

Initially, every C-BSR assumes itself to be the BSR of its own PIM-SM domain and uses the `c-bsr` command to specify an interface IP address as the BSR address to send bootstrap messages.

When a C-BSR receives a bootstrap message of another C-BSR, it first compares its own priority with the other C-BSR's priority carried in the message. The C-BSR with a higher priority wins. If a tie exists in the priority, the C-BSR with a higher IP address wins. The loser uses the winner's BSR address to replace its own BSR address and no longer assumes itself to be the BSR, and the winner retains its own BSR address and continues to assume itself to be the BSR.

Example

Set a C-BSR for group 225.0.0.1/24 on vlan10 with hash length 2 and priority 3.

```
Switch(config-vlanif-10)#
Switch(config-vlanif-10)#ip pim c-bsr group 225.0.0.1/24 hash-length 2 priority 3
```

7.4.21 ip pim c-rp group

Function

The **ip pim c-rp group** command sets an interface as a C-RP.

The **no ip pim c-rp group** command removes C-RP configuration from an interface.

Format

- **ip pim c-rp group** *group-address/mask-len*
- **ip pim c-rp group** *group-address/mask-len* **priority** *priority*
- **ip pim c-rp group default**
- **no ip pim c-rp group** *group-address/mask-len*
- **no ip pim c-rp group default**

Parameter

Parameter	Description	Value
group-address	Group address	The value is in dotted decimal notation.
mask-len	Group address mask range	The value is in dotted decimal notation.
priority	Priority of C-RP	The value is an integer ranging from 0 to 255. Default value: 0.

Default Value

By default, no C-RP is configured on interfaces.

View

VLANIF configuration view, loopback interface configuration view

Usage Guidelines

An RP is the core of the PIM-SM network, so the C-RP should maintain good connectivity with all other devices. It is recommended that the C-RP be configured on the backbone device and that a large communication bandwidth be reserved between this device and other devices.

The rules to elect an RP from multiple C-RPs are as follows:

The C-RP with the longest mask length of the served group address range matching the multicast group that users have joined wins.

If the length is the same, the C-RP with the highest priority wins (the larger the numerical priority value, the lower the priority).

If a tie exists in the priority, the hash function is executed and the C-RP with the largest hash value wins.

If all of the above are equal, the C-RP with the largest address wins.

Example

Configure vlan10 as C-RP for group 225.0.0.1/24 with priority 5.

```
Switch(config-vlanif-10)#
Switch(config-vlanif-10)#ip pim c-rp group 225.0.0.1/24 priority 5
```

7.4.22 ip pim dr-priority**Function**

The **ip pim dr-priority** command sets the priority for an interface to be elected as a DR.

The **ip pim dr-priority default** command restores the default value.

Format

- **ip pim dr-priority priority**
- **ip pim dr-priority default**

Parameter

Parameter	Description	Value
priority	Specifies the DR priority.	The value is an integer ranging from 0 to 4294967295. Default: 1.

Default Value

By default, the DR priority of the interface is 1.

View

VLANIF configuration view

Usage Guidelines

A designated router (DR) needs to be elected on a shared network segment in PIM-SM, which allows registration of local multicast sources and joining of receivers.

The DR is elected based on priority and IP address. Switches send Hello messages to each other with priority parameters to be elected as a DR. The switch with the highest priority wins. If a tie exists in the priority, the switch with a larger IP address wins.

Example

Set the priority of vlan10 to 10 for DR election.

```
Switch(config-vlanif-10)#
Switch(config-vlanif-10)#ip pim dr-priority 10
```

7.4.23 ip pim silent

Function

The **ip pim silent enable** command enables PIM Silent on interfaces.

The **ip pim silent disable** command disables PIM Silent on interfaces.

Format

- **ip pim silent enable**
- **ip pim silent disable**

Parameter

NA

Default Value

By default, PIM Silent is disabled on interfaces.

View

VLANIF configuration view

Usage Guidelines

If this command is run, the interface will not elect a DR and assume itself as the DR.

Example

Enable PIM Silent on vlan10.

```
Switch(config-vlanif-10)#
Switch(config-vlanif-10)#ip pim silent enable
```

7.4.24 ip pim hello-interval

Function

The **ip pim hello-interval** command sets the interval at which the PIM interface sends Hello messages.

The **ip pim hello-interval default** command restores the default value.

Format

- **ip pim hello-interval interval**
- **ip pim hello-interval default**

Parameter

Parameter	Description	Value
interval	Specifies the interval for sending Hello messages, in seconds.	The value is an integer ranging from 1 to 65535.

Default Value

By default, the interval at which the PIM interface sends Hello messages is 30s.

View

VLANIF configuration view

Usage Guidelines

Switches in a PIM-SM network need to maintain PIM neighbor relationships through periodic Hello messages.

Example

Configure the period for sending Hello messages on vlan10 is 60s.

```
Switch(config-vlanif-10)#ip pim-sm(pim-dm)
Switch(config-vlanif-10)#ip pim hello-interval 60
```

7.4.25 ip pim hello-option holdtime

Function

The **ip pim hello-option holdtime** command sets the holdtime for the PIM interface to wait to receive a Hello message from its neighbor.

The **ip pim hello-option holdtime default** command restores the default value.

Format

- **ip pim hello-option holdtime interval**
- **ip pim hello-option holdtime default**

Parameter

Parameter	Description	Value
interval	Holdtime, in seconds	The value is an integer ranging from 1 to 65535.

Default Value

By default, the holdtime for the PIM interface to wait to receive a Hello message from its neighbor is 105s.

View

VLANIF configuration view

Usage Guidelines

If the switch does not receive a Hello message from the PIM neighbor within the holdtime, the neighbor is considered disabled or unreachable. If the switch needs to quickly sense PIM neighbor changes, the holdtime can be set shorter. However, it should always be greater than the interval for sending Hello messages configured on the PIM neighbor.

Example

Set the holdtime on vlan10 for waiting to receive a Hello message to 120s.

```
Switch(config-vlanif-10)#ip pim-sm(pim-dm)
Switch(config-vlanif-10)#ip pim hello-option holdtime 120
```


7.4.26 ip pim hello-option override-interval

Function

The **ip pim hello-option override-interval** command sets the interval for overriding the prune action in a Hello message sent from the PIM interface.

The **ip pim hello-option override-interval default** command restores the default value.

Format

- **ip pim hello-option override-interval interval**
- **ip pim hello-option override-interval default**

Parameter

Parameter	Description	Value
interval	Specifies the interval for overriding the prune action in a Hello message sent from the PIM interface.	The value is an integer that ranges from 1 to 65535, in milliseconds.

Default Value

By default, the interval for overriding the prune action in a Hello message sent from the PIM interface is 2500 ms.

View

VLANIF configuration view

Usage Guidelines

Hello messages sent by the switch carry lan-delay and override-interval. The override-interval parameter refers to the period during which a downstream switch module overrides the prune action and lan-delay refers to the delay time for transmitting messages within the LAN.

When a device receives a Prune message from an upstream interface, it indicates that there are other downstream switches in the LAN. If this device still requests the multicast data, it needs to send a Join message to the upstream interface in the override-interval period.

When receiving a Prune message from a downstream interface, the switch does not perform the prune action until the PPT times out. The value of PPT is obtained by the value of lan-delay plus the value of override-interval. If the switch receives a Join message from the downstream interface in PPT, the interface cancels the Prune action.

Example

Set the interval for overriding the prune action in a Hello message sent from vlan10 to 1000 ms.

```
Switch(config-vlanif-10)#ip pim-sm(pim-dm)
Switch(config-vlanif-10)#ip pim hello-option override-interval 1000
```

7.4.27 ip pim hello-option prune-delay

Function

The **ip pim hello-option prune-delay** command sets the delay of the PIM interface in transmitting Prune messages in a shared network.

The **ip pim hello-option prune-delay default** command restores the default value.

Format

- **ip pim hello-option prune-delay interval**
- **ip pim hello-option prune-delay default**

Parameter

Parameter	Description	Value
interval	Specifies the delay of the PIM interface in transmitting Prune messages in the shared network.	The value is an integer that ranges from 1 to 32767, in milliseconds.

Default Value

By default, the delay of the PIM interface in transmitting Prune messages in the shared network is 500 ms.

View

VLANIF configuration view

Usage Guidelines

Hello messages sent by the switch carry lan-delay and override-interval. The override-interval parameter refers to the period during which a downstream switch module overrides the prune action and lan-delay refers to the delay time for transmitting messages within the LAN.

When a device receives a Prune message from an upstream interface, it indicates that there are other downstream switches in the LAN. If this device still requests the multicast data, it needs to send a Join message to the upstream interface in the override-interval period.

When receiving a Prune message from a downstream interface, the switch does not perform the prune action until the PPT times out. The value of PPT is obtained by the value of `lan-delay` plus the value of `override-interval`. If the switch receives a Join message from the downstream interface in PPT, the interface cancels the Prune action.

Example

Set the delay of vlan10 in transmitting Prune messages in the shared network to 1000 ms.

```
Switch(config-vlanif-10)#ip pim-sm(pim-dm)
Switch(config-vlanif-10)#ip pim hello-option prune-delay 1000
```

7.4.28 ip pim join-prune holdtime

Function

The **ip pim join-prune holdtime** command sets the holdtime in a Join/Prune message sent by the PIM interface.

The **ip pim join-prune holdtime default** command restores the default value.

Format

- **ip pim join-prune holdtime interval**
- **ip pim join-prune holdtime default**

Parameter

Parameter	Description	Value
interval	Specifies the value of holdtime in a Join/Prune message sent by the PIM interface.	The value is an integer ranging from 1 to 65535, in seconds.

Default Value

By default, the holdtime in a Join/Prune message sent by the PIM interface is 210s.

View

VLANIF configuration view

Usage Guidelines

After an upstream switch receives a Join/Prune message from its downstream interface, the holdtime value determines how long the downstream interface remains in the Join or Prune state.

The holdtime of Join/Prune messages must be larger than the interval for sending Join/Prune messages.

Example

Set the holdtime in a Join/Prune message sent by the vlan10 to 150s.

```
Switch(config-vlanif-10)#ip pim-sm
Switch(config-vlanif-10)#ip pim join-prune holdtime 150
```

7.4.29 ip pim join-prune interval

Function

The **ip pim join-prune interval** command sets interval for the PIM interface to send Join/Prune messages to an upstream interface.

The **ip pim join-prune interval default** command restores the default value.

Format

- **ip pim join-prune interval interval**
- **ip pim join-prune interval default**

Parameter

Parameter	Description	Value
interval	Specifies the interval for the PIM interface to send Join/Prune messages to an upstream interface.	The value is an integer ranging from 1 to 65535, in seconds.

Default Value

By default, the interval for the PIM interface to send Join/Prune messages to an upstream interface is 60s.

View

VLANIF configuration view

Usage Guidelines

The interval at which the PIM interface sends Join/Prune messages upstream must be less than the holdtime value of the Join/Prune message.

Example

Set the interval for sending Join/Prune messages to 80s on vlan10.

```
Switch(config-vlanif-10)#ip pim-sm
Switch(config-vlanif-10)#ip pim join-prune interval 80
```

7.4.30 ip pim graft retry-time

Function

The **ip pim graft retry-time** command sets the time interval for enabling retransmission of graft messages for PIM-DM interfaces.

Format

- **ip pim graft retry-time default**
- **ip pim graft retry-time** *interval*

Parameter

Parameter	Description	Value
interval	Specifies the interval for retransmitting graft messages.	The value is an integer ranging from 1 to 65535.

Default Value

By default, the interval for retransmitting graft messages on an interface with PIM-DM enabled is 3s.

View

VLANIF configuration view

Usage Guidelines

This command sets the time interval for retransmitting graft messages to the PIM-DM interface on the device. If no graft acknowledgement message is received from the upstream within the specified time, the graft message is retransmitted, expecting that the graft operation would be acknowledged by the upstream device. By default, the time interval for retransmitting graft messages is 3s, in the range of 1 to 65535.

Example

Set the interval for retransmitting graft messages to 10s in VLAN10 view.

```
Switch(config-vlanif-10)#ip pim graft retry-time 10
Switch(config-vlanif-10)#
```

7.4.31 ip pim state-refresh-capable

Function

The **ip pim state-refresh-capable** command enables / disables PIM-DM state refresh on an interface.

Format

- **ip pim state-refresh-capable enable**
- **ip pim state-refresh-capable disable**

Parameter

NA

Default Value

By default, PIM-DM state refresh is enabled in VLAN views.

View

VLANIF configuration view

Usage Guidelines

This command enables / disables the state refresh on the VLANIF interface with PIM-DM enabled on the switch. If state refresh is enabled, the switch directly connected to the source sends state refresh messages periodically through a PIM-DM enabled VLANIF interface. If state refresh is disabled, the switch does not send any state refresh messages.

Example

Enable PIM-DM state refresh in VLAN10 view.

```
Switch(config-vlanif-10)#ip pim state-refresh-capable enable
Switch(config-vlanif-10)#
```

7.4.32 reset pim routing-table

Function

The **reset pim routing-table** command removes all route entries in the PIM instance.

Format

- **reset pim routing-table**

Description

NA

Default Value

NA

View

PIM instance view

Usage Guidelines

This command manually deletes all route tables in the corresponding PIM instance.

Example

Delete all route tables in the PIM public network instance.

```
Switch(config-pim)#reset pim routing-table
Switch(config-pim)#
```

7.4.33 debug pim**Function**

The **debug pim** command enables PIM debugging.

The **no debug pim** command disables PIM debugging.

Format

- **debug pim { all | bsr | error | graft | hardware | hello | igmp | interface | join-prune | message | msdp | neighbor | packet | register | route | rp | srm | sync }**

Parameter

Parameter	Description	Value
all	All PIM debugging information	-
bsr	BSR-related debugging information	-
error	Error debugging information	-
graft	Graft debugging information	-
hardware	Hardware debugging information	-
hello	Debugging information of hello messages	-
igmp	Debugging information of IGMP communication	-
interface	Interface debugging information	-
join-prune	Join-prune debugging information	-
message	Debugging information of received packets	-
msdp	MSDP debugging information	-
neighbor	Debugging information of neighbors	-

Parameter	Description	Value
packet	Debugging information of received packets	-
register	Debugging information of registration	-
route	Debugging information of route tables	-
rp	Debugging information of RP	-
srm	Debugging information of state fresh	-
sync	Debugging information of synchronization	-

Default Value

By default, PIM debugging is disabled.

View

Privileged user view

Usage Guidelines

This command is used to maintain and debug the PIM function of the switch.

Example

Enable synchronized PIM debugging.

```
Switch#debug pim sync
Switch#
```

7.4.34 show ip pim config

Function

The **show ip pim config** command displays PIM-related configuration information.

Format

- **show ip pim config**

Parameter

NA

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

Displays PIM-related configuration information.

```
Switch>show ip pim config
!
ip multicast-routing
pim
  c-rp hold-time 90
  spt-switch enable
  rp-address 10.1.1.1 group 225.0.0.1/24
pim vpn-instance aa
  spt-switch enable
```

7.4.35 show ip pim anycast-rp**Function**The **show ip pim anycast-rp** command displays information about PIM's anycast RPs.**Format**

- **show ip pim anycast-rp**

Parameter

NA

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

Display information about PIM's anycast RPs.

```
Switch>show ip pim anycast-rp
Vpn-Instance: public net
  Anycast RP      :10.1.1.1
  Local Address   :2.2.2.2
```

Peer Address	:3.3.3.3

7.4.36 show ip pim bsr

Function

The **show ip pim bsr** command displays BSR information of the PIM.

Format

- **show ip pim bsr**

Parameter

NA

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

Display BSR information of the PIM.

```
Switch>show ip pim bsr
Vpn-Instance: public net
  BSR Address           :10.1.1.1
  BSR Group              :225.0.0.1
  BSR Mask Length        :24
  BSR Priority            :3
  BSR Hash Length        :2
  BSR Expire Time        :0s
  BSR C-RP Count         :1
  CBSR Address           :10.1.1.1
  CBSR Priority           :3
  CBSR Hash Length       :2
```

7.4.37 show ip pim c-rp

Function

The **show ip pim c-rp** command displays C-RP information of the PIM.

Format

- **show ip pim c-rp**

Parameter

NA

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

Display C-RP information of the PIM.

```
Switch>show ip pim c-rp
Vpn-Instance: public net
  C-RP Address           :10.1.1.1
  C-RP Group             :225.0.0.1
  C-RP Mask Length       :24
  C-RP Priority           :5
  C-RP BSR Address       :10.1.1.1
```

7.4.38 show ip pim interface**Function**The **show ip pim interface** command displays information about the PIM interface.**Format**

- **show ip pim interface**
- **show ip pim interface vlan *vlan-id***
- **show ip pim interface loopback *loopback-id***

Parameter

Parameter	Description	Value
vlan-id	PIMvlan interface number	-
loopback-id	ID of a PIM-enabled loopback	-

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

Display information about the PIM interface.

Switch>show ip pim interface

Interface	State	Nbr-Cnt	Hello-Interval	DR-Pri	DR-Address
vlan10	up	1	30	100	10.1.1.1

7.4.39 show ip pim neighbor**Function**The **show ip pim neighbor** command displays information about PIM neighbors.**Format**

- **show ip pim neighbor**
- **show ip pim neighbor address**

Parameter

Parameter	Description	Value
address	Specifies the IP address of a PIM neighbor.	The value is in dotted decimal notation.

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

Display information about the PIM neighbor.

Switch>show ip pim neighbor				
Neighbor-Address	Interface	DR priority	State	ExpiryTime(s)
10.1.1.6	vlan10	1	NON-DR	81

7.4.40 show ip pim route

Function

The **show ip pim route** command displays information about the PIM's route table.

The **show ip pim route verbose** command displays details of the PIM's route table.

Format

- **show ip pim route**
- **show ip pim route verbose**
- **show ip pim route group group-address**
- **show ip pim route group group-address verbose**
- **show ip pim route group group-address source address**
- **show ip pim route group group-address source address verbose**
- **show ip pim route source address**
- **show ip pim route source address verbose**
- **show ip pim route vpn-instance**
- **show ip pim route vpn-instance verbose**
- **show ip pim route vpn-instance vpn-name**
- **show ip pim route vpn-instance vpn-name verbose**

Parameter

Parameter	Description	Value
group-address	Specifies a group address.	The value is in dotted decimal notation.
address	Specifies a source address.	The value is in dotted decimal notation.
vpn-name	Specifies an instance name.	-

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

Display route table information of the PIM.

```
Switch>show ip pim route
Vpn-Instance: public net
(*,225.0.0.1):  RP: 10.1.1.1
Incoming Interface: N/A, RPF: N/A
Outgoing Interface:
vlan10          Forwarding Expires: 00:00:00
```

7.4.41 show ip pim rp

Function

The **show ip pim rp** command displays information about the RP of the PIM.

The **show ip pim rp group** command displays information about the RP elected by a specific PIM group.

Format

- **show ip pim rp**
- **show ip pim rp group group-address**

Parameter

Parameter	Description	Value
group-address	Specifies a group address.	The value is in dotted decimal notation.

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

Display RP information of the PIM.

```
Switch>show ip pim rp
Group                RP                Priority    State    BSR-Address
ExpiryTime(s)
Vpn-Instance: public net
225.0.0.1/24        10.1.1.1          5          no-static 10.1.1.1    0
```

7.4.42 show ip pim statistic

Function

The **show ip pim rp** command displays statistics of packets sent and received by the PIM.

Format

- **show ip pim statistic interface**
- **show ip pim statistic interface vlan vlan-id**
- **show ip pim statistic vpn-instance**

Parameter

Parameter	Description	Value
vlan-id	Specifies a VLAN ID.	-

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

Display statistics of packets sent and received by the PIM instance.

```
Switch>show ip pim statistic vpn-instance
Vpn-Instance: public net
Total Receive Packets: 0
Receive Hello          :0
Receive Join-Prune     :0
Receive Assert         :0
Receive Bootstrap      :0
```

```

Receive Srm           :0
Receive Crp-Adv       :0
Receive Register      :0
Receive Register-Stop :0
Receive Graft         :0
Receive Graft-Ack     :0
Receive Bad Packets   :0
Total Send Packets: 0
Send Hello           :0
Send Join-Prune       :0
Send Assert          :0
Send Bootstrap        :0
Send Srm             :0
Send Crp-Adv         :0
Send Register        :0
Send Register-Stop    :0
Send Graft           :0
Send Graft-Ack       :0
Multicast Data: 0
IGMP Message Count: 0
MSDP Message Count: 0

```

7.4.43 show ip pim vpn-instance

Function

The **show ip pim vpn-instance** displays information about the PIM instance.

Format

- **show ip pim vpn-instance**

Parameter

NA

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

Display information about the PIM instance.

```
Switch>show ip pim vpn-instance
Vpn-Instance                :public net
SPT Switch                  :enable
SPT Threshold                :0
SPT Switch Checksum Interval :15(s)
Admin Scope                  :disable
Register Extension Checksum  :disable
Register Fragment           :disable
Register Suppress Time       :60(s)
Register Probe Interval      :60(s)
Register MTU                 :1500
Send Checksum Neighbor       :enable
Receive Checksum Neighbor    :enable
Accept Unknown RP            :disable
BSR Send Interval            :60(s)
C-RP Send Interval           :60(s)
C-RP Hold Time               :90(s)
Assert Time                  :180(s)
State Refresh TTL            :255
State Refresh Interval        :60(s)
State Refresh Rate Limit     :30(s)
Source Life Time              :210(s)
C-RP State                   :NO
Current Interface Count       :1
Current Route Count           :0
Current RP Count              :1
Current C-RP Count            :0
Current Scope Count           :0
Current Anycast-RP Count     :0
```

Chapter 8 Service Security Commands

This chapter introduces the commands for configuring security functions on the Switch, including Time-range, ACL, Anti-attack, AAA/Radius, 802.1x, and defense.

8.1 Time-range Configuration Commands

8.1.1 debug time-range

Function

The **debug time-range** command enables time-range debugging.

The **no debug time-range** command disables time-range debugging.

Format

- **debug time-range**
- **no debug time-range**

Parameter

NA

Default Value

By default, time-range debugging is disabled.

View

Privileged user view

Usage Guidelines

NA

Example

Enable time-range debugging.

```
Switch#debug time-range
Switch#
```

8.1.2 name

Function

The **name** command sets the descriptive name for a specified time-range module.

Format

name *name*

Parameter

Parameter	Description	Value
name	Specifies the descriptive name for a specified time-range module.	The value consists of 1 to 63 characters.

Default Value

NA

View

Time-range configuration view

Usage Guidelines

You can run this command to set the descriptive name for a specified time-range module.

Example

Set the name of the time-range list 1 module to test.

```
Switch(config-timerange1)#name test
Switch(config-timerange1)#
```

8.1.3 time-range list

Function

The **time-range list** command enters a time-range module.

The **no time-range list** command deletes the configuration of the time-range module.

Format

- **time-range list** *list-number*
- **no time-range list** *list-number*

Parameter

Parameter	Description	Value
list-number	Specifies the name of a time-range module list.	The value is an integer ranging from 1 to 128.

Default Value

NA

View

Global configuration view

Usage Guidelines

You can run this command to enter a time-range module.

You can run this command together with ACL to set an ACL time-range list for a device.

Example

Enter the time-range module of the list 1.

```
Switch(config)#time-range list 1
Switch(config-timerange1)#
```

8.1.4 no time-range**Function**

The **no time-range** command deletes the range configuration from a specified time-range module.

Format

no time-range *range-number*

Parameter

Parameter	Description	Value
range-number	Specifies a range number.	The value is an integer ranging from 1 to 16.

Default Value

NA

View

Time-range configuration view

Usage Guidelines

NA

Example

Delete the configuration of range 10 from the time-range module in the list 1.

```
Switch(config-timerange1)#no time-range 10
Switch(config-timerange1)#
```

8.1.5 time-range absolute

Function

The **time-range absolute** command sets the absolute start and end time of a time-range module.

Format

time-range *range-number* **absolute** { **from** | **to** } *hh:mm:ss YY/MM/DD*

Parameter

Parameter	Description	Value
range-number	Specifies a range number.	The value is an integer ranging from 1 to 16.
hh:mm:ss	Specifies the start or end time, in the format of hh:mm:ss.	The value is an integer ranging <0-23>:<0-59>:<0-59>.
YY/MM/DD	Specifies the start or end time, in the format of yy:mm:dd.	The value is an integer ranging <2001-2036>:<1-12>:<1-31>.

Default Value

NA

View

Time-range configuration view

Usage Guidelines

NA

Example

Set the start and end time of the time-range module to 1:1:1 2018/1/1 and 2:2:2 2019/2/2 respectively.

```
Switch(config-timerange1)#time-range 10 absolute from 1:1:1 2018/1/1 to 2:2:2 2019/2/2
Switch(config-timerange1)#
```

8.1.6 time-range everyday

Function

The **time-range everyday** command sets the daily time range of a time-range module.

Format

time-range *range-number* **everyday** *hh:mm:ss to hh:mm:ss*

Parameter

Parameter	Description	Value
range-number	Specifies a range number.	The value is an integer ranging from 1 to 16.
hh:mm:ss	Specifies the start or end time, in the format of hh:mm:ss.	The value is an integer ranging <0-23>:<0-59>:<0-59>.

Default Value

NA

View

Time-range configuration view

Usage Guidelines

NA

Example

Set the start and end time of the time-range module to 11:11:11 to 22:22:22.

```
Switch(config-timerange1)#time-range 10 everyday 11:11:11 to 22:22:22
Switch(config-timerange1)#
```

8.1.7 time-range everyhour

Function

The **time-range everyhour** command sets the hourly time range of a time-range module.

Format

time-range *range-number* **everyhour** *mm:ss to mm:ss*

Parameter

Parameter	Description	Value
range-number	Specifies a range number.	The value is an integer ranging from 1 to 16.
mm:ss	Specifies the start or end time, in the format of mm:ss.	The value is an integer in the range of<0-59>:<0-59>.

Default Value

NA

View

Time-range configuration view

Usage Guidelines

NA

Example

Set the start and end time of the time-range module to 33:33 to 44:44.

```
Switch(config-timerange1)#time-range 10 everyhour 33:33 to 44:44
Switch(config-timerange1)#
```

8.1.8 time-range everymonth

Function

The **time-range everymonth** command sets the monthly time range of a time-range module.

Format

time-range *range-number* **everymonth** *hh:mm:ss MM to hh:mm:ss MM*

Parameter

Parameter	Description	Value
range-number	Specifies a range number.	The value is an integer ranging from 1 to 16.
hh:mm:ss	Specifies the start or end time, in the format of hh:mm:ss.	The value is an integer ranging <0-23>:<0-59>:<0-59>.
MM	Specifies a date.	The value is an integer in the range of <1-31>.

Default Value

NA

View

Time-range configuration view

Usage Guidelines

NA

Example

Set the start and end time of the time-range module to 11:11:11 of the first day to 22:22:22 of the second day of every month.

```
Switch(config-timerange1)#time-range 10 everymonth 11:11:11 1 to 22:22:22 2
```

```
Switch(config-timerange1)#
```

8.1.9 time-range everyweek

Function

The **time-range everyweek** command sets the weekly time range of a time-range module.

Format

time-range *range-number* **everyweek** *hh:mm:ss* { **mon** | **tue** | **wed** | **thu** | **fri** | **sat** | **sun** } **to** *hh:mm:ss* { **mon** | **tue** | **wed** | **thu** | **fri** | **sat** | **sun** }

Parameter

Parameter	Description	Value
range-number	Specifies a range number.	The value is an integer ranging from 1 to 16.
hh:mm:ss	Specifies the start or end time, in the format of hh:mm:ss.	The value is an integer ranging <0-23>:<0-59>:<0-59>.
(mon tue wed thu fri sat sun)	Specifies a weekday.	-

Default Value

NA

View

Time-range configuration view

Usage Guidelines

NA

Example

Set the start and end time of the time-range module to 11:11:11 of every Monday to 22:22:22 of every Tuesday.

```
Switch(config-timerange1)#time-range 10 everyweek 11:11:11 mon to 22:22:22 tue
Switch(config-timerange1)#
```

8.1.10 time-range everyweekday

Function

The **time-range everyweekday** command sets the time range on every weekday of a time-range module.

Format

time-range *range-number* **everyweekday** *hh:mm:ss to hh:mm:ss*

Parameter

Parameter	Description	Value
range-number	Specifies a range number.	The value is an integer ranging from 1 to 16.
hh:mm:ss	Specifies the start or end time, in the format of hh:mm:ss.	The value is an integer ranging <0-23>:<0-59>:<0-59>.

Default Value

NA

View

Time-range configuration view

Usage Guidelines

NA

Example

Set the start and end time of the time-range module to 11:11:11 to 22:22:22 on every weekday.

```
Switch(config-timerange1)#time-range 10 everyweekday 11:11:11 to 22:22:22
Switch(config-timerange1)#
```

8.1.11 time-range everyweekend

Function

The **time-range everyweekend** command sets the time range on every weekend of a time-range module.

Format

time-range *range-number* **everyweekend** *hh:mm:ss to hh:mm:ss*

Parameter

Parameter	Description	Value
range-number	Specifies a range number.	The value is an integer ranging from 1 to 16.
hh:mm:ss	Specifies the start or end time, in the format of hh:mm:ss.	The value is an integer ranging <0-23>:<0-59>:<0-59>.

Default Value

NA

View

Time-range configuration view

Usage Guidelines

NA

Example

Set the start and end time of the time-range module to 11:11:11 to 22:22:22 on every weekend.

```
Switch(config-timerange1)#time-range 10 everyweekend 11:11:11 to 22:22:22
Switch(config-timerange1)#
```

8.1.12 time-range everyyear**Function**

The **time-range everyyear** command sets the time range in every year of a time-range module.

Format

time-range *range-number* **everyyear** *hh:mm:ss MM/DD to hh:mm:ss MM/DD*

Parameter

Parameter	Description	Value
range-number	Specifies a range number.	The value is an integer ranging from 1 to 16.
hh:mm:ss	Specifies the start or end time, in the format of hh:mm:ss.	The value is an integer ranging <0-23>:<0-59>:<0-59>.
MM/DD	Specifies the start or end time, in the format of mm:dd.	The value is an integer ranging <1-12>:<1-31>.

Default Value

NA

View

Time-range configuration view

Usage Guidelines

NA

Example

Set the start and end time of the time-range module to 11:11:11 on January 1 to 22:22:22 on February 2 in every year.

```
Switch(config-timerange1)#time-range 10 everyyear 11:11:11 1/1 to 22:22:22 2/2
Switch(config-timerange1)#
```

8.1.13 show time-range config

Function

The **show time-range config** command displays the configuration of all the current time-range modules.

Format

show time-range config

Parameter

NA

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

Display all the configuration of the time-range module.

```
Switch>show time-range config
current time is 02:07:58 2/6/2019 Tuesday
time-range list:10
Switch>
```

8.1.14 show time-range list

Function

The **show time-range list** command displays the list of all or a specified time-range module.

Format

- **show time-range list**
- **show time-range list** *list-number*

Parameter

Parameter	Description	Value
list-number	Specifies the name of a time-range module list.	The value is an integer ranging from 1 to 128.

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

Display all the lists of the time-range module.

```
Switch>show time-range list
current time is 02:22:11 2100-1-1 Friday
time-range list:1
Switch>
```

8.2 IP Address Prefix Filter List Configuration Commands

8.2.1 debug prefix-list {config|match|error|all}

Function

The **debug prefix-list {config|match|error|all}** command enables debugging the IP address prefix filter list.

The **no debug prefix-list {config|match|error|all}** command disables debugging the IP address prefix filter list.

Format

- **debug prefix-list { config | match | error | all }**
- **no debug prefix-list { config | match | error | all }**

Parameter

NA

Default Value

By default, debugging the IP address prefix filter list is disabled.

View

Privileged user view

Usage Guidelines

NA

Example

Enable debugging the IP address prefix filter list.

```
Switch#debug prefix-list all
Switch#
```

8.2.2 ip prefix-list**Function**

The **ip prefix-list** command configures an IPv4 prefix list.

The **no ip prefix-list** command cancels the configuration.

Format

- **ip prefix-list** *list-name* { **deny** | **permit** } *ipv4-address/mask-length*
- **ip prefix-list** *list-name* { **deny** | **permit** } *ipv4-address/mask-length* { **greater-equal** | **less-equal** } *prefix-length*
- **ip prefix-list** *list-name* { **deny** | **permit** } *ipv4-address/mask-length* **greater-equal** *prefix length* **less-equal** *prefix-length*
- **ip prefix-list** *list-name* **index** *index-number* { **deny** | **permit** } *ipv4-address/mask-length*
- **ip prefix-list** *list-name* **index** *index-number* { **deny** | **permit** } *ipv4-address/mask-length* { **greater-equal** | **less-equal** } *prefix-length*
- **ip prefix-list** *list-name* **index** *index-number* { **deny** | **permit** } *ipv4-address/mask-length* **greater-equal** *prefix length* **less-equal** *prefix-length*
- **no ip prefix-list** *list-name*

- **no ip prefix-list** *list-name* **index** *index-number*

Parameter

Parameter	Description	Value
list-name	Specifies the name of a prefix list.	-
deny permit	Specifies the action of allowing or rejecting a packet with the IP address in the list.	-
ipv4-address	Specifies an IPv4 address.	The value is in dotted decimal notation.
mask-length	Specifies the mask length of an IPv4 address.	The value is an integer ranging from 0 to 32.
greater-equal less-equal	Specifies an action taken when the length of a prefix is no longer than or no shorter than the length of the IPv4 address prefix.	-
prefix-length	Specifies a prefix length.	The value is an integer ranging from 0 to 32.
index	Specifies an index.	-
Index-number	Specifies an index number.	The value is an integer ranging from 1 to 65535.

Default Value

NA

View

Global configuration view

Usage Guidelines

NA

Example

Configure the action of permitting entry 123 with IPv4 address 10.10.10.10, mask length 24, and prefix of no shorter than 20.

```
Switch(config)#ip prefix-list 123 permit 10.10.10.10/24 greater-equal 20
Switch(config)#
```

8.2.3 ipv6 prefix-list

Function

The **ipv6 prefix-list** command sets an IPv6 prefix list.

The **no ipv6 prefix-list** command cancels the configuration.

Format

- **ipv6 prefix-list** *list-name* { **deny** | **permit** } *ipv6-address/mask-length* { **greater-equal** | **less-equal** } *prefix-length*
- **ipv6 prefix-list** *list-name* { **deny** | **permit** } *ipv6-address/mask-length* **greater-equal** *prefix length* **less-equal** *prefix-length*
- **ipv6 prefix-list** *list-name* { **deny** | **permit** } *ipv6-address/mask-length*
- **ipv6 prefix-list** *list-name* **index** *index-number* { **deny** | **permit** } *ipv6-address/mask-length*
- **ipv6 prefix-list** *list-name* **index** *index-number* { **deny** | **permit** } *ipv6-address/mask-length* { **greater-equal** | **less-equal** } *prefix-length*
- **ipv6 prefix-list** *list-name* **index** *index-number* { **deny** | **permit** } *ipv6-address/mask-length* **greater-equal** *prefix length* **less-equal** *prefix-length*
- **no ipv6 prefix-list** *list-name*
- **no ipv6 prefix-list** *list-name* **index** *index-number*

Parameter

Parameter	Description	Value
<i>list-name</i>	Specifies the name of a prefix list.	-
<i>deny</i> <i>permit</i>	Specifies the action of allowing or rejecting a packet with the IP address in the list.	-
<i>ipv6-address</i>	Specifies an IPv6 address.	The value is in dotted decimal notation.
<i>mask-length</i>	Specifies the mask length of an IPv6 address.	The value is an integer ranging from 0 to 128.
<i>greater-equal</i> <i>less-equal</i>	Specifies an action taken when the length of a prefix is no longer than or no shorter than the length of the IPv6 address prefix.	-
<i>prefix-length</i>	Specifies a prefix length.	The value is an integer ranging from 0 to 128.
<i>index</i>	Specifies an index.	-
<i>Index-number</i>	Specifies an index number.	The value is an integer ranging from 1 to 65535.

Default Value

NA

View

Global configuration view

Usage Guidelines

NA

Example

Configure the action of permitting entry 123 with IPv6 address 10:10::10:10, mask length 24, and prefix of no shorter than 20.

```
Switch(config)#ipv6 prefix-list 123 permit 10.10::10.10/24 greater-equal 20
Switch(config)#
```

8.2.4 show {ip|ipv6} prefix-list**Function**

The **show ip prefix-list** command displays rules in a rule table. (This command applies to IPv4 networks.)

The **show ipv6 prefix-list** command displays rules in a rule table. (This command applies to IPv6 networks.)

Format

- **show ip prefix-list** [*list-name*]
- **show ipv6 prefix-list** [*list-name*]

Parameter

Parameter	Description	Value
list-name	Specifies the IP type of the table of the created routing rule. It is used to distinguish different tables.	The name must be unique and consists of 1 to 32 characters.

Default Value

NA

View

Common user view

Usage Guidelines

If no rule name is specified, this command displays content of all rule tables with the same address type.

Example

View rules in a rule table.

```
Switch>show ip prefix-list
ip prefix-list : test
  index: 10    permit 1.1.0.0/16
  index: 11    permit 2.2.0.0/16
ip prefix-list : tes
  index: 11    permit 2.2.0.0/16
Switch>
```

8.2.5 show ip prefix-list information

Function

The **show ip prefix-list information** command displays the IP address prefix rule information. (This command applies to IPv4 networks.)

Format

show ip prefix-list information

Parameter

NA

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

View the IP address prefix rule information.

```
Switch>show ip prefix-list information
Version IPPREFIX_VB3.00.00.00
ipprefix global structure size 184
RouteSocket=3
```

Memory Statistics

Configuration Params:

List:32

Rule:256

Total Allocate memory:28672 Bytes

Detailed Memory Operation

Index	Add	Fail	Free	Current	Size	Description
0	0	0	0	0	224	Ip Prefix List
1	0	0	0	0	84	Ip Prefix Rule

Switch>

8.3 ACL Configuration Commands

8.3.1 filter action {permit|deny}

Function

The **filter action {permit|deny}** command sets the action for an ACL rule to permit or deny, which means to forward or drop packets matching the rule.

Format

filter *rule-number* **action** { **permit** | **deny** }

Parameter

Parameter	Description	Value
rule-number	Specifies an ACL rule number.	The value is an integer ranging from 1 to 2048.
permit	Permits packets in compliance with the ACL rule.	-
deny	Denies packets in compliance with the ACL rule.	-

Default Value

NA

View

L2 Filter configuration view, Filter configuration view, filter-hybrid configuration view, Filter configuration view (IPv6)

Usage Guidelines

If the action defined in the ACL rule is **deny**, a packet matching the ACL rule will be dropped.

If the action defined in the ACL rule is **permit**, a packet matching the ACL rule will be forwarded or processed.

Example

Set the action in rule 1 of ACL 100 to deny.

```
Switch(configure-filter-l2-100)#filter 100 action deny
Switch(configure-filter-l2-100)#
```

8.3.2 filter action {cos|precedence|priority}

Function

The **filter action {cos|precedence|priority}** command sets the action for an ACL rule to set the priority of packets in a port queue or change most significant three bits in the Precedence field of IP packets.

Format

filter *rule-number* **action** { **cos** | **precedence** } *priority-value*

Parameter

Parameter	Description	Value
rule-number	Specifies an ACL rule number.	The value is an integer ranging from 1 to 2048.
cos	Specifies the priority of packets in a port queue.	-
precedence	Specifies the three most significant bits in the TOS field of an IP packet.	-
priority-value	Specifies the value of the CoS, precedence, and priority fields.	The value is an integer ranging from 0 to 7.

Default Value

NA

View

L2 Filter configuration view, Filter configuration view, filter-hybrid configuration view, Filter configuration view (IPv6)

Usage Guidelines

NA

Example

Configure the action for an ACL rule.

```
Switch(configure-filter-l2-3050)#filter 2 action cos 1
Switch(configure-filter-l2-3050)#
Switch(configure-filter-l2-3050)#filter 2 action precedence 2
Switch(configure-filter-l2-3050)#
```

8.3.3 filter action counter**Function**

The **filter action counter** command configures a QoS traffic counter to measure traffic of a specified data flow.

Format

filter *filter-rule-number* **action counter** *counter-number*

Parameter

Parameter	Description	Value
filter-rule-number	Specifies a filter rule number.	The value is an integer ranging from 1 to 2048.
counter-number	Specifies a counter number.	The value is an integer ranging from 1 to 1024.

Default Value

NA

View

L2 Filter configuration view, Filter configuration view, filter-hybrid configuration view, Filter configuration view (IPv6)

Usage Guidelines

Traffic measurement can measure packets of a specified data flow, that is, data information in a forwarded packet matching the pre-defined flow rule.

You must configure a counter using the **counter** command and bind it to the filter.

```
Switch(config)#counter 100 all sort total
```

```
Switch(config)#
```

```
Switch(config)#filter-list 100
```

```
Switch(configure-filter-l2-100)#
```

```
Switch(configure-filter-l2-3050)#(configure-filter-l2-100)#filter 100 mac any any
```

```
Switch(configure-filter-l2-100)#
```

If different counters are configured, you need to unbind the previously bound counter. Otherwise, the following symptom may occur:

```
Switch(configure-filter-l2-100)#filter 100 action counter 200
```

%Cannot modify, please release the counter from filter firstly.

Before entering the filter list, enter the ACL, which can be an L2 ACL, IPv4 ACL, hybrid ACL, or IPv6 ACL.

Example

Set the QoS traffic counter.

```
Switch(configure-filter-l2-100)#filter 100 action counter 100
```

```
Switch(configure-filter-l2-100)#
```

8.3.4 filter action cpu

Function

The **filter action cpu** command sets the action for an ACL rule to CPU forwarding, which means to forward packets matching the rule to the CPU only.

Format

filter *rule-number* **action cpu**

Parameter

Parameter	Description	Value
rule-number	Specifies an ACL rule number.	The value is an integer ranging from 1 to 2048.
cpu	Indicates that only packets matching the rule are forwarded to the CPU for processing.	-

Default Value

NA

View

L2 Filter configuration view, Filter configuration view, filter-hybrid configuration view, Filter configuration view (IPv6)

Usage Guidelines

After this command is executed, the switch forwards a packet that matches the ACL rule to the CPU.

Example

Set the action for rule 2 of ACL 100 to CPU forwarding.

```
Switch(configure-filter-l2-100)#filter 2 action cpu
Switch(configure-filter-l2-100)#
```

8.3.5 filter action dscp**Function**

The **filter action dscp** command set the action for an ACL rule to Differentiated Services CodePoint (DSCP) re-marking, which means to change the DSCP field (most significant six bits of the ToS field) value of IP packets matching the rule.

Format

filter *rule-number* **action dscp** *dscp-value*

Parameter

Parameter	Description	Value
rule-number	Specifies an ACL rule number.	The value is an integer ranging from 1 to 2048.
dscp-value	Specifies the Differentiated Services Code Point (DSCP) value of packets.	The DSCP value is an integer or a name. When the value is an integer, it ranges from 0 to 63. When the value is a name, it is af11, af12, af13, af21, af22, af23, af31, af32, af33, af41, af42, af43, cs1, cs2, cs3, cs4, cs5, cs6, cs7, default, or ef.

Default Value

NA

View

L2 Filter configuration view, Filter configuration view, filter-hybrid configuration view, Filter configuration view (IPv6)

Usage Guidelines

After this command is executed, the switch changes the DSCP field in a received packet that matches the ACL rule to the configured value. For details about DSCP priorities, see the parameter description.

Example

Set the action for an ACL rule to DSCP re-marking (changing the value of the most significant six bits of the ToS field) for IP data packets matching the rule.

```
Switch(configure-filter-l2-100)#filter 2 action dscp 20
Switch(configure-filter-l2-100)#
```

8.3.6 filter action insert-inner-vid|insert-outer-vid

Function

The **filter action insert-inner-vid|insert-outer-vid** command sets an action for an ACL rule to insert an inner VLAN tag or replace the value of the inner VLAN ID.

Format

filter *rule-number* **action** { **insert-inner-vid** | **insert-outer-vid** } *vlan-id*

Parameter

Parameter	Description	Value
rule-number	Specifies an ACL rule number.	The value is an integer ranging from 1 to 2048.
vlan-id	Specifies the VLAN ID to be inserted or replace the original outer VLAN ID.	The value is an integer ranging from 1 to 4094.
insert-outer-vid	Inserts an outer VLAN tag.	-
insert-inner-vid	Inserts an inner VLAN tag.	-

Default Value

NA

View

L2 Filter configuration view, Filter configuration view, filter-hybrid configuration view, Filter configuration view (IPv6)

Usage Guidelines

After this command is executed, the system inserts a VLAN tag or replaces the original outer/inner VLAN tag in the received data packets matching the ACL rule.

Example

Set an action for an ACL rule to insert an inner VLAN tag.

```
Switch(configure-filter-l2-100)#filter 2 action insert-inner-vid 10
Switch(configure-filter-l2-100)#
```

8.3.7 filter action mirror

Function

The **filter action mirror** command mirrors streams matching the rule to a specified image group or CPU.

Format

filter *filter-rule-number* **action mirror** **group** *group-number*

Parameter

Parameter	Description	Value
filter-rule-number	Specifies a filter rule number.	The value is an integer ranging from 1 to 2048.
group-number	Specifies a group number.	The value is an integer ranging from 1 to 10.

Default Value

NA

View

L2 Filter configuration view, Filter configuration view, filter-hybrid configuration view, Filter configuration view (IPv6)

Usage Guidelines



Caution

The source port of traffic mirroring cannot be a Trunk interface.

Example

Mirror streams matching the rule to a CPU.

```
Switch(configure-filter-l2-100)#filter 100 action mirror cpu
Switch(configure-filter-l2-100)#
```

8.3.8 filter action redirect cpu

Function

The **filter action redirect cpu** command sets the action for an ACL rule to packet redirection to the CPU.

Format

filter *rule-number* **action redirect cpu**

Parameter

Parameter	Description	Value
rule-number	Specifies an ACL rule number.	The value is an integer ranging from 1 to 2048.
cpu	Indicates that only packets matching the rule are forwarded to the CPU for processing.	-

Default Value

NA

View

L2 Filter configuration view, Filter configuration view, filter-hybrid configuration view, Filter configuration view (IPv6)

Usage Guidelines

After this command is executed, the switch forwards a packet that matches the ACL rule to the CPU.

Example

Set the action for rule 2 of ACL 100 to CPU forwarding.

```
Switch(configure-filter-l2-100)#filter 2 action redirect cpu
Switch(configure-filter-l2-100)#
```

8.3.9 filter action redirect

{ethernet|xgigaethernet|10gigaethernet|25gigaethernet|40gigaethernet|100gigaethernet}

Function

The **filter action redirect**

{ethernet|xgigaethernet|10gigaethernet|25gigaethernet|40gigaethernet|100gigaethernet}

command sets the action for an ACL rule to packet redirection to a specified port.

Format

- **filter rule-number action redirect { ethernet | xgigaethernet | 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet } interface-number**
- **filter rule-number action redirect eth-trunk trunk-number**

Parameter

Parameter	Description	Value
rule-number	Specifies an ACL rule number.	The value is an integer ranging from 1 to 2048.

Parameter	Description	Value
interface-number	Redirects a packet to a specified port.	The value is an integer in the range of <1-1>/<0-1>/<1-48> (For reference only. The specific value range depends on the slot number and card type).
trunk-number	Specifies an aggregation interface number.	The value is an integer ranging from 1 to 128.

Default Value

NA

View

L2 Filter configuration view, Filter configuration view, filter-hybrid configuration view, Filter configuration view (IPv6)

Usage Guidelines

After this command is executed, the switch redirects a packet that matches the ACL rule to a specified port. The ACL including the redirection action can only be applied in the inbound direction.

Redirection process: Upon receiving a packet, the switch performs VLAN, L2, and L3 processing, redirects the packet to the specified port, and stops forwarding the original packet.

Example

Set the action for the ACL rule to redirection of data packets to a specified interface.

```
Switch(configure-filter-l2-100)#filter 100 action redirect xgigaethernet 1/0/1
Switch(configure-filter-l2-100)#
```

8.3.10 filter action

{replace-inner-vid|replace-outer-vid|remove-inner-vid|remove-outer-vid}

Function

The **filter action {replace-inner-vid|replace-outer-vid}** command sets an action for an ACL rule to insert an outer VLAN tag or replace the value of the outer VLAN ID.

The **remove-inner-vid** command sets an action for an ACL rule to delete the inner VLAN tag.

The **remove-outer-vid** command sets an action for an ACL rule to delete the outer VLAN tag.

Format

- **filter** *rule-number* **action** **replace-inner-vid** *vlan-id*

- **filter rule-number action replace-outer-vid** *vlan-id*
- **filter rule-number action remove-inner-vid**
- **filter rule-number action remove-outer-vid**

Parameter

Parameter	Description	Value
rule-number	Specifies an ACL rule number.	The value is an integer ranging from 1 to 2048.
vlan-id	Specifies the VLAN ID to be inserted or replace the original outer VLAN ID.	The value is an integer ranging from 1 to 4094.
replace-outer-vid	Replaces the outer VLAN tag.	-
replace-inner-vid	Replaces an inner VLAN tag.	
remove-outer-vid	Deletes an outer VLAN tag.	
remove-inner-vid	Deletes an inner VLAN tag.	-

Default Value

NA

View

L2 Filter configuration view, Filter configuration view, filter-hybrid configuration view, Filter configuration view (IPv6)

Usage Guidelines

NA

Example

Set an action for an ACL rule to delete an inner VLAN tag.

```
Switch(configure-filter-l2-100)#filter 2 action remove-inner-vid
Switch(configure-filter-l2-100)#
```

8.3.11 filter action tos

Function

The **filter action tos** command sets an action for an ACL rule to modify the IP ToS value of the specified packet.

Format

filter rule-number action tos *tos-number*

Parameter

Parameter	Description	Value
rule-number	Specifies an ACL number.	The value is an integer ranging from 1 to 2048.
tos-number	Specifies a ToS number.	The value is an integer ranging from 0 to 15.

Default Value

NA

View

L2 Filter configuration view, Filter configuration view, filter-hybrid configuration view, Filter configuration view (IPv6)

Usage Guidelines

NA

Example

Set an action for an ACL rule.

```
Switch(configure-filter-l2-100)#filter 100 action tos 1
Switch(configure-filter-l2-100)#
```

8.3.12 filter car outaction drop**Function**

The **filter car outaction drop** command sets the action for an ACL rule to dropping excess data packets when the rate of packets exceeds the bandwidth limit of 16 kbit/s x N.

Format

filter *rule-number* **car** *car-value* **outaction drop**

Parameter

Parameter	Description	Value
rule-number	Specifies an ACL rule number.	The value is an integer ranging from 1 to 2048.
car-value	Specifies the control granularity (16 Kbps).	The value is an integer ranging from 0000 to 102400000.

Default Value

NA

View

L2 Filter configuration view, Filter configuration view, filter-hybrid configuration view, Filter configuration view (IPv6)

Usage Guidelines

After this command is executed, the system determines whether the traffic rate exceeds the limit upon receiving packets matching the ACL rule on an interface. If yes, the system drops the packets beyond the traffic limit.

Example

Set the action for an ACL rule to dropping excess data packets when the rate of packets exceeds the bandwidth limit of 16 kbit/s x N.

```
Switch(configure-filter-l2-100)#filter 100 car 128 outaction drop
Switch(configure-filter-l2-100)#
```

8.3.13 filter meter

Function

The **filter meter** command binds an ACL rule to a meter.

The **no filter meter** command unbinds an ACL rule from a meter.

Format

- **filter** *rule-number* **meter** *meter-number*
- **no filter** *rule-number* **meter**

Parameter

Parameter	Description	Value
rule-number	Specifies an ACL rule number.	The value is an integer ranging from 1 to 2048.
meter-number	Specifies the number of a single/dual-rate-three-color meter.	The value is an integer ranging from 1 to 256.

Default Value

NA

View

L2 Filter configuration view, Filter configuration view, filter-hybrid configuration view, Filter configuration view (IPv6)

Usage Guidelines

After this command is executed, the switch limits the rate of packets matching the ACL rule according to the meter value.



Caution

This command is similar to **filter action counter**. You must configure a meter and bind it to the filter (see meter).

```
Switch(config)#meter 100 cir 100 cbs 20000 ebs 20000 aware
Switch(config)#
Switch(config)#filter-list 100
Switch(configure-filter-l2-100)#
Switch(configure-filter-l2-100)#filter 100 mac any any
Switch(configure-filter-l2-100)#
```

Example

Bind an ACL rule to a meter.

```
Switch(configure-filter-l2-100)#filter 100 meter 100
Switch(configure-filter-l2-100)#
```

8.3.14 filter outaction

Function

The **filter outaction** command configures the out-action action for an ACL rule to dropping data packets marked with a single/dual-rate-three-color marker, re-marking the DSCP priority of IP packets, or re-marking the 802.1p priority of VLAN packets.

The **no filter outaction** command deletes the out-action action for an ACL rule, which can drop, DSCP re-marking for IP packets, or 802.1p priority re-marking for VLAN packets.

Format

- **filter rule-number outaction { red | yellow } drop**
- **filter rule-number outaction { red | yellow } remark-cfi cfi-value**
- **filter rule-number outaction { red | yellow } remark-dscp dscp**
- **filter rule-number outaction { red | yellow } remark-dot1p priority**
- **no filter rule-number outaction**

Parameter

Parameter	Description	Value
rule-number	Specifies an ACL rule number.	The value is an integer ranging from 1 to 2048.
red yellow	Specifies the color marked for a packet.	-
drop	Drops a packet.	-
remark-cfi	Resets the CFI field in the VLAN tag (marks the drop priority of the packet).	-
cfi-value	Specifies a CFI value.	The value is an integer ranging from 0 to 1.
remark-dscp	Resets a DSCP value.	-
dscp	Specifies the Differentiated Services Code Point (DSCP) value of packets.	The DSCP value is an integer or a name. When the value is an integer, it ranges from 0 to 63. When the value is a name, it is af11, af12, af13, af21, af22, af23, af31, af32, af33, af41, af42, af43, cs1, cs2, cs3, cs4, cs5, cs6, cs7, default, or ef.
remark-dot1p	Changes a 802.1p priority.	-
priority	Specifies the value of the 802.1p priority in the VLAN tag.	The value is an integer ranging from 0 to 7.

Default Value

NA

View

L2 Filter configuration view, Filter configuration view, filter-hybrid configuration view, Filter configuration view (IPv6)

Usage Guidelines

Re-marking the DSCP priority of packets does not affect the QoS processing on the Switch. This operation only affects the QoS processing on downstream L3 or higher layer devices.

Re-marking the 802.1p priority of packets does not affect the QoS processing on the Switch. This operation only affects the QoS processing on downstream L2 devices.

When you use this command to configure re-marking multiple times, only the last configuration takes effect.

Example

```
# Configure the out-action action for an ACL rule to drop packets marked with a single/dual-rate-three-color marker.
```

```
Switch(configure-filter-l2-100)#filter 100 outaction red drop
Switch(configure-filter-l2-100)#

Switch(configure-filter-l2-100)#filter 100 outaction red remark-dot1p 1
Switch(configure-filter-l2-100)#

Switch(configure-filter-l2-100)#filter 100 outaction red remark-dscp ef
Switch(configure-filter-l2-100)#
```

8.3.15 filter time-range

Function

The **filter time-range** command binds an ACL rule to a time range specified by time-range to make a rule in the ACL to take effect in the specified time range.

The **no filter time-range** command unbinds an ACL rule from time-range.

Format

- **filter** *rule-number* **time-range** *time-index*
- **no filter** *rule-number* **time-range**

Parameter

Parameter	Description	Value
rule-number	Specifies an ACL rule number.	The value is an integer ranging from 1 to 2048.
time-index	Specifies the index of a specified time range.	The value is an integer ranging from 1 to 128.

Default Value

NA

View

L2 Filter configuration view, Filter configuration view, filter-hybrid configuration view, Filter configuration view (IPv6)

Usage Guidelines

Before running this command, you must configure a time-range module and specify a valid time range.

Time ranges are divided into periodical time ranges and absolute time ranges. You can use numbers 1 to 128 to index time ranges. You can set multiple valid time within one time range corresponding

to an index. The validity principle is as follows: The periodical time ranges are in Or relation, and periodical time ranges and absolute time ranges are in AND relation. For example, the following three valid time are set for the time range corresponding to the index 1:

From 00:00 on 2011-01-01 to 23:59 on 2009-12-31 (which is an absolute time range)

From 08:30 to 17:30 from Monday to Friday (which is a periodical time range)

From 14:30 to 18:30 on Saturday and Sunday (which is a periodical time range)

Then, the valid time range of index 1 is: from 08:30 to 17:30 from Monday to Friday and from 14:30 to 18:30 on Saturday and Sunday from 2011-01-01 to 2011-12-31.

If no start date is configured, the time range is the earliest time that the system can represent to the end date. If no end date is configured, the time range is the configured start date to the maximum time that the system can represent.

Example

Bind an ACL rule to a time range specified by time-range to make a rule in the ACL to take effect in the specified time range.

```
Switch(configure-filter-l2-100)#filter 100 time-range 100
Switch(configure-filter-l2-100)#
```

8.3.16 filter-list {in|out}

Function

The **filter-list {in|out}** command applies an ACL to a physical interface, a trunk interface, or a VLAN interface.

The **no filter-list {in|out}** command cancels the application of an ACL to a physical interface, a trunk interface, or a VLAN interface.

Format

- **filter-list { in | out } *acl-number***
- **filter-list { in | out } **name** *filter-name***
- **no filter-list { in | out } [*acl-number*]**

Parameter

Parameter	Description	Value
acl-number	Specifies an ACL number.	The value is an integer ranging from 1 to 4000.

Parameter	Description	Value
filter-name	Specifies an ACL name.	The value is a character string.

Default Value

NA

View

Ethernet bridge interface configuration view, Ethernet routing interface configuration view, interface configuration view (Trunk), VLAN configuration view

Usage Guidelines

You can use this command to apply an ACL to a physical interface or a trunk interface in the interface configuration view.

Example

Enter the port xgigetherenet and bind the ACL 100 of this port.

```
Switch(config)#interface xgigaethernet 1/0/1
Switch(config-10ge1/0/1)#filter-list in 100
Switch(config-10ge1/0/1)#
```

Create a trunk interface, enter the trunk interface view, and apply ACL 100 to the interface.

```
Switch(config)#interface eth-trunk 2
Switch(config-eth-trunk2)#filter-list in 100
Switch(config-eth-trunk2)#
```

8.3.17 no filter action**Function**

The **no filter action** command deletes the action for an ACL rule.

Format

no filter *rule-number* **action**

Parameter

Parameter	Description	Value
rule-number	Specifies an ACL rule number.	The value is an integer ranging from 1 to 2048.

Default Value

NA

View

L2 Filter configuration view, Filter configuration view, filter-hybrid configuration view, Filter configuration view (IPv6)

Usage Guidelines

After using this command, the action corresponding to the ACL rule is deleted.

Example

Delete the action for an ACL rule.

```
Switch(configure-filter-l2-100)#no filter 100 action
Switch(configure-filter-l2-100)#
```

8.3.18 no filter

Function

The **no filter** command deletes an ACL rule.

Format

no filter *rule-number*

Parameter

Parameter	Description	Value
rule-number	Specifies a filter number.	The value is an integer ranging from 1 to 2048.

Default Value

NA

View

L2 Filter configuration view, Filter configuration view, filter-hybrid configuration view, Filter configuration view (IPv6)

Usage Guidelines

NA

Example

Delete an ACL rule.

```
Switch(configure-filter-ipv4-1500)#no filter 100
Switch(configure-filter-ipv4-1500)#
```

8.3.19 no filter outaction

Function

The **no filter outaction** command deletes the out-action action for an ACL rule, which can drop, DSCP re-marking for IP packets, or 802.1p priority re-marking for VLAN packets.

Format

no filter *rule-number* **outaction**

Parameter

Parameter	Description	Value
rule-number	Specifies an ACL number.	The value is an integer ranging from 1 to 2048.

Default Value

NA

View

L2 Filter configuration view, Filter configuration view, filter-hybrid configuration view, Filter configuration view (IPv6)

Usage Guidelines

After using this command, the action corresponding to the ACL rule is deleted.

Example

Delete the out-action action for an ACL rule

```
Switch(configure-filter-l2-100)#no filter 100 outaction
Switch(configure-filter-l2-100)#
```

8.3.20 show filter-list

Function

The **show filter-list** command displays the ACL configuration.

Format

- **show filter-list**

- **show filter-list** *acl-number*

Parameter

Parameter	Description	Value
acl-number	(Optional) Specifies the number of the ACL to be checked.	The value is an integer ranging from 1 to 4000.

Default Value

NA

View

Common user view

Usage Guidelines

If *acl-number* is not specified in the command, the command displays all ACLs and all ACL rules under each ACL. If *acl-number* is specified, the command displays information about the specified ACL.

Example

```
Switch>show filter-list

filter-list 1001 filter 2
filter-list 1001
filter 1 ip 10.1.1.2/32 any
filter 1 action permit

filter 2 ip 10.1.1.3/32 any
filter 2 action permit

filter-list 1002 filter 2
filter-list 1002
filter 1 ip 10.1.1.4/32 any
filter 1 action permit

filter 2 ip 10.1.1.5/32 any
filter 2 action permit

filter-list 1003 filter 1
filter-list 1003
filter 1 ip any any
filter 1 action deny
```

```
Switch>show filter-list
```

8.3.21 show filter-list brief

Function

The **show filter-list brief** command displays brief ACL information.

Format

show filter-list brief

Parameter

NA

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

Display brief ACL information.

```
Switch>show filter-list brief
Filter-List    RuleNumber  Name
-----
1001           2          acl1001
1002           2          acl1002
1003           1          acl1003
Switch>
```

8.3.22 show filter-list config

Function

The **show filter-list config** command displays the ACL configuration file information on the switch.

Format

show filter-list config

Parameter

NA

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

Display ACL configuration file information.

```
Switch>show filter-list config
filter-list 1001 filter 2
  filter-list 1001
  filter 1 ip 10.1.1.2/32 any
  filter 1 action permit

  filter 2 ip 10.1.1.3/32 any
  filter 2 action permit

filter-list 1002 filter 2
  filter-list 1002
  filter 1 ip 10.1.1.4/32 any
  filter 1 action permit

  filter 2 ip 10.1.1.5/32 any
  filter 2 action permit

filter-list 1003 filter 1
  filter-list 1003
  filter 1 ip any any
  filter 1 action deny
Switch>
```

8.3.23 show filter-list global

Function

The **show filter-list global** command displays the global configuration of ACLs.

Format**show filter-list global****Parameter**

NA

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

View the ACL global configuration.

Switch>show filter-list global

Switch>

8.3.24 show filter-list interface**Function**

The **show filter-list interface** command displays information about all interfaces with ACLs applied.

Format**show filter-list interface****Parameter**

NA

Default Value

NA

View

Common user view

Usage Guidelines

You can use this command to check information about ACL-enabled interfaces.

Example

```
Switch>show filter-list interface
Switch>
```

8.3.25 show filter-list name

Function

The **show filter-list name** command displays the configuration of a specified ACL.

Format

show filter-list name *acl-name*

Parameter

Parameter	Description	Value
acl- name	Specifies the name of an ACL.	The value is a character string.

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

View the configuration of the ACL acl1001.

```
Switch>show filter-list name acl1001

filter-list 1001 filter 2
filter-list 1001
filter 1 ip 10.1.1.2/32 any
filter 1 action permit

filter 2 ip 10.1.1.3/32 any
filter 2 action permit
Switch>
```

8.3.26 show filter-list statistic

Function

The **show filter-list statistic** command displays ACL statistics.

Format

show filter-list statistic

Parameter

NA

Default Value

NA

View

Common user view

Usage Guidelines

The ACL statistics include the Direction, Packets, Bytes, Interface, and SwCounterId fields.

Example

```
Switch>show filter-list statistic
Switch>
```

8.3.27 debug filter

Function

The **debug filter** command enables ACL debugging.

The **no debug filter** command disables ACL debugging.

Format

- **debug filter { global | if | config | statistic | rule | device | all }**
- **no debug filter { global | if | config | statistic | rule | device | all }**

Parameter

Parameter	Description	Value
global	Specifies global information.	-
if	Displays interface information.	-
config	Debugs configuration information.	-

Parameter	Description	Value
statistic	Displays statistics.	-
rule	Displays rule information.	-
device	Displays device information.	-
all	Displays all the preceding information.	-

Default Value

NA

View

Privileged user view

Usage Guidelines

NA

Example

Enable ACL debugging.

```
Switch#debug filter all
Switch#
```

8.3.28 filter icmp

Function

The **filter icmp** command configures an ACL rule matching packets based on source and destination IPv4 addresses and the ICMP field.

Format

- **filter rule-number icmp** { *src-ip-address/M* | **any** } { *dst-ip-address/M* | **any** }
- **filter rule-number icmp** { *src-ip-address/M* | **any** } { *dst-ip-address/M* | **any** } { *icmp-type* | **any** } { *icmp-code* | **any** } [**fragment**]
- **filter rule-number icmp src-ip** { *src-ip-address* | **any** } **src-mask** { *src-mask-address* | **any** } **dst-ip** { *dst-ip-address* | **any** } **dst-mask** { *dst-mask-address* | **any** }
- **filter rule-number icmp src-ip** { *src-ip-address* | **any** } **src-mask** { *src-mask-address* | **any** } **dst-ip** { *dst-ip-address* | **any** } **dst-mask** { *dst-mask-address* | **any** } { *icmp-type* | **any** } { *icmp-code* | **any** }

Parameter

Parameter	Description	Value
rule-number	Specifies a filter number.	The value is an integer ranging from 1 to 2048.
src-ip-address/M any	Specifies a source IP address in an ACL rule.	<i>src-ip-address</i> is in dotted decimal notation. <i>M</i> is an integer ranging from 1 to 32. any means any source IP address.
dst-ip-address/M any	Specifies a destination IP address in an ACL rule.	<i>dst-ip-address</i> is in dotted decimal notation. <i>M</i> is an integer ranging from 1 to 32. any means any destination IP address.
src-mask-address	Specifies the mask of a source IP address in an ACL rule.	The value is in dotted decimal notation.
dst-mask-address	Specifies the mask of a destination IP address in an ACL rule.	The value is in dotted decimal notation.
icmp-type	Specifies an ICMP type range in an ACL rule.	The value is an integer ranging from 0 to 255.
icmp-code	Specifies an ICMP code range in an ACL rule.	The value is an integer ranging from 0 to 255.

Default Value

NA

View

Filter configuration view, filter-hybrid configuration view

Usage Guidelines

NA

Example

Configure an ACL rule matching packets based on source and destination IPv4 addresses and the ICMP field.

```
Switch(configure-filter-ipv4-1500)#filter 100 icmp 1.1.1.1/10 2.2.2.2/20 20 30
Switch(configure-filter-ipv4-1500)#
Switch(configure-filter-ipv4-1500)#filter 100 icmp src-ip 1.1.1.1 src-mask 255.255.255.0 dst-ip 2.2.2.2
dst-mask 255.255.255.0 10 20
Switch(configure-filter-ipv4-1500)#
```

8.3.29 filter igmp

Function

The **filter ip igmp** command configures an ACL rule based on the source/destination IPv4 address and IGMP type or code field.

Format

filter *rule-number* **igmp** { *src-ip-address/M* | **any** } { *dst-ip-address/M* | **any** } [**fragment**]

filter *rule-number* **igmp** **src-ip** { *src-ip-address* | **any** } **src-mask** { *src-mask-address* | **any** } **dst-ip** { *dst-ip-address* | **any** } **dst-mask** { *dst-mask-address* | **any** }

Parameter

Parameter	Description	Value
<i>rule-number</i>	Specifies a filter number.	The value is an integer ranging from 1 to 2048.
<i>src-ip-address/M</i> any	Specifies a source IP address in an ACL rule.	<i>src-ip-address</i> is in dotted decimal notation. <i>M</i> is an integer ranging from 1 to 32. any means any source IP address.
<i>dst-ip-address/M</i> any	Specifies a destination IP address in an ACL rule.	<i>dst-ip-address</i> is in dotted decimal notation. <i>M</i> is an integer ranging from 1 to 32. any means any destination IP address.
<i>src-mask-address</i>	Specifies the mask of a source IP address in an ACL rule.	The value is in dotted decimal notation.
<i>dst-mask-address</i>	Specifies the mask of a destination IP address in an ACL rule.	The value is in dotted decimal notation.

Default Value

NA

View

Filter configuration view, filter-hybrid configuration view

Usage Guidelines

NA

Example

```
Switch(configure-filter-ipv4-1500)#filter 100 igmp 1.1.1.1/10 2.2.2.2/20
Switch(configure-filter-ipv4-1500)#
Switch(configure-filter-ipv4-1500)#filter 100 igmp src-ip 1.1.1.1 src-mask 255.255.255.0 dst-ip 2.2.2.2
dst-mask 255.255.255.0
Switch(configure-filter-ipv4-1500)#
```

8.3.30 filter ip**Function**

The **filter ip** command sets an ACL rule based on the source IPv4 address and destination IP address.

Format

filter rule-number ip { *src-ip-address/M* | **any** } { *dst-ip-address/M* | **any** }

filter rule-number igmp src-ip { *src-ip-address* | **any** } **src-mask** { *src-mask-address* | **any** } **dst-ip** { *dst-ip-address* | **any** } **dst-mask** { *dst-mask-address* | **any** }

Parameter

Parameter	Description	Value
rule-number	Specifies an ACL rule number.	The value is an integer ranging from 1 to 2048.
src-ip-address/M any	Specifies a source IP address in an ACL rule.	<i>src-ip-address</i> is in dotted decimal notation. <i>M</i> is an integer ranging from 1 to 32. any means any source IP address.
dst-ip-address/M any	Specifies a destination IP address in an ACL rule.	<i>dst-ip-address</i> is in dotted decimal notation. <i>M</i> is an integer ranging from 1 to 32. any means any destination IP address.
src-ip-mask	Specifies the mask of a source IP address in an ACL rule.	The value is in dotted decimal notation.
dst-ip-mask	Specifies the mask of a destination IP address in an ACL rule.	The value is in dotted decimal notation.

Default Value

NA

View

Filter configuration view, filter-hybrid configuration view

Usage Guidelines

After the ACL rule is applied to an interface, the system filters data packets received on the interface based on the IP addresses in the packets. Packets matching the ACL rule are processed based on the action configured for the ACL rule.

ACLs are classified into four levels. The **filter ip** and associated commands are applicable only to IPv4/hybrid ACLs 1001 to 3000.

Example

Configure an ACL rule based on the source and destination IPv4 address.

```
Switch(configure-filter-ipv4-2000)#filter 100 ip 1.1.1.1/10 2.2.2.2/20
```

```
Switch(configure-filter-ipv4-2000)#
```

8.3.31 filter ip {customer|provider}

Function

The **filter ip {customer|provider}** command sets to match the inner or outer VLAN of a specified IP address.

Format

filter rule-number ip { *src-ip-address/M* | **any** } { *dst-ip-address/M* | **any** } { **customer** | **provider** }
 { **any** | *vlan-id* } { **any** | *priority* }

Parameter

Parameter	Description	Value
rule-number	Specifies an ACL rule number.	The value is an integer ranging from 1 to 2048.
src-ip-address/M any	Specifies a source IP address in an ACL rule.	<i>src-ip-address</i> is in dotted decimal notation. <i>M</i> is an integer ranging from 1 to 32. any means any source IP address.
dst-ip-address/M any	Specifies a destination IP address in an ACL rule.	<i>dst-ip-address</i> is in dotted decimal notation. <i>M</i> is an integer ranging from 1 to 32. any means any destination IP address.
vlan-id	Specifies the priority of any VLAN.	The value is an integer ranging from 1 to 4094.
priority	Specifies a Dot1p priority.	The value is an integer ranging from 0 to 7.

Default Value

NA

View

Filter-hybrid configuration view

Usage Guidelines

NA

Example

Set to match the inner or outer VLAN of a specified IP address.

```
Switch(configure-filter-ipv4-2000)#filter 100 ip 1.1.1.1/10 2.2.2.2/20 customer any any
Switch(configure-filter-ipv4-2000)#
```

8.3.32 filter ip dscp

Function

The **filter ip dscp** command sets an ACL rule based on the source/destination IPv4 address and DSCP field.

Format

- **filter rule-number ip** { *src-ip-address/M* | **any** } { *dst-ip-address/M* | **any** } **dscp dscp** [**fragment**]
- **filter rule-number src-ip** { *src-ip-address* | **any** } **src-mask** {*src-ip-mask* | **any** } **dst-ip** { *dst-ip-address* | **any** } **dst-mask** { *dst-ip-mask* | **any** } **dscp dscp** [**fragment**]

Parameter

Parameter	Description	Value
rule-number	Specifies an ACL rule number.	The value is an integer ranging from 1 to 2048.
src-ip-address/M any	Specifies a source IP address in an ACL rule.	<i>src-ip-address</i> is in dotted decimal notation. <i>M</i> is an integer ranging from 1 to 32. any means any source IP address.
dst-ip-address/M any	Specifies a destination IP address in an ACL rule.	<i>dst-ip-address</i> is in dotted decimal notation. <i>M</i> is an integer ranging from 1 to 32. any means any destination IP address.
dscp	Specifies the Differentiated Services Code Point (DSCP) value of packets.	The DSCP value is an integer or a name. When the value is an integer, it ranges from 0 to 63. When the value is a name, it is af11, af12, af13, af21, af22, af23, af31, af32, af33, af41, af42, af43, cs1, cs2, cs3, cs4, cs5, cs6, cs7, default, or ef.
src-ip-mask	Specifies the mask of a source IP address in an ACL rule.	The value is in dotted decimal notation.
dst-ip-mask	Specifies the mask of a destination IP address in an ACL rule.	The value is in dotted decimal notation.

Default Value

NA

View

Filter configuration view, filter-hybrid configuration view

Usage Guidelines

After the ACL entry is applied, a port filters received packets according to the IP addresses and DSCP field in the packets. The port takes the corresponding actions for packets matching the ACL rule.

Example

Configure an ACL rule matching packets based on source and destination IPv4 addresses and the DSCP field.

```
Switch(configure-filter-ipv4-1500)#filter 100 ip 1.1.1.1/10 2.2.2.2/20 dscp 10
Switch(configure-filter-ipv4-1500)#
Switch(configure-filter-ipv4-1500)#filter 100 src-ip 1.1.1.1 src-mask 255.255.255.0 dst-ip 2.2.2.2 dst-mask
255.255.255.0 dscp 10
Switch(configure-filter-ipv4-1500)#
```

8.3.33 filter ip fragment

Function

The **filter ip fragment** command sets an ACL rule based on the source/destination IPv4 address and fragment field.

Format

filter rule-number ip { *src-ip-address/M* | **any** } { *dst-ip-address/M* | **any** } **fragment**

Parameter

Parameter	Description	Value
rule-number	Specifies an ACL rule number.	The value is an integer ranging from 1 to 2048.
src-ip-address/M any	Specifies a source IP address in an ACL rule.	<i>src-ip-address</i> is in dotted decimal notation. <i>M</i> is an integer ranging from 1 to 32. any means any source IP address.
dst-ip-address/M any	Specifies a destination IP address in an ACL rule.	<i>dst-ip-address</i> is in dotted decimal notation. <i>M</i> is an integer ranging from 1 to 32. any means any destination IP address.
fragment	Specifies whether the rule is valid for the non-first fragment message only.	-

Default Value

NA

View

Filter configuration view, filter-hybrid configuration view

Usage Guidelines

After the ACL entry is applied, the switch matches the IP addresses in the received packets and determines whether the packets are non-first fragment packets. If the IP addresses of the packets match the ACL rule and the packets are non-first fragment packets, the switch takes the corresponding actions for packets according to the ACL rule.

Example

Configure an ACL rule matching packets based on source and destination IPv4 addresses and the fragment field.

```
Switch(configure-filter-ipv4-1500)#filter 100 ip 1.1.1.1/10 2.2.2.2/20 fragment
Switch(configure-filter-ipv4-1500)#
Switch(configure-filter-ipv4-1500)#filter 100 src-ip 1.1.1.1 src-mask 255.255.255.0 dst-ip 2.2.2.2 dst-mask
255.255.255.0 fragment
Switch(configure-filter-ipv4-1500)#
```

8.3.34 filter ip precedence

Function

The **filter ip precedence** command sets an ACL rule based on the source/destination IPv4 address and ToS field.

Format

filter rule-number ip { *src-ip-address/M* | **any** } { *dst-ip-address/M* | **any** } **precedence tos-priority**

filter rule-number src-ip { *src-ip-address* | **any** } **src-mask** {*src-ip-mask* | **any** } **dst-ip** { *dst-ip-address* | **any** } **dst-mask** { *dst-ip-mask* | **any** } **precedence tos-priority** [**fragment**]

Parameter

Parameter	Description	Value
rule-number	Specifies an ACL rule number.	The value is an integer ranging from 1 to 2048.
src-ip-address/M any	Specifies a source IP address in an ACL rule.	<i>src-ip-address</i> is in dotted decimal notation. <i>M</i> is an integer ranging from 1 to 32. any means any source IP address.
dst-ip-address/M any	Specifies a destination IP address in an ACL rule.	<i>dst-ip-address</i> is in dotted decimal notation. <i>M</i> is an integer ranging from 1 to 32. any means any destination IP address.
tos-priority	Specifies the priority value in the ToS field.	The value is an integer ranging from 0 to 7.

Parameter	Description	Value
src-ip-mask	Specifies the mask of a source IP address in an ACL rule.	The value is in dotted decimal notation.
dst-ip-mask	Specifies the mask of a destination IP address in an ACL rule.	The value is in dotted decimal notation.

Default Value

NA

View

Filter configuration view, filter-hybrid configuration view

Usage Guidelines

After the ACL entry is applied to an interface, the system filters packets received on the interface based on the IP addresses and ToS fields in the packets. Packets matching the ACL rule are processed based on the action configured for the ACL rule.

Example

Configure an ACL rule matching packets based on source and destination IPv4 addresses and the ToS field.

```
Switch(configure-filter-ipv4-1500)#filter 100 ip 1.1.1.1/10 2.2.2.2/20 precedence 1
Switch(configure-filter-hybrid-1500)#
Switch(configure-filter-ipv4-1500)#filter 100 src-ip 1.1.1.1 src-mask 255.255.255.0 dst-ip 2.2.2.2 dst-mask
255.255.255.0 precedence 2
Switch(configure-filter-hybrid-1500)#
```

8.3.35 filter ip precedence fragment

Function

The **filter ip precedence fragment** command sets an ACL rule based on the source/destination IPv4 address, ToS field, and fragment field.

Format

filter rule-number ip { *src-ip-address/M* | **any** } { *dst-ip-address/M* | **any** } **precedence tos-priority fragment**

Parameter

Parameter	Description	Value
rule-number	Specifies a filter number.	The value is an integer ranging from 1 to 2048.

Parameter	Description	Value
src-ip-address/M any	Specifies a source IP address in an ACL rule.	<i>src-ip-address</i> is in dotted decimal notation. <i>M</i> is an integer ranging from 1 to 32. any means any source IP address.
dst-ip-address/M any	Specifies a destination IP address in an ACL rule.	<i>dst-ip-address</i> is in dotted decimal notation. <i>M</i> is an integer ranging from 1 to 32. any means any destination IP address.
tos-priority	Specifies a ToS field in an ACL rule.	The value is an integer ranging from 0 to 7.
fragment	Specifies whether the rule is valid for the non-first fragment message only.	-

Default Value

NA

View

Filter configuration view, filter-hybrid configuration view

Usage Guidelines

NA

Example

Configure an ACL rule matching packets based on source and destination IPv4 addresses, the ToS field, and the fragment field.

```
Switch(configure-filter-ipv4-1500)#filter 100 ip 1.1.1.1/10 2.2.2.2/20 precedence 1 fragment
Switch(configure-filter-hybrid-1500)#
Switch(configure-filter-ipv4-1500)#filter 100 src-ip 1.1.1.1 src-mask 255.255.255.0 dst-ip 2.2.2.2 dst-mask
255.255.255.0 precedence 2 fragment
Switch(configure-filter-hybrid-1500)#
```

8.3.36 filter ip proto-type

Function

The **filter ip proto-type** command sets an ACL rule based on the source/destination IPv4 address and protocol type field.

Format

filter *rule-number* **ip** { *src-ip-address/M* | **any** } { *dst-ip-address M* | **any** } **proto-type**
proto-type-value

filter *rule-number* **src-ip** { *src-ip-address* | **any** } **src-mask** { *src-ip-mask* | **any** } **dst-ip** { *dst-ip-address* | **any** } **dst-mask** { *dst-ip-mask* | **any** } **proto-type** *proto-type-value*

Parameter

Parameter	Description	Value
rule-number	Specifies a filter number.	The value is an integer ranging from 1 to 2048.
src-ip-address/M any	Specifies a source IP address in an ACL rule.	<i>src-ip-address</i> is in dotted decimal notation. <i>M</i> is an integer ranging from 1 to 32. any means any source IP address.
dst-ip-address/M any	Specifies a destination IP address in an ACL rule.	<i>dst-ip-address</i> is in dotted decimal notation. <i>M</i> is an integer ranging from 1 to 32. any means any destination IP address.
proto-type-value	Specifies a protocol type in an ACL rule.	The value is an integer ranging from 1 to 255.
src-ip-mask	Specifies the mask of a source IP address in an ACL rule.	The value is in dotted decimal notation.
dst-ip-mask	Specifies the mask of a destination IP address in an ACL rule.	The value is in dotted decimal notation.

Default Value

NA

View

Filter configuration view, filter-hybrid configuration view

Usage Guidelines

NA

Example

Configure an ACL rule matching packets based on the source and destination IPv4 addresses and the protocol type field.

```
Switch(configure-filter-ipv4-1500)#filter 100 ip 1.1.1.1/10 2.2.2.2/20 proto-type 10
Switch(configure-filter-ipv4-1500)#
```

8.3.37 filter ip tos

Function

The **filter ip tos** command sets an ACL rule based on the source/destination IPv4 address and ToS field.

Format

- **filter rule-number ip** { *src-ip-address/M* | **any** } { *dst-ip-address/M* | **any** } **tos tos-value**
- **filter rule-number ip** { *src-ip-address/M* | **any** } { *dst-ip-address/M* | **any** } **tos tos-value fragment**
- **filter rule-number src-ip** { *src-ip-address* | **any** } **src-mask** { *src-ip-mask* | **any** } **dst-ip** { *dst-ip-address* | **any** } **dst-mask** { *dst-ip-mask* | **any** } **tos tos-value**
- **filter rule-number src-ip** { *src-ip-address* | **any** } **src-mask** { *src-ip-mask* | **any** } **dst-ip** { *dst-ip-address* | **any** } **dst-mask** { *dst-ip-mask* | **any** } **tos tos-value fragment**

Parameter

Parameter	Description	Value
rule-number	Specifies a filter number.	The value is an integer ranging from 1 to 2048.
src-ip-address/M any	Specifies a source IP address in an ACL rule.	<i>src-ip-address</i> is in dotted decimal notation. <i>M</i> is an integer ranging from 1 to 32. any means any source IP address.
dst-ip-address/M any	Specifies a destination IP address in an ACL rule.	<i>dst-ip-address</i> is in dotted decimal notation. <i>M</i> is an integer ranging from 1 to 32. any means any destination IP address.
tos-value	Specifies a TTL field in an ACL rule.	The value is an integer ranging from 0 to 15.
src-ip-mask	Specifies the mask of a source IP address in an ACL rule.	The value is in dotted decimal notation.
dst-ip-mask	Specifies the mask of a destination IP address in an ACL rule.	The value is in dotted decimal notation.

Default Value

NA

View

Filter configuration view, filter-hybrid configuration view

Usage Guidelines

NA

Example

Configure an ACL rule matching packets based on the source and destination IPv4 addresses and the ToS field.

```
Switch(configure-filter-ipv4-1500)#filter 100 ip 1.1.1.1/10 2.2.2.2/20 tos 10
```

```
Switch(configure-filter-ipv4-1500)#
```

8.3.38 filter ip ttl

Function

The **filter ip ttl** command sets an ACL rule based on the source/destination IPv4 address and TTL field.

Format

filter *rule-number* **ip** { *src-ip-address/M* | **any** } { *dst-ip-address/M* | **any** } **ttl** *ttl-value*

filter *rule-number* **src-ip** { *src-ip-address* | **any** } **src-mask** { *src-ip-mask* | **any** } **dst-ip** { *dst-ip-address* | **any** } **dst-mask** { *dst-ip-mask* | **any** } **ttl** *ttl-value*

Parameter

Parameter	Description	Value
rule-number	Specifies a filter number.	The value is an integer ranging from 1 to 2048.
src-ip-address/M any	Specifies a source IP address in an ACL rule.	<i>src-ip-address</i> is in dotted decimal notation. <i>M</i> is an integer ranging from 1 to 32. any means any source IP address.
dst-ip-address/M any	Specifies a destination IP address in an ACL rule.	<i>dst-ip-address</i> is in dotted decimal notation. <i>M</i> is an integer ranging from 1 to 32. any means any destination IP address.
ttl-value	Specifies a TTL field in an ACL rule.	The value is an integer ranging from 1 to 255.
src-ip-mask	Specifies the mask of a source IP address in an ACL rule.	The value is in dotted decimal notation.
dst-ip-mask	Specifies the mask of a destination IP address in an ACL rule.	The value is in dotted decimal notation.

Default Value

NA

View

Filter configuration view, filter-hybrid configuration view

Usage Guidelines

NA

Example

Configure an ACL rule matching packets based on source and destination IPv4 addresses and the TTL field.

```
Switch(configure-filter-ipv4-1500)#filter 100 ip 1.1.1.1/10 2.2.2.2/20 ttl 20
Switch(configure-filter-ipv4-1500)#
Switch(configure-filter-ipv4-1500)#filter 100 src-ip 1.1.1.1 src-mask 255.255.255.0 dst-ip 2.2.2.2 dst-mask
255.255.255.0 ttl 20
Switch(configure-filter-ipv4-1500)#
```

8.3.39 filter mac

Function

The **filter mac** command configures an ACL rule matching packets based on MAC address entries.

Format

L2 Filter configuration view

- **filter rule-number mac** { *src-mac-address/M* | **any** } { *dst-mac-address/M* | **any** }
- **filter rule-number mac** { *src-mac-address/M* | **any** } { *dst-mac-address/M* | **any** } { **customer** | **provider** } { **any** | *vlan-id* | *vlan-id1/vlan-id2* } { **any** | *priority* }
- **filter rule-number mac** { *src-mac-address/M* | **any** } { *dst-mac-address/M* | **any** } **eth-type** { **ip** | **arp** | *digital-protocol-value* }
- **filter rule-number mac** { *src-mac-address/M* | **any** } { *dst-mac-address/M* | **any** } **provider** *vlan-id1/vlan-id2* { **any** | *priority* } **customer** { **any** | *vlan-id* } { **any** | *priority* }
- **filter rule-number mac** { *src-mac-address/M* | **any** } { *dst-mac-address/M* | **any** } **provider** { **any** | *vlan-id* } { **any** | *priority* } **customer** *vlan-id1/vlan-id2* { **any** | *priority* }
- **filter rule-number mac** { *src-mac-address/M* | **any** } { *dst-mac-address/M* | **any** } **provider** { **any** | *vlan-id* } { **any** | *priority* } **customer** { **any** | *vlan-id* } { **any** | *priority* }

Filter-hybrid configuration view

- **filter rule-number mac** { *src-mac-address/M* | **any** } { *dst-mac-address/M* | **any** } **eth-type** { **ip** | **arp** | **any** | *digital-protocol-value* } **provider** { **any** | *vlan-id* } { **any** | *priority* } **customer** { **any** | *vlan-id* } { **any** | *priority* } **ip** { *src-ip-address/M* | **any** } { *dst-ip-address/M* | **any** } **proto-type** { *protocol-type-value* | **any** }
- **filter rule-number mac** { *src-mac-address/M* | **any** } { *dst-mac-address/M* | **any** } **eth-type** { **ip** | **arp** | **any** | *digital-protocol-value* } **provider** { **any** | *vlan-id* | *vlan-id1/vlan-id2* } { **any** | *priority* } **customer** { **any** | *vlan-id* | *vlan-id1/vlan-id2* } { **any** | *priority* } **ip** { *src-ip-address/M*

| **any** } { *dst-ip-address/M* | **any** } **proto-type** { **tcp** | **udp** } { *src-port-number* | **any** |
source-port-number-range } { *dst-port-number* | **any** | *destination-port-number-range* }

Filter-hybrid configuration view, L2 Filter configuration view

- **filter rule-number src-mac** { *src-mac-address* | **any** } **src-mask** { *src-mask* | **any** } **dst-mac**
{ *dst-mac-address* | **any** } **dst-mask** { *dst-mask* | **any** }
- **filter rule-number src-mac** { *src-mac-address* | **any** } **src-mask** { *src-mask* | **any** } **dst-mac**
{ *dst-mac-address* | **any** } **dst-mask** { *dst-mask* | **any** } { **customer** | **provider** } { **any** | *vlan-id* }
{ **any** | *priority* }
- **filter rule-number src-mac** { *src-mac-address* | **any** } **src-mask** { *src-mask* | **any** } **dst-mac**
{ *dst-mac-address* | **any** } **dst-mask** { *dst-mask* | **any** } **eth-type** { **ip** | **arp** |
digital-protocol-value }
- **filter rule-number src-mac** { *src-mac-address* | **any** } **src-mask** { *src-mask* | **any** } **dst-mac**
{ *dst-mac-address* | **any** } **dst-mask** { *dst-mask* | **any** } **provider** *vlan-id1/vlan-id2* { **any** |
priority } **customer** { **any** | *vlan-id* } { **any** | *priority* }
- **filter rule-number src-mac** { *src-mac-address/M* | **any** } **src-mask** { *src-mask* | **any** } **dst-mac**
{ *dst-mac-address* | **any** } **dst-mask** { *dst-mask* | **any** } **provider** { **any** | *vlan-id* } { **any** |
priority } **customer** *vlan-id1/vlan-id2* { **any** | *priority* }
- **filter rule-number src-mac** { *src-mac-address/M* | **any** } **src-mask** { *src-mask* | **any** } **dst-mac**
{ *dst-mac-address* | **any** } **dst-mask** { *dst-mask* | **any** } **provider** { **any** | *vlan-id* } { **any** |
priority } **customer** { **any** | *vlan-id* } { **any** | *priority* }

Parameter

Parameter	Description	Value
rule-number	Specifies a filter number.	The value is an integer ranging from 1 to 2048.
src-mac-address/M any	Specifies a source MAC address in an ACL rule.	<i>M</i> is an integer ranging from 1 to 32. any means any source MAC address.
dst-mac-address/M any	Specifies a destination MAC address in an ACL rule.	<i>M</i> is an integer ranging from 1 to 32. any means any destination MAC address.
vlan-id,vlan-id1/vlan-id2	Specifies the priority of any VLAN.	The value is an integer ranging from 1 to 4094.
priority	Specifies the Dot1p priority.	The value is an integer ranging from 0 to 7.
digital-protocol-value	Specifies a protocol value.	The value is an integer ranging <0x0600-0xffff>.
src-ip-address	Specifies a source IP address and its mask length.	The value is in dotted decimal notation.

Parameter	Description	Value
dst-ip-address	Specifies a destination IP address and its mask length.	The value is in dotted decimal notation.
protocol-type-value	Specifies a protocol type value.	The value is an integer ranging from 1 to 255.
src-port-number	Specifies a source port number.	The value is an integer ranging from 0 to 65535.
dst-port-number	Specifies a destination port number.	The value is an integer ranging from 0 to 65535.
source-port-number-range destination-port-number-range	Specifies the range of source and destination port numbers.	The value is an integer in the range of <0-65535>/<0-65535>.

Default Value

NA

View

Filter-hybrid configuration view, L2 Filter configuration view

Usage Guidelines

NA

Example

Configure an ACL rule matching packets based on MAC addresses.

```
Switch(configure-filter-l2-100)#filter 100 src-mac 11:11:11:11:11:11 src-mask 22:22:22:22:22:22 dst-mac
33:33:33:33:33:33 dst-mask 44:44:44:44:44:44 customer 10/20 2
Switch(configure-filter-l2-100)#
Switch(configure-filter-l2-100)#filter 100 mac 11:11:11:11:11:11/10 22:22:22:22:22:22/20 customer 10 1
Switch(configure-filter-l2-100)#
Switch(configure-filter-l2-100)#filter 100 src-mac 11:11:11:11:11:11 src-mask 22:22:22:22:22:22 dst-mac
33:33:33:33:33:33 dst-mask 44:44:44:44:44:44 eth-type 0x2
Switch(configure-filter-l2-100)#
```

8.3.40 filter tcp

Function

The **filter tcp** command configures an ACL rule matching packets based on source and destination IPv4 addresses and the TCP fields (including syn, synack, ack, and fin fields).

Format

- **filter rule-number tcp** { *src-ip-address/M* | **any** } { *src-port-number* | **any** | *source-port-number-range* } { *dst-ip-address/M* | **any** } { *dst-port-number* | **any** | *destination-port-number-range* }
- **filter rule-number tcp** { *src-ip-address/M* | **any** } { *src-port-number* | **any** | *source-port-number-range* } { *dst-ip-address/M* | **any** } { *dst-port-number* | **any** | *destination-port-number-range* } { **syn** | **synack** | **ack** | **fin** }
- **filter rule-number tcp** { *src-ip-address/M* | **any** } { *src-port-number* | **any** | *source-port-number-range* } { *dst-ip-address/M* | **any** } { *dst-port-number* | **any** | *destination-port-number-range* } { **syn** | **synack** | **ack** | **fin** } **fragment**
- **filter rule-number tcp** { *src-ip-address/M* | **any** } { *src-port-number* | **any** | *source-port-number-range* } { *dst-ip-address/M* | **any** } { *dst-port-number* | **any** | *destination-port-number-range* } **fragment**
- **filter rule-number tcp src-ip** { *src-ip-address* | **any** } **src-mask** { *src-ip-mask* | **any** } { *src-port-number* | *source-port-number-range/destination-port-number-range* | **any** } **dst-ip** { *src-ip-mask* | **any** } **dst-mask** { *dst-ip-mask* | **any** } { *dst-port-number* | **any** | *source-port-number-range/destination-port-number-range* } [**fragment**]
- **filter rule-number tcp src-ip** { *src-ip-address* | **any** } **src-mask** { *src-ip-mask* | **any** } { *src-port-number* | *source-port-number-range/destination-port-number-range* | **any** } **dst-ip** { *src-ip-mask* | **any** } **dst-mask** { *dst-ip-mask* | **any** } { *dst-port-number* | **any** | *source-port-number-range/destination-port-number-range* } { **syn** | **synack** | **ack** | **fin** } [**fragment**]

Parameter

Parameter	Description	Value
rule-number	Specifies a filter number.	The value is an integer ranging from 1 to 2048.
src-ip-address/M any	Specifies a source IP address in an ACL rule.	<i>src-ip-address</i> is in dotted decimal notation. <i>M</i> is an integer ranging from 1 to 32. any means any source IP address.
dst-ip-address/M any	Specifies a destination IP address in an ACL rule.	<i>dst-ip-address</i> is in dotted decimal notation. <i>M</i> is an integer ranging from 1 to 32. any means any destination IP address.
src-port-number	Specifies a source port number.	The value is an integer ranging from

Parameter	Description	Value
		0 to 65535.
dst-port-number	Specifies a destination port number.	The value is an integer ranging from 0 to 65535.
source-port-number-range destination-port-number-range	Specifies a source port number range and destination port number range.	Both the start and end port numbers are integers ranging from 0 to 65535.
fragment	Specifies whether the rule is valid for the non-first fragment message only.	-
src-ip-mask	Specifies the mask of a source IP address in an ACL rule.	The value is in dotted decimal notation.
dst-ip-mask	Specifies the mask of a destination IP address in an ACL rule.	The value is in dotted decimal notation.

Default Value

NA

View

Filter configuration view, filter-hybrid configuration view

Usage Guidelines

NA

Example

Configure an ACL rule matching packets based on source and destination IPv4 addresses and the TCP fields (including syn, synack, ack, and fin fields).

```
Switch(configure-filter-ipv4-1500)#filter 100 tcp 1.1.1.1/10 10/20 2.2.2.2/20 20/30 syn fragment
Switch(configure-filter-ipv4-1500)#
Switch(configure-filter-ipv4-1500)#filter 100 tcp src-ip 1.1.1.1 src-mask 255.255.255.0 10/20 dst-ip 2.2.2.2
dst-mask 255.255.255.0 20/30 syn fragment
Switch(configure-filter-ipv4-1500)#
```

8.3.41 filter udp

Function

The **filter udp** command configures an ACL rule matching packets based on source and destination IPv4 addresses and the UDP field.

Format

- **filter rule-number udp** { *src-ip-address/M* | **any** } { *src-port-number* | **any** | *src-port-range* } { *dst-ip-address/M* | **any** } { *dst-port-number* | **any** | *dst-port-range* }
- **filter rule-number udp** { *src-ip-address/M* | **any** } { *src-port-number* | **any** | *src-port-range* } { *dst-ip-address/M* | **any** } { *dst-port-number* | **any** | *dst-port-range* } **fragment**
- **filter rule-number udp src-ip** { *src-ip-address* | **any** } { *src-ip-mask* | **any** } { *src-port-number* | *source-port-number-range/destination-port-number-range* | **any** } **dst-ip** { *src-ip-mask* | **any** } **dst-mask** { *dst-ip-mask* | **any** } { *dst-port-number* | **any** | *source-port-number-range/destination-port-number-range* } [**fragment**]

Parameter

Parameter	Description	Value
rule-number	Specifies a filter number.	The value is an integer ranging from 1 to 2048.
src-ip-address/M any	Specifies a source IP address in an ACL rule.	<i>src-ip-address</i> is in dotted decimal notation. <i>M</i> is an integer ranging from 1 to 32. any means any source IP address.
dst-ip-address/M any	Specifies a destination IP address in an ACL rule.	<i>dst-ip-address</i> is in dotted decimal notation. <i>M</i> is an integer ranging from 1 to 32. any means any destination IP address.
src-port-number	Specifies a source port number.	The value is an integer ranging from 0 to 65535.
src-port-range	Specifies a source port number range.	Both the start and end port numbers are integers ranging from 0 to 65535.
dst-port-number	Specifies a destination port number.	The value is an integer ranging from 0 to 65535.
dst-port-range	Specifies a destination port number range.	Both the start and end port numbers are integers ranging from 0 to 65535.
fragment	Specifies whether the rule is valid for the non-first fragment message only.	-
src-ip-mask	Specifies the mask of a source IP address in an ACL rule.	The value is in dotted decimal notation.
dst-ip-mask	Specifies the mask of a destination IP address in an ACL rule.	The value is in dotted decimal notation.

Default Value

NA

View

Filter configuration view, filter-hybrid configuration view

Usage Guidelines

NA

Example

Configure an ACL rule matching packets based on source and destination IPv4 addresses and the UDP field.

```
Switch(configure-filter-ipv4-1500)#filter 100 udp 1.1.1.1/10 10/20 2.2.2.2/20 20/30 fragment
Switch(configure-filter-ipv4-1500)#
Switch(configure-filter-ipv4-1500)#filter 100 udp src-ip 1.1.1.1 src-mask 255.255.255.0 10/20 dst-ip 2.2.2.2
dst-mask 255.255.255.0 20/30 fragment
Switch(configure-filter-ipv4-1500)#
```

8.3.42 filter-list

Function

The **filter-list** command creates a numbered access control list (ACL) and displays the ACL view.

Format

- **filter-list** *acl-number*
- **no filter-list** *acl-number*
- **filter-list** *acl-number name filter-name*

Parameter

Parameter	Description	Value
acl-number	Specifies an ACL number.	The value is an integer ranging from 1 to 4000.
filter-name	Specifies an ACL name.	The value is a character string.

Default Value

NA

View

Global configuration view

Usage Guidelines

One ACL consists of several ACL rules.

When creating an ACL, you need to specify a number, indicating the ACL category. For example, a number ranging from 1 to 1000 indicates a basic L2 ACL.



Note:

An ACL must be created before defining ACL rules.

Before configuring the subsequent ACL functional command, configure and bind filter entries.

Example

Create an ACL numbered 100.

```
Switch(config)#filter-list 100
Switch(configure-filter-l2-100)#
Switch(config)#no filter-list 100
Switch(config)#
```

8.3.43 filter-list-hybrid {in|out}

Function

The **filter-list-hybrid {in|out}** command configures hybrid ACLs in the inbound and outbound directions on all types of interfaces.

The **no filter-list-hybrid {in|out}** command deletes the hybrid ACL settings of interfaces.

Format

- **filter-list-hybrid { in | out } *acl-number***
- **filter-list-hybrid { in | out } **name** *acl-name***
- **no filter-list-hybrid { in | out }**

Parameter

Parameter	Description	Value
acl- name	Specifies the name of an ACL.	The value is a character string.
acl-number	Specifies a hybrid ACL value.	The value is an integer ranging from 2001 to 3000.

Default Value

NA

View

TDM configuration view, STM configuration view, Ethernet bridge interface configuration view, Ethernet router interface configuration view, interface configuration view (Trunk), Peerlink configuration view, VLAN configuration view

Usage Guidelines

NA

Example

Configure hybrid ACLs in the inbound and outbound directions.

```
Switch(config-10ge1/0/1)#filter-list-hybrid in 2001
Switch(config-10ge1/0/1)#
```

8.3.44 filter-list-ipv4 {in|out}

Function

The **filter-list-ipv4 {in|out}** command configures L3 ACLs in the inbound and outbound directions on all types of interfaces.

The **no filter-list-ipv4 {in|out}** command deletes the L3 ACL settings of interfaces.

Format

- **filter-list-ipv4 { in | out } *acl-number***
- **filter-list-ipv4 { in | out } **name** *acl-name***
- **no filter-list-ipv4 { in | out }**

Parameter

Parameter	Description	Value
acl- name	Specifies the name of an ACL.	The value is a character string.
acl-number	Specifies a hybrid ACL value.	The value is an integer ranging from 1001 to 2000.

Default Value

NA

View

Ethernet bridge interface configuration view, Ethernet router interface configuration view, interface configuration view (trunk), Peerlink configuration view, VLAN configuration view

Usage Guidelines

NA

Example

Configure L3 ACLs in the inbound and outbound directions.

```
Switch(config-10ge1/0/1)#filter-list-ipv4 in 1001
Switch(config-10ge1/0/1)#
```

8.3.45 filter-list-ipv6 {in|out}

Function

The **filter-list-ipv6 {in|out}** command configures IPv6 ACLs in the inbound and outbound directions on all types of interfaces.

The **no filter-list-ipv6 {in|out}** command deletes the IPv6 ACL settings of interfaces.

Format

- **filter-list-ipv6 { in | out } *acl-number***
- **filter-list-ipv6 { in | out } *name acl-name***
- **no filter-list-ipv6 { in | out }**

Parameter

Parameter	Description	Value
acl- name	Specifies the name of an ACL.	The value is a character string.
acl-number	Specifies a hybrid ACL value.	The value is an integer ranging from 3001 to 4000.

Default Value

NA

View

Ethernet bridge interface configuration view, Ethernet router interface configuration view, interface configuration view (trunk), Peerlink configuration view, VLAN configuration view

Usage Guidelines

NA

Example

Configure IPv6 ACLs in the inbound and outbound directions.

```
Switch(config-10ge1/0/1)#filter-list-ipv6 in 3001
Switch(config-10ge1/0/1)#
```

8.3.46 filter-list-l2 {in|out}

Function

The **filter-list-l2 {in|out}** command configures L2 ACLs in the inbound and outbound directions on all types of interfaces.

The **no filter-list-l2 {in|out}** command deletes the L2 ACL settings of interfaces.

Format

- **filter-list-l2 { in | out } *acl-number***
- **filter-list-l2 { in | out } **name** *acl-name***
- **no filter-list-l2 { in | out }**

Parameter

Parameter	Description	Value
acl- name	Specifies the name of an ACL.	The value is a character string.
acl-number	Specifies a hybrid ACL value.	The value is an integer ranging from 1 to 1000.

Default Value

NA

View

Ethernet bridge interface configuration view, Ethernet router interface configuration view, interface configuration view (trunk), Peerlink configuration view, VLAN configuration view

Usage Guidelines

NA

Example

Configure L2 ACLs in the inbound and outbound directions.

```
Switch(config-10ge1/0/1)#filter-list-l2 in 1
Switch(config-10ge1/0/1)#
```

8.3.47 filter action {outer-tag-priority|inner-tag-priority}

Function

The **filter action {outer-tag-priority|inner-tag-priority}** command configures an ACL rule to modify the outer or inner tag priority.

Format

- **filter rule-number action { outer-tag-priority | inner-tag-priority } priority-value**

Parameter

Parameter	Description	Value
rule-number	Specifies an ACL rule number.	The value is an integer ranging from 1 to 2048.
priority-value	Specifies an outer or inner tag priority.	The value is an integer ranging from 0 to 7.

Default Value

NA

View

L2 Filter configuration view, Filter configuration view, filter-hybrid configuration view, Filter configuration view (IPv6)

Usage Guidelines

NA

Example

Configure an ACL rule to modify the outer tag priority.

```
Switch(configure-filter-l2-100)#filter 1 action outer-tag-priority 1
Switch(configure-filter-l2-100)#
```

8.3.48 filter-list-hybrid global {in|out}

Function

The **filter-list-hybrid {in|out}** command globally configures hybrid ACLs in the inbound and outbound directions.

The **filter-list-hybrid {in|out}** command deletes hybrid ACL global settings.

Format

- **filter-list-hybrid global { in | out } acl-number**

- **no filter-list-hybrid global { in | out }**

Parameter

Parameter	Description	Value
acl- name	Specifies the name of an ACL.	The value is a character string.
acl-number	Specifies a hybrid ACL value.	The value is an integer ranging from 2001 to 3000.

Default Value

NA

View

Global configuration view

Usage Guidelines

NA

Example

Globally configure hybrid ACLs in the inbound and outbound directions.

```
Switch(config)#filter-list-hybrid global in 2001
Switch(config)#
```

8.3.49 filter-list-ipv4 global {in|out}

Function

The **filter-list-ipv4 global {in|out}** command globally configures L3 ACLs in the inbound and outbound directions.

The **no filter-list-ipv4 global {in|out}** command deletes L3 ACL global settings.

Format

- **filter-list-ipv4 global { in | out } *acl-number***
- **no filter-list-ipv4 global { in | out }**

Parameter

Parameter	Description	Value
acl- name	Specifies the name of an ACL.	The value is a character string.
acl-number	Specifies a hybrid ACL value.	The value is an integer ranging from 1001 to 2000.

Default Value

NA

View

Global configuration view

Usage Guidelines

NA

Example

Globally configure L3 ACLs in the inbound and outbound directions.

```
Switch(config)#filter-list-ipv4 global in 1001
Switch(config)#
```

8.3.50 filter-list-ipv6 global {in|out}**Function**

The **filter-list-ipv6 global {in|out}** command globally configures IPv6 ACLs in the inbound and outbound directions.

The **no filter-list-ipv6 global {in|out}** command deletes the IPv6 ACL global settings.

Format

- **filter-list-ipv6 global { in | out } *acl-number***
- **no filter-list-ipv6 global { in | out }**

Parameter

Parameter	Description	Value
acl- name	Specifies the name of an ACL.	The value is a character string.
acl-number	Specifies a hybrid ACL value.	The value is an integer ranging from 3001 to 4000.

Default Value

NA

View

Global configuration view

Usage Guidelines

NA

Example

Globally configure IPv6 ACLs in the inbound and outbound directions.

```
Switch(config)#filter-list-ipv6 global in 3001
Switch(config)#
```

8.3.51 filter-list-l2 global {in|out}**Function**

The **filter-list-l2 global {in|out}** command globally configures L2 ACLs in the inbound and outbound directions.

The **no filter-list-l2 global{in|out}** command deletes L2 ACL global settings.

Format

- **filter-list-l2 global { in | out } *acl-number***
- **no filter-list-l2 global { in | out }**

Parameter

Parameter	Description	Value
acl- name	Specifies the name of an ACL.	The value is a character string.
acl-number	Specifies a hybrid ACL value.	The value is an integer ranging from 1 to 1000.

Default Value

NA

View

Global configuration view

Usage Guidelines

NA

Example

Globally configure L2 ACLs in the inbound and outbound directions.

```
Switch(config)#filter-list-l2 global in 1
Switch(config)#
```

8.4 ACL6 Configuration Commands

8.4.1 filter icmp6

Function

The **filter ip icmp6** command configures an ACL rule matching packets based on source and destination IPv6 addresses and the ICMP6 field.

Format

- **filter rule-number icmp6** { *src-ip6-address/M* | **any** } { *dst-ip6-address/M* | **any** } [**fragment**]
- **filter rule-number icmp6** { *src-ip6-address/M* | **any** } { *dst-ip6-address/M* | **any** } { *icmp-type* | **any** } { *icmp-code* | **any** } [**fragment**]

Parameter

Parameter	Description	Value
rule-number	Specifies a filter number.	The value is an integer ranging from 1 to 2048.
src-ip6-address/M any	Specifies a source IP address in an ACL rule.	<i>src-ip6-address</i> is in dotted hexadecimal notation, in the X:X::X:X format. <i>M</i> is an integer ranging from 1 to 128. any means any source IP address.
dst-ip6-address/M any	Specifies a destination IP address in an ACL rule.	<i>dst-ip6-address</i> is in dotted decimal notation. <i>M</i> is an integer ranging from 1 to 128. any means any destination IP address.
icmp-type	Specifies an ICMP type range in an ACL rule.	The value is an integer ranging from 0 to 255.
icmp-code	Specifies an ICMP code range in an ACL rule.	The value is an integer ranging from 0 to 255.

Default Value

NA

View

Filter configuration view (IPv6)

Usage Guidelines

NA

Example

Configure an ACL rule matching packets based on source and destination IPv6 addresses and ICMP6 field.

```
Switch(configure-filter-ipv6-3500)#filter 100 icmp6 1:1::1/10 2:2::2/20 100 100
Switch(configure-filter-ipv6-3500)#
```

8.4.2 filter igmp6

Function

The **filter ip igmp6** command configures an ACL rule matching packets based on source and destination IPv6 addresses and the IGMP6 code field.

Format

filter *rule-number* **igmp6** { *src-ip6-address/M* | **any** } { *dst-ip6-address/M* | **any** }

Parameter

Parameter	Description	Value
rule-number	Specifies a filter number.	The value is an integer ranging from 1 to 2048.
src-ip6-address/M any	Specifies a source IP address in an ACL rule.	<i>src-ip6-address</i> is in dotted hexadecimal notation, in the X:X::X:X format. <i>M</i> is an integer ranging from 1 to 128. any means any source IP address.
dst-ip6-address/M any	Specifies a destination IP address in an ACL rule.	<i>dst-ip6-address</i> is in dotted hexadecimal notation, in the X:X::X:X format. <i>M</i> is an integer ranging from 1 to 128. any means any destination IP address.

Default Value

NA

View

Filter configuration view (IPv6)

Usage Guidelines

NA

Example

Configure an ACL rule matching packets based on source and destination IPv6 addresses and the IGMP6 code field.

```
Switch(configure-filter-ipv6-3500)#filter 100 igmp6 1:1::1/10 2:2::2/20
```



```
Switch(configure-filter-ipv6-3500)#
```

8.4.3 filter ip6

Function

The **filter ip6** command configures an ACL rule matching packets based on source and destination IPv6 addresses.

Format

filter *rule-number* **ip6** { *src-ip6-address/M* | **any** } { *dst-ip6-address/M* | **any** }

Parameter

Parameter	Description	Value
rule-number	Specifies an ACL rule number.	The value is an integer ranging from 1 to 2048.
src-ip6-address/M any	Specifies a source IP address in an ACL rule.	<i>src-ip6-address</i> is in dotted hexadecimal notation, in the X:X::X:X format. <i>M</i> is an integer ranging from 1 to 128. any means any source IP address.
dst-ip6-address/M any	Specifies a destination IP address in an ACL rule.	<i>dst-ip6-address</i> is in dotted hexadecimal notation, in the X:X::X:X format. <i>M</i> is an integer ranging from 1 to 128. any means any destination IP address.

View

Filter configuration view (IPv6)

Usage Guidelines

After the ACL rule is applied to an interface, the system filters data packets received on the interface based on the IPv6 addresses in the packets. Packets matching the ACL rule are processed based on the action configured for the ACL rule.



Caution

ACLs are classified into four levels:

Switch(config)#filter-list

in In direction

out Out direction

<1-1000> L2 filter list number

<1001-2000> Ipv4 filter list number

<2001-3000> Hybrid filter list number

<3001-4000> Ipv6 filter list number

Therefore, the **filter ip6** and associated commands are applicable only to IPv6 ACLs 3001 to 4000.

Example

Configure an ACL rule based on the source and destination IPv6 address.

```
Switch(configure-filter-ipv6-3500)#filter 100 ip6 1:1::1:1/10 2:2::2:2/20
Switch(configure-filter-ipv6-3500)#
```

8.4.4 filter ip6 hop-limit

Function

The **filter ip6 hop-limit** command configures an ACL rule matching packets based on source and destination IPv6 addresses.

Format

filter *rule-number* **ip6** { *src-ip6-address/M* | **any** } { *dst-ip6-address/M* | **any** } **hop-limit** *hop-limit-value*

Parameter

Parameter	Description	Value
rule-number	Specifies an ACL rule number.	The value is an integer ranging from 1 to 2048.
src-ip6-address/M any	Specifies a source IP address in an ACL rule.	<i>src-ip6-address</i> is in dotted hexadecimal notation, in the X:X::X:X format. <i>M</i> is an integer ranging from 1 to 128. any means any source IP address.
dst-ip6-address/M any	Specifies a destination IP address in an ACL rule.	<i>dst-ip6-address</i> is in dotted hexadecimal notation, in the X:X::X:X format. <i>M</i> is an integer ranging from 1 to 128. any means any destination IP address.
hop-limit-value	Specifies the limit on the number of hops.	The value is an integer ranging from 1 to 255.

View

Filter configuration view (IPv6)

Usage Guidelines

After the ACL rule is applied to an interface, the system filters data packets received on the interface based on the IPv6 addresses in the packets. Packets matching the ACL rule are processed based on the action configured for the ACL rule, including the limit on the number of hops for the next packet.

Example

Configure an ACL rule based on the source and destination IPv6 address.

```
Switch(configure-filter-ipv6-3500)#filter 100 ip6 1:1::1:1/10 2:2::2:2/20 hop-limit 10
Switch(configure-filter-ipv6-3500)#
```

8.4.5 filter ip6 next-header

Function

The **filter ip6 next-header** command configures an ACL rule matching packets based on source and destination IPv6 addresses.

Format

filter *rule-number* **ip6** { *src-ip6-address/M* | **any** } { *dst-ip6-address/M* | **any** } **next-header** *next-header-value*

Parameter

Parameter	Description	Value
rule-number	Specifies an ACL rule number.	The value is an integer ranging from 1 to 2048.
src-ip6-address/M any	Specifies a source IP address in an ACL rule.	<i>src-ip6-address</i> is in dotted hexadecimal notation, in the X:X::X:X format. <i>M</i> is an integer ranging from 1 to 128. any means any source IP address.
dst-ip6-address/M any	Specifies a destination IP address in an ACL rule.	<i>dst-ip6-address</i> is in dotted hexadecimal notation, in the X:X::X:X format. <i>M</i> is an integer ranging from 1 to 128. any means any destination IP address.
next-header-value	Specifies the value of the next header.	The value is an integer ranging from 1 to 255.

View

Filter configuration view (IPv6)

Usage Guidelines

After the ACL rule is applied to an interface, the system filters data packets received on the interface based on the IPv6 addresses in the packets. Packets matching the ACL rule are processed based on the action configured for the ACL rule, including the processing of the next packet's header value.

Example

Configure an ACL rule based on the source and destination IPv6 address.

```
Switch(configure-filter-ipv6-3500)#filter 100 ip6 1::1:1/10 2::2:2/20 next-header 10
Switch(configure-filter-ipv6-3500)#
```

8.4.6 filter ip6 traffic-class

Function

The **filter ip6 traffic-class** command configures an ACL rule matching packets based on source and destination IPv6 addresses and the traffic class.

Format

filter *rule-number* { *src-ip6-address/M* | **any** } { *dst-ip6-address/M* | **any** } **traffic-class** *traffic-value*

Parameter

Parameter	Description	Value
rule-number	Specifies an ACL rule number.	The value is an integer ranging from 1 to 2048.
src-ip6-address/M any	Specifies a source IPv6 address in an ACL rule.	<i>src-ip6-address</i> is in dotted hexadecimal notation, in the X:X::X:X format. <i>M</i> is an integer ranging from 1 to 128. any means any source IP address.
dst-ip6-address/M any	Specifies a destination IPv6 address in an ACL rule.	<i>dst-ip6-address</i> is in dotted hexadecimal notation, in the X:X::X:X format. <i>M</i> is an integer ranging from 1 to 128. any means any destination IP address.
traffic-value	Specifies a traffic class value.	The value is an integer ranging from 0 to 255.

View

Filter configuration view (IPv6)

Usage Guidelines

After the ACL rule is applied to an interface, the system filters data packets received on the interface based on the IPv6 addresses and traffic class value in the packets. Packets matching the ACL rule are processed based on the action configured for the ACL rule.

Example

Configure an ACL rule based on the source and destination IPv6 address.

```
Switch(configure-filter-ipv6-3500)#filter 100 ip6 1:1::1/10 2:2::2/20 traffic-class 10
Switch(configure-filter-ipv6-3500)#
```

8.4.7 filter tcp6**Function**

The **filter tcp6** command configures an ACL rule matching packets based on source and destination IPv6 addresses and the TCP6 fields (including syn, synack, ack, and fin fields).

Format

- **filter rule-number tcp6** { *src-ip6-address/M* | **any** } { *src-port-number* | **any** | *src-port-range* } { *dst-ip6-address/M* | **any** } { *dst-port-number* | **any** | *dst-port-range* }
- **filter rule-number tcp6** { *src-ip6-address/M* | **any** } { *src-port-number* | **any** | *src-port-range* } { *dst-ip6-address/M* | **any** } { *dst-port-number* | **any** | *dst-port-range* } **fragment**
- **filter rule-number tcp6** { *src-ip6-address/M* | **any** } { *src-port-number* | **any** | *src-port-range* } { *dst-ip6-address/M* | **any** } { *dst-port-number* | **any** | *dst-port-range* } { **syn** | **synack** | **ack** | **fin** }
- **filter rule-number tcp6** { *src-ip6-address/M* | **any** } { *src-port-number* | **any** | *src-port-range* } { *dst-ip6-address/M* | **any** } { *dst-port-number* | **any** | *dst-port-range* } { **syn** | **synack** | **ack** | **fin** } **fragment**

Parameter

Parameter	Description	Value
rule-number	Specifies a filter number.	The value is an integer ranging from 1 to 2048.
src-ip6-address/M any	Specifies a source IP address in an ACL rule.	<i>src-ip6-address</i> is in dotted hexadecimal notation, in the X:X::X:X format. <i>M</i> is an integer ranging from 1 to 128. any means any source IP address.
dst-ip6-address/M any	Specifies a destination IP address in an ACL rule.	<i>dst-ip6-address</i> is in dotted hexadecimal notation, in the X:X::X:X format. <i>M</i> is an integer ranging from 1 to 128. any means any destination IP address.
src-port-number	Specifies a source port number.	The value is an integer ranging from 0 to 65535.
dst-port-number	Specifies a destination port number.	The value is an integer ranging from 0 to

Parameter	Description	Value
		65535.
src-port-range	Specifies a source port number range.	Both the start and end port numbers are integers ranging from 0 to 65535.
dst-port-range	Specifies a destination port number range.	Both the start and end port numbers are integers ranging from 0 to 65535.
fragment	Specifies whether the rule is valid for the non-first fragment message only.	-

Default Value

NA

View

Filter configuration view (IPv6)

Usage Guidelines

NA

Example

Configure an ACL rule matching packets based on source and destination IPv6 addresses and the TCP6 fields (including syn, synack, ack, and fin fields).

```
Switch(configure-filter-ipv6-3500)#filter 100 tcp6 1:1::1/10 10/20 2:2::2/20 20/30 fragment
Switch(configure-filter-ipv6-3500)#
```

8.4.8 filter udp6

Function

The **filter ip udp6** command configures an ACL rule matching packets based on source and destination IPv6 addresses and the UDP6 field.

Format

- **filter rule-number udp6** { *src-ip6-address/M* | **any** } { *src-port-number* | **any** | *src-port-range* } { *dst-ip6-address/M* | **any** } { *dst-port-number* | **any** | *dst-port-range* }
- **filter rule-number udp6** { *src-ip6-address/M* | **any** } { *src-port-number* | **any** | *src-port-range* } { *dst-ip6-address/M* | **any** } { *dst-port-number* | **any** | *dst-port-range* } **fragment**

Parameter

Parameter	Description	Value

Parameter	Description	Value
rule-number	Specifies a filter number.	The value is an integer ranging from 1 to 2048.
src-ip6-address/M any	Specifies a source IP address in an ACL rule.	<i>src-ip6-address</i> is in dotted hexadecimal notation, in the X:X::X:X format. <i>M</i> is an integer ranging from 1 to 128. any means any source IP address.
dst-ip6-address/M any	Specifies a destination IP address in an ACL rule.	<i>dst-ip6-address</i> is in dotted hexadecimal notation, in the X:X::X:X format. <i>M</i> is an integer ranging from 1 to 128. any means any destination IP address.
src-port-number src-port-range any	Specifies a source port number or its range.	The value is an integer in the range of 0-65535 or 0-65535/0-65535.
dst-port-number dst-port-range any	Specifies a destination port number or its range.	The value is an integer in the range of 0-65535 or 0-65535/0-65535.
fragment	Specifies whether the rule is valid for the non-first fragment message only.	-

Default Value

NA

View

Filter configuration view (IPv6)

Usage Guidelines

NA

Example

Configure an ACL rule matching packets based on source and destination IPv6 addresses and the UDP6 field.

```
Switch(configure-filter-ipv6-3500)#filter 100 udp6 1:1::1:1/10 10/20 2:2::2:2/20 20/30 fragment
Switch(configure-filter-ipv6-3500)#
```

8.5 CPU Defense Configuration Commands

8.5.1 debug cpu-defend

Function

The **debug cpu-defend** command enables debugging of the CPU defense function.

The **no debug cpu-defend** command disables debugging of the CPU defense function.

Format

- **debug cpu-defend**
- **no debug cpu-defend**

Parameter

NA

Default Value

NA

View

Privileged user view

Usage Guidelines

NA

Example

Enable debugging of the CPU defense function.

```
Switch#debug cpu-defend
Switch#
```

8.5.2 cpu-defend policy

Function

The **cpu-defend policy** command binds a CPU defense policy.

The **no cpu-defend policy** command unbinds a CPU defense policy.

Format

- **cpu-defend policy** *policy-name*
- **no cpu-defend policy** *policy-name*

Parameter

Parameter	Description	Value
policy-name	Specifies a CPU defense policy name.	The value is a character string.

Default Value

NA

View

Global configuration view

Usage Guidelines

NA

Example

Bind CPU defense policy **aaa** to the system.

```
Switch(config)#cpu-defend policy aaa
Switch(config)#
```

8.5.3 car packet-type**Function**

The **car packet-type** command configures the Committed Information Rate (CIR) and Committed Burst Size (CBS) for protocol packets.

The **no car packet-type** command deletes the CIR and CBS settings of protocol packets.

Format

- **car packet-type { bpdutunnel | fib6hit | fibhit | icmp | snmp | ssh | tcp | telnet | total } cir { cir | default }**
- **car packet-type { bpdutunnel | fib6hit | fibhit | icmp | snmp | ssh | tcp | telnet | total } cir { cir | default } cbs { cbs | default }**
- **no car packet-type { bpdutunnel | fib6hit | fibhit | icmp | snmp | ssh | tcp | telnet | total }**

Parameter

Parameter	Description	Value
bpdutunnel fib6hit fibhit icmp snmp ssh tcp telnet total	Specifies the protocol type of packets.	-
cir	Specifies a CIR range.	The value is an integer ranging

Parameter	Description	Value
		from 64 to 4294967295.
cbs	Specifies a CBS range.	The value is an integer ranging from 10000 to 4294967295.

Default Value

NA

View

CPU defense policy configuration

Usage Guidelines

NA

Example

Configure the CIR and CBS for protocol packets.

```
Switch(config-policy-111)#car packet-type telnet cir 12000 cbs 300000
Switch(config-policy-111)#
```

8.5.4 description**Function**The **description** command configures the description of a CPU defense policy.The **no description** command cancels the description settings of a CPU defense policy.**Format**

- **description** *descr*
- **no description**

Parameter

Parameter	Description	Value
descr	Specifies the value of a user-defined flow.	The value is a character string.

Default Value

NA

View

CPU defense policy configuration

Usage Guidelines

NA

Example

Cancel the description settings of a CPU defense policy.

```
Switch(config-policy-111)#no description
Switch(config-policy-111)#
```

8.5.5 show cpu-defend config**Function**

The **show cpu-defend config** command displays the CPU defense configuration.

Format

show cpu-defend config

Parameter

NA

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

Display the CPU defense configuration.

```
Switch>show cpu-defend config
  cpu-defend policy 1
Switch>
```

8.5.6 packet-type queue**Function**

The **packet-type queue** command configures the number of the queue for sending protocol packets to the CPU.

Format

packet-type { **bpdutunnel** | **fib6hit** | **fibhit** | **icmp** | **snmp** | **ssh** | **tcp** | **telnet** | **total** } **queue**
 { *queue-value* **default** }

Parameter

Parameter	Description	Value
queue-value	Specifies a queue number.	The value is an integer ranging from 0 to 7.

Default Value

7

View

CPU defense policy configuration

Usage Guidelines

The greater the queue number is, the higher the priority is.

Example

Set the number of the queue for sending protocol packets to the CPU to 1.

```
Switch(config-policy-1)#packet-type tcp queue 1
Switch(config-policy-1)#
```

8.5.7 cpu-defend bind-policy**Function**

The **cpu-defend bind-policy** command binds a specified CPU defense policy.

The **no cpu-defend bind-policy** command unbinds a CPU defense policy.

Format

- **cpu-defend bind-policy** *policy-name*
- **no cpu-defend bind-policy** *policy-name*

Parameter

Parameter	Description	Value
policy-name	Specifies the name of a CPU defense policy.	The value is a string of no more than 31 bytes.

Default Value

NA

View

Global configuration view

Usage Guidelines

NA

Example

Bind a specified CPU defense policy.

```
Switch(config)#cpu-defend bind-policy name1
Switch(config)#
```

8.5.8 show cpu-defend policy**Function**

The **show cpu-defend policy** command displays information about all CPU defense policies or a specified CPU defense policy.

Format

- **show cpu-defend policy**
- **show cpu-defend policy *policy-name***

Parameter

Parameter	Description	Value
policy-name	Specifies the name of a defense policy.	The value is a character string.

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

Display information about all CPU defense policies.

```

Switch>show cpu-defend policy
Current in use: default
Policy Name                               :default
Description                               :
Car Packet Configuration
Packet Type      Cir      Cbs      Pps      Priority  Queue  Action
total            800      6400    ---      2         0      no deny
bpdutunnel       64       6400    ---      2         2      no deny

Switch>

```

8.5.9 cpu-defend application-apperceive

Function

The **cpu-defend application-apperceive** command enables or disables dynamic link protection.

Format

cpu-defend application-apperceive { isis | ospf | bgp | isis6 | ospf6 | bgp6 } { enable | disable }

Parameter

Parameter	Description	Value
enable	Enables dynamic link protection.	-
disable	Disables dynamic link protection.	-

Default Value

Disable

View

Global configuration view

Usage Guidelines

When packets are sent to the CPU, they are allocated to a CPU queue. If the rate of sending the packets to the CPU exceeds the configured CAR value, the packets are discarded. After protocol linkage is configured for packets by running this command, the protocol packets for which a connection is established are allocated to a special protocol linkage queue. This prevents the packet rate from exceeding the CAR value resulting in discarded packets.

Example

Enable protocol linkage for OSPF packets.

```
Switch(config)#cpu-defend application-apperceive ospf enable
Switch(config)#
```

8.6 Anti-attack Configuration Commands

8.6.1 show antiattack config

Function

The **show antiattack config** command displays the anti-attack configuration.

Format

show antiattack config

Parameter

NA

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

Display the anti-attack configuration.

```
Switch> show antiattack config
Version: ANTIATTACK_VX2.10.00.00
Switch>
```

8.6.2 debug antiattack

Function

The **debug antiattack** command enables debugging of the anti-attack function.

The **no debug antiattack** command disables debugging of the anti-attack function.

Format

- **debug antiattack**
- **no debug antiattack**

Parameter

NA

Default Value

By default, debugging of the anti-attack function is disabled.

View

Privileged user view

Usage Guidelines

NA

Example

Enable debugging of the anti-attack function.

```
Switch#debug antiattack
2100/01/01 01:08:40 antiattack:antiAttackSetApi is OK.
Switch#
```

8.6.3 antiattack pkt-limit {enable|disable}**Function**

The **antiattack pkt-limit {enable|disable}** command globally enables or disables packet limiting.

Format

antiattack pkt-limit { enable | disable }

Parameter

Parameter	Description	Value
enable	Enables packet limiting.	-
disable	Disables packet limiting.	-

Default Value

By default, packet limiting is disabled.

View

Global configuration view

Usage Guidelines

After packet limiting is enabled, packets exceeding the set limit are discarded.

Example

Enable packet limiting for the switch.

```
Switch(config)#antiattack pkt-limit enable
Switch(config)#
```

8.6.4 antiattack pkt-limit

Function

The **antiattack pkt-limit** command sets the limit on a specified packet type.

Format

antiattack pkt-limit *packet-type max-num*

Parameter

Parameter	Description	Value
packet-type	Specifies a packet type.	arp-request: limit on request packets of the Address Resolution Protocol (ARP)
		arp-replay: limit on response ARP packets
		stp: limit on packets of the Spanning Tree Protocol (STP)
		icmp: limit on packets of the Internet Control Message Protocol (ICMP)
		igmp: limit on packets of the Internet Group Management Protocol (IGMP)
		dhcp: limit on packets of the Dynamic Host Configuration Protocol (DHCP)
		udp: limit on all protocol packets except Routing Information Protocol (RIP) packets
		tcp: limit on all protocol packets except Border Gateway Protocol (BGP) packets
		sgm: limit on packets of the Switch Group Management (SGM) protocol
		other: limit on packets of any other types
		ip-to-self: limit on IP packets except ICMP, IGMP, UDP, TCP, BGP, RIP, and OSPF packets
		ip-forward: limit on IP packets except ICMP, IGMP, UDP,

Parameter	Description	Value
		TCP, BGP, RIP, and OSPF packets
		ospf: limit on OSPF packets forwarded by the switch
		bgp: limit on BGP packets forwarded by the switch
		rip: limit on RIP packets forwarded by the switch
max-num	Specifies the maximum packet rate.	The value is an integer ranging from 0 to 3000, in packets/sec. 0 means denial of all packets.

Default Value

NA

View

Global configuration view

Usage Guidelines

Before using this command to set an ARP packet limit for the switch, run **antiattack pkt-limit enable** to enable the packet limit function.

Example

Configure the switch to permit up to 300 request packets of ARP-based address resolution to pass per second.

```
Switch(config)#antiattack pkt-limit arp-request 300
Switch(config)#
```

8.6.5 arp-antiattack {src-ip|src-mac|arp-cheat|gratuitous-arp}

Function

The **arp-antiattack {src-ip|src-mac|arp-cheat|gratuitous-arp}** command enables or disables the ARP anti-attack function, that is, packet check against the ARP table.

Format

arp-antiattack { src-ip | src-mac | arp-cheat } { enable | disable }

Parameter

Parameter	Description	Value
src-ip	Checks whether the source IP address conflicts with the ARP table.	-
src-mac	Checks whether the source MAC address conflicts with the ARP table.	-
arp-cheat	Indicates ARP anti-snooping.	-

Parameter	Description	Value
enable	Enables the ARP anti-attack function.	-
disable	Disables the ARP anti-attack function.	-

Default Value

Disable

View

Global configuration view

Usage Guidelines

This command enables the switch to check received packets with the specified check items to prevent ARP snooping.

Example

Enable the switch to check whether the source IP address in a packet conflicts with the ARP entry.

```
Switch(config)#arp-antiattack src-ip enable
```

```
Switch(config)#
```

8.6.6 arp-antiattack check user-bind {enable|disable}

Function

The **arp-antiattack check user-bind {enable|disable}** command enables or disables the check of ARP packets against the binding table on an interface.

Format

arp-antiattack check user-bind { enable | disable }

Parameter

Parameter	Description	Value
enable	Enables the check of ARP packets against the binding table on an interface.	-
disable	Disables the check of ARP packets against the binding table on an interface.	-

Default Value

By default, the function of checking whether ARP packets match the binding table on the interface is disabled.

View

Ethernet bridge interface configuration view, Ethernet routing interface configuration view, interface configuration view (Trunk)

Usage Guidelines

After you enable the check of ARP packets against the binding table on an interface using this command, the system matches all ARP packets passing received on the interface with the binding table. Only the ARP packets matching the binding table are forwarded.

This command can prevent unauthorized users from accessing the external network through the switch and protects authorized users against interference and spoofing from unauthorized users.

Example

Enable the check of ARP packets against the binding table on an interface.

```
Switch(config-10ge1/0/1)#arp-antiattack check user-bind enable
Switch(config-10ge1/0/1)#
```

8.6.7 arp-antiattack check user-bind alarm

Function

The **arp-antiattack check user-bind alarm {enable|disable}** command enables or disables the alarm function for the check of ARP packets against the binding table on an interface.

Format

arp-antiattack check user-bind alarm { enable | disable }

Parameter

Parameter	Description	Value
enable	Enables the alarm function for the check of ARP packets against the binding table on an interface.	-
disable	Disables the alarm function for the check of ARP packets against the binding table on an interface.	-

Default Value

By default, the alarm function for the check of ARP packets against the binding table on an interface is disabled.

View

Ethernet router interface configuration view, interface configuration view (trunk)

Usage Guidelines

NA

Example

Enable the alarm function for the check of ARP packets against the binding table on an interface.

```
Switch(config-10ge1/0/1)#arp-antiattack check user-bind alarm enable
Switch(config-10ge1/0/1)#
```

8.6.8 arp-antiattack check user-bind alarm threshold**Function**

The **arp-antiattack check user-bind alarm threshold** command sets an alarm threshold for the check of ARP packets against the binding table on an interface.

Format

arp-antiattack check user-bind alarm threshold { *threshold-value* | **default** }

Parameter

Parameter	Description	Value
threshold-value	Specifies an alarm threshold for the check of ARP packets against the binding table.	The value ranges from 1 to 1000.
default	Specifies the default value.	100

Default Value

100

View

Ethernet bridge interface configuration view, Ethernet routing interface configuration view, interface configuration view (Trunk)

Usage Guidelines

NA

Example

Set an alarm threshold for the check of ARP packets against the binding table.

```
Switch(config-10ge1/0/1)#arp-antiattack check user-bind alarm threshold 200
Switch(config-10ge1/0/1)#
```

8.6.9 arp-antiattack check user-bind check-item

Function

The **arp-antiattack check user-bind check-item** command configures the check items when the switch matches ARP packets with the binding table.

The **no arp-antiattack check user-bind check-item** command restores the check items to default values.

Format

- **arp-antiattack check user-bind check-item { ip-address | mac-address | vlan }**
- **arp-antiattack check user-bind check-item ip-address vlan**
- **arp-antiattack check user-bind check-item mac-address vlan**
- **arp-antiattack check user-bind check-item ip-address mac-address**
- **no arp-antiattack check user-bind check-item**

Parameter

Parameter	Description	Value
ip-address	Indicates the IP address concerned in the check.	-
mac-address	Indicates the MAC address concerned in the check.	-
vlan	Indicates the VLAN concerned in the check.	-

Default Value

By default, the IP address, MAC address, and VLAN must be checked.

View

Ethernet bridge interface configuration view, Ethernet routing interface configuration view, interface configuration view (Trunk)

Usage Guidelines

Before using this command, run **arp-antiattack check user-bind enable** to enable the function of checking whether ARP packets match the binding table on the interface.



Note:

The ARP packet check does not take effect to users configured with the static binding table. Packets of these users are still checked in accordance with the static binding table.

Example

Configure the system to check IP addresses of ARP packets when matching ARP packets with the binding table.

```
Switch(config)#interface xgigaethernet 1/0/1
Switch(config-10ge1/0/1)#arp-antiattack check user-bind enable
Switch(config-10ge1/0/1)#arp-antiattack check user-bind check-item ip-address
Switch(config-10ge1/0/1)#
```

8.6.10 arp-antiattack gratuitous-arp {enable|disable}**Function**

The **arp-antiattack gratuitous-arp {enable|disable}** command enables or disables gratuitous ARP packet active transmission for the ARP anti-attack function.

Format

arp-antiattack gratuitous-arp { enable | disable }

Parameter

Parameter	Description	Value
enable	Enables gratuitous ARP packet active transmission for the ARP anti-attack function.	-
disable	Disables gratuitous ARP packet active transmission for the ARP anti-attack function.	-

Default Value

Disable

View

Global configuration view

Usage Guidelines

NA

Example

Enable gratuitous ARP packet active transmission for the ARP anti-attack function.

```
Switch(config)#arp-antiattack gratuitous-arp enable
Switch(config)#
```

8.6.11 debug arp-antiattack

Function

The **debug arp-antiattack** command enables ARP anti-attack debugging.

The **no debug arp-antiattack** command disables ARP anti-attack debugging.

Format

- **debug arp-antiattack**
- **no debug arp-antiattack**

Parameter

NA

Default Value

By default, ARP anti-attack debugging is disabled.

View

Privileged user view

Usage Guidelines

NA

Example

Enable ARP anti-attack debugging.

```
Switch#debug arp-antiattack
Switch#
```

8.6.12 arp-antiattack gateway-cheat {enable|disable}

Function

The **arp-antiattack gateway-cheat {enable|disable}** command enables or disables ARP gateway anti-spoofing.

Format

arp-antiattack gateway-cheat { enable | disable }

Parameter

Parameter	Description	Value

Parameter	Description	Value
enable	Enables ARP gateway anti-spoofing.	-
disable	Disables ARP gateway anti-spoofing.	-

Default Value

NA

View

Global configuration view

Usage Guidelines

NA

Example

Enable ARP gateway anti-spoofing.

```
Switch(config)#arp-antiattack gateway-cheat enable
Switch(config)#
```

8.6.13 reset arp-antiattack statistic check user-bind**Function**

The **reset arp-antiattack statistic check user-bind** command resets the counter of packets dropped to binding table mismatch.

Format**reset arp-antiattack statistic check user-bind****Parameter**

NA

Default Value

NA

View

Ethernet bridge interface configuration view, Ethernet routing interface configuration view, interface configuration view (Trunk)

Usage Guidelines

After ARP packet match is enabled, dropped packets are counted. You can use this command to reset the counter.

Example

Reset the counter of packets dropped to binding table mismatch.

```
Switch(config)#interface xgigaethernet 1/0/1
Switch(config-10ge1/0/1)#arp-antiattack check user-bind enable
Switch(config-10ge1/0/1)#reset arp-antiattack statistic check user-bind
Switch(config-10ge1/0/1)#
```

8.6.14 reset arp-antiattack statistic gateway-cheat

Function

The **reset arp-antiattack statistic gateway-cheat** command clears the statistics of ARP gateway anti-spoofing.

Format

reset arp-antiattack statistic gateway-cheat

Parameter

NA

Default Value

NA

View

Global configuration view

Usage Guidelines

NA

Example

Clear the statistics of ARP gateway anti-spoofing.

```
Switch(config)# reset arp-antiattack statistic gateway-cheat
Switch(config)#
```

8.6.15 show arp-antiattack check user-bind

Function

The **show arp-antiattack check user-bind** command displays the check items for ARP packet check against the binding table.

Format

show arp-antiattack check user-bind

Parameter

NA

Default Value

By default, the IP address, MAC address, interface, and VLAN must be checked.

View

Common user view

Usage Guidelines

NA

Example

Display check items for ARP packet check against the binding table.

```
Switch>show arp-antiattack check user-bind
Switch>
```

8.6.16 show arp-antiattack config

Function

The **show arp-antiattack config** command displays the ARP anti-attack configuration.

Format

show arp-antiattack config

Parameter

NA

Default Value

By default, the IP address, MAC address, interface, and VLAN must be checked.

View

Common user view

Usage Guidelines

NA

Example

Display the ARP anti-attack configuration.

```
Switch>show arp-antiattack config
Version: ANTIARP_VX2.10.00.00
Switch>
```

8.6.17 show arp-antiattack statistic**Function**The **show arp-antiattack statistic** command displays anti-ARP attack statistics.**Format****show arp-antiattack statistic****Parameter**

NA

Default Value

By default, the IP address, MAC address, interface, and VLAN must be checked.

View

Common user view

Usage Guidelines

NA

Example

Display anti-ARP attack statistics.

```
Switch>show arp-antiattack statistic
Untrust host attack number : ---
Source Ip conflict number : 0
Source Mac conflict number : 0
Gateway cheat number : 0
Dynamic learning host number : ---
No-DHCP user attack number : ---
Switch>
```

8.6.18 show auto-defend attack-source packet-type

Function

The **show auto-defend attack-source packet-type** command displays the attack source traceback information on automatic defense based on a specified packet type.

Format

- **show auto-defend attack-source packet-type { bpdutunnel | fib6hit | fibhit | icmp | snmp | ssh | tcp | telnet | total }**
- **show auto-defend attack-source packet-type all**

Parameter

NA

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

Display the attack source traceback information on automatic defense for packets received in all slots.

```
Switch>show auto-defend attack-source packet-type all
Switch>
```

8.6.19 show cpu-defend statistic

Function

The **show cpu-defend statistic** command displays CPU defense statistics.

Format

- **show cpu-defend statistic all**
- **show cpu-defend statistic packet-type { bpdutunnel | fib6hit | fibhit | icmp | snmp | ssh | tcp | telnet | total }**

Parameter

NA

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

Display CPU defense statistics of all slots.

Switch>show cpu-defend statistic all

Switch>

8.6.20 debug cpufend**Function**The **debug cpufend** command enables debugging of the CPU defense function.The **no debug cpufend** command disables debugging of the CPU defense function.**Format**

- **debug cpufend { event | error | carpkt | timer | trap | autodefend | sync | device }**
- **no debug cpufend { event | error | carpkt | timer | trap | autodefend | sync | device }**
- **no debug cpufend all**

Parameter

NA

Default Value

NA

View

Privileged user view

Usage Guidelines

NA

Example

Enable debugging of CPU defense events.

```
Switch#debug cpudefend event
Switch#
```

8.6.21 error-down auto-recovery cause auto-defend interval**Function**

The **error-down auto-recovery cause auto-defend interval** command sets the automatic recovery interval after automatic defense is disabled due to an error.

The **no error-down auto-recovery cause auto-defend** command deletes the configuration.

Format

- **error-down auto-recovery cause auto-defend interval** *interval-value*
- **no error-down auto-recovery cause auto-defend**

Parameter

Parameter	Description	Value
interval-value	Specifies the automatic recovery interval after automatic defense is disabled due to an error.	The value is an integer ranging from 30 to 86400, in seconds.

Default Value

NA

View

Global configuration view

Usage Guidelines

NA

Example

Set the automatic recovery interval after automatic defense is disabled due to an error.

```
Switch(config)#error-down auto-recovery cause auto-defend interval 50
Switch(config)#
```

8.6.22 reset cpu-defend statistics

Function

The **reset cpu-defend statistics** command clears CPU defense statistics.

Format

reset cpu-defend statistics

Parameter

NA

Default Value

NA

View

Global configuration view

Usage Guidelines

NA

Example

Clear CPU defense statistics.

```
Switch(config)#reset cpu-defend statistics
Switch(config)#
```

8.6.23 auto-defend {enable|disable}

Function

The **auto-defend {enable|disable}** command enables or disables the attack source traceback function.

Format

auto-defend { enable | disable }

Parameter

Parameter	Description	Value
enable	Enables the attack source traceback function.	-
disable	Disables the attack source traceback function.	-

Default Value

Disable

View

CPU defense policy configuration

Usage Guidelines

NA

Example

Enable the attack source traceback function.

```
Switch(config-policy-test1)#auto-defend enable
Switch(config-policy-test1)#
```

8.6.24 auto-defend action {deny|error-down}

Function

The **auto-defend action {deny|error-down}** command configures an attack source traceback action.

The **no auto-defend action** command deletes the configuration.

Format

- **auto-defend action { deny | error-down }**
- **no auto-defend action**

Parameter

Parameter	Description	Value
deny	Sets the attack source traceback action to "deny".	-
error-down	Sets the attack source traceback action to "disable due to an error".	-

Default Value

NA

View

CPU defense policy configuration

Usage Guidelines

NA

Example

Configure an attack source traceback action.

```
Switch(config-policy-test1)#auto-defend deny
Switch(config-policy-test1)#
```

8.6.25 auto-defend action deny timeout

Function

The **auto-defend action deny timeout** command sets the denial time for an attack source traceback action.

Format

auto-defend action deny timeout { *timeout-value* | **default** }

Parameter

Parameter	Description	Value
timeout-value	Specifies the denial time for an attack source traceback action.	The value is an integer ranging from 1 to 86400, in seconds.
default	Uses the default denial time for an attack source traceback action.	-

Default Value

NA

View

CPU defense policy configuration

Usage Guidelines

NA

Example

Set the denial time for an attack source traceback action.

```
Switch(config-policy-test1)#auto-defend action deny timeout 100
Switch(config-policy-test1)#
```

8.6.26 auto-defend alarm {enable|disable}

Function

The **auto-defend alarm {enable|disable}** command enables or disables the attack source traceback alarm function.

Format

auto-defend alarm { enable | disable }

Parameter

Parameter	Description	Value
enable	Enables the attack source traceback alarm function.	-
disable	Disables the attack source traceback alarm function.	-

Default Value

NA

View

CPU defense policy configuration

Usage Guidelines

NA

Example

Enable the attack source traceback alarm function.

```
Switch(config-policy-test1)#auto-defend alarm enable
Switch(config-policy-test1)#
```

8.6.27 auto-defend alarm threshold

Function

The **auto-defend alarm threshold** command sets an alarm threshold range for attack source traceback.

Format

auto-defend alarm threshold { threshold-value | default }

Parameter

Parameter	Description	Value
threshold-value	Specifies the alarm threshold range for attack source traceback.	The value is an integer ranging from 1 to 65535.
default	Uses the default alarm threshold range for attack source traceback.	128

Default Value

128

View

CPU defense policy configuration

Usage Guidelines

NA

Example

Set the alarm threshold range for attack source traceback.

```
Switch(config-policy-test1)#auto-defend alarm threshold 256
Switch(config-policy-test1)#
```

8.6.28 auto-defend attack-packet sample**Function**

The **auto-defend attack-packet sample** command sets the sample value range for automatic defense of attack packets.

Format**auto-defend attack-packet sample** { *threshold-value* | **default** }**Parameter**

Parameter	Description	Value
threshold-value	Specifies the alarm threshold range for attack source traceback.	The value is an integer ranging from 1 to 1024.
default	Uses the default alarm threshold range for attack source traceback.	8

Default Value

8

View

CPU defense configuration view

Usage Guidelines

NA

Example

Set the sample value range for automatic defense of attack packets.

```
Switch(config-policy-test1)#auto-defend attack-packet sample 100
Switch(config-policy-test1)#
```

8.6.29 auto-defend protocol {enable|disable}

Function

The **auto-defend protocol {enable|disable}** command enables or disables the attack source traceback protocol.

Format

**auto-defend protocol { bpdutunnel | fib6hit | fibhit | icmp | snmp | ssh | tcp | telnet | total }
{ enable | disable }**

Parameter

Parameter	Description	Value
enable	Enables the attack source traceback protocol type.	-
disable	Disables the attack source traceback protocol type.	-

Default Value

NA

View

CPU defense policy configuration

Usage Guidelines

NA

Example

Enable the attack source traceback protocol.

```
Switch(config-policy-test1)#auto-defend protocol total enable
Switch(config-policy-test1)#
```

8.6.30 auto-defend threshold

Function

The **auto-defend threshold** command sets a threshold range for attack source traceback.

Format

auto-defend threshold { *threshold-value* | **default** }

Parameter

Parameter	Description	Value
threshold-value	Specifies the threshold range for attack source traceback.	The value is an integer ranging from 1 to 65535.
default	Uses the default threshold range for attack source traceback.	128

Default Value

128

View

CPU defense policy configuration

Usage Guidelines

NA

Example

Set the threshold range for attack source traceback.

```
Switch(config-policy-test1)#auto-defend threshold 100
Switch(config-policy-test1)#
```

8.6.31 auto-defend trace-type

Function

The **auto-defend trace-type** command sets a traceback type for automatic port defense.

Format

auto-defend trace-type { **source-mac** | **source-ip** | **source-mac-ip** | **source-portvlan** | **source-mac-portvlan** | **source-ip-portvlan** | **source-mac-ip-portvlan** }

Parameter

NA

Default Value

NA

View

CPU defense policy configuration

Usage Guidelines

NA

Example

Set a traceback type for automatic port defense.

```
Switch(config-policy-test1)#auto-defend trace-type source-mac
Switch(config-policy-test1)#
```

8.6.32 auto-port-defend aging-time**Function**

The **auto-port-defend aging-time** command sets a detection interval for automatic port defense.

Format

auto-port-defend aging-time { *time-value* | **default** }

Parameter

Parameter	Description	Value
time-value	Specifies a detection interval.	The value is an integer ranging from 30 to 86400, in seconds.
default	Uses the default detection interval.	-

Default Value

NA

View

CPU defense configuration view

Usage Guidelines

NA

Example

Set a detection interval for automatic port defense.

```
Switch(config-policy-test1)#auto-port-defend aging-time 300
Switch(config-policy-test1)#
```

8.6.33 auto-port-defend protocol {enable|disable}**Function**

The **auto-port-defend protocol {enable|disable}** command enables or disables the attack source traceback protocol.

Format

**auto-port-defend protocol { bpdutunnel | fib6hit | fibhit | icmp | snmp | ssh | tcp | telnet | total }
{ enable | disable }**

Parameter

Parameter	Description	Value
enable	Enables automatic attack source traceback on protocol interfaces.	-
disable	Disables automatic attack source traceback on protocol interfaces.	-

Default Value

NA

View

CPU defense policy configuration

Usage Guidelines

NA

Example

Enable automatic attack source traceback on protocol interfaces.

```
Switch(config-policy-test1)#auto-port-defend protocol total enable
Switch(config-policy-test1)#
```

8.6.34 reset auto-defend packet-type

Function

The **reset auto-defend packet-type** command resets attack source traceback information based on a data packet type.

Format

reset auto-defend packet-type { bpdutunnel | fib6hit | fibhit | icmp | snmp | ssh | tcp | telnet | total }

Parameter

NA

Default Value

NA

View

CPU defense configuration view

Usage Guidelines

NA

Example

Reset attack source traceback information based on a data packet type.

```
Switch(config-policy-test1)#reset auto-defend packet-type total
Switch(config-policy-test1)#
```

8.6.35 reset cpu-defend statistics packet-type**Function**The **reset cpu-defend statistics** command clears CPU defense statistics based on a data packet type.**Format**

```
reset cpu-defend statistics packet-type { bpdutunnel | fib6hit | fibhit | icmp | snmp | ssh | tcp |
telnet | total }
```

Parameter

NA

Default Value

NA

View

CPU defense policy configuration

Usage Guidelines

NA

Example

Clear CPU defense statistics based on a data packet type.

```
Switch(config-policy-test1)#reset cpu-defend statistics packet-type total
Switch(config-policy-test1)#
```

8.6.36 reset antiattack dos-limit statistics

Function

The **reset antiattack dos-limit statistics** command resets the anti-attack DoS limit statistics.

Format

reset antiattack dos-limit statistics

Parameter

NA

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

Reset the anti-attack DoS limit statistics.

```
Switch>reset antiattack dos-limit statistics
Switch>
```

8.6.37 show antiattack dos-limit config

Function

The **show antiattack dos-limit config** command displays the anti-attack DoS limit configuration.

Format

show antiattack dos-limit config

Parameter

NA

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

Display the anti-attack DoS limit configuration.

```
Switch>show antiattack dos-limit config
!
antiattack dos-limit fragment car cir 512000
antiattack dos-limit tcp-syn car cir 512000
antiattack dos-limit icmp-flood car cir 512000
Switch>
```

8.6.38 show antiattack dos-limit statistics

Function

The **show antiattack dos-limit statistics** command displays the anti-attack DoS limit statistics.

Format

show antiattack dos-limit statistics

Parameter

NA

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

Display the anti-attack DoS limit statistics.

```
Switch>show antiattack dos-limit statistics
Packets Statistic Information:
-----
AntiAtkType   TotalPacketNum   DropPacketNum   PassPacketNum
```

	(H)	(L)	(H)	(L)	(H)	(L)
Abnormal	0	0	0	0	0	0
Fragment	0	0	0	0	0	0
Tcp-syn	0	0	0	0	0	0
Udp-flood	0	0	0	0	0	0
Icmp-flood	0	0	0	0	0	0
Switch>						

8.6.39 debug dos-antiattack

Function

The **debug dos-antiattack** command enables the DoS anti-attack debugging function.

The **no debug dos-antiattack** command disables the DoS anti-attack debugging function.

Format

- **debug dos-antiattack { config | info | dev | all }**
- **no debug dos-antiattack { config | info | dev | all }**

Parameter

NA

Default Value

NA

View

Privileged user view

Usage Guidelines

NA

Example

Enable the DoS anti-attack debugging function.

```
Switch#debug dos-antiattack all
Switch#
```

8.6.40 antiattack dos-limit {enable|disable}

Function

The **antiattack dos-limit {enable|disable}** command enables or disables the anti-attack DoS limit function.

Format

antiattack dos-limit { abnormal | fragment | tcp-syn | udp-flood | icmp-flood } { enable | disable }

Parameter

Parameter	Description	Value
enable	Enables the anti-attack DoS limit function.	-
disable	Disables the anti-attack DoS limit function.	-
abnormal	Specifies an abnormal packet.	-
fragment	Specifies a fragment packet.	-
tcp-syn	Specifies a TCP SYN.	-
udp-flood	Specifies an UDP flood.	-
icmp-flood	Specifies an ICMP flood.	-

Default Value

Disable

View

Global configuration view

Usage Guidelines

NA

Example

Enable the anti-attack DoS limit function.

```
Switch(config)#antiattack dos-limit abnormal enable
Switch(config)#
```

8.6.41 dosantiattack dos-limit car cir

Function

The **antiattack dos-limit car cir** command configures the committed access rate and committed information rate of anti-attack DoS limit to the specified packet.

Format

antiattack dos-limit { fragment | tcp-syn | icmp-flood } car cir { value | default }

Parameter

Parameter	Description	Value
value	Specifies a CIR value.	The value is an integer ranging from 8000 to 155000000, in bps.
default	Specifies the default CIR value.	512000 bit/s

Default Value

NA

View

Global configuration view

Usage Guidelines

NA

Example

Configure the committed access rate and committed information rate of anti-attack DoS limit to the specified packet.

```
Switch(config)#antiattack dos-limit fragment car cir default
Switch(config)#
```

8.7 IP Source Guard Configuration Commands

8.7.1 debug ip source check

Function

The **debug ip source check** command enables IP Source Guard debugging.

The **no debug ip source check** command disables IP Source Guard debugging.

Format

- **debug ip source check**
- **no debug ip source check**

Parameter

NA

Default Value

By default, IP Source Guard debugging is disabled.

View

Privileged user view

Usage Guidelines

NA

Example

Enable IP Source Guard debugging.

```
Switch#debug ip source check
Switch#
```

8.7.2 ip source check user-bind {enable|disable}**Function**

The **ip source check user-bind enable** command enables the IP packet check function on an interface.

The **ip source check user-bind disable** command disables the IP packet check function on an interface.

Format

- **ip source check user-bind enable**
- **ip source check user-bind disable**

Parameter

NA

Default Value

By default, the switch does not check whether an IP packet matches the binding table.

View

Ethernet bridge interface configuration view, Ethernet router interface configuration view, trunk interface configuration view, interface configuration view (trunk), VLAN configuration view

Usage Guidelines

This command configures the switch to check whether IP packets match the binding table and determine whether to forward the packets.

To prevent IP packets of unauthorized users from reaching external networks through the Switch, configure IP packet check on interfaces of the Switch. Only the IP packets matching the binding entries can be forwarded.

For DHCP users, a dynamic binding table is generated after DHCP snooping is enabled.

For users with static addresses, you need to manually create static binding entries.

Example

Enable the IP packet check function on an interface

```
Switch(config-10ge1/0/1)#ip source check user-bind enable
Switch(config-10ge1/0/1)#
```

8.7.3 ip source check user-bind alarm {enable|disable}

Function

The **ip source check user-bind alarm enable** command enables the IP packet alarm check function on an interface.

The **ip source check user-bind alarm disable** command disables the IP packet alarm check function on an interface.

Format

- **ip source check user-bind alarm enable**
- **ip source check user-bind alarm disable**

Parameter

NA

Default Value

NA

View

Ethernet bridge interface configuration view, Ethernet routing interface configuration view

Usage Guidelines

NA

Example

Enable the IP packet alarm check function on an interface


```
Switch(config-10ge1/0/1)#ip source check user-bind alarm enable
Switch(config-10ge1/0/1)#
```

8.7.4 ip source check user-bind alarm threshold

Function

The **ip source check user-bind alarm threshold** command sets the alarm threshold for IP packet check.

Format

ip source check user-bind alarm threshold { *threshold* | **default** }

Parameter

Parameter	Description	Value
threshold	Specifies the alarm threshold for IP packet check.	The value is an integer ranging from 1 to 1000.

Default Value

NA

View

Ethernet bridge interface configuration view, Ethernet routing interface configuration view

Usage Guidelines

NA

Example

Set the alarm threshold for IP packet check.

```
Switch(config-10ge1/0/1)#ip source check user-bind threshold 800
Switch(config-10ge1/0/1)#
```

8.7.5 ip source check user-bind check-item

Function

The **ip source check user-bind check-item** command sets the item for IP packet check.

The **no ip source check user-bind check-item** command restores the item for IP packet check to the default option.

Format

VLAN configuration view:

- **ip source check user-bind check-item { ip-address | mac-address | interface }**
- **ip source check user-bind check-item ip-address interface**
- **ip source check user-bind check-item ip-address mac-address**
- **ip source check user-bind check-item mac-address interface**
- **no ip source check user-bind check-item**

Ethernet bridge interface configuration view, Ethernet route interface configuration view, and Trunk interface configuration view

- **ip source check user-bind check-item { ip-address | mac-address | vlan }**
- **ip source check user-bind check-item ip-address vlan**
- **ip source check user-bind check-item ip-address mac-address**
- **ip source check user-bind check-item mac-address vlan**
- **no ip source check user-bind check-item**

Parameter

Parameter	Description	Value
ip-address	Checks whether the IPv4 or IPv6 address of an IP packet matches the binding table.	-
mac-address	Checks whether the MAC address of an IP packet matches the binding table.	-
vlan	Checks whether the VLAN of an IP packet matches the binding table.	-
interface	Checks whether the interface of an IP packet matches the binding table.	-

Default Value

By default, the system checks the IP addresses (IPv4 or IPv6), MAC addresses, and VLANs of IP packets.

View

The view is specified in the command.

Usage Guidelines

Before using this command, enable IP packet check on the interface.

Example

```
# Enable the IP Source Guard function on an interface and specify VLAN as the check item for IP packet check.
```

```
Switch(config-10ge1/0/1)#ip source check user-bind enable
Switch(config-10ge1/0/1)#ip source check user-bind check-item vlan
Switch(config-10ge1/0/1)#
```

8.7.6 reset ip source statistic check user-bind

Function

The **reset ip source statistic check user-bind** command resets the IP Source Guard statistics.

Format

reset ip source statistic check user-bind

Parameter

NA

Default Value

NA

View

Ethernet bridge interface configuration view, Ethernet router interface configuration view, trunk interface configuration view, interface configuration view (trunk), VLAN configuration view

Usage Guidelines

Before using this command, enable IP packet check on the interface.

Example

Reset the IP Source Guard statistics.

```
Switch(config-10ge1/0/1)#ip source check user-bind enable
Switch(config-10ge1/0/1)#reset ip source statistic check user-bind
Switch(config-10ge1/0/1)#
```

8.7.7 show ip source check user-bind

Function

The **show ip source check user-bind** command displays information about the IP packet check function.

Format

show ip source check user-bind

Parameter

NA

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

Display information about the IP packet check function

```
Switch>show ip source check user-bind

      interface eth-trunk 1
      ip source check user-bind enable
      ip source check dropped IP packets 0/0
Switch>
```

8.7.8 show user-bind**Function**The **show user-bind** command displays information about static binding entries.**Format****show user-bind****Parameter**

NA

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

Display information about static binding entries.

```
Switch>show user-bind
  1 Version : IPSG_VB3.00.04.00
  0 entries in user-bind table
Switch>
```

8.7.9 show user-bind config**Function**

The **show user-bind config** command displays the configuration of static binding entries.

Format

show user-bind config

Parameter

NA

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

Display the configuration of static binding entries.

```
Switch>show user-bind config
ip source check user-bind enable
Switch>
```

8.7.10 user-bind alarm untrust-user**Function**

The **user-bind alarm untrust-user {enable|disable}** command enables or disables the alarm function for untrusted IP packet reception.

The **user-bind alarm untrust-user threshold** command sets an alarm threshold for untrusted IP packet reception.

Format

- **user-bind alarm untrust-user { enable | disable }**
- **user-bind alarm untrust-user threshold { threshold | default }**

Parameter

Parameter	Description	Value
enable	Enables the IP packet checking alarm function.	-
disable	Disables the IP packet checking alarm function.	-
threshold	Indicates the IP packet checking alarm threshold.	The value is an integer ranging from 1 to 1000.
default	Default IP packet checking alarm threshold	100

Default Value

NA

View

Global configuration view

Usage Guidelines

NA

Example

Enable the IP packet checking alarm function.

```
Switch(config)#user-bind alarm untrust-user enable
Switch(config)#
```

8.7.11 user-bind black-list

Function

The **user-bind black-list** command enables or disables the IP packet blacklist feature.

Format

user-bind black-list { enable | disable }

Parameter

Parameter	Description	Value

Parameter	Description	Value
enable	Enables the IP packet blacklist feature.	-
disable	Disables the IP packet blacklist feature.	-

Default Value

NA

View

Global configuration view

Usage Guidelines

NA

Example

Enable the IP packet blacklist feature.

```
Switch(config)#user-bind black-list enable
Switch(config)#
```

8.7.12 user-bind static ip|ip6 mac

Function

The **user-bind static ip|ip6 mac** command configures static binding entries.

The **no user-bind static** command deletes static binding entries.

Format

- **user-bind static ip** { *ipv4-address* | **any** } **mac** { *src-mac-address* | **any** } **interface** { **ethernet** | **xgigaethernet** | **10gigaethernet** | **25gigaethernet** | **40gigaethernet** | **100gigaethernet** } *interface-number* **vlan** { **any** | *vlan-id* }
- **user-bind static ip** { *ipv4-address* | **any** } **mac** { *src-mac-address* | **any** } **vlan** { **any** | *vlan-id* }
- **user-bind static ip6** { *ipv6-address* | **any** } **mac** { *src-mac-address* | **any** } **interface** { **ethernet** | **xgigaethernet** | **10gigaethernet** | **25gigaethernet** | **40gigaethernet** | **100gigaethernet** } *interface-number* **vlan** { **any** | *vlan-id* }
- **user-bind static ip6** { *ipv6-address* | **any** } **mac** { *src-mac-address* | **any** } **vlan** { **any** | *vlan-id* }

- **no user-bind static ip** { *ipv4-address* | **any** } **mac** { *src-mac-address* | **any** } **interface** { **ethernet** | **xgigaethernet** | **10gigaethernet** | **25gigaethernet** | **40gigaethernet** | **100gigaethernet** } *interface-number* **vlan** { **any** | *vlan-id* }
- **no user-bind static ip** { *ipv4-address* | **any** } **mac** { *src-mac-address* | **any** } **vlan** { **any** | *vlan-id* }
- **no user-bind static ip6** { *ipv6-address* | **any** } **mac** { *src-mac-address* | **any** } **interface** { **ethernet** | **xgigaethernet** | **10gigaethernet** | **25gigaethernet** | **40gigaethernet** | **100gigaethernet** } *interface-number* **vlan** { **any** | *vlan-id* }
- **no user-bind static ip6** { *ipv6-address* | **any** } **mac** { *src-mac-address* | **any** } **vlan** { **any** | *vlan-id* }
- **no user-bind static interface** { **ethernet** | **xgigaethernet** | **10gigaethernet** | **25gigaethernet** | **40gigaethernet** | **100gigaethernet** } *interface-number*
- **no user-bind static interface eth-trunk** *trunk-number*
- **no user-bind static ip** *ipv4-address*
- **no user-bind static ip6** *ipv6-address*
- **no user-bind static mac** *src-mac-address*
- **no user-bind static vlan** *vlan-id*
- **no user-bind static all**

Parameter

Parameter	Description	Value
<i>ipv4-address</i>	Specifies a source IP address.	The value is in dotted decimal notation, for example, <i>A.B.C.D</i> , in which <i>A</i> to <i>D</i> are decimal digits ranging from 0 to 255.
<i>ipv6-address</i>	Specifies a source IPv6 address.	-
<i>src-mac-address</i> any	Specifies the source MAC address of a specified ACL rule.	<i>src-ip-address</i> is in dotted decimal notation. <i>M</i> is an integer ranging from 1 to 128. any means any source MAC address.
any <i>vlan-id</i>	any indicates that the parameter is not matched. <i>vlan-id</i> specifies the VID entry to which the user belongs.	The value is an integer ranging from 1 to 4094. any means any VID.
<i>interface-number</i>	Specifies an Ethernet interface number.	The value is an integer in the range of <1-1>/<0-1>/<1-48> (For reference only. The specific value range depends on the slot

Parameter	Description	Value
		number and card type).
trunk-number	Specifies the number of a Trunk interface.	The value is an integer ranging from 1 to 128.

Default Value

NA

View

Global configuration view

Usage Guidelines

NA

Example

Configure a static binding entry.

```
Switch(config)# user-bind static ip 10.1.1.1 mac 01:01:01:01:01:01 interface xgigaethernet 1/0/1 vlan 1
Switch(config)#
```

8.8 AAA /RADIUS Configuration Commands

8.8.1 aaa

Function

The **aaa** command switches to the AAA configuration view from the global configuration view.

Format**aaa****Parameter**

NA

Default Value

NA

View

Global configuration view

Usage Guidelines

NA

Example

Switch to the AAA configuration view from the global configuration view.

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

8.8.2 aaa {authentication|accounting}

Function

The **aaa {authentication|accounting}** command configures an AAA authentication method name or AAA accounting method name.

Format

- **aaa { authentication | accounting } { login | dot1x } method name server-group group-name**
- **aaa { authentication | accounting } { login | dot1x } method name server-group group-name { local | none }**
- **aaa { authentication | accounting } { login | dot1x } method name server-group group-name local none**
- **aaa { authentication | accounting } { login | dot1x } method name server-group group-name group-name**
- **aaa { authentication | accounting } { login | dot1x } method name server-group group-name group-name { local | none }**
- **aaa { authentication | accounting } { login | dot1x } method name server-group group-name group-name local none**
- **aaa { authentication | accounting } { login | dot1x } local method name server-group group-name**
- **aaa { authentication | accounting } { login | dot1x } local method name server-group group-name group-name**
- **aaa { authentication | accounting } { login | dot1x } local method name server-group group-name group-name none**
- **aaa { authentication | accounting } { login | dot1x } local method name server-group group-name none**
- **aaa authentication { login | dot1x } method name local**

- **aaa authentication { login | dot1x } local method *name***

Parameter

Parameter	Description	Value
authentication	Indicates certification.	-
account	Indicates accounting.	-
dot1x	Indicates the IEEE 802.1X protocol.	-
ppp	Specifies a point-to-point protocol.	-
login	Indicates login authentication.	-
web-auth	Indicates Web authentication.	-
mac-auth	Indicates MAC address authentication.	-
name	Specifies a method list name.	The value is a character string.
group-name	Specifies a server group name.	The value is a character string.
local	Enables local authentication.	-
none	Disables authentication or accounting.	-

Default Value

NA

View

AAA configuration view

Usage Guidelines

NA

Example

Configure an AAA authentication method name or AAA accounting method name.

```
Switch(config-aaa)#aaa authentication login method 11 server-group test
Switch(config-aaa)#aaa account login method 11 server-group aaa bbb
Switch(config-aaa)#
```

8.8.3 aaa authentication enable method

Function

The **aaa authentication enable** method command creates a secondary authentication method.

Format

- **aaa authentication enable method *name* local**
- **aaa authentication enable method *name* server-group *group-name***

- **aaa authentication enable method** *name server-group group-name { local | none }*
- **aaa authentication enable method** *name server-group group-name group-name*
- **aaa authentication enable method** *name server-group group-name group-name { local | none }*
- **aaa authentication enable method** *name server-group group-name group-name local none*
- **aaa authentication enable method** *name server-group group-name local none*
- **aaa authentication enable local method** *name*
- **aaa authentication enable local method** *name server-group group-name*
- **aaa authentication enable local method** *name server-group group-name group-name*
- **aaa authentication enable local method** *name server-group group-name group-name none*
- **aaa authentication enable local method** *name server-group group-name none*

Parameter

Parameter	Description	Value
name	Specifies a method list name.	The value is a character string.
group-name	Specifies a server group name.	The value is a character string.
local	Enables local authentication.	-
none	Disables authentication.	-

Default Value

NA

View

AAA configuration view

Usage Guidelines

NA

Example

Create a secondary authentication method.

```
Switch(config-aaa)#aaa authentication enable method 11 local
Switch(config-aaa)#
```

8.8.4 aaa authorization method

Function

The **aaa authorization method** command creates an AAA authorization method.

Format

- **aaa authorization method** *name* **local**
- **aaa authorization method** *name* **server-group** *group-name*
- **aaa authorization method** *name* **server-group** *group-name* { **local** | **none** }
- **aaa authorization method** *name* **server-group** *group-name* *group-name*
- **aaa authorization method** *name* **server-group** *group-name* *group-name* { **local** | **none** }
- **aaa authorization method** *name* **server-group** *group-name* *group-name* **local none**
- **aaa authorization method** *name* **server-group** *group-name* **local none**

Parameter

Parameter	Description	Value
name	Specifies a method list name.	The value is a character string.
group-name	Specifies a server group name.	The value is a character string.
local	Enables local authentication.	-
none	Disables authentication.	-

Default Value

NA

View

AAA configuration view

Usage Guidelines

NA

Example

Create an AAA authorization method.

```
Switch(config-aaa)#aaa authorization method 11 local
Switch(config-aaa)#
```

8.8.5 aaa none-author privilege

Function

The **aaa none-author privilege** command configures the default user privilege when no authentication is configured.

Format

aaa none-author privilege { administrators | operators | users | guests | default }

Parameter

Parameter	Description	Value
administrators	Specifies the administrator privilege.	-
operators	Specifies the operator privilege.	-
users	Specifies the user privilege.	-
guests	Specifies the guest privilege.	-
default	Specifies that the guest privilege is used as the default privilege.	-

Default Value

Guest privilege

View

AAA configuration view

Usage Guidelines

NA

Example

Set the default privilege to the user privilege.

```
Switch(config-aaa)#aaa none-author privilege users
Switch(config-aaa)#
```

8.8.6 accounting realtime**Function**

The **accounting realtime** command sets the AAA real-time accounting report interval.

Format

accounting realtime { realtime | default }

Parameter

Parameter	Description	Value
realtime	Specifies a report interval.	The value is an integer ranging from 300 to 4294967290, in seconds.
default	Uses the default value.	The default value is 300 seconds.

Default Value

300 seconds

View

AAA configuration view

Usage Guidelines

NA

Example

Set the AAA real-time accounting report interval.

```
Switch(config-aaa)#accounting realtime 1000
Switch(config-aaa)#
```

8.8.7 debug aaa

Function

The **debug aaa** command enables AAA debugging.

The **no debug aaa** command disables AAA debugging.

Format

- **debug aaa { auth | author | acct | sys | method | server | session | radius | tacacs | all }**
- **no debug aaa { auth | author | acct | sys | method | server | session | radius | tacacs | all }**

Parameter

Parameter	Description	Value
auth	Specifies authentication.	-
author	Specifies authorization.	-
acct	Specifies accounting.	-
sys	Specifies a system.	-
method	Specifies method processing.	-
server	Specifies server processing.	-
session	Specifies session processing.	-
radius	Specifies a RADIUS server.	-
tacacs	Specifies a TACACS server.	-
all	Specifies all AAA debugging.	-

Default Value

NA

View

Privileged user view

Usage Guidelines

NA

Example

Enable all AAA debugging.

```
Switch#no debug aaa all
Switch#
```

8.8.8 no aaa method

Function

The **no aaa method** command deletes an AAA method or a server group in an AAA method.

Format

- **no aaa method** *name*
- **no aaa method** *name server-group group-name*

Parameter

Parameter	Description	Value
name	Specifies an AAA method name.	The value is a character string.
group-name	Specifies a server group name.	The value is a character string.

Default Value

NA

View

AAA configuration view

Usage Guidelines

NA

Example

Delete an AAA method or a server group in an AAA method.

```
Switch(config-aaa)#no aaa method 11
Switch(config-aaa)#
Switch(config-aaa)#no aaa method 11 server-group aaa
Switch(config-aaa)#
```


8.8.9 no radius-server

Function

The **no radius-server** command deletes an AAA RADIUS server.

The **no radius-server src-ip** command deletes the source IPv4 address of a specified AAA RADIUS server.

The **no radius-server src-ip v6** command deletes the source IPv6 address of a specified AAA RADIUS server.

Format

- **no radius-server** *name*
- **no radius-server** *name* **src-ip**
- **no radius-server** *name* **src-ipv6**

Parameter

Parameter	Description	Value
name	Specifies a RADIUS server name.	The value is a character string.

Default Value

NA

View

AAA configuration view

Usage Guidelines

NA

Example

Delete an AAA RADIUS server.

```
Switch(config-aaa)#no radius-server 111
Switch(config-aaa)#
```

8.8.10 no server-group

Function

The **no server-group** command deletes an AAA server group or deletes a server from the AAA server group.

Format

- **no server-group** *name*
- **no server-group** *name* **radius-server** *server-name*
- **no server-group** *name* **tacacs-server** *server-name*

Parameter

Parameter	Description	Value
name	Specifies a server group name.	The value is a character string.
server-name	Specifies a RADIUS server name.	The value is a character string.

Default Value

NA

View

AAA configuration view

Usage Guidelines

NA

Example

Delete a server from the AAA server group.

```
Switch(config-aaa)#no server-group aaa radius-server ccc
Switch(config-aaa)#
```

8.8.11 no tacacs-server**Function**

The **no tacacs-server** command deletes a TACACS server.

The **no tacacs-server src-ip** command deletes the source IPv4 address of a specified TACACS server.

The **no tacacs-server src-ip v6** command deletes the source IPv6 address of a specified TACACS server.

Format

- **no tacacs-server** *name*
- **no tacacs-server** *name* **src-ip**

- **no tacacs-server name src-ipv6**

Parameter

Parameter	Description	Value
name	Specifies a TACACS server name.	The value is a character string.

Default Value

NA

View

AAA configuration view

Usage Guidelines

NA

Example

Delete a TACACS server.

```
Switch(config-aaa)#no tacacs-server fhn
Switch(config-aaa)#
```

8.8.12 radius-server acct-port**Function**The **radius-server acct-port** command configures an accounting port for a RADIUS server.**Format****radius-server name acct-port { acct-port | default }****Parameter**

Parameter	Description	Value
name	Specifies a RADIUS server name.	The value is a character string.
acct-port	Specifies an accounting port number.	The value is an integer ranging from 1 to 65535.
default	Specifies the default value.	1813

Default Value

1813

View

AAA configuration view

Usage Guidelines

NA

Example

Configure an accounting port for a RADIUS server.

```
Switch(config-aaa)#radius-server 111 acc-port 100
Switch(config-aaa)#
```

8.8.13 radius-server auth-port**Function**

The **radius-server auth-port** command configures an authentication port for a RADIUS server.

Format

radius-server *name* **auth-port** { *auth-port* | **default** }

Parameter

Parameter	Description	Value
name	Specifies a RADIUS server name.	The value is a character string.
auth-port	Specifies an authentication port number.	The value is an integer ranging from 1 to 65535.
default	Specifies the default value.	1812

Default Value

1812

View

AAA configuration view

Usage Guidelines

NA

Example

Set the authentication port number of the RADIUS server to 100.

```
Switch(config-aaa)#radius-server 111 auth-port 100
Switch(config-aaa)#
```

8.8.14 radius-server deadtime**Function**

The **radius-server deadtime** command sets the dead time for a RADIUS server.

Format

- **radius-server deadtime** { *deadtime* | **default** }
- **radius-server name deadtime** { *deadtime* | **default** }

Parameter

Parameter	Description	Value
name	Specifies a RADIUS server name.	The value is a character string.
deadtime	Specifies a dead time.	The value is an integer ranging from 3 to 4294967290, in seconds.
default	Specifies the default value.	60 seconds

Default Value

60 seconds

View

AAA configuration view

Usage Guidelines

NA

Example

Set the dead time for a RADIUS server.

```
Switch(config-aaa)#radius-server deadtime 100
Switch(config-aaa)#
Switch(config-aaa)#radius-server 111 deadtime 100
Switch(config-aaa)#
```

8.8.15 radius-server {ip-address|ip6-address} key

Function

The **radius-server ip-address key** command creates a RADIUS server and sets its name, IPv4 address, and shared key.

The **radius-server ip6-address key** command creates a RADIUS server and sets its name, IPv6 address, and shared key.

Format

- **radius-server name ip-address ip4-address key key**

- **radius-server** *name* **ip-address** *ipv4-address* **key** *key* **vpn-instance** *vpn-name*
- **radius-server** *name* **ip6-address** *ipv6-address* **key** *key*
- **radius-server** *name* **ip6-address** *ipv6-address* **key** *key* **vpn-instance** *vpn-name*

Parameter

Parameter	Description	Value
name	Specifies a RADIUS server name.	The value is a character string.
ip4-address	Specifies an IPv4 address.	The value is in dotted decimal notation, for example, <i>A.B.C.D</i> , in which <i>A</i> to <i>D</i> are decimal digits ranging from 0 to 255.
ip6-address	Specifies an IPv6 address.	The value is in dotted hexadecimal notation, in the <i>X:X::X:X</i> format.
key	Indicates the key of a RADIUS server.	-
vpn-name	Specifies a VPN instance name.	The value is a character string.

Default Value

NA

View

AAA configuration view

Usage Guidelines

NA

Example

Create a RADIUS server and set its name, IPv4 and IPv6 addresses, and shared key.

```
Switch(config-aaa)#radius-server 111 ip-address 1.1.1.1 key 123
Switch(config-aaa)#
Switch(config-aaa)#radius-server 111 ip6-address 1:1::1:1 key 123
Switch(config-aaa)#
```

8.8.16 radius-server {ip-address|ip6-address} key auth-port acct-port

Function

The **radius-server ip-address key auth-port acct-port** command creates an IPv4 RADIUS server.

The **radius-server ip6-address key auth-port acct-port** command creates an IPv6 RADIUS server.

Format

- **radius-server** *name* **ip-address** *ipv4-address* **key** *key* **auth-port** { *auth-port* | **default** } **acct-port** { *acct-port* | **default** }
- **radius-server** *name* **ip6-address** *ipv6-address* **key** *key* **auth-port** { *auth-port* | **default** } **acct-port** { *acct-port* | **default** }

Parameter

Parameter	Description	Value
name	Specifies a RADIUS server name.	-
ipv4-address	Specifies an IPv4 address.	The value is in dotted decimal notation, for example, <i>A.B.C.D</i> , in which <i>A</i> to <i>D</i> are decimal digits ranging from 0 to 255.
ipv6-address	Specifies an IPv6 address.	The value is in dotted hexadecimal notation, in the <i>X:X::X:X</i> format.
key	Specifies the shared key of a RADIUS server.	-
auth-port	Specifies an authentication port number.	The value is an integer ranging from 1 to 65535.
default	Specifies the default authentication port number.	1812
acct-port	Specifies an accounting port number.	The value is an integer ranging from 1 to 65535.
default	Specifies the default accounting port number.	1813

Default Value

auth-port: 1812

acct-port: 1813

View

AAA configuration view

Usage Guidelines

NA

Example

Create an IPv4 RADIUS server and an IPv6 RADIUS server.

```
Switch(config-aaa)#radius-server 111 ip-address 1.1.1.1 key 123 auth-port 100 acc-port 100
Switch(config-aaa)#
Switch(config-aaa)#radius-server 111 ip6-address 1::1:1 key 123 auth-port 100 acc-port 100
Switch(config-aaa)#
```

8.8.17 radius-server max-retransmit

Function

The **radius-server max-retransmit** command sets the global maximum number of retransmissions for all RADIUS servers or sets the maximum number of retransmissions for a specified server.

Format

- **radius-server max-retransmit** { *max-retransmit* | **default** }
- **radius-server** *name* **max-retransmit** { *max-retransmit* | **default** }

Parameter

Parameter	Description	Value
name	Specifies a RADIUS server name.	The value is a character string.
max-retransmit	Specifies the maximum number of retransmissions.	The value is an integer ranging from 0 to 5.
default	Specifies the default value.	The default value is 3 in the global configuration view.

Default Value

3

View

AAA configuration view

Usage Guidelines

NA

Example

Set the global maximum number of RADIUS server retransmissions.

```
Switch(config-aaa)#radius-server 111 max-retransmit 2
Switch(config-aaa)#
Switch(config-aaa)#radius-server max-retransmit 2
Switch(config-aaa)#
```

8.8.18 radius-server retransmit-interval

Function

The **radius-server retransmit-interval** command sets the global retransmission interval for RADIUS servers or the retransmission interval for a specified server.

Format

- **radius-server retransmit-interval** { *retransmit-interval* | **default** }
- **radius-server name retransmit-interval** { *retransmit-interval* | **default** }

Parameter

Parameter	Description	Value
name	Specifies a RADIUS server name.	The value is a character string.
retransmit-interval	Specifies a retransmission interval.	The value is an integer ranging from 1 to 10, in seconds.
default	Specifies the default value.	The default value is 2 in the global configuration view.

Default Value

2 seconds

View

AAA configuration view

Usage Guidelines

NA

Example

Set the global retransmission interval for all the RADIUS servers.

```
Switch(config-aaa)#radius-server retransmit-interval 2
Switch(config-aaa)#
Switch(config-aaa)#radius-server 111 retransmit-interval 2
Switch(config-aaa)#
```

8.8.19 radius-server {src-ip|src-ipv6}**Function**

The **radius-server {src-ip|src-ipv6}** command configures the source IP address of packets sent to a RADIUS server.

The **no radius-server {src-ip|src-ipv6}** command deletes the configuration.

Format

- **radius-server name src-ip** *ip-address*
- **radius-server name src-ip** *ip-address* **vpn-instance** *vpn-name*

- **radius-server** *name* **src-ipv6** *ipv6-address*
- **radius-server** *name* **src-ipv6** *ipv6-address* **vpn-instance** *vpn-name*
- **no radius-server** *name* **src-ip**
- **no radius-server** *name* **src-ipv6**

Parameter

Parameter	Description	Value
ip-address	Specifies a source IP address for the packet.	The value is in dotted decimal notation.
ipv6-address	Specifies a source IP address for the packet.	The value is in the IPv6 address format.
name	Specifies an RADIUS server name.	The value is a character string.
vpn-name	Specifies a VPN name.	The value is a character string.

Default Value

NA

View

AAA configuration view

Usage Guidelines

NA

Example

Configure the source IP address of packets sent to a RADIUS server.

```
Switch(config-aaa)#radius-server server1 src-ip 1.1.1.1
Switch(config-aaa)#
```

8.8.20 reset server statistic**Function**The **reset server statistic** command resets statistics about a specified TACACS server.**Format****reset server** *name* **statistic****Parameter**

Parameter	Description	Value
name	Specifies a TACACS server name.	The value is a character string.

Default Value

NA

View

AAA configuration view

Usage Guidelines

NA

Example

Reset statistics about a specified TACACS server

```
Switch(config-aaa)#reset server test1 statistic
Switch(config-aaa)#
```

8.8.21 sever-group {radius-server|tacacs-server}**Function**

The **server-group {radius-server|tacacs-server}** command creates a server group, defines the protocol type for the server, and adds a server to the group.

Format

- **server-group** *name* **radius-server** *server-name*
- **server-group** *name* **tacacs-server** *server-name*

Parameter

Parameter	Description	Value
name	Specifies a server group name.	The value is a character string.
server-name	Specifies the name of a server in the server group.	The value is a character string.
radius-server	Sets the protocol type of the server group to RADIUS.	-
tacacs-server	Sets the protocol type of the server group to TACACS.	

Default Value

NA

View

AAA configuration view

Usage Guidelines

NA

Example

Create a server group, define its protocol type, and add a server to the group.

```
Switch(config-aaa)#server-group aaa radius-server aaa
Switch(config-aaa)#
```

8.8.22 show aaa**Function**

The **show aaa** command displays AAA information.

Format

show aaa

Parameter

NA

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

Display AAA information.

```
Switch>show aaa
  Version                               : AAA_VB3.00.00.00
  Accounting Realtime                   : 300
  Radius-server Retransmit Interval     : 2
  Radius-server Max Retransmit          : 3
  Radius-server Deadtime                : 60
  Tacacs-server Timeout                 : 2
  Tacacs-server Deadtime               : 60
Switch>
```

8.8.23 show aaa config**Function**

The **show aaa config** command displays the global AAA configuration on the switch.

Format

show aaa config

Parameter

NA

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

Display AAA configuration file information.

```
Switch>show aaa config
Version                               : AAA_VB3.00.00.00
Switch>
```

8.8.24 show aaa method

Function

The **show aaa method** command displays information about configured AAA methods.

Format

- **show aaa method**
- **show aaa method *name***

Parameter

Parameter	Description	Value
name	Specifies an AAA method name.	The value is a character string.

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

Display information about a configured AAA method.

```
Switch>show aaa method
Method Name                : 1
Method Apply Type          : enable
Method Apply Function       : authentication
Method Local                : enable
Method None                 : disable
Switch>
```

8.8.25 show aaa server

Function

The **show aaa server** command displays AAA RADIUS server configuration.

Format

- **show aaa server**
- **show aaa server** *name*

Parameter

Parameter	Description	Value
name	Specifies a RADIUS server name.	The value is a character string.

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

Displays the configuration of an AAA RADIUS server.

```

Switch>show aaa server 111
show aaa server
Server Name                : 1
Server IP Address          : 2.2.2.2
Server IP Instance         : public
Server Source IP Instance  : public
Server Key                  : 123
Server Protocol Type       : radius
Radius-server Authentication Port : 1812
Radius-server Accounting Port   : 1813
Radius-server Retransmit Interval : 2
Radius-server Max Retransmit    : 3
Radius-server Deadtime        : 60
Radius-server Source IP Address : N/A
Server State                 : active
Switch>

```

8.8.26 show aaa server-group

Function

The **show aaa server-group** command displays AAA server group configuration.

Format

- **show aaa server-group**
- **show aaa server-group** *group-name*

Parameter

Parameter	Description	Value
group-name	Specifies a server group name.	The value is a character string.

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

Display the configuration of an AAA server group.

```
Switch>show aaa server-group aaa
Server-group Name           : 1
  Server-group Protocol Type : radius
  Primary Server             : 1(2.2.2.2:1812:1813)

  Current Active Server      : 1(2.2.2.2:1812:1813)
Switch>
```

8.8.27 show aaa tacacs-server statistic

Function

The **show aaa tacacs-server statistic** command displays statistics about a TACACS server.

Format

- **show aaa tacacs-server *name* statistic**
- **show aaa tacacs-server statistic**

Parameter

Parameter	Description	Value
name	Specifies a TACACS server name.	The value is a character string.

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

Display statistics about a TACACS server.

```
Switch>show aaa tacacs-server ts1 statistic
Server Name           : 2
  Server IP Instance   : public
  Server Key           : 123
  Server Port          : 49
  Socket Opens         : 0
  Socket Closes        : 0
  Socket Errors        : 0
```



```

Socket Timeouts           : 0
Total Packets Sent        : 0
Total Packets Recv        : 0
Switch>

```

8.8.28 show radius client

Function

The **show radius client** command displays AAA RADIUS client information.

Format

show radius client

Parameter

NA

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

Display AAA RADIUS client information.

```

Switch>show radius client
Authentication :
  Invalid Server Addresses      : 0
  Identifier                    : NAS
Accounting :
Switch>

```

8.8.29 tacacs-server deadtime

Function

The **tacacs-server deadtime** command configures the dead time for a TACACS server.

Format

- **tacacs-server deadtime** { *dead-time* | **default** }
- **tacacs-server name deadtime** { *dead-time* | **default** }

Parameter

Parameter	Description	Value
dead-time	Specifies the dead time for a TACACS server.	The value is an integer ranging from 3 to 4294967290, in seconds.
default	Uses the default value.	The default value is 60s.
name	Specifies a TACACS server name.	The value is a character string.

Default Value

60 seconds

View

AAA configuration view

Usage Guidelines

NA

Example

Configure the dead time for a TACACS server.

```
Switch(config-aaa)#tacacs-server deadtime 120
Switch(config-aaa)#
Switch(config-aaa)#tacacs-server fhk deadtime 100
Switch(config-aaa)#
```

8.8.30 tacacs-server {ip-address|ipv6-address} key

Function

The **tacacs-server {ip-address|ipv6-address} key** command creates a TACACS server and sets its name, IPv4 address, and shared key.

Format

- **tacacs-server name ip-address ip-address key key**
- **tacacs-server name ip6-address ipv6-address key key**
- **tacacs-server name ip-address ip-address key key [vpn-instance vpn-name]**
- **tacacs-server name ip6-address ipv6-address key key [vpn-instance vpn-name]**

Parameter

Parameter	Description	Value
name	Specifies a TACACS server name.	The value is a character string.
ip-address	Specifies an IPv4 address.	The value is in dotted decimal notation.
Ipv6-address	Specifies an IPv6 address.	-
key	Indicates a shared key.	The length is up to 64 characters.
vpn-name	Specifies a VPN instance name.	The value is a character string.

Default Value

NA

View

AAA configuration view

Usage Guidelines

NA

Example

Create a TACACS server and configure the server name, IPv4 address, and shared key

```
Switch(config-aaa)#tacacs-server fhf ip -address 10.18.2.36 key fhf
Switch(config-aaa)#
```

8.8.31 tacacs-server {ip-address|ipv6-address} key port single-connection {enable|disable}

Function

The **tacacs-server {ip-address|ipv6-address} key port single-connection {enable|disable}** command creates a TACACS server, sets its name, IPv4 address, service port, and shared key, and enables or disables the single connection function.

Format

- **tacacs-server** *name* **ip-address** *ip-address* **key** *key* **port** { *port-num* | **default** } **single-connection** { **enable** | **disable** }
- **tacacs-server** *name* **ip-address** *ip-address* **key** *key* **port** { *port-num* | **default** } **single-connection** { **enable** | **disable** } **vpn-instance** *vpn-name*
- **tacacs-server** *name* **ip6-address** *ipv6-address* **key** *key* **port** { *port-num* | **default** } **single-connection** { **enable** | **disable** }
- **tacacs-server** *name* **ip6-address** *ipv6-address* **key** *key* **port** { *port-num* | **default** } **single-connection** { **enable** | **disable** } **vpn-instance** *vpn-name*

Parameter

Parameter	Description	Value
name	Specifies a TACACS server name.	The value is a character string.
ip-address	Specifies an IPv4 address.	The value is in dotted decimal notation.
Ipv6-address	Specifies an IPv6 address.	-
key	Indicates a shared key.	The length is up to 64 characters.
port-num	Specifies a service port.	The value is an integer ranging from 1 to 65535. The default value is 49.
enable disable	Enables or disables the single-connection function.	-
vpn-name	Specifies a VPN instance name.	The value is a character string.

Default Value

Service port 49

View

AAA configuration view

Usage Guidelines

NA

Example

Create and configure a TACACS server.

```
Switch(config-aaa)# tacacs-server fhf ip-address 10.18.2.36 key fhf port default single-connection enable
Switch(config-aaa)#
```

8.8.32 tacacs-server port**Function**

The **tacacs-server port** command configures the service port for TACACS server.

Format

tacacs-server *name* **port** { *port-number* | **default** }

Parameter

Parameter	Description	Value
name	Specifies a TACACS server name.	The value is a character string.
port-number	Specifies a service port.	The value is an integer ranging from 1 to 65535.
default	Specifies the default service	The default value is 49.

Parameter	Description	Value
	port.	

Default Value

The default value is 49.

View

AAA configuration view

Usage Guidelines

NA

Example

Configure the service port for a TACACS server .

```
Switch(config-aaa)#tacacs-server fh port 100
Switch(config-aaa)#
```

8.8.33 tacacs-server single-connection {enable|disable}**Function**

The **tacacs-server single-connection {enable|disable}** command enables or disables the single connection function for a TACACS server.

Format

tacacs-server *name* **single-connection** { **enable** | **disable** }

Parameter

Parameter	Description	Value
name	Specifies a TACACS server name.	The value is a character string.
enable disable	Enables or disables the single connection function.	-

Default Value

Disable

View

AAA configuration view

Usage Guidelines

NA

Example

Enable the single connection function for a TACACS server.

```
Switch(config-aaa)#tacacs-server aaa single-connection enable
Switch(config-aaa)#
```

8.8.34 tacacs-server {src-ip|src-ipv6}**Function**

The **tacacs-server {src-ip|src-ipv6}** command sets the source IP address of packets sent to a TACACS server.

Format

- **tacacs-server** *name* **src-ip** *ip-address*
- **tacacs-server** *name* **src-ip** *ip-address* **vpn-instance** *vpn-name*
- **tacacs-server** *name* **src-ipv6** *ipv6-address*
- **tacacs-server** *name* **src-ipv6** *ipv6-address* **vpn-instance** *vpn-name*
- **no tacacs-server** *name* **src-ip**
- **no tacacs-server** *name* **src-ipv6**

Parameter

Parameter	Description	Value
ip-address	Specifies a source IP address for the packet.	The value is in dotted decimal notation.
ipv6-address	Specifies a source IP address for the packet.	The value is in the IPv6 address format.
name	Specifies a TACACS server name.	The value is a character string.
vpn-name	Specifies a VPN name.	The value is a character string.

Default Value

NA

View

AAA configuration view

Usage Guidelines

NA

Example

Set the source IP address of packets sent to a TACACS server.

```
Switch(config-aaa)#tacacs-server server2 src-ip 2.2.2.2
Switch(config-aaa)#
```

8.8.35 tacacs-server timeout**Function**

The **tacacs-server timeout** command sets the timeout duration for a TACACS server.

Format

- **tacacs-server name timeout { timeout | default }**
- **tacacs-server timeout { timeout | default }**

Parameter

Parameter	Description	Value
name	Specifies a TACACS server name.	The value is a character string.
timeout	Specifies a timeout duration.	The value is an integer ranging from 1 to 10, in seconds.
default	Uses the default timeout duration.	The default value is 2 seconds.

Default Value

2 seconds

View

AAA configuration view

Usage Guidelines

NA

Example

Set the timeout duration for a TACACS server.

```
Switch(config-aaa)#tacacs-server fhn timeout 10
Switch(config-aaa)#
Switch(config-aaa)#tacacs-server timeout 5
Switch(config-aaa)#
```

8.8.36 aaa authorization console**Function**

The **aaa authorization console** command enables the console to use AAA authorization.

The **no aaa authorization console** command disables the console from using AAA authorization.

Format

- **aaa authorization console**
- **no aaa authorization console**

Parameter

NA

Default Value

NA

View

Global configuration view

Usage Guidelines

NA

Example

Enable the console to use AAA authorization.

```
Switch(config)#aaa authorization console
Switch(config)#
```

8.8.37 login accounting aaa method

Function

The **login accounting aaa method** command configures an AAA accounting method name for user login on the terminal.

The **no login accounting aaa method** command deletes an AAA accounting method name for user login on the terminal.

Format

- **login accounting aaa method** *name*
- **no login accounting aaa method**

Parameter

Parameter	Description	Value

Parameter	Description	Value
name	Indicates the AAA charging method name.	The value is a character string.

Default Value

NA

View

Line configuration view

Usage Guidelines

NA

Example

Configure an AAA accounting method.

```
Switch(config-line)#login accounting aaa method accounttest
Switch (config-line)#
```

8.8.38 login authentication**Function**

The **login authentication** command configures the AAA authentication type for Telnet or console login on the terminal.

Format

- **login authentication aaa method** *name* **auth-type** { **pap** | **chap** | **ascii** }
- **login authentication local**
- **login authentication none**

Parameter

Parameter	Description	Value
name	Specifies an AAA remote authentication method name.	The value is a character string.
ppp chap ascii	Specifies an AAA authentication type.	-
local	Indicates local authentication.	-
none	Disables authentication.	-

Default Value

NA

View

Line configuration view

Usage Guidelines

NA

Example

Configure local authentication for the terminal.

```
Switch(config-line)#login authentication local
Switch (config-line)#
```

8.8.39 login authorization aaa method

Function

The **login authorization aaa method** command sets the login authorization method on the terminal.

The **no login authorization aaa method** command deletes the configured login authorization method on the terminal.

Format

- **login authorization aaa method** *name*
- **no login authorization aaa method**

Parameter

Parameter	Description	Value
name	Specifies an AAA authorization method name.	The value is a character string.

Default Value

NA

View

Line configuration view

Usage Guidelines

NA

Example

Configure a login authorization method named 111 for the terminal.

```
Switch(config-line)#login authorization aaa method 111
Switch (config-line)#
```

8.9 802.1x Configuration Commands

8.9.1 debug dot1x {config|out|in|timer|fsm|all}

Function

The **debug dot1x {config|out|in|timer|fsm|all}** command enables debugging of the 802.1x protocol.

The **no debug dot1x {config|out|in|timer|fsm|all}** command disables debugging of the 802.1x protocol.

Format

- **debug dot1x { config | out | in | timer | fsm | all }**
- **no debug dot1x { config | out | in | timer | fsm | all }**

Parameter

Parameter	Description	Value
config	Enables network management configuration debugging for the dot1x module.	-
out	Enables Tx packet debugging for the dot1x module.	-
in	Enables Rx packet debugging for the dot1x module.	-
timer	Enables the timer of the dot1x module.	-
fsm	Enables the dot1x state machine.	-
all	Enables all debugging functions of the dot1x module.	-

Default Value

NA

View

Privileged user view

Usage Guidelines

NA

Example

Enable debugging of the 802.1x protocol.

```
Switch#debug dot1x all
Switch#
```

8.9.2 dot1x {enable|disable}

Function

The **dot1x {enable|disable}** command enables or disables the 802.1x function on an interface.

Format

dot1x { enable | disable }

Parameter

Parameter	Description	Value
enable	Enables the 802.1x function on an interface.	-
disable	Disables the 802.1x function on an interface.	-

Default Value

By default, the 802.1x function is disabled on an interface.

View

Ethernet bridge interface configuration view, Ethernet routing interface configuration view

Usage Guidelines

Before using this command, you are advised to run the **dot1x {start|stop}** command to enable the global 802.1x function.

Before disabling the 802.1x function on an interface, ensure that this interface is not connected to any online user.

Example

Enable the 802.1x function on interface xgigaethernet 1/0/1.

```
Switch(config-10ge1/0/1)#dot1x enable
Switch(config-10ge1/0/1)#
```

8.9.3 dot1x {start|stop}

Function

The **dot1x {start|stop}** command enables or disables the 802.1x protocol globally.

Format

dot1x { start | stop }

Parameter

Parameter	Description	Value
start	Enables the 802.1x protocol globally.	-
stop	Disables the 802.1x protocol globally.	-

Default Value

By default, the 802.1x protocol is disabled globally.

View

Global configuration view

Usage Guidelines

You can use this command to enable or disable the 802.1x protocol globally. This command is a prerequisite for configuring other 802.1x parameters. Other configuration takes effect only after the 802.1x protocol is enabled globally.

Example

Enable the 802.1x protocol globally.

```
Switch(config)#dot1x start
Switch(config)#
```

8.9.4 dot1x aaa-accounting**Function**

The **dot1x aaa-accounting** command binds an AAA accounting method to an interface.

The **no dot1x aaa-accounting** command unbinds the AAA accounting method from the interface.

Format

- **dot1x aaa-accounting** *accountingname*
- **no dot1x aaa-accounting**

Parameter

Parameter	Description	Value
accountingname	Specifies an AAA accounting method name.	The value is a character string.

Default Value

NA

View

Ethernet bridge interface configuration view, Ethernet routing interface configuration view

Usage Guidelines

You can use this command to bind an AAA accounting method name to an interface.

Before using this command, run the **dot1x interface aaa** command.



Caution

Before using this command, you must run **dot1x start** in the dot1x module in the global configuration view (dot1x {start|stop}), and enable the interface AAA function in the dot1x module in the global configuration view (dot1x interface aaa).

Example

Bind AAA authentication method **accountingtest** to interface xgigaethernet 1/0/1.

```
Switch(config-10ge1/0/1)#dot1x aaa-accounting accountingtest
Switch(config-10ge1/0/1)#
```

8.9.5 dot1x aaa-authentication

Function

The **dot1x aaa-authentication** command binds an AAA authentication method to an interface.

The **no dot1x aaa-authentication** command unbinds the AAA authentication method from the interface.

Format

- **dot1x aaa-authentication** *authname*
- **no dot1x aaa-authentication**

Parameter

Parameter	Description	Value
authname	Specifies an AAA authentication method name.	The value is an integer ranging from 0 to 32, in character string format.

Default Value

NA

View

Ethernet bridge interface configuration view, Ethernet routing interface configuration view

Usage Guidelines

You can use this command to bind an AAA authentication method name to an interface.

Before using this command, run the **dot1x interface aaa** command.

Example

Bind AAA authentication method **authentictetest** to interface xgigaethernet 1/0/1.

```
Switch(config-10ge1/0/1)#dot1x aaa- authentication authentictetest
Switch(config-10ge1/0/1)#
```

8.9.6 dot1x authentication auth-method

Function

The **dot1x authentication auth-method** command specifies an authentication method for 802.1x users.

Format

dot1x authentication auth-method { eap | chap | pap }

Parameter

Parameter	Description	Value
eap	Uses Extensible Authentication Protocol (EAP) authentication.	-
chap	Uses Challenge Handshake Authentication Protocol (CHAP) authentication.	-
pap	Uses Password Authentication Protocol (PAP) authentication.	-

Default Value

By default, CHAP is adopted for authenticating 802.1x users.

View

Ethernet bridge interface configuration view, Ethernet routing interface configuration view

Usage Guidelines

Different from the CHAP authentication mode, the EAP authentication mode enables the switch to directly send 802.1x user authentication information to the RADIUS server in EAP packets, rather than converting EAP packets to standard RADIUS packets. You need to enable only the EAP authentication if any of the PEAP, EAP-TLS, EAP-TTLS, or EAP-MD5 authentication modes is adopted.

**Caution**

When local authentication is using, you do not need to configure the EAP authentication mode for 802.1x users.

If you repeatedly run the **dot1x authentication-method** command in the same view, the new configuration will overwrite the old configuration.

Example

Set the 802.1x authentication mode on interface xgigaethernet1/0/1 to EAP.

```
Switch(config-10ge1/0/1)#dot1x authentication auth-method eap
Switch(config-10ge1/0/1)#
```

8.9.7 dot1x authentication client-timeout**Function**

The **dot1x authentication client-timeout** command sets the timeout duration for the response from a supplicant (802.1x client) after the authenticator (Switch) sends a Request/MD5-Challenge packet to the supplicant.

Format

dot1x authentication client-timeout { *client-timeout* | **default** }

Parameter

Parameter	Description	Value
client-timeout	Specifies an authentication request retransmission interval.	The value is an integer ranging from 1 to 65535, in seconds.
default	Specifies the default value.	30 seconds

Default Value

By default, the response timeout duration is 30 seconds.

View

Ethernet bridge interface configuration view, Ethernet routing interface configuration view

Usage Guidelines

The 802.1x protocol starts multiple timers to maintain effective, ordered interactions between users (supplicants), access authenticator, and authentication server.

You can use this command to configure the authentication timeout timer of the client. Generally, the default value is recommended. In special situations or a poor network environment, you can set the parameter depending on the actual conditions.

After the authenticator (Switch) sends a Request/Challenge packet to a supplicant (client) to request for the MD5 encrypted data, the Switch starts the client-timeout timer. If the Switch does not receive any response from the client within the timeout duration, it retransmits the packet and resets the timer.

The Switch does not keep retransmitting the authentication requests. The number of retransmissions is set by dot1x authentication max-request.

Example

Set the authentication timeout timer of the client to 20000 seconds.

```
Switch(config-10ge1/0/1)#dot1x authentication client-timeout 20000
Switch(config-10ge1/0/1)#
```

8.9.8 dot1x authentication logical-port

Function

The **dot1x authentication logical-port** command sets the logical port generation mode.

Format

dot1x authentication logical-port { port-mac | port }

Parameter

Parameter	Description	Value
port-mac	Indicates that a logical port is generated based on the physical port and MAC address.	-
port	Indicates that a logical port is generated only based on the physical port.	-

Default Value

By default, a logical port is generated only based on the port-mac.

View

Ethernet bridge interface configuration view, Ethernet routing interface configuration view

Usage Guidelines

You can use this command to configure the generation mode of the logical port for 802.1x authentication.

Example

Set the logical port generation mode on interface xgigaethernet1/0/1 to port-mac.

```
Switch(config-10ge1/0/1)#dot1x authentication logical-port port-mac
Switch(config-10ge1/0/1)#
```

8.9.9 dot1x authentication max-request**Function**

The **dot1x authentication max-request** command sets the maximum number of authentication request retransmissions. This parameter determines how many times the Switch can retransmit authentication requests to a client.

Format

dot1x authentication max-request { *max-request* | **default** }

Parameter

Parameter	Description	Value
max-request	Specifies the maximum number of retransmissions.	The value is an integer ranging from 1 to 10.
default	Specifies the default value.	2

Default Value

By default, the maximum number of retransmissions is 2.

View

Ethernet bridge interface configuration view, Ethernet routing interface configuration view

Usage Guidelines

If the Switch does not receive any response from a user within the specified time after sending the first authentication request frame, it retransmits the authentication request frame. The number of retransmission attempts is set by this command. If the Switch still does not receive the response after the maximum number of retransmissions is reached, it does not send the authentication request to the user again.

Example

Set the maximum number of authentication request retransmissions to 8 on interface xgigaethernet 1/0/1.

```
Switch(config-10ge1/0/1)#dot1x authentication max-request 8
```

```
Switch(config-10ge1/0/1)#
```

8.9.10 dot1x authentication max-user

Function

The **dot1x authentication max-user** command sets the maximum number of 802.1x users allowed on an interface.

Format

dot1x authentication max-user { *max-user* | **default** }

Parameter

Parameter	Description	Value
max-user	Specifies the maximum number of users.	The value is an integer ranging from 1 to 256.

Default Value

The default number of users varies on different devices. It is the maximum number of users divided by the maximum number of ports. The maximum number of 802.1x users allowed by an interface is 256.

View

Ethernet bridge interface configuration view, Ethernet routing interface configuration view

Usage Guidelines

You can use this command to configure the maximum number of 802.1x users allowed on an interface. If the maximum number of users configured for an interface exceeds the maximum number of users supported by the switch, the actual number of access users may be different from the configuration.

Example

Set the maximum number of 802.1x users allowed on interface xgigaethernet1/0/1 to 100.

```
Switch(config-10ge1/0/1)#dot1x authentication max-user 100
Switch(config-10ge1/0/1)#
```

8.9.11 dot1x authentication quiet-period

Function

The **dot1x authentication quiet-period** command sets the quiet period for 802.1x users who fail the authentication on an interface.

Format

dot1x authentication quiet-period { *quiet-period* | **default** }

Parameter

Parameter	Description	Value
quiet-period	Specifies the quiet period for users who fail the authentication.	The value is an integer ranging from 1 to 120, in seconds.
default	Specifies the default value.	60 seconds

Default Value

By default, the quiet period for users who fail the authentication is set to 60 seconds.

View

Ethernet bridge interface configuration view, Ethernet routing interface configuration view

Usage Guidelines

After the quiet timer is enabled, the switch sets an 802.1x user to the quiet state if the 802.1x user fails the authentication. This can prevent the impact on the system due to frequent authentication. During the quiet period, the Switch drops the 802.1x authentication requests from the user and does not handle authentication for the user.

Generally, the default value is recommended. In special situations or a poor network environment, you can set the parameter depending on the actual conditions.

Example

Set quiet period for 802.1x users who fail the authentication to 80 seconds on interface xgigaethernet 1/0/1.

```
Switch(config-10ge1/0/1)#dot1x authentication quiet-period 80
Switch(config-10ge1/0/1)#
```

8.9.12 dot1x authentication reauthenticate-period**Function**

The **dot1x authentication reauthenticate-period** command sets the 802.1x reauthentication interval on an interface.

Format

dot1x authentication reauthenticate-period { *reauthenticate-period* | **default** }

Parameter

Parameter	Description	Value
reauthenticate-period	Specifies a re-authentication interval.	The value is an integer ranging from 60 to 7200, in seconds.
default	Specifies the default value.	3600 seconds

Default Value

The default 802.1x re-authentication interval is 3600 seconds.

View

Ethernet bridge interface configuration view, Ethernet routing interface configuration view

Usage Guidelines

You can use this command to set the 802.1x re-authentication interval.

Generally, the default value is recommended. In special situations or a poor network environment, you can set the parameter depending on the actual conditions.

Example

Set 802.1x reauthentication interval to 1000 seconds on interface xgigaehternet 1/0/1.

```
Switch(config-10ge1/0/1)#dot1x authentication reauthenticate-period 1000
Switch(config-10ge1/0/1)#
```

8.9.13 dot1x authentication server-timeout**Function**

The **dot1x authentication server-timeout** command sets the timeout duration for the authentication server on an interface.

Format

dot1x authentication server-timeout { *server-timeout* | **default** }

Parameter

Parameter	Description	Value
server-timeout	Sets the timeout duration of the authentication server.	The value is an integer ranging from 1 to 65535, in seconds.
default	Specifies the default value.	30 seconds

Default Value

By default, the timeout duration of the authentication server is 30 seconds.

View

Ethernet bridge interface configuration view, Ethernet routing interface configuration view

Usage Guidelines

You can use this command to set the authentication server timeout timer. If the authentication server does not respond within the timeout duration, the Switch retransmits authentication request packets.

Generally, the default value is recommended. In special situations or a poor network environment, you can set the parameter depending on the actual conditions.

Example

Set the timeout duration of the authentication server to 100 seconds on interface xgigaethernet 1/0/1.

```
Switch(config-10ge1/0/1)#dot1x authentication reauthenticate-period 100
Switch(config-10ge1/0/1)#
```

8.9.14 dot1x authentication tx-period

Function

The **dot1x authentication tx-period** command sets the authentication request retransmission interval upon timeout of the response from a client after the Switch sends a Request/Identity packet to the client.

Format

dot1x authentication tx-period { *tx-period* | **default** }

Parameter

Parameter	Description	Value
tx-period	Specifies an authentication request retransmission interval.	The value is an integer ranging from 1 to 65535, in seconds.
default	Specifies the default value.	30 seconds

Default Value

By default, the authentication request retransmission interval is 30 seconds.

View

Ethernet bridge interface configuration view, Ethernet routing interface configuration view

Usage Guidelines

You can use this command to enable the 802.1x tx-period timer on the Switch.

The switch starts the timer after it sends a unicast Request/Identity request to a client in the case of authentication initiated by the client. If the switch does not receive any response from the client before the timer expires, the switch retransmits the request.

For an 802.1x client that does not initiate authentication, the switch periodically sends multicast Request/Identity requests to the client through an 802.1x port at an interval of tx-period.

Generally, the default value is recommended. In special situations or a poor network environment, you can set the parameter depending on the actual conditions.

Example

On interface xgigaethernet 1/0/1, set the interval for retransmitting Request/Identity requests after the timer expires to 100 seconds.

```
Switch(config-10ge1/0/1)#dot1x authentication tx-period 100
Switch(config-10ge1/0/1)#
```

8.9.15 dot1x default aaa-accounting

Function

The **dot1x default aaa-accounting** command binds an AAA accounting method name to the system.

The **no dot1x default aaa-accounting** command unbinds an AAA accounting method name.

Format

- **dot1x default aaa-accounting** *accounting-name*
- **no dot1x default aaa-accounting**

Parameter

Parameter	Description	Value
accounting-name	Specifies an AAA accounting method name.	The value is a string of no more than 63 characters.

Default Value

NA

View

Global configuration view

Usage Guidelines

You can use this command to bind/unbind an AAA accounting method name.

Example

Bind the AAA accounting method named **accountingtest** to the system.

```
Switch(config)#dot1x default aaa-accounting accountingtest
Switch(config)#
```

8.9.16 dot1x default aaa-authentication

Function

The **dot1x default aaa-authentication** command binds an AAA authentication method name to the system.

The **no dot1x default aaa-authentication** command unbinds an AAA authentication method name from the system.

Format

- **dot1x default aaa-authentication** *auth-name*
- **no dot1x default aaa-authentication**

Parameter

Parameter	Description	Value
auth-name	Specifies an AAA authentication method name.	The value is a string of no more than 63 characters.

Default Value

NA

View

Global configuration view

Usage Guidelines

You can use this command to bind/unbind an AAA authentication method name.

Example

Bind the AAA authentication method named **authtest** to the system.

```
Switch(config)#dot1x default aaa-authentication authtest
```



```
Switch(config)#
```

8.9.17 dot1x default supplicant-support

Function

The **dot1x default supplicant-support** command globally configures the default client type.

Format

dot1x default supplicant-support { normal | sep }

Parameter

Parameter	Description	Value
normal	Specifies the normal mode.	-
sep	Specifies the Symantec mode.	-

Default Value

Normal

View

Global configuration view

Usage Guidelines

In normal mode, the client actively sends a start request. In Symantec mode, the switch actively sends a request when the port link changes to the Up state.

Example

Globally configure the default client type to Symantec mode.

```
Switch(config)#dot1x default supplicant-support
Switch(config)#
```

8.9.18 dot1x default vlan-assginment-mode

Function

The **dot1x default vlan-assginment-mode {integer|string}** command sets the VLAN assignment mode used for 802.1x authentication.

Format

dot1x default vlan-assginment-mode { integer | string }

Parameter

Parameter	Description	Value
integer	Specifies an integer type.	-
string	Specifies a string type.	-

Default Value

String

View

Global configuration view

Usage Guidelines

Generally, the dot1x authentication server supports INT and STRING types of VLAN assignment. You can determine the configuration on the switch using this command based on the VLAN assignment type of the dot1x authentication server.

In string mode, a special server is required to achieve the function.

Example

Set the VLAN assignment type to integer.

```
Switch(config)#dot1x start
Switch(config)#dot1x default vlan-assginment-mode integer
Switch(config)#
```

8.9.19 dot1x authentication retry

Function

The **dot1x authentication retry** command sets the maximum retransmission time for interface authentication Req/Ide and handshake.

Format

dot1x authentication retry { *retry-value* | **default** }

Parameter

Parameter	Description	Value
retry-value	Specifies the maximum retransmission time for interface authentication Req/Ide and handshake.	The value is an integer ranging from 1 to 10.
default	Uses the default the maximum retransmission time for interface authentication Req/Ide and handshake.	2

Default Value

2

View

Ethernet bridge interface configuration view, Ethernet routing interface configuration view

Usage Guidelines

NA

Example

Set the maximum retransmission time for interface authentication Req/Ide and handshake.

```
Switch(config-10ge1/0/1)#dot1x authentication retry 5
Switch(config-10ge1/0/1)#
```

8.9.20 dot1x guest vlan**Function**

The **dot1x guest vlan** command configures a guest VLAN on an interface.

The **no dot1x guest vlan** command deletes the guest VLAN on an interface.

Format

- **dot1x guest vlan** *vlan-id*
- **no dot1x guest vlan**

Parameter

Parameter	Description	Value
vlan-id	Specifies the ID of a guest VLAN.	The value is an integer ranging from 1 to 4094.

Default Value

By default, the guest VLAN is not configured for an interface.

View

Ethernet bridge interface configuration view, Ethernet routing interface configuration view

Usage Guidelines

You can use this command to configure a guest VLAN on an interface.

After the guest VLAN is configured, a user who fails the authentication can access only the resources in the guest VLAN. After the authentication succeeds, the user is switched to the original service VLAN. The service VLAN must be different from the guest VLAN.



Caution

The guest VLAN must have been created and cannot be the PVID of the interface.

After the guest VLAN is configured for an interface, you cannot add this interface to the VLAN again or delete the VLAN.

Different interfaces can be added to different guest VLANs.

If you run this command repeatedly in the same view, the new configuration will overwrite the old configuration.

Before configuring a guest VLAN on an interface, set **dot1x authentication max-user** to 1.

Example

Set the guest VLAN on interface xgigaethernet 1/0/1 to VLAN 100.

```
Switch(config-10ge1/0/1)#dot1x guest vlan 100
Switch(config-10ge1/0/1)#
```

8.9.21 dot1x link-mode

Function

The **dot1x link-mode** command sets the working mode of an interface.

Format

dot1x link-mode { **passive** | **active** }

Parameter

Parameter	Description	Value
passive	Indicates that the interface works in passive mode.	-
active	Indicates that the interface works in active mode.	-

Default Value

By default, an interface works in passive mode.

View

Ethernet bridge interface configuration view, Ethernet routing interface configuration view

Usage Guidelines

You can use this command to set the working mode of an interface to active or passive.

Example

Configure interface xgigaethernet 1/0/1 to work in active mode.

```
Switch(config-10ge1/0/1)#dot1x link-mode active
Switch(config-10ge1/0/1)#
```

8.9.22 dot1x mac-delete-notify

Function

The **dot1x mac-delete-notify** command determines whether to delete a user when the matching MAC address entry ages.

Format

dot1x mac-delete-notify { enable | disable }

Parameter

Parameter	Description	Value
enable	Enables the system to delete a user when the matching MAC address entry ages.	-
disable	Disables the system from deleting a user a user when the matching MAC address entry ages.	-

Default Value

Disable

View

Ethernet bridge interface configuration view, Ethernet routing interface configuration view

Usage Guidelines

NA

Example

Enable the system to delete a user when the matching MAC address entry ages.

```
Switch(config-10ge1/0/1)#dot1x mac-delete-notify enable
Switch(config-10ge1/0/1)#
```

8.9.23 dot1x reauthenticate

Function

The **dot1x reauthenticate** command enables or disables 802.1x reauthentication on an interface.

Format

dot1x reauthenticate { enable | disable }

Parameter

Parameter	Description	Value
enable	Enables reauthentication on an interface.	-
disable	Disables reauthentication on an interface.	-

Default Value

By default, 802.1x reauthentication is disabled on an interface.

View

Ethernet bridge interface configuration view, Ethernet routing interface configuration view

Usage Guidelines

You can use this command to enable or disable 802.1x reauthentication on an interface. After this function is enabled, the Switch triggers reauthentication based on the configured reauthentication interval. During reauthentication, users do not need to enter their user name and password.

Example

Enable 802.1x reauthentication on interface xgigabitEthernet 1/0/1.

```
Switch(config-10ge1/0/1)#dot1x reauthenticate enable
Switch(config-10ge1/0/1)#
```

8.9.24 dot1x reauthenticate user-mac

Function

The **dot1x reauthenticate user-mac** command sets a MAC address for a re-authenticated user.

Format

dot1x reauthenticate user-mac mac-address

Parameter

Parameter	Description	Value

Parameter	Description	Value
mac-address	Specifies the MAC address of a user.	The value is in the AA:BB:CC:DD:EE:FF format, where A to F are hexadecimal digits.

Default Value

NA

View

Ethernet bridge interface configuration view, Ethernet routing interface configuration view

Usage Guidelines

NA

Example

Set a MAC address for a re-authenticated user.

```
Switch(config-10ge1/0/1)#dot1x reauthenticate user-mac 00:00:00:00:00:01
Switch(config-10ge1/0/1)#
```

8.9.25 dot1x supplicant-support**Function**The **dot1x supplicant-support** command globally configures the default client type.**Format****dot1x supplicant-support { normal | sep }****Parameter**

Parameter	Description	Value
normal	Specifies the normal mode.	-
sep	Specifies the Symantec mode.	-

Default Value

Normal

View

Ethernet bridge interface configuration view, Ethernet routing interface configuration view

Usage Guidelines

The default mode is normal. In normal mode, the client actively sends a start request. In Symantec mode, the switch actively sends a request when the port link changes to the Up state.

Example

Configure the default client type.

```
Switch(config-10ge1/0/1)#dot1x supplicant-support sep
Switch(config-10ge1/0/1)#
```

8.9.26 dot1x unicast-trigger

Function

The **dot1x unicast-trigger** command enables or disables, in the interface configuration view, the function of triggering 802.1x authentication by unicast packets on a specified interface.

Format

dot1x unicast-trigger { enable | disable }

Parameter

Parameter	Description	Value
enable	Enables the function of triggering 802.1x authentication by unicast packets on a specified interface.	-
disable	Disables the function of triggering 802.1x authentication by unicast packets on a specified interface.	-

Default Value

NA

View

Ethernet bridge interface configuration view, Ethernet routing interface configuration view

Usage Guidelines

NA

Example

Enable the function of triggering 802.1x authentication by unicast packets on a specified interface.


```
Switch(config)#dot1x start
Switch(config)#interface gigabitEthernet 1/0/1
Switch(config-10ge1/0/1)#dot1x enable
Switch(config-10ge1/0/1)#dot1x unicast-trigger enable
Switch(config-10ge1/0/1)#
```

8.9.27 dot1x vlan-assignment-mode

Function

The **dot1x vlan-assignment-mode** command sets the VLAN assignment mode used for 802.1x authentication on an interface.

Format

dot1x vlan-assignment-mode { integer | string }

Parameter

Parameter	Description	Value
integer	Specifies an integer type.	-
string	Specifies a string type.	-

Default Value

string

View

Ethernet bridge interface configuration view, Ethernet routing interface configuration view

Usage Guidelines

Generally, the dot1x authentication server supports INT and STRING types of VLAN assignment. You can determine the configuration on the switch using this command based on the VLAN assignment type of the dot1x authentication server.

Example

Set the VLAN assignment type to integer on an interface.

```
Switch(config)#dot1x start
Switch(config)#interface gigabitEthernet 1/0/1
Switch(config-10ge1/0/1)#dot1x enable
Switch(config-10ge1/0/1)#dot1x vlan-assignment-mode integer
Switch(config-10ge1/0/1)#
```

8.9.28 dot1x interface aaa

Function

The **dot1x interface aaa** command enables or disables AAA method binding to interfaces.

Format

dot1x interface aaa { enable | disable }

Parameter

Parameter	Description	Value
enable	Enables AAA method name binding to interfaces.	-
disable	Disables AAA method name binding to interfaces.	-

Default Value

By default, AAA method name binding with the interface is disabled.

View

Global configuration view

Usage Guidelines

You can use this command to determine whether to allow AAA method name binding to all interfaces of the switch.

Example

Enable AAA method name binding to interfaces.

```
Switch(config)#dot1x interface aaa enable
Switch(config)#
```

8.9.29 no dot1x authentication user all

Function

The **no dot1x authentication user all** command deletes all 802.1x users.

Format

no dot1x authentication user all

Parameter

NA

Default Value

NA

View

Global configuration view

Usage Guidelines

You can use this command to delete all 802.1x users.

Example

Delete all 802.1x users.

```
Switch(config)#no dot1x authentication user all
Switch(config)#
```

8.9.30 no dot1x interface user all**Function**

The **no dot1x interface user all** command deletes all users on an interface.

Format

no dot1x interface { ethernet | xgigaethernet | 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet } interface-number user all

Parameter

Parameter	Description	Value
interface-number	Specifies an Ethernet interface number.	The value is an integer in the range of <1-1>/<0-1>/<1-48> (For reference only. The specific value range depends on the slot number and card type).

Default Value

NA

View

Global configuration view

Usage Guidelines

You can use this command to delete all users on an interface.

Example

Delete all users on interface xgigaethernet 1/0/1.

```
Switch(config)#no dot1x interface xgigaethernet 1/0/1 user all
Switch(config)#
```

8.9.31 show dot1x authentication user

Function

The **show dot1x authentication user** command displays user information on interfaces.

Format

show dot1x authentication user

Parameter

NA

Default Value

NA

View

Common user view

Usage Guidelines

You can use this command to check user information on interfaces of the switch.

Example

Display user information on interfaces.

```
Switch>show dot1x authentication user
interface      Mac-Addr          Vlan    State      Name
xge-1/0/1      00:11:22:33:44:55  1       authenticated  fhn
xge-1/0/2      00:11:22:33:44:55  3       authenticating wri
Switch>
```

8.9.32 show dot1x config

Function

The **show dot1x config** command displays global dot1x configuration.

Format

show dot1x config

Parameter

NA

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

Display global dot1x configuration.

```
Switch>show dot1x config
Version                :DOT1X_VB3.00.00.00
Switch>
```

8.9.33 show dot1x interface**Function**

The **show dot1x interface** command displays 802.1x information on all interfaces or a specified interface.

Format

- **show dot1x interface**
- **show dot1x interface { ethernet | xgigaethernet | 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet } interface-number**

Parameter

Parameter	Description	Value
interface-number	Specifies an interface number in the card number/interface number format.	The value is an integer in the range of <1-1>/<0-1>/<1-48> (For reference only. The specific value range depends on the slot number and card type).

Default Value

NA

View

Common user view

Usage Guidelines

If no interface number is specified, this command displays all interface information. If an interface number is specified, this command displays information about the specified interface.

Example

Display 802.1x information on interface xgigaethernet 1/0/1.

```
Switch>show dot1x interface xgigaethernet 1/0/1
dot1x enable
dot1x authentication max-user :1
dot1x reauthenticate :enable
dot1x authentication quiet-period :100
dot1x authentication reauthenticate-period :100
dot1x authentication tx-period :100
dot1x authentication client-timeout :100
dot1x authentication max-request :3
dot1x authentication logical-port :port-mac
dot1x authentication auth-method :eap
dot1x link-mode :passive
Switch>
```

8.9.34 show dot1x statistic

Function

The **show dot1x statistic** command displays dot1x statistics.

Format

show dot1x statistic

Parameter

NA

Default Value

NA

View

Common user view

Usage Guidelines

You can use this command to check dot1x statistics.

Example

Display dot1x statistics.

```
Switch>show dot1x statistic
xge-1/0/1 dot1x statistic information, Receive Protocol Version Number :1
Receive Source MAC Address :0000:0000:0000
EAPOL Packets statistic, Sent Packets:0          Receive Packets:0
Sent          EAPOL Request/Identity Packets   :0
              EAPOL Request/Challenge Packets   :0
EAPOL Success Packets          :0
EAPOL Failure Packets          :0
Received      EAPOL Start Packets    :0
              EAPOL LogOff Packets    :0
              EAPOL Response/Identity Packets :0
              EAPOL Response/Challenge Packets :0
              EAPOL Invalid Packets   :0
              EAPOL Length Error Packets :0

Switch>
```

8.9.35 show dot1x statistic {ethernet|xgigaethernet|10gigaethernet|25gigaethernet|40gigaethernet|100gigaethernet}

Function

The **show dot1x statistic**

{ethernet|xgigaethernet|10gigaethernet|25gigaethernet|40gigaethernet|100gigaethernet} command displays dot1x statistics on a specified interface.

Format

show dot1x statistic { ethernet | xgigaethernet | 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet } interface-number

Parameter

Parameter	Description	Value
interface-number	Specifies a card number or interface number.	The value is an integer in the range of <1-1>/<0-1>/<1-48> (For reference only. The specific value range depends on the slot number and card type).

Default Value

NA

View

Common user view

Usage Guidelines

You can use this command to check dot1x statistics on an interface.

Example

Display dot1x statistics on interface xgigaethernet 1/0/1.

```
Switch>show dot1x statistic xgigaethernet 1/0/1
xge-1/0/1 dot1x statistic information, Receive Protocol Version Number :1
Receive Source MAC Address: 0000:0000:0000
EAPOL Packets statistic, Sent Packets:0          Receive Packets:0
Sent          EAPOL Request/Identity Packets  :0
              EAPOL Request/Challenge Packets :0
EAPOL Success Packets          :0
EAPOL Failure Packets          :0
Received    EAPOL Start Packets   :0
            EAPOL LogOff Packets  :0
            EAPOL Response/Identity Packets :0
            EAPOL Response/Challenge Packets :0
            EAPOL Invalid Packets  :0
            EAPOL Length Error Packets :0

Switch>
```

8.10 Store Suppression Configuration Commands

8.10.1 debug storm-suppression

Function

The **debug storm-suppression** command enables storm suppression debugging.

The **no debug storm-suppression** command disables storm suppression debugging.

Format

- **debug storm-suppression { nm | multicast | broadcast | dlf | event | trap | sync | all }**
- **no debug storm-suppression { nm | multicast | broadcast | dlf | event | trap | sync | all }**

Parameter

NA

Default Value

Disable

View

Privileged user view

Usage Guidelines

NA

Example

Enable storm suppression debugging.

```
Switch#debug storm-suppression nm
Switch#
```

8.10.2 storm-suppression log {enable|disable}**Function**

The **storm-suppression log {enable|disable}** command enables or disables the storm suppression logging function.

Format

storm-suppression log { enable | disable }

Parameter

Parameter	Description	Value
enable	Enables storm suppression logging.	-
disable	Disables storm suppression logging.	-

Default Value

Disable

View

Global configuration view

Usage Guidelines

NA

Example

Enable storm suppression logging.

```
Switch(config)#storm-suppression log enable
Switch(config)#
```

8.10.3 storm-suppression trap {enable|disable}

Function

The **storm-suppression trap {enable|disable}** command enables or disables the storm suppression trap function.

Format

storm-suppression trap { enable | disable }

Parameter

Parameter	Description	Value
enable	Enables the storm suppression trap function.	-
disable	Disables the storm suppression trap function.	-

Default Value

Disable

View

Global configuration view

Usage Guidelines

NA

Example

Enable the storm suppression trap function.

```
Switch(config)#storm-suppression trap enable
Switch(config)#
```

8.10.4 storm-suppression {multicast|broadcast|dlf} min-rate max-rate

Function

The **storm-suppression {multicast|broadcast|dlf} min-rate max-rate** command sets the maximum and minimum rates (expressed as percent or values in kbit/s, Mbit/s, or Gbit/s) of storm suppression.

The **no storm-suppression {multicast|broadcast|dlf}** command restores the default value of storm suppression on an interface.

Format

- **storm-suppression** { **multicast** | **broadcast** | **dlf** } **min-rate** *percent percent* **max-rate** *percent percent*
- **storm-suppression** { **multicast** | **broadcast** | **dlf** } **min-rate** { **kbits** | **mbps** | **gbps** } *value* **max-rate** { **kbits** | **mbps** | **gbps** } *value*
- **no storm-suppression** { **multicast** | **broadcast** | **dlf** }

Parameter

Parameter	Description	Value
multicast	Specifies multicast packets.	-
broadcast	Specifies broadcast packets.	-
dlf	Specifies unicast packets.	-
percent	Specifies a percent.	The value is an integer ranging from 1 to 100.
value	Specifies a value in kbit/s, Mbit/s, or Gbit/s.	When the unit is Mbit/s, the bandwidth value ranges from 1 to 10000. When the unit is Gbit/s, the bandwidth value ranges from 1 to 10. When the unit is kbit/s, the bandwidth value ranges from 1 to 10000000.

Default Value

NA

View

Ethernet bridge interface configuration view, Ethernet routing interface configuration view

Usage Guidelines

NA

Example

Set the maximum and minimum rates of storm suppression to 50% and 10%, respectively.

```
Switch(config-10ge1/0/1)#storm-suppression multicast min-rate percent 10 max-rate percent 50
Switch(config-10ge1/0/1)#
```

8.10.5 storm-suppression action {block|error-down|none}**Function**

The **storm-suppression action {block|error-down|none}** command configures a storm suppression action.

Format

storm-suppression action { block | error-down | none }

Parameter

Parameter	Description	Value
block	Blocks packets.	-
error-down	Disables interfaces.	-
none	Specifies no action.	-

Default Value

NA

View

Ethernet bridge interface configuration view, Ethernet routing interface configuration view

Usage Guidelines

NA

Example

Set the storm suppression action to "block".

```
Switch(config-10ge1/0/1)#storm-suppression action block
Switch(config-10ge1/0/1)#
```

8.10.6 storm-suppression interval

Function

The **storm-suppression interval** command configures a detection interval for storm suppression.

Format

storm-suppression interval { interval | default }

Parameter

Parameter	Description	Value
interval	Specifies a detection interval.	The value is an integer ranging from 1 to 108, in seconds.

Parameter	Description	Value
default	Uses the default interval.	5 seconds

Default Value

5 seconds

View

Ethernet bridge interface configuration view, Ethernet routing interface configuration view

Usage Guidelines

NA

Example

Set the detection interval for storm suppression to 10 seconds.

```
Switch(config-10ge1/0/1)#storm-suppression interval 10
Switch(config-10ge1/0/1)#
```

8.10.7 show storm-suppression interface**Function**

The **show storm-suppression interface** command displays the storm suppression information on an Ethernet interface.

Format

- **show storm-suppression interface**
- **show storm-suppression interface { ethernet | xgigaethernet | 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet } interface-number**

Parameter

Parameter	Description	Value
interface-number	Specifies an Ethernet interface number.	The value is an integer in the range of <1-1>/<0-1>/<1-48> (For reference only. The specific

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

Display the storm suppression information on an Ethernet interface.

```

Switch>show storm-suppression interface
  Version                               :STORMSUPPR_VB3.00.00.00
  Trap                                  :disable
  Log                                    :enable
Interface      Type      mode      Status  Min-rate  Max-rate  Action      Current-action
Interval
Switch>

```

8.10.8 show storm-suppression config**Function**The **show storm-suppression config** command displays the storm suppression configuration.**Format****show storm-suppression config****Parameter**

NA

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

Display the storm suppression configuration.

```

Switch>show storm-suppression config
Version: STORMSUPPR_VB3.00.00.00
!
storm-suppression log enable
Switch>

```

Chapter 9 Reliability Commands

This chapter introduces the commands for configuring reliability functions on the Switch, including MSTP and BFD.

9.1 MSTP Configuration Commands

9.1.1 stp

Function

The **stp** command displays the STP configuration view.

Format

stp

Parameter

NA

Default Value

NA

View

Global configuration view

Usage Guidelines

You can use this command to switch to the STP configuration view from the global configuration view to configure STP parameters.

Example

Switch to the STP configuration view from the global configuration view.

```
Switch#configure
    %Enter configuration commands.End with Ctrl+Z or command "quit" & "end"
Switch(config)#stp
Switch(config-stp)#
```

9.1.2 stp v-stp

Function

The **stp v-stp** command enables or disables the function of STP entering cross-switch combined work mode.

Format

stp v-stp { enable | disable }

Parameter

Parameter	Description	Value
enable	Enables the function of STP entering cross-switch combined work mode.	-
disable	Disables the function of STP entering cross-switch combined work mode.	-

Default Value

By default, this function is disabled.

View

STP configuration view

Usage Guidelines

The Virtual Spanning Tree Protocol (V-STP) is an L2 topology management feature of the M-LAG solution. It virtualizes the STP protocols of two switches into the STP protocol of a single switch, allowing STP calculation on the single switch.

Two switches in V-STP mode have the same requirements of M-LAG interface STP configuration, calculation results, and sent packets. The two switches send the same STP packet to the connected device at the aggregation layer or access layer, ensuring correct L2 topology calculation in the entire network.

The V-STP mode and the global/multi-process MSTP mode are mutually exclusive.

Example

Enable the function of STP entering cross-switch combined work mode.

```
Switch(config-stp)#stp v-stp enable
Switch(config-stp)#
```

9.1.3 stp trap

Function

The **stp trap** command enables or disables the STP trap function.

Format

stp trap { enable | disable }

Parameter

Parameter	Description	Value
enable	Enables the STP trap function.	-
disable	Disables the STP trap function.	-

Default Value

By default, the STP trap function is disabled.

View

STP configuration view

Usage Guidelines

NA

Example

Enable the STP trap function.

```
Switch(config-stp)#stp trap enable
Switch(config-stp)#
```

9.1.4 stp transmit-limit**Function**

The **stp transmit-limit** command sets the number of BPDUs sent in a Hello interval of STP.

Format

stp transmit-limit { limit-value | default }

Parameter

Parameter	Description	Value
limit-value	Specifies the number of BPDUs sent in a Hello interval of STP.	The value is an integer ranging from 1 to 10.
default	Specifies the default value.	6

Default Value

By default, the number of BPDUs sent in a Hello interval is 6.

View

STP configuration view

Usage Guidelines

The more the BPDU packets sent in a Hello interval, the more the system resources are occupied. This command can limit the BPDU packets sent in a Hello interval to avoid excessive bandwidth resource occupation during network topology flapping.

Example

Set the number of BPDUs sent in a Hello interval of STP to 2.

```
Switch(config-stp)#stp transmit-limit 2
Switch(config-stp)#
```

9.1.5 stp timer-factor

Function

The **stp timer-factor** command sets the timeout duration multiple of STP.

Format

stp timer-factor { *timer-value* | **default** }

Parameter

Parameter	Description	Value
timer-value	Specifies the timeout duration multiple of STP.	The value is an integer ranging from 1 to 20.
default	Restores the multiplier of the Hello interval to the default value.	6

Default Value

6

View

STP configuration view

Usage Guidelines

NA

Example

Set the timeout duration multiple of STP.

```
Switch(config-stp)#stp timer-factor 8
Switch(config-stp)#
```

9.1.6 stp tc-protection

Function

The **stp tc-protection** command enables or disables TC-BPDU protection.

Format

stp tc-protection { enable | disable }

Parameter

Parameter	Description	Value
enable	Enables TC-BPDU protection.	-
disable	Disables TC-BPDU protection.	-

Default Value

By default, TC-BPDU protection is disabled.

View

STP configuration view and STP process view

Usage Guidelines

The system starts the Hold-off timer for an interface after the interface receives a TC-BPDU, and drops received TC-BPDUs before the Hold-off timer times out. This function filters out redundant TC-BPDUs and protects the system against malicious attacks.

Example

Enable TC-BPDU protection.

```
Switch(config-stp)#stp tc-protection enable
Switch(config-stp)#
```

9.1.7 stp tc-protection threshold

Function

The **stp tc-protection threshold** command sets the threshold on the number of TC packets.

Format

stp tc-protection threshold { threshold-value | default }

Parameter

Parameter	Description	Value
threshold-value	Specifies the threshold on the number of TC	The value is an integer ranging from 1

Parameter	Description	Value
	packets.	to 255.
default	Uses the default threshold on the number of TC packets.	2

Default Value

By default, the threshold on the number of TC packets is 2.

View

STP process view

Usage Guidelines

NA

Example

Set the threshold on the number of TC packets to 10.

```
Switch(config-stp)#stp process 1
Switch(config-stp-process-1)#stp tc-protection threshold 10
Switch(config-stp-process-1)#
```

9.1.8 stp tc-hold-off

Function

The **stp tc-hold-off** command sets the topology change delay (suppression time) for TC protection.

Format

stp tc-hold-off { *time* | **default** }

Parameter

Parameter	Description	Value
time	Specifies a delay or suppression time.	The value is an integer ranging from 4 to 30, in seconds.
default	Specifies the default value.	10 seconds

Default Value

The default topology change delay/suppression time is 10 seconds.

View

STP configuration view

Usage Guidelines

In normal situations, upon receiving a TC-BPDU packet, the switch deletes the local MAC address entry and updates the ARP address table based on the STP instances in the updated MAC address table. When a user forges TC-BPDU packets to maliciously attack the switch, the switch receives a large number of TC-BPDU packets within a short period of time. The switch frequently deletes the local MAC address entries, resulting in frequent refresh of the ARP table. This affects the spanning tree calculation and occupies a large amount of bandwidth resources, resulting in a high CPU usage. With TC-BPDU protection enabled, the switch deletes the local MAC address entry after receiving a TC-BPDU packet and starts a 10-second timer. If the switch receives TC-BPDU packets again within the timeout duration, it deletes the MAC address entry for a maximum of six times only. This prevents frequent MAC address entry deletion and improves the network stability.

This command must be used together with the `stp tc-protection threshold`

Function

The `stp tc-protection threshold` command sets the threshold on the number of TC packets.

Format

stp tc-protection threshold { *threshold-value* | **default** }

Parameter

Parameter	Description	Value
threshold-value	Specifies the threshold on the number of TC packets.	The value is an integer ranging from 1 to 255.
default	Uses the default threshold on the number of TC packets.	2

Default Value

By default, the threshold on the number of TC packets is 2.

View

STP process view

Usage Guidelines

NA

Example

Set the threshold on the number of TC packets to 10.

```
Switch(config-stp)#stp process 1
```

```
Switch(config-stp-process-1)#stp tc-protection threshold 10
Switch(config-stp-process-1)#
```

command.

Example

Set the topology change delay/suppression time to 15 seconds.

```
Switch(config-stp)#stp tc-hold-off 15
Switch(config-stp)#
```

9.1.9 stp tc-flush-arp

Function

The **stp tc-flush-arp** command enables or disables protection against TC-flush-ARP packets.

Format

stp tc-flush-arp { enable | disable }

Parameter

Parameter	Description	Value
enable	Enables protection against TC-flush-ARP packets.	-
disable	Disables protection against TC-flush-ARP packets.	-

Default Value

Disable

View

STP configuration view and STP process view

Usage Guidelines

NA

Example

Enable TC-BPDU protection.

```
Switch(config-stp)#stp tc-flush-arp enable
Switch(config-stp)#
```

9.1.10 stp root-guard

Function

The **stp root-guard** command configures the root protection function on the switch.

Format

stp root-guard { enable | disable }

Parameter

Parameter	Description	Value
enable	Enables the root protection function.	-
disable	Disables the root protection function.	-

Default Value

disable

View

Interface configuration view (Ethernet and Trunk), interface group configuration view, Peerlink configuration view

Usage Guidelines

NA

Example

Enable the root protection function on the switch.

```
Switch(config-10ge1/0/1)#stp root-guard enable
Switch(config-10ge1/0/1)#
```

9.1.11 stp revision-level

Function

The **stp revision-level** command configures the MSTP revision level.

Format

stp revision-level { range | default }

Parameter

Parameter	Description	Value
range	Specifies an STP revision level.	The value is an integer ranging from 0 to 65535.
default	Specifies the default value.	0

Default Value

The default STP revision level is 0.

View

STP configuration view

Usage Guidelines

You can use this command to set the STP revision level. The STP revision level, domain name, and VLAN mapping table determine the MST domain to which the switch belongs together.

Example

Set the STP revision level to 2.

```
Switch(config-stp)#stp revision-level 2
Switch(config-stp)#
```

9.1.12 stp reset statistic**Function**

The **stp reset statistic** command resets the STP statistics.

Format

stp reset statistic

Parameter

NA

Default Value

NA

View

Interface configuration view (Ethernet and Trunk), interface group configuration view, Peerlink configuration view

Usage Guidelines

NA

Example

Reset the STP statistics.

```
Switch(config-10ge1/0/1)#stp reset statistic
Switch(config-10ge1/0/1)#
```


9.1.13 stp process

Function

The **stp process** command creates an STP process and enters the view of the created STP process.

The **no stp process** command deletes the STP process of a specified ID.

Format

- **stp process** *process-id*
- **no stp process** *process-id*

Parameter

Parameter	Description	Value
process-id	Specifies an STP process ID.	The value is an integer ranging from 1 to 63.

Default Value

By default, all the STP-related configuration of the switch belongs to the STP process of ID 0.

View

STP process view

Usage Guidelines

If each of the switches on a public link of an STP-enabled L2 network is connected to multiple access rings independent of each other without interconnection, the ring formed by all switches cannot be calculated as a large spanning tree when STP is started. In this case, you can use different processes to enable STP independently on the rings connected to each switch for calculation. The calculations on various switches do not affect each other.

You can configure multiple processes for a switch and bind different ports to different processes. Then, these ports participate in STP calculation in the same process. The STP calculations among different processes do not affect each other.

After running this command, run **stp binding process** to bind ports to the STP process of the specified ID.

Example

Create an STP process and enter the view of the created STP process.

```
Switch(config-stp)#stp process 1
Switch(config-stp-process-1)#
```

9.1.14 stp priority (STP configuration view)

Function

The **stp priority** command sets the priority of CIST instance 0.

Format

- **stp priority** { *priority* | **default** }

Parameter

Parameter	Description	Value
priority	Specifies the Switch priority. The smaller the value is, the higher the priority is.	The value is an integer ranging from 0 to 61440. The step is 4096. That is, you can configure 16 priority values such as 0, 4096, and 8192.
default	Specifies the default value.	32768

Default Value

The default priority of the CIST instance is 32768.

View

STP configuration view and STP process view

Usage Guidelines

The step of priority values is 4096. If the priority value is not configured based on this step, the system displays the following information:

%Failed. Bridge Priority must be in increments of 4096.

%Allowed values are:

0 4096 8192 12288 16384 20480 24576 28672

32768 36864 40960 45056 49152 53248 57344 61440

Example

Set the priority of CIST instance 0 to 8192.

```
Switch(config-stp)#stp priority 8192
Switch(config-stp)#
```

9.1.15 stp priority (interface configuration view)

Function

The **stp priority** command sets the priority of an interface.

The **stp process priority** command sets the priority of the interface to which the current process belongs.

Format

- **stp priority** { *priority* | **default** }
- **stp process** *process-id* **priority** { *priority* | **default** }

Parameter

Parameter	Description	Value
priority	Specifies an interface priority.	The value is an integer ranging from 0 to 240, with a step of 16.
default	Specifies the default value.	128
process-id	Specifies an MSTP process ID.	The value is an integer ranging from 1 to 256.

Default Value

The default priority of an STP interface is 128.

View

Interface configuration view (Ethernet and Trunk), interface group configuration view, Peerlink configuration view

Usage Guidelines

You can use this command to set interface priorities for role selection.

Example

Set the priority of interface xgigaethernet 1/0/1 to 240.

```
Switch(config-10ge1/0/1)#stp priority 240
Switch(config-10ge1/0/1)#
```

9.1.16 stp point-to-point

Function

The **stp point-to-point** command enables or disables point-to-point interface management.

Format

stp point-to-point { **force-true** | **force-false** | **auto** }

Parameter

Parameter	Description	Value

Parameter	Description	Value
force-true	Enables point-to-point interface management.	-
force-false	Disables point-to-point interface management.	-

Default Value

By default, point-to-point interface management is enabled.

View

Interface configuration view (Ethernet and Trunk), interface group configuration view, Peerlink configuration view

Usage Guidelines

The fast negotiation mechanisms of RSTP and MSTP are valid only on point-to-point links.

Example

Disable point-to-point management on the xgigaethernet 1/0/1 interface.

```
Switch(config-10ge1/0/1)#stp point-to-point force-false
Switch(config-10ge1/0/1)#
```

9.1.17 Stp pathcost-standard

Function

The **stp pathcost-standard** command configures the standard to calculate the STP port path cost.

Format

stp pathcost-standard { dot1t | dot1d-1998 }

Parameter

Parameter	Description	Value
{ dot1t dot1d-1998 }	Specifies the standard to calculate the STP port path cost. "dot1t" specifies the IEEE 802.1t standard and "dot1d-1998" specifies the IEEE 802.1D-1998 standard.	-

Default Value

By default, the standard to calculate the STP port path cost is **dot1t**.

View

STP configuration view and STP process view

Usage Guidelines

Normally, all devices in the same network should use the same standard to calculate the STP port path cost.

Example

Set the standard to calculate the STP port path cost to **dot1d-1998**.

```
Switch(config-stp)#stp pathcost-standard dot1d-1998
Switch(config-stp)#
```

9.1.18 stp path-cost

Function

The **stp path-cost** command configures the management path cost of the current interface in instance 0.

The **stp path-cost** command configures the management path cost of the current process in instance 0.

Format

- **stp path-cost** { *cost* | **default** }
- **stp process** *process-id* **path-cost** { *cost* | **default** }

Parameter

Parameter	Description	Value
cost	Specifies the path cost of an interface.	The value is an integer ranging from 1 to 200000.
default	Specifies the default value.	The path cost is adaptive to the port rate.
process-id	Specifies an MSTP process ID.	The value is an integer ranging from 1 to 256.

Default Value

By default, the management path cost is 0. The path cost is automatically calculated based on the port rate.

View

Interface configuration view (Ethernet and Trunk), interface group configuration view, Peerlink configuration view

Usage Guidelines

You can use this command to set the management path cost of an interface.

Example

Set the management path cost of interface xgigaethernet 1/0/1 in instance 0 to 10000.

```
Switch(config-10ge1/0/1)#stp path-cost 10000
Switch(config-10ge1/0/1)#
```

9.1.19 stp mode**Function**

The **stp mode** command configures the STP working mode of the switch.

Format

stp mode { stp | rstp | mstp | default }

Parameter

Parameter	Description	Value
stp	Indicates the STP mode.	-
rstp	Indicates the RSTP mode.	-
mstp	Indicates the MSTP mode.	-
default	Specifies the default value.	mstp

Default Value

The default working mode of the STP is MSTP.

View

STP configuration view and STP process view

Usage Guidelines

In the STP-compatible mode, each port of the switch sends STP BPDU packets.

In the RSTP mode, each port of the switch sends RSTP BPDU packets. Upon discovering that the switch is connected to an STP device, the port automatically migrates to the STP-compatible mode.

In the MSTP mode, each port of the switch sends MSTP BPDU packets. Upon discovering that the switch is connected to an STP device, the port automatically migrates to the STP-compatible mode.

Example

Set the STP working mode to RSTP.

```
Switch(config-stp)#stp mode rstp
Switch(config-stp)#
```

9.1.20 stp migration-time

Function

The **stp migration-time** command sets an STP migration interval.

Format

stp migration-time { *migration-time* | **default** }

Parameter

Parameter	Description	Value
migration-time	Specifies an STP migration interval.	The value is an integer ranging from 1 to 10, in seconds.
default	Specifies the default value.	3 seconds

Default Value

The default STP migration interval is 3 seconds.

View

STP configuration view

Usage Guidelines

Use this command to set an STP migration interval. This parameter is used by the switch's state machine for port protocol migration. Before the switch's port receives a BPDU causing the port to change the type of sent BPDUs, the other RSTP bridges in the same LAN can synchronize their synchronization statuses based on the port status.

Example

Set the STP migration interval to 6 seconds.

```
Switch(config-stp)#stp migration-time 6
Switch(config-stp)#
```

9.1.21 stp mcheck

Function

The **stp mcheck** command configures the current interface to perform the mode check.

Format

stp mcheck

Parameter

NA

Default Value

NA

View

Interface configuration view (Ethernet and Trunk), interface group configuration view, Peerlink configuration view

Usage Guidelines

A device working in RSTP/MSTP mode can automatically migrate to the STP-compatible mode. However, a device working in the STP-compatible mode cannot automatically migrate to the RSTP/MSTP mode. In this case, you must perform the mode check operation to forcibly trigger the migration. If an MSTP (or a RSTP) device is connected to an STP device on the switching network, the port automatically migrates to the STP-compatible mode. If the STP device is removed, the port cannot automatically migrate to the MSTP (or RSTP) mode, and still works in the STP-compatible mode. In this situation, you can perform the mode check operation to forcibly trigger the port to migrate to the MSTP (or RSTP) mode.

Example

Configure interface xgigaethernet 1/0/1 to perform the mode check.

```
Switch(config-10ge1/0/1)#stp mcheck
Switch(config-10ge1/0/1)#
```

9.1.22 stp max-hops**Function**

The **stp max-hops** command configures the maximum hop count of a spanning tree in the MST region.

Format

stp max-hops { *max-hop* | **default** }

Parameter

Parameter	Description	Value
max-hop	Specifies the maximum hop count of a spanning tree.	The value is an integer ranging from 4 to 30.
default	Specifies the default maximum hop count.	20

Default Value

The default maximum hop count of the spanning tree is 20.

View

STP configuration view and STP process view

Usage Guidelines

You can use this command to set the maximum hop count of a spanning tree in the MST region, limiting the network scale.

Example

Set the maximum hop count of a spanning tree to 10.

```
Switch(config-stp)#stp max-hops 10
Switch(config-stp)#
```

9.1.23 stp max-age**Function**

The **stp max-age** command configures the maximum aging time of the spanning tree.

Format

stp max-age { *max-age* | **default** }

Parameter

Parameter	Description	Value
max-age	Specifies the maximum aging time of the spanning tree.	The value is an integer ranging from 6 to 40, in seconds.
default	Specifies the default maximum aging time.	20 seconds

Default Value

The default maximum aging time of the spanning tree is 20 seconds.

View

STP configuration view and STP process view

Usage Guidelines

If the port does not receive any configuration message within a specified period of time, the maximum aging timer is triggered. If the lifetime reaches the maximum aging time, the bridge considers that the link connected to the port is faulty and performs fault identification.

Generally, the default forward delay is adopted. Ultra-long maximum aging time results in the failure of identifying link faults in a timely manner. Ultra-short maximum aging time makes the switch incorrectly identify a link fault and perform the spanning tree re-calculation frequently.

Example

Set the maximum aging time of the spanning tree to 10 seconds.

```
Switch(config-stp)#stp max-age 10
Switch(config-stp)#
```

9.1.24 stp loop-guard

Function

The **stp loop-guard** command enables or disables the spanning tree loop guard function.

Format

stp loop-guard { enable | disable }

Parameter

Parameter	Description	Value
enable	Enables the spanning tree loop guard function.	-
disable	Disables the spanning tree loop guard function.	-

Default Value

disable

View

Interface configuration view (Ethernet and Trunk), interface group configuration view, Peerlink configuration view

Usage Guidelines

NA

Example

Enable the loop guard function.

```
Switch(config-10ge1/0/1)#stp loop-guard enable
Switch(config-10ge1/0/1)#
```

9.1.25 stp link-share binding process

Function

The **stp link-share binding process** command includes interfaces in status calculation by multiple MSTP processes.

The **no stp binding process** command removes the current interface from the STP process of a specified ID.

Format

- **stp link-share binding process** *process-list*
- **no stp binding process** *process-list*

Parameter

Parameter	Description	Value
process-list	Specifies a list of MSTP process IDs.	The value is an integer ranging from 1 to 63.

Default Value

NA

View

Interface configuration view (Ethernet and Trunk), interface group configuration view, Peerlink configuration view

Usage Guidelines

NA

Example

Include interfaces in status calculation by multiple MSTP processes.

```
Switch(config-10ge1/0/1)#stp link-share binding process 1-3
Switch(config-10ge1/0/1)#
```

9.1.26 stp link-detection

Function

The **stp link-detection** command enables or disables point-to-point link detection.

Format

stp link-detection { enable | disable }

Parameter

Parameter	Description	Value
enable	Enables point-to-point link detection.	-
disable	Disables point-to-point link detection.	-

Default Value

By default, point-to-point link detection is enabled.

View

STP configuration view

Usage Guidelines

Most switches in the network are connected by point-to-point links.

Example

Disable point-to-point link detection.

```
Switch(config-stp)#stp link-detection disable
Switch(config-stp)#
```

9.1.27 stp instance path-cost**Function**

The **stp instance path-cost** command configures the management path cost of the current port in a specified MST instance (MSTI).

Format

stp instance *instance-id* **path-cost** { *path-cost* | **default** }

Parameter

Parameter	Description	Value
instance-id	Specifies the ID of an STP instance.	The value is an integer ranging from 1 to 63.
path-cost	Specifies a port cost.	The value is an integer ranging from 1 to 200000.
default	Specifies the default value.	The path cost is adaptive to the port rate.

Default Value

By default, the instance management path cost is 0. The port path cost is automatically calculated based on the port rate.

View

Interface configuration view (Ethernet and Trunk), interface group configuration view, Peerlink configuration view

Usage Guidelines

The port path cost in a specified MST instance is a major parameter for spanning tree calculation. You can configure different path costs for the same interface in different MSTI instances to enable the switch to forward traffic of different VLANs along different physical links, achieving load balancing among VLANs.

Example

Set the port cost of interface xgigaethernet 1/0/1 in instance 63 to 1000.

```
Switch(config-10ge1/0/1)#stp instance 63 path-cost 1000
Switch(config-10ge1/0/1)#
```

9.1.28 stp instance priority (STP configuration view)

Function

The **stp instance priority** command configures the MSTI priority of the switch.

Format

stp instance *instance-id* **priority** { *priority* | **default** }

Parameter

Parameter	Description	Value
instance-id	Specifies the ID of an STP instance.	The value is an integer ranging from 1 to 63.
priority	Specifies the Switch priority. The smaller the value is, the higher the priority is.	The value is an integer ranging from 0 to 61440. The step is 4096. That is, you can configure 16 priority values such as 0, 4096, and 8192.
default	Specifies the default value.	32768

Default Value

The default priority value is 32768.

View

STP configuration view

Usage Guidelines

The priority configured using this command is a major element for the spanning tree calculation. You can configure different priority values for each switch in different MSTI instances.

The step of priority values is 4096. If the priority value is not configured based on this step, the system displays the following information:

%Failed. Bridge Priority must be in increments of 4096.

%Allowed values are:

0 4096 8192 12288 16384 20480 24576 28672
32768 36864 40960 45056 49152 53248 57344 61440

Example

Set the priority value of the switch in instance 25 to 4096.

```
Switch(config-stp)#stp instance 25 priority 4096
Switch(config-stp)#
```

9.1.29 stp instance priority (interface configuration view)

Function

The **stp instance priority** command configures the MSTI priority of the current interface

Format

stp instance *instance-id* **priority** { *priority* | **default** }

Parameter

Parameter	Description	Value
instance-id	Specifies the ID of an STP instance.	The value is an integer ranging from 1 to 63.
priority	Specifies an interface priority.	The value is an integer ranging from 0 to 240, with a step of 16.
default	Specifies the default value.	128

Default Value

By default, the priority of the port matching the spanning tree instance is 128.

View

Interface configuration view (Ethernet and Trunk), interface group configuration view, Peerlink configuration view

Usage Guidelines

The interface priority is the basis for role selection of an interface in the specified MSTI instance. You can configure different priority values for the same interface in different MSTI instances, achieving load balancing among VLANs.

Example

Set the priority of interface gigabitEthernet 1/0/1 in an STP instance to 16.

```
Switch(config-10ge1/0/1)#stp instance 1 priority 16
Switch(config-10ge1/0/1)#
```

9.1.30 stp instance vlan**Function**

The **stp instance vlan** command maps specified VLANs to an STP instance of a specified ID.

The **no stp instance vlan** command deletes the mapping between specified VLANs and an STP instance of a specified ID.

Format

- **stp instance** *instance-id* **vlan** *vlan-list*
- **no stp instance** *instance-id* **vlan** *vlan-list*

Parameter

Parameter	Description	Value
vlan-list	Specifies a VLAN list.	The value is an integer ranging from 1 to 4094.
instance-id	Specifies the ID of an STP instance.	The value is an integer ranging from 1 to 63.

Default Value

By default, all VLANs are mapped to CIST, that is, instance 0.

View

STP configuration view

Usage Guidelines

This command maps an MSTI to VLANs.

MSTP divides a switching network into multiple domains, each of which has multiple independent spanning trees. Each spanning tree is called an MSTI, and each domain is called an MST domain.

The following configurations of two switches in the same MST domain are the same:

- MST domain name
- MSTI-VLAN mapping
- MST domain revision level

Example

Map VLAN 16 to STP instance 1.

```
Switch(config-stp)#stp instance 1 vlan 16
Switch(config-stp)#
```

9.1.31 stp hello-time**Function**

The **stp hello-time** command sets the interval for sending Hello packets.

Format

stp hello-time { *hello-interval* | **default** }

Parameter

Parameter	Description	Value
hello-interval	Specifies the interval for sending STP Hello packets.	The value is an integer ranging from 1 to 10, in seconds.
default	Specifies the default interval.	2 seconds

Default Value

By default, the interval for sending STP Hello packets is 2 seconds.

View

STP configuration view and STP process view

Usage Guidelines

The switch sends BPDU packets based on the Hello Time to maintain the stability of the spanning tree.

The Hello time, Forward Delay, and Max Age must satisfy the following relations:

- $2 \times (\text{Forward Delay} - 1.0 \text{ second}) \geq \text{Max Age}$
- $\text{Max Age} \geq 2 \times (\text{Hello Time} + 1.0 \text{ second})$

MSTP can work effectively on the entire network only if the preceding relations are satisfied. If the relations are not satisfied, network flapping frequently occurs.

Generally, the default forward delay is adopted.

Example

Set the interval for sending STP Hello packets to 3 seconds.


```
Switch(config-stp)#stp hello-time 3
Switch(config-stp)#
```

9.1.32 stp forward-delay

Function

The **stp forward-delay** command sets the STP forwarding delay.

Format

stp forward-delay { *forward-delay* | **default** }

Parameter

Parameter	Description	Value
forward-delay	Specifies a spanning tree forward delay.	The value is an integer ranging from 4 to 30, in seconds.
default	Specifies the default value.	15 seconds

Default Value

The default the STP forwarding delay is 15 seconds.

View

STP configuration view and STP process view

Usage Guidelines

When the topology changes, the new configuration message spreads across the network after a period of time. This delay is called forward delay.

Generally, the default forward delay is adopted.

Example

Set the STP forwarding delay to 10 seconds.

```
Switch(config-stp)#stp forward-delay 10
Switch(config-stp)#
```

9.1.33 stp flush

Function

The **stp flush enable** command enables MAC address refresh for the topology change packets received by a spanning tree.

The **stp flush disable** command disables MAC address refresh for the topology change packets received by a spanning tree.

Format

stp flush { enable | disable }

Parameter

Parameter	Description	Value
enable	Enables MAC address refresh for the topology change packets received by a spanning tree.	-
disable	Disables MAC address refresh for the topology change packets received by a spanning tree.	-

Default Value

Disable

View

STP configuration view and STP process view

Usage Guidelines

NA

Example

Enable MAC address refresh for the topology change packets received by a spanning tree.

```
Switch(config-stp)#stp flush enable
Switch(config-stp)#
```

9.1.34 stp edge-port

Function

The **stp edge-port** command enables or disables an edge port.

Format

stp edge-port { enable | disable }

Parameter

Parameter	Description	Value
enable	Enables an edge port.	-
disable	Disables an edge port.	-

Default Value

By default, the edge port is disabled.

View

Interface configuration view (Ethernet and Trunk), interface group configuration view, Peerlink configuration view

Usage Guidelines

An edge port can directly enter the forwarding state without any delay. Generally, the port that is directly connected to a non-switching device such as a user terminal or a server is configured as an edge port.

Example

Configure interface xgigaethernet 1/0/1 as an edge port.

```
Switch(config-10ge1/0/1)#stp edge-port enable
Switch(config-10ge1/0/1)#
```

9.1.35 stp edge-default**Function**

The **stp edge-default** command enables or disables the edge port feature for all ports of the switch.

Format

stp edge-default { enable | disable }

Parameter

Parameter	Description	Value
enable	Enables the edge port feature for all ports of the switch.	-
disable	Disables the edge port feature for all ports of the switch.	-

Default Value

By default, all ports of the switch are non-edge ports.

View

STP configuration view

Usage Guidelines

In an STP-enabled L2 network, the ports connected to terminals do not participate in STP calculation. Otherwise, the speed of network topology convergence is affected, and any port status change may

result in network flapping, interrupting user traffic. You can run this command to configure the current port as an edge port to remove the port from STP calculation. This accelerates network topology convergence and improves network stability.

Example

Enable the edge port feature for all ports of the switch.

```
Switch(config-stp)#stp edge-default enable
Switch(config-stp)#
```

9.1.36 stp config-name

Function

The **stp config-name** command sets the STP region name.

The **no stp config-name** command clears an STP domain name.

Format

- **stp config-name** *string*
- **no stp config-name**

Parameter

Parameter	Description	Value
string	Specifies a spanning tree domain name.	The value is a character string. No space can be contained.

Default Value

F-engine

View

STP configuration view

Usage Guidelines

The MSTP domain name, MSTP domain, VLAN mapping table, and MSTP revision level determine the domain of a switch together.

Example

Set the STP region name to **test**.

```
Switch(config-stp)#stp config-name test
Switch(config-stp)#
```

9.1.37 stp bridge-address

Function

The **stp bridge-address** command sets the bridge MAC address of the current switch for STP calculation.

Format

stp bridge-address *mac-address*

Parameter

Parameter	Description	Value
mac-address	Specifies the bridge MAC address for STP calculation.	The value is in the AA:BB:CC:DD:EE:FF format, where A to F are hexadecimal digits.

Default Value

By default, the bridge MAC address of the current switch for STP calculation is the switch's MAC address.

View

STP configuration view

Usage Guidelines

A bridge ID is the identifier of a switch. A switch considers the packets with the same bridge ID received from other switches to be the packets from the same switch. Therefore, use this command with caution.

Example

Set the bridge MAC address of the current switch for STP calculation.

```
Switch(config-stp)#stp bridge-address 00:01:00:01:00:01
Switch(config-stp)#
```

9.1.38 stp bpdu-guard

Function

The **stp bpdu-guard** command enables or disables the BPDU guard function.

Format

stp bpdu-guard { **enable** | **disable** }

Parameter

Parameter	Description	Value
enable	Enables the BPDU guard function.	-
disable	Disables the BPDU guard function.	-

Default Value

By default, the BPDU guard function is disabled.

View

STP configuration view and STP process view

Usage Guidelines

For access-layer devices, generally, the access port is directly connected to the user terminal (such as PC) or file server. At this time, you can set the access port as the edge port to achieve fast migration of these ports. In normal situations, the edge port does not receive spanning tree configuration messages (BPDU packets). However, if someone forges a configuration message and maliciously attacks the switch, the system automatically sets the edge port as a non-edge port upon receiving the configuration message. This will cause re-calculation of the spanning tree and result in network topology flapping. The BPDU guard function can prevent this problem.

Example

Enable the BPDU guard function.

```
Switch(config-stp)#stp bpduguard enable
Switch(config-stp)#
```

9.1.39 stp bpduguard**Function**

The **stp bpduguard** command enables or disables the BPDU filter function.

Format

stp bpduguard { enable | disable }

Parameter

Parameter	Description	Value
enable	Enables the STP BPDU filter function.	-
disable	Disables the STP BPDU filter function.	-

Default Value

disable

View

Interface configuration view (Ethernet and Trunk), interface group configuration view, Peerlink configuration view

Usage Guidelines

After the STP BPDU filter function is enabled on an interface, the interface no longer sends and receives STP packets. This causes a network loop. Do not use this command unless necessary.

Example

Enable the STP BPDU filter function.

```
Switch(config-10ge1/0/1)#stp bpdu-filter enable
Switch(config-10ge1/0/1)#
```

9.1.40 stp binding process

Function

The **stp binding process** command adds the current interface to the STP process of a specified ID.

The **no stp binding process** command removes the current interface from the STP process of a specified ID.

Format

- **stp binding process** *process-id*
- **no stp binding process** *process-list*

Parameter

Parameter	Description	Value
process-id	Specifies an STP process ID.	The value is an integer ranging from 1 to 63.
process-list	Specifies an STP process ID list.	The value is an integer ranging from 1 to 63.

Default Value

By default, interfaces belong to the STP process of ID 0.

View

Interface configuration view (Ethernet and Trunk), interface group configuration view, Peerlink configuration view

Usage Guidelines

After the MSTP-enabled switch is started properly, the MSTP-related configuration of the current interface belongs to the MSTP process of ID 0. The link connecting the MSTP-enabled switch to the access ring is called an access link. To isolate various access rings in multi-process mode, run this command to add the port on the access link to the MSTP process of a specified ID.

Before using this command, run **stp process** to create an MSTP process to ensure that the ID of the MSTP process to which the current port will be added already exists.

Example

Add the current interface to the MSTP process of a specified ID.

```
Switch(config-10ge1/0/1)#stp binding process 1
Switch(config-10ge1/0/1)#
```

9.1.41 stp {enable|disable}

Function

The **stp {enable|disable}** command enables or disables STP on an interface.

Format

stp { enable | disable }

Parameter

Parameter	Description	Value
enable	Enables the spanning tree function.	-
disable	Disables the spanning tree function.	-

Default Value

By default, the STP is disabled on an interface.

View

Interface configuration view (Ethernet and Trunk), interface group configuration view, Peerlink configuration view, and STP process view

Usage Guidelines

NA

Example

Enable STP on interface xgigaethernet 1/0/1.

```
Switch(config-10ge1/0/1)#stp enable
Switch(config-10ge1/0/1)#
```


9.1.42 stp enhance-mode {enable|disable}

Function

The **stp enhance-mode {enable|disable}** command enables or disables enhanced STP.

Format

stp enhance-mode { enable | disable }

Parameter

Parameter	Description	Value
enable	Enables enhanced STP.	-
disable	Disables enhanced STP.	-

Default Value

By default, enhanced STP is enabled.

View

STP configuration view and STP process view

Usage Guidelines

NA

Example

Disable enhanced STP.

```
Switch(config-stp)#stp enhance-mode disable
Switch(config- stp)#
```

9.1.43 debug stp

Function

The **debug stp** command enables STP debugging.

The **no debug stp** command disables STP debugging.

Format

- **debug stp { error | statemachine | protection | timer | in | out | packet | protocol | event | sync | ptx | prx | ppm | bdm | pim | prs | prt | pst | tcm | all } interface { ethernet | xgigaethernet | 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet } interface-number [instance mst-instance]**

- **debug stp { error | statemachine | protection | timer | in | out | packet | protocol | event | sync | ptx | prx | ppm | bdm | pim | prs | prt | pst | tcm | all } interface eth-trunk trunk-number [instance mst-instance]**
- **no debug stp { error | statemachine | protection | timer | in | out | packet | protocol | event | sync | ptx | prx | ppm | bdm | pim | prs | prt | pst | tcm | all } interface { ethernet | xgigaethernet | 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet } interface-number [instance mst-instance]**
- **no debug stp { error | statemachine | protection | timer | in | out | packet | protocol | event | sync | ptx | prx | ppm | bdm | pim | prs | prt | pst | tcm | all } interface eth-trunk trunk-number [instance mst-instance]**
- **no debug stp all**

Parameter

Parameter	Description	Value
error	Specifies error debugging information.	-
statemachine	Specifies state machine debugging information.	-
timer	Indicates debugging information on the timer.	-
in	Indicates debugging information on packets received by the protocol.	-
out	Indicates debugging information on packets sent by the protocol.	-
packet	Indicates protocol packet debugging information.	-
protocol	Specifies protocol debugging information.	-
event	Indicates debugging information on the event.	-
sync	Specifies synchronization debugging information.	-
ptx	Specifies Tx state machine debugging information.	-
prx	Specifies Rx state machine debugging information.	-
ppm	Specifies debugging information about the protocol migration state machine.	-
bdm	Specifies debugging information about the bridge boundary detection state machine.	-
pim	Indicates the debugging information on the interface instance information state machine.	-
prs	Specifies debugging information about the interface instance role selection state machine.	-

Parameter	Description	Value
prt	Specifies debugging information about the interface instance role conversion state machine.	-
pst	Specifies debugging information about the interface instance state machine.	-
protection	Specifies the bpdu-guard root-guard loop-guard tc-guard debugging information.	-
tcm	Specifies debugging information about the interface instance topology change state machine.	-
all	Indicates debugging information on preceding types.	-
interface-number	Specifies an Ethernet interface number.	The value is an integer in the range of <1-1>/<0-1>/<1-48> (For reference only. The specific value range depends on the slot number and card type).
trunk-number	Specifies an aggregation port number.	The value ranges from 1 to 128.
mst-instance	Specifies the ID of an STP instance.	The value is an integer ranging from 1 to 63.

Default Value

By default, spanning tree debugging is disabled.

View

Privileged user view

Usage Guidelines

You can use this command to debug, maintain, and identify functional problems of STP.

Example

Enable STP debugging.

```
Switch#debug stp all
Switch#
```

Disable STP debugging.

```
Switch#no debug stp all
Switch#
```

9.1.44 no stp instance

Function

The **no stp instance** command deletes a spanning tree instance.

Format

no stp instance *instance-id*

Parameter

Parameter	Description	Value
instance-id	Specifies the ID of an STP instance.	The value is an integer ranging from 1 to 63.

Default Value

NA

View

STP configuration view

Usage Guidelines

You can use this command to delete a spanning tree instance.

Example

Delete STP instance 10.

```
Switch(config-stp)#no stp instance 10
Switch(config-stp)#
```

9.1.45 show stp

Function

The **show stp** command displays the configuration of the STP protocol on the switch.

Format

show stp

Parameter

NA

Default Value

NA

View

Common user view

Usage Guidelines

You can use this command to check the configuration of the STP protocol on the switch.

Example

Check the configuration of the STP protocol on the switch.

```
Switch>show stp
Version                               : MSTP_VB3.01.00.00
Oper Configuration
Stp Mode                             : mstp
Stp Trap                             : disable
Stp Bridge                           : customer
Stp BPDU-guard                       : disable
Stp TC-protection                    : disable
Stp TC-protection Threshold           : 2
Bridge Times      : Hello 2s MaxAge 20s FwDly 15s MaxHop 20 Timer Factor 6
Format Selector   : 0
Revision Level    : 0
Stp Config Name   : region
Stp TC-flush-arp   : disable
Stp Migration-time : 3
Stp Pathcost-standard : dot1t
Stp Tc-hold-off    : 10
Stp Transmit-limit : 6 packets/s
Stp Link-detection : enable
Stp Edge-default   : disable
Stp Instance max Number : 64
Stp Instance used Number : 1
Stp Interface max Number : 332
Stp Interface used Number : 29
Stp Interface Instance max Number : 21248
Stp Interface Instance used Number : 29

Instance Priority Vlans Mapped
0      32768    1-4094

Switch#
```

9.1.46 show stp brief

Function

The **show stp brief** command displays the STP status information on link-up interfaces and protected interfaces.

Format

show stp brief

Parameter

NA

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

Display the STP status information on link-up interfaces and protected interfaces.

```
Switch>show stp brief
```

MSTID	Port	Role	STP State	Protection	Region
0	xge-1/0/1	designated	forward	N/A	same
0	xge-1/0/2	designated	forward	N/A	same

```
Switch#
```

9.1.47 show stp config

Function

The **show stp config** command displays the configuration file information on the STP protocol on the switch.

Format

show stp config

Parameter

NA

Default Value

NA

View

Common user view

Usage Guidelines

You can use this command to check the configuration file information on STP protocol on the switch.

Example

Display the configuration file information on the STP protocol on the switch.

```
Switch>show stp config
Version: MSTP_VB3.01.00.00
stp
  stp bpdu-guard enable
interface xgigaethernet 1/0/1
  stp root-guard enable

Switch#
```

9.1.48 show stp information**Function**

The **show stp information** command displays information about the STP protocol on the switch.

Format

show stp information

Parameter

NA

Default Value

NA

View

Common user view

Usage Guidelines

You can use this command to check information about the STP protocol on the switch, including the CIST and MSTI.

Example

Check information about the STP protocol on the switch.

```
Switch>show stp information
CIST Bridge           : 32768.0005-67fc-c1cb
Bridge Times          : Hello 2s MaxAge 20s FwDly 15s RemainingHops 20
CIST Root/ERPC        : 32768.0005-67fc-c1cb/ 0
CIST RegRoot/IRPC     : 32768.0005-67fc-c1cb/ 0
Number of TC          : 0
Last TC occurred      : N/A
```

Switch#

9.1.49 show stp instance interface

Function

The **show stp instance interface** command displays the spanning tree instance configuration on all interfaces.

The **show stp instance interface {ethernet|xgigaethernet|10gigaethernet|25gigaethernet|40gigaethernet|100gigaethernet}** command displays the STP instance configuration on a specified interface of the switch.

Format

- **show stp instance *instance-id* interface**
- **show stp instance *instance-id* interface { ethernet | xgigaethernet | 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet } *interface-number***
- **show stp instance *instance-id* interface eth-trunk *trunk-number***

Parameter

Parameter	Description	Value
instance-id	Specifies an MSTI number	The value is an integer ranging from 1 to 63.
interface-number	Specifies an Ethernet interface number.	The value is an integer in the range of <1-1>/<0-1>/<1-48> (For reference only. The specific value range depends on the slot number and card type).
trunk-number	Specifies a Trunk interface number.	The value is an integer ranging from 1 to 128.

Default Value

NA

View

Common user view

Usage Guidelines

You can use this command to check the STP information on all interfaces or a specified interface.

Example

Display information about spanning tree instance 0 on interface xgigaethernet 1/0/1.

```
Switch>show stp instance 0 interface xgigaethernet 1/0/1
-----[CIST Info]-----
CIST Bridge           : 32768.0005-67fc-c1cb
Bridge Times          : Hello 2s MaxAge 20s FwDly 15s RemainingHops 20
CIST Root/ERPC        : 32768.0005-67fc-c1cb / 0
CIST RegRoot/IRPC     : 32768.0005-67fc-c1cb / 0
Number of TC          : 0
Last TC occurred      : N/A

-----[PORT Info]-----
Description           : xge-1/0/1
Port Role             : disable
STP State             : discarding
Priority              : 128
Port Cost(Dot1t)      : config=auto / active=200000000
Desg. Bridge/Port     : 32768.0005-67fc-c1cb / 128.1089
TC or TCN TX         : 0
TC or TCN RX         : 0
Last forwarding time   : 2019/10/17 09:07:03
Port Edged           : config=disable / active=disable
Point-to-point        : config=auto / active=false
TCN RX               : 0
Config RX            : 0
RSTP RX              : 0
MSTP RX              : 0
TCN TX              : 0
Config TX            : 0
RSTP TX              : 0
MSTP TX              : 0
BPDU Filter          : disable
Protection Type       : root
Switch#
```

Display information about spanning tree instance 0 on all the interfaces.

```
Switch>show stp instance 0 interface
```

MSTID	Port	Role	STP State	Protection
0	xge-1/0/1	disable	discarding	root
0	xge-1/0/2	disable	discarding	N/A
0	xge-1/0/3	disable	discarding	N/A
0	xge-1/0/4	disable	discarding	N/A
0	xge-1/0/5	disable	discarding	N/A
0	xge-1/0/6	disable	discarding	N/A
0	xge-1/0/7	disable	discarding	N/A
0	xge-1/0/8	disable	discarding	N/A
0	xge-1/0/9	disable	discarding	N/A
0	xge-1/0/10	disable	discarding	N/A
0	xge-1/0/11	disable	discarding	N/A
0	xge-1/0/12	disable	discarding	N/A
0	xge-1/0/13	disable	discarding	N/A
0	xge-1/0/14	disable	discarding	N/A
0	xge-1/0/15	disable	discarding	N/A
...				
0	eth-trunk-1	disable	discarding	N/A

```
Switch#
```

9.1.50 show stp interface

Function

The **show stp interface** command displays the STP configuration on all interfaces.

Format

show stp interface

Parameter

NA

Default Value

NA

View

Common user view

Usage Guidelines

You can use this command to check the STP configuration on all interfaces.

Example

Display the STP configuration on all interfaces.

Switch>show stp interface					
MSTID	Port	Role	STP State	Protection	Region
0	xge-1/0/1	disable	discarding	root	N/A
0	xge-1/0/2	disable	discarding	N/A	N/A
0	xge-1/0/3	disable	discarding	N/A	N/A
0	xge-1/0/4	disable	discarding	N/A	N/A
0	xge-1/0/5	disable	discarding	N/A	N/A
0	xge-1/0/6	disable	discarding	N/A	N/A
0	xge-1/0/7	disable	discarding	N/A	N/A
0	xge-1/0/8	disable	discarding	N/A	N/A
0	xge-1/0/9	disable	discarding	N/A	N/A
0	xge-1/0/10	disable	discarding	N/A	N/A
0	xge-1/0/11	disable	discarding	N/A	N/A
0	xge-1/0/12	disable	discarding	N/A	N/A
0	xge-1/0/13	disable	discarding	N/A	N/A
0	xge-1/0/14	disable	discarding	N/A	N/A
0	xge-1/0/15	disable	discarding	N/A	N/A
...					
0	eth-trunk-1	disable	discarding	N/A	N/A
Switch#					

9.1.51 show stp interface {ethernet|xgigaethernet|10gigaethernet|25gigaethernet|40gigaethernet|100gigaethernet}

Function

The **show stp interface {ethernet|xgigaethernet|10gigaethernet|25gigaethernet|40gigaethernet|100gigaethernet}** command displays the STP configuration of a specified interface of the switch.

Format

- **show stp interface { ethernet | xgigaethernet | 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet } interface-number**
- **show stp interface eth-trunk trunk-number**

Parameter

Parameter	Description	Value
interface-number	Specifies an Ethernet interface number.	The value is an integer in the range of <1-1> / <0-1> / <1-48> (For reference only. The specific value range depends on the slot number and card type).

Parameter	Description	Value
trunk-number	Specifies a Trunk interface number.	The value is an integer ranging from 1 to 128.

Default Value

NA

View

Common user view

Usage Guidelines

You can use this command to check the STP configuration on an interface.

Example

Display the STP configuration on interface xgigaethernet 1/0/1.

```
Switch>show stp interface xgigaethernet 1/0/1
-----[CIST Info]-----
CIST Bridge           : 32768.0005-67fc-c1cb
Bridge Times          : Hello 2s MaxAge 20s FwDly 15s RemainingHops 20
CIST Root/ERPC        : 32768.0005-67fc-c1cb / 0
CIST RegRoot/IRPC     : 32768.0005-67fc-c1cb / 0

-----[PORT Info instance 0]-----
Description           : xge-1/0/1
Port Role             : disable
STP State             : discarding
Priority              : 128
Port Cost(Dot1t)      : config=auto / active=200000000
Desg. Bridge/Port     : 32768.0005-67fc-c1cb / 128.1089
TC or TCN TX         : 0
TC or TCN RX         : 0
Last forwarding time   : 2019/10/17 09:07:03
Port Edged            : config=disable / active=disable
Point-to-point        : config=auto / active=false
TCN RX               : 0
Config RX             : 0
RSTP RX              : 0
MSTP RX              : 0
TCN TX               : 0
Config TX             : 0
RSTP TX              : 0
MSTP TX              : 0
```

```

BPDU Filter          : disable
Protection Type      : root
Switch#

```

9.1.52 show stp process brief

Function

The **show stp process brief** command displays the STP status of the current working interface in STP multi-process mode.

Format

show stp process *process-id* **brief**

Parameter

Parameter	Description	Value
process-id	Specifies an MSTP process ID.	The value is an integer ranging from 1 to 63.

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

Display the STP status of the current working interface in STP multi-process mode.

```

Switch>show stp process 1 brief
MSTID Port    Role    STP State  Protection  Region
0   xge-1/0/4  designated forward    N/A        different
0   eth-trunk-1 root    forward    N/A        different
Switch#

```

9.1.53 show stp process interface

Function

The **show stp process interface** command displays specific information about the current interface in STP multi-process mode.

Format

- **show stp process** *process-id* **interface** { **ethernet** | **xgigaethernet** | **10gigaethernet** | **25gigaethernet** | **40gigaethernet** | **100gigaethernet** } *interface-number*
- **show stp process** *process-id* **interface eth-trunk** *trunk-number*
- **show stp process interface**

Parameter

Parameter	Description	Value
interface-number	Specifies an Ethernet interface number.	The value is an integer in the range of <1-1>/<0-1>/<1-48> (For reference only. The specific value range depends on the slot number and card type).
trunk-number	Specifies a Trunk interface number.	The value is an integer ranging from 1 to 128.
process-id	Specifies an MSTP process ID.	The value is an integer ranging from 1 to 63.

Default Value

NA

View

Common user view

Usage Guidelines

You can use this command to check the STP configuration on an interface.

Example

Display specific information about the current interface in STP multi-process mode.

```
Switch>show stp process 1 interface xgigaethernet 1/0/4
-----[CIST Info]-----
STP Process:           : 1
CIST Bridge            : 61440.0004-67fb-6325
Bridge Times           : Hello 2s MaxAge 20s FwDly 15s RemainingHops 20
CIST Root/ERPC         : 4096.0004-67f9-62da / 10000
CIST RegRoot/IRPC      : 61440.0004-67fb-6325 / 0
CIST RootPort          : Eth-Trunk1

-----[PORT Info instance 0]-----
Description            : xge-1/0/4
Port Role              : designated
STP State              : forward
Priority               : 128
```

```

Port Cost(Dot1t)      : config=auto / active=20000
Desg. Bridge/Port     : 61440.0004-67fb-6325 / 128.1092
TC or TCN TX          : 5
TC or TCN RX          : 2
Last forwarding time   : 2020/11/30 00:00:08
Protection Type        : N/A
Switch>show stp process 1 interface eth-trunk 1
-----[CIST Info]-----
STP Process:          : 1
CIST Bridge           : 61440.0004-67fb-6325
Bridge Times          : Hello 2s MaxAge 20s FwDly 15s RemainingHops 20
CIST Root/ERPC        : 4096.0004-67f9-62da / 10000
CIST RegRoot/IRPC     : 61440.0004-67fb-6325 / 0
CIST RootPort         : Eth-Trunk1

-----[PORT Info instance 0]-----
Description           : eth-trunk-1
Port Role             : root
STP State             : forward
Priority              : 128
Port Cost(Dot1t)      : config=auto / active=10000
Desg. Bridge/Port     : 4096.0004-67f9-62da / 128.1
TC or TCN TX          : 4
TC or TCN RX          : 2
Last forwarding time   : 2020/11/30 00:00:09
Protection Type        : N/A
Switch#

```

9.1.54 show stp tc-bpdu statistic

Function

The **show stp tc-bpdu statistic** command displays statistics on the TC/TCN packets sent and received on interfaces.

Format

show stp tc-bpdu statistic

Parameter

NA

Default Value

NA

View

Common user view

Usage Guidelines

When you need to identify the ports with abnormal transmission of TC/TCN packets, run this command to check for any network fault and then locate the cause based on interface information.

Example

Display statistics on the TC/TCN packets sent and received on interfaces.

```
Switch>show stp tc-bpdu statistic
----- STP TC/TCN information -----
MSTID   Port                TC(Send/Receive)  TCN(Send/Receive)
0       xge-1/0/1           0/0               0/0
0       xge-1/0/2           0/0               0/0
0       xge-1/0/3           0/0               0/0
0       xge-1/0/4           0/0               0/0
0       xge-1/0/5           0/0               0/0
0       xge-1/0/6           0/0               0/0
0       xge-1/0/7           0/0               0/0
0       xge-1/0/8           0/0               0/0
0       xge-1/0/9           0/0               0/0
0       xge-1/0/10          0/0               0/0
0       xge-1/0/11          0/0               0/0
0       xge-1/0/12          0/0               0/0
0       xge-1/0/13          0/0               0/0
0       xge-1/0/14          0/0               0/0
0       xge-1/0/15          0/0               0/0
...
0       eth-trunk-1        0/0               0/0
Switch#
```

9.1.55 show stp topology-change**Function**

The **show stp topology-change** command displays topology change statistics.

Format

show stp topology-change

Parameter

NA

Default Value

NA

View

Common user view

Usage Guidelines

A switch in an MSTP-enabled L2 network clears ARP and MAC entries after receiving a topology change packet. The switch will experience high CPU usage when it frequently clears ARP and MAC entries due to reception of excessive topology change packets. This causes unstable network traffic.

Run this command to check statistics on MSTP/VBST topology changes. Network flapping exists when topology changes increase.

Example

Display topology change statistics.

```
Switch>show stp topology-change
CIST topology change information
  Number of topology changes           :0
  Time since last topology change      :0 weeks 0 days 0 hours 29 minutes 33 seconds
  Topology change last received from   :0005-67fc-c1cb
  Number of generated topologychange traps :0
  Number of suppressed topologychange traps :0

Switch#
```

9.2 BFD Configuration Commands

9.2.1 show bfd config

Function

The **show bfd config** command displays the BFD session configuration.

Format

show bfd config

Parameter

NA

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

Display the BFD session configuration.

Switch>show bfd config

Version :BFD_VX2.10.00.00

Switch>

9.2.2 show bfd interface**Function**The **show bfd interface** command displays the BFD-enabled interface information.**Format****show bfd interface****Parameter**

NA

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

Display information about interface gigabitEthernet 1/0/1 after it is enabled with BFD.

```
Switch>show bfd interface
Interface: ge-1/0/1
Version: v1.0
Role: active
Mode: asynch
Min out interval(ms): 1000
Min in interval(ms): 1000
Multiplier: 3
Authentication: disabled
Switch>
```

9.2.3 show bfd track

Function

The **show bfd track** command displays the static BFD session information.

Format

- **show bfd track**
- **show bfd track** *track-number*
- **show bfd track interface** { **ethernet** | **xgigaethernet** | **10gigaethernet** | **25gigaethernet** | **40gigaethernet** | **100gigaethernet** } *interface-number*
- **show bfd track interface eth-trunk** *trunk-number*
- **show bfd track interface vlan** *vlan-id*

Parameter

Parameter	Description	Value
track-number	Specifies the ID of a static BFD session.	The value is an integer ranging from 1 to 512.
interface-number	Specifies an Ethernet interface number.	The value is an integer in the range of <1-1>/<0-1>/<1-48> (For reference only. The specific value range depends on the slot number and card type).
trunk-number	Specifies the number of a Trunk interface.	The value is an integer ranging from 1 to 128.
vlan-id	Specifies a VLAN entry.	The value is an integer ranging from 1 to 4094.

Default Value

NA

View

Common user view

Usage Guidelines

Static BFD sessions are mainly used by VRRP linkage.

Example

Display the static BFD session information.

```
Switch> show bfd track
TrackIndex  Interface    Remote-bind  Local-addr    SessionDiscr  SessionState
1           ge-1/0/20    N/A         00:04:67:90:04:04    1             failure
Switch>
```

9.2.4 show bfd session**Function**

The **show bfd session** command displays information about dynamically established BFD sessions.

Format

- **show bfd session**
- **show bfd session verbose**
- **show bfd session remote-ip *ipv4-address* verbose**
- **show bfd session remote-ip *ipv6-address* verbose**
- **show bfd session remote-mac *mac-address* verbose**

Parameter

Parameter	Description	Value
ipv4-address	Specifies a remote IPv4 address.	The value is in dotted decimal notation.
ipv6-address	Specifies a remote IPv6 address.	In this format, a 128-digit IP address is divided into 8 segments. Each segment consists of 16 digits and is represented by 4 hexadecimal characters (0-9 and A-F). Segments are separated by colons (:). Every "X" represents a group of hexadecimal digits.
mac-address	Specifies a remote MAC address.	The value is in the AA:BB:CC:DD:EE:FF format, where A to F are hexadecimal digits.

Default Value

NA

View

Common user view

Usage Guidelines

The OSPF and BGP protocols generate sessions by dynamically triggering BFD.

Example

Display information about dynamically established BFD sessions (two switches connected to each other are used as an example).

```
Switch> show bfd session verbose
Interface: ge1/0/1
Version: v1.0
Role: active
Mode: asynch
Operate Mode: asynch-without-echo
Local Discriminator: 1
Remote Discriminator: 1
Diagnose: 0
Echo State: disabled
Min tx interval: 200
Min rx interval: 200
Multiplier: 3
Negotiate interval: 200
Negotiate echo interval: 0
Negotiate multiplier: 3
Session State: up
Session Addr: 00:04:67:98:10:1d
Authentication: disabled

#####At the peer end of the session#####
Switch> show bfd session verbose
Interface: ge-1/0/1
Version: v1.0
Role: active
Mode: asynch
Operate Mode: asynch-without-echo
Local Discriminator: 1
Remote Discriminator: 1
Diagnose: 0
```

```

Echo State: disabled
Min tx interval: 200
Min rx interval: 200
Multiplier: 3
Negotiate interval: 200
Negotiate echo interval: 0
Negotiate multiplier: 3
Session State: up
Session Addr: 00:04:67:97:db:7d
Authentication: disabled
Switch>

```

9.2.5 show bfd link-bundle session

Function

The **show bfd link-bundle session** command displays the BFD for Link-bundle session information.

Format

show bfd link-bundle session [**track** *track-number*]

Parameter

Parameter	Description	Value
track-number	Specifies the ID of a static BFD session.	The value is an integer ranging from 1 to 512.

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

Display the BFD for Link-bundle session information.

```

Switch> show bfd link-bundle session track 1
Track Id: 1
Interface      State    Local-Discr  Remote-Discr  local-addr  remote-addr
eth-trunk1     failure  134217729    134217729     0.0.0.0     1.1.1.1

```

```
Switch>
```

9.2.6 bfd {enable|disable}

Function

The **bfd {enable|disable}** command enables or disables BFD on an interface.

Format

bfd { enable | disable }

Parameter

Parameter	Description	Value
enable	Enables BFD.	-
disable	Disables BFD.	-

Default Value

By default, BFD is disabled on interfaces.

View

VLANIF configuration view, loopback interface configuration view, Ethernet bridge interface configuration view, Ethernet router interface configuration view, interface configuration view (trunk)

Usage Guidelines

NA

Example

Enable BFD on interface gigaethernet1/0/1.

```
Switch(config-10ge1/0/1)#bfd enable
Switch(config-10ge1/0/1)#
```

9.2.7 bfd {start|stop}

Function

The **bfd {start|stop}** command globally enables or disables BFD.

Format

bfd { start | stop }

Parameter

Parameter	Description	Value
start	Globally enables BFD.	-
stop	Globally disables BFD.	-

Default Value

By default, BFD is disabled globally.

View

Global configuration view

Usage Guidelines

Before configuring basic BFD functions, configure an interface VLAN and IP address. Before testing network connectivity, configure a routing protocol.

Example

Globally enable BFD.

```
Switch(config)#bfd start
```

```
Switch(config)#
```

9.2.8 bfd min-echo

Function

The **bfd min-echo** command sets the minimum ECHO packet reception interval.

Format

bfd min-echo *echo-interval*

Parameter

Parameter	Description	Value
echo-interval	Specifies the minimum ECHO packet reception interval.	The value is an integer ranging from 0 to 1000, in milliseconds. 0 indicates that the echo function is disabled.

Default Value

By default, the echo function is disabled.

View

Interface configuration view (Ethernet and Trunk), VLANIF configuration view, loopback configuration view, interface group configuration view

Usage Guidelines

NA

Example

Sets the minimum ECHO packet reception interval to 300 milliseconds.

```
Switch(config-10ge1/0/1)#bfd min-echo 300
```

```
Switch(config-10ge1/0/1)#
```

9.2.9 bfd min-tx min-rx multiplier**Function**

The **bfd min-tx min-rx multiplier** command sets the BFD minimum packet sending interval, minimum packet reception interval, and detection timeout multiple.

Format

bfd min-tx *tx-interval* **min-rx** *rx-interval* **multiplier** *timeout-multiple*

Parameter

Parameter	Description	Value
tx-interval	Specifies the BFD minimum packet sending interval.	The value is an integer ranging from 100 to 1000, in milliseconds. The default value is 1000 milliseconds.
rx-interval	Specifies the BFD minimum packet reception interval.	The value is an integer ranging from 100 to 1000, in milliseconds. The default value is 1000 milliseconds.
timeout-multiple	Specifies the detection timeout multiple.	The value is an integer ranging from 3 to 50. The default value is 3.

Default Value

By default, the BFD minimum packet sending interval is 1000 milliseconds, the minimum packet reception interval is 1000 milliseconds, and the detection timeout multiple is 3 times.

View

VLANIF configuration view, loopback interface configuration view, Ethernet bridge interface configuration view, Ethernet router interface configuration view, interface configuration view (trunk)

Usage Guidelines

NA

Example

Set the BFD minimum packet sending interval to 300 milliseconds, the minimum packet reception interval to 300 milliseconds, and the detection timeout multiple to 5 times.

```
Switch(config-10ge1/0/1)#bfd min-tx 300 min-rx 300 multiplier 5
Switch(config-10ge1/0/1)#
```

9.2.10 bfd track

Function

The **bfd track remote-ip|local-ip** command adds an IPv4- or IPv6-based static BFD session.

The **no bfd track** command deletes track information from a physical interface.

Format

Global configuration view:

- **bfd track track-number subsession link-auto switch**
- **bfd track track-number remote-ip ipv4-address1 local-ip ipv4-address2 vlan vlan-id**
- **bfd track track-number remote-ip ipv4-address1 local-ip ipv4-address2 vlan vlan-id one-arm-echo**
- **bfd track track-number remote-ip ipv4-address1 { ethernet | xgigaethernet | 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet } interface-number**
- **bfd track track-number remote-ip ipv4-address1 local-ip ipv4-address2 { ethernet | xgigaethernet | 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet } interface-number one-arm-echo**
- **bfd track track-number remote-ip ipv4-address1 local-ip ipv4-address2 { ethernet | xgigaethernet | 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet } interface-number**
- **bfd track track-number remote-ip ipv4-address1 local-ip ipv4-address2**
- **bfd track track-number remote-ip ipv4-address1 vlan vlan-id**
- **bfd track track-number remote-ip ipv4-address1**
- **bfd track track-number remote-ip6 ipv6-address1 local-ip ipv6-address2 vlan vlan-id**
- **bfd track track-number remote-ip6 ipv6-address1 local-ip ipv6-address2 vlan vlan-id one-arm-echo**

- **bfd track track-number remote-ip6 ipv6-address1 { ethernet | xgigaethernet | 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet } interface-number**
- **bfd track track-number remote-ip ipv4-address1 { ethernet | xgigaethernet | 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet } interface-number.subinterface**
- **bfd track track-number remote-ip6 ipv6-address1 local-ip ipv6-address2 { ethernet | xgigaethernet | 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet } interface-number one-arm-echo**
- **bfd track track-number remote-ip ipv4-address1 local-ip ipv4-address2 { ethernet | xgigaethernet | 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet } interface-number.subinterface one-arm-echo**
- **bfd track track-number remote-ip6 ipv6-address1 local-ip ipv6-address2 { ethernet | xgigaethernet | 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet } interface-number**
- **bfd track track-number remote-ip6 ipv6-address1 { ethernet | xgigaethernet | 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet } interface-number.subinterface**
- **bfd track track-number remote-ip6 ipv6-address1 local-ip6 ipv6-address2 { ethernet | xgigaethernet | 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet } interface-number.subinterface one-arm-echo**
- **bfd track track-number remote-ip6 ipv6-address1 local-ip ipv6-address2**
- **bfd track track-number remote-ip6 ipv6-address1 vlan vlan-id**
- **bfd track track-number remote-ip6 ipv6-address1**
- **no bfd track all**
- **no bfd track track-number**
- **no bfd track track-number subsession link-auto switch**

Parameter

Parameter	Description	Value
track-number	Specifies the ID of a static BFD session.	The value is an integer ranging from 1 to 512.
ipv4-address1	Specifies a remote IPv4 address.	The value is in dotted decimal notation.
ipv4-address2	Specifies a local IPv4 address.	The value is in dotted decimal notation.
ipv6-address1	Specifies a remote IPv6 address.	In this format, a 128-digit IP address is divided into 8

Parameter	Description	Value
		segments. Each segment consists of 16 digits and is represented by 4 hexadecimal characters (0-9 and A-F). Segments are separated by colons (:). Every "X" represents a group of hexadecimal digits.
ipv6-address2	Specifies a local IPv6 address.	In this format, a 128-digit IP address is divided into 8 segments. Each segment consists of 16 digits and is represented by 4 hexadecimal characters (0-9 and A-F). Segments are separated by colons (:). Every "X" represents a group of hexadecimal digits.
vlan-id	Specifies a VLAN entry.	The value is an integer ranging from 1 to 4094.
interface-number	Specifies an Ethernet interface number.	The value is an integer in the range of <1-1>/<0-1>/<1-48> (For reference only. The specific value range depends on the slot number and card type).
subinterface	Specifies a sub-interface number.	The value is an integer ranging from 1 to 4094.

Default Value

NA

View

VLANIF configuration view, loopback interface configuration view, Ethernet bridge interface configuration view, Ethernet router interface configuration view, interface configuration view (trunk), and global configuration view

Usage Guidelines

NA

Example

In the VLAN1 interface configuration view, configure track information with remote address 1.1.1.1 and local address 2.2.2.2.

```
Switch(config-vlanif-1)#bfd track 1 remote-ip 1.1.1.1 local-ip 2.2.2.2
Switch(config-vlanif-1)#
```

9.2.11 bfd track link-bundle remote-ip

Function

The **bfd track link-bundle remote-ip** command creates a BFD for Link-bundle session for detecting the IPv4 Eth-trunk link.

The **bfd track link-bundle remote-ip6** command creates a BFD for Link-bundle session for detecting the IPv6 Eth-trunk link.

Format

- **bfd track track-number link-bundle remote-ip ipv4-address1 eth-trunk trunk-number**
- **bfd track track-number link-bundle remote-ip ipv4-address1 local-ip ipv4-address2 eth-trunk trunk-number**
- **bfd track track-number link-bundle remote-ip6 ipv6-address1 eth-trunk trunk-number**
- **bfd track track-number link-bundle remote-ip6 ipv6-address1 local-ip ipv6-address2 eth-trunk trunk-number**

Parameter

Parameter	Description	Value
track-number	Specifies the ID of a static BFD session.	The value is an integer ranging from 1 to 512.
ipv4-address1	Specifies a remote IPv4 address.	The value is in dotted decimal notation.
ipv4-address2	Specifies a local IPv4 address.	The value is in dotted decimal notation.
ipv6-address1	Specifies a remote IPv6 address.	In this format, a 128-digit IP address is divided into 8 segments. Each segment consists of 16 digits and is represented by 4 hexadecimal characters (0-9 and A-F). Segments are separated by colons (:). Every "X" represents a group of hexadecimal digits.
ipv6-address2	Specifies a local IPv6 address.	In this format, a 128-digit IP address is divided into 8 segments. Each segment consists of 16 digits and is represented by 4 hexadecimal characters (0-9 and A-F). Segments are separated by colons (:). Every "X" represents a group of hexadecimal digits.
trunk-number	Specifies the number of a Trunk interface.	The value is an integer ranging from 1 to 128.

Default Value

NA

View

Global configuration view

Usage Guidelines

NA

Example

Create a BFD for Link-bundle session for detecting the IPv4 Eth-trunk link.

```
Switch(config)#bfd track 1 link-bundle remote-ip 1.1.1.1 eth-trunk 1
Switch(config)#
```

9.2.12 bfd track bind vxlan peer-ip source-ip peer-mac

Function

The **bfd track link-bundle remote-ip** command creates a BFD over VXLAN static session.

Format

bfd track *track-number* **bind vxlan peer-ip** *ipv4-address1* **source-ip** *ipv4-address2* **peer-mac** *mac-address*

Parameter

Parameter	Description	Value
track-number	Specifies the ID of a static BFD session.	The value is an integer ranging from 1 to 512.
ipv4-address1	Specifies a remote IPv4 address.	The value is in dotted decimal notation.
ipv4-address2	Specifies a source IPv4 address.	The value is in dotted decimal notation.
mac-address	Specifies a remote MAC address.	The value is in the AA:BB:CC:DD:EE:FF format, where A to F are hexadecimal digits.

Default Value

NA

View

Global configuration view

Usage Guidelines

NA

Example

Create a BFD over VXLAN static session.

```
Switch(config)#bfd track 1 link-bundle remote-ip 1.1.1.1 eth-trunk 1
Switch(config)#
```

9.2.13 bfd track min-tx min-rx multiplier

Function

The **bfd track min-tx min-rx multiplier** command sets the minimum packet sending interval, minimum packet reception interval, and detection timeout multiple for a BFD session.

Format

bfd track *track-number* **min-tx** { *tx-interval* | **default** } **min-rx** { *rx-interval* | **default** } **multiplier** *timeout-multiple*

Parameter

Parameter	Description	Value
tx-interval	Specifies the BFD minimum packet sending interval.	The value is an integer ranging from 100 to 1000, in milliseconds. The default value is 1000 milliseconds.
rx-interval	Specifies the BFD minimum packet reception interval.	The value is an integer ranging from 100 to 1000, in milliseconds. The default value is 1000 milliseconds.
timeout-multiple	Specifies the detection timeout multiple.	The value is an integer ranging from 3 to 50. The default value is 3.
track-number	Specifies the ID of a static BFD session.	The value is an integer ranging from 1 to 512.

Default Value

By default, the BFD minimum packet sending interval is 1000 milliseconds, the minimum packet reception interval is 1000 milliseconds, and the detection timeout multiple is 3 times.

View

VLANIF configuration view, loopback interface configuration view, Ethernet bridge interface configuration view, Ethernet router interface configuration view, interface configuration view (trunk)

Usage Guidelines

NA

Example

Set the BFD minimum packet sending interval to 300 milliseconds, the minimum packet reception interval to 300 milliseconds, and the detection timeout multiple to 5 times.

```
Switch(config-10ge1/0/1)#bfd min-tx 300 min-rx 300 multiplier 5
Switch(config-10ge1/0/1)#
```

9.2.14 bfd trap

Function

The **bfd trap {enable|disable}** command enables or disables the BFD session status (up or down) trap function.

Format

bfd trap { enable | disable }

Parameter

Parameter	Description	Value
enable	Enables the BFD trap function.	-
disable	Disables the BFD trap function.	-

Default Value

By default, the BFD trap function is disabled.

View

Global configuration view

Usage Guidelines

NA

Example

Enable the BFD trap function.

```
Switch(config)#bfd trap enable
Switch(config)#
```

9.2.15 debug bfd

Function

The **debug bfd** command enables BFD debugging.

The **no debug bfd** command disables BFD debugging.

Format

- **debug bfd { session | rx | rxpkt | tx | txpkt | event | all }**
- **no debug bfd { session | rx | rxpkt | tx | txpkt | event | all }**

Parameter

Parameter	Description	Value
session	Specifies debugging of BFD session information.	-
rx	Specifies debugging of BFD Rx information.	-
rxpkt	Specifies debugging of BFD received packet information.	-
tx	Specifies debugging of BFD Tx information.	-
txpkt	Specifies debugging of BFD sent packet information.	-
event	Specifies debugging of BFD event information.	-
all	Specifies debugging of all BFD information.	-

Default Value

By default, BFD debugging is disabled.

View

Privileged user view

Usage Guidelines

Use this command to locate BFD-related faults and problems.

Example

Debug BFD Rx information.

```
Switch#debug bfd rx
Switch#
```

9.2.16 bfd bind ingress (global configuration view)

Function

The **bfd bind ingress** command binds a BFD session.

Format

- **bfd bind ingress interface** { **ethernet** | **xgigaethernet** | **10gigaethernet** | **25gigaethernet** | **40gigaethernet** | **100gigaethernet** } *interface-number* **egress track track-number trigger if-down**
- **bfd bind ingress track track-number trigger down egress track track-number**
- **bfd bind ingress track track-number trigger if-down egress interface** { **ethernet** | **xgigaethernet** | **10gigaethernet** | **25gigaethernet** | **40gigaethernet** | **100gigaethernet** } *interface-number*

- **no bfd bind ingress interface** { **ethernet** | **xgigaethernet** | **10gigaethernet** | **25gigaethernet** | **40gigaethernet** | **100gigaethernet** } *interface-number* **egress track track-number trigger if-down**
- **no bfd bind ingress track track-number trigger down egress track track-number**
- **no bfd bind ingress track track-number trigger if-down egress interface** { **ethernet** | **xgigaethernet** | **10gigaethernet** | **25gigaethernet** | **40gigaethernet** | **100gigaethernet** } *interface-number*

Parameter

Parameter	Description	Value
interface-number	Specifies an Ethernet interface number.	The value is an integer in the range of <1-1>/<0-1>/<1-48> (For reference only. The specific value range depends on the slot number and card type).
track-number	Specifies the ID of a static BFD session.	The value is an integer ranging from 1 to 512.

Default Value

NA

View

Global configuration view

Usage Guidelines

NA

Example

Bind a BFD session.

```
Switch(config)#bfd bind ingress interface 10gigaethernet 1/0/1 egress track 1 trigger-if-down
Switch(config)#
```

9.2.17 bfd bind ingress (interface configuration view)

Function

The **bfd bind ingress** command binds a BFD session in the inbound direction on an interface.

Format

- **bfd bind ingress track track-number trigger if-down**

- **no bfd bind ingress track *track-number* trigger if-down**

Parameter

Parameter	Description	Value
track-number	Specifies the ID of a static BFD session.	The value is an integer ranging from 1 to 512.

Default Value

NA

View

Interface configuration view (Ethernet and Trunk), VLANIF configuration view, interface group configuration view

Usage Guidelines

NA

Example

Bind a BFD session in the inbound direction on an interface.

```
Switch(config-10ge1/0/1)#bfd bind ingress track 1 trigger-if-down
Switch(config-10ge1/0/1)#
```

9.2.18 bfd bind egress (interface configuration view)

Function

The **bfd bind egress** command binds a BFD session in the outbound direction on an interface.

Format

- **bfd bind egress track *track-number* trigger if-down**
- **no bfd bind egress track *track-number* trigger if-down**

Parameter

Parameter	Description	Value
track-number	Specifies the ID of a static BFD session.	The value is an integer ranging from 1 to 512.

Default Value

NA

View

Interface configuration view (Ethernet and Trunk), VLANIF configuration view, interface group configuration view

Usage Guidelines

NA

Example

Bind a BFD session in the outbound direction on an interface.

```
Switch(config-10ge1/0/1)#bfd bind egress track 1 trigger-if-down
Switch(config-10ge1/0/1)#
```

9.2.19 process-interface-status {enable|disable}

Function

The **process-interface-status {enable|disable}** command enables or disables status linkage between the current BFD session and the bound interface.

Format

process-interface-status { enable | disable }

Parameter

Parameter	Description	Value
enable	Enables status linkage between the current BFD session and the bound interface.	-
disable	Disables status linkage between the current BFD session and the bound interface.	-

Default Value

By default, status linkage between the current BFD session and the bound interface is disabled.

View

Global configuration view

Usage Guidelines

After this command is executed, change of the BFD session status causes change of the interface status in the interface management module. When the BFD session detects a fault and the interface enters the Down state, the interface status changes to BFD Down. In this state, the interface's direct route is canceled at the control plane but remains unaffected at the forwarding plane.



Caution

This command is only applicable to single-hop BFD sessions that use default multicast IP address detection.

When multiple BFD sessions are bound to the same interface, you can run this command in only one of these sessions. That is, the status of only one session can change the BFD status of the bound interface.

To use interface status linkage, ensure that the two connected switches have the correct and symmetric BFD configuration. If the BFD status of the local interface is Down, check whether the BFD configuration at the peer end is correct and whether the peer interface is shut down.

Example

Enable status linkage between the current BFD session and the bound interface.

```
Switch(config)#process-interface-status enable
Switch(config)#
```

9.3 VRRP Configuration Commands

9.3.1 show ip vrrp associate interface

Function

The **show ip vrrp associate interface** command shows information about an interface associated with VRRP.

Format

- **show ip vrrp associate interface**
- **show ip vrrp associate interface { ethernet | xgigaethernet | 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet } interface-number virtual-route-id**
- **show ip vrrp associate interface { ethernet | xgigaethernet | 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet } interface-number**

- **show ip vrrp associate interface { ethernet | xgigaethernet | 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet } interface-number.subinterface virtual-route-id**
- **show ip vrrp associate interface { ethernet | xgigaethernet | 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet } interface-number.subinterface**
- **show ip vrrp associate interface vlan vlan-id virtual-route-id**
- **show ip vrrp associate interface vlan vlan-id**

Parameter

Parameter	Description	Value
virtual-route-id	Specifies the global ID of a virtual router.	The value is an integer ranging from 1 to 255.
vlan-id	Specifies the VLAN ID to be bound.	The value is an integer ranging from 1 to 4094.
interface-number	Specifies a remote observation port.	The value is an integer in the range of <1-16>/<0-0>/<1-48> (For reference only. The specific value range depends on the slot number and card type).
subinterface	Specifies a sub-interface number.	The value is an integer ranging from 1 to 4094.

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

Show information about an interface associated with VRRP.

```
Switch>show ip vrrp associate interface
Switch>
```

9.3.2 show ip vrrp binding admin-vrrp interface

Function

The **show ip vrrp binding admin-vrrp interface** command shows binding relation between the management VRRP backup group and the member VRRP backup group.

Format

- **show ip vrrp binding admin-vrrp interface { ethernet | xgigaethernet | 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet } interface-number virtual-route-id**
- **show ip vrrp binding admin-vrrp interface { ethernet | xgigaethernet | 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet } interface-number.subinterface virtual-route-id**
- **show ip vrrp binding admin-vrrp interface vlan vlan-id virtual-route-id**

Parameter

Parameter	Description	Value
interface-number	Specifies a remote observation port.	The value is an integer in the range of <1-16>/<0-0>/<1-48> (For reference only. The specific value range depends on the slot number and card type).
virtual-route-id	Specifies a member VRRP backup group ID.	The value is an integer ranging from 1 to 255.
subinterface	Specifies a sub-interface number.	The value is an integer ranging from 1 to 4094.
vlan-id	Specifies a VLANIF interface number.	The value is an integer ranging from 1 to 4094.

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

Show binding relation between the management VRRP backup group and the member VRRP backup group.

```
Switch>show ip vrrp binding admin-vrrp interface vlan 1 2
Member-Interface      Member-VRID    VR-State
vlan-1                2              Initial
Switch>
```

9.3.3 show ip vrrp interface

Function

The **show ip vrrp interface** command displays details of the VRRP router (applicable to IPv4).

Format

- **show ip vrrp interface vlan** *vlan-id virtual-route-id*
- **show ip vrrp interface vlan** *vlan-id*
- **show ip vrrp interface { ethernet | xgigaethernet | 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet }** *interface-number virtual-route-id*
- **show ip vrrp interface { ethernet | xgigaethernet | 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet }** *interface-number*
- **show ip vrrp interface { ethernet | xgigaethernet | 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet }** *interface-number.subinterface virtual-route-id*
- **show ip vrrp interface { ethernet | xgigaethernet | 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet }** *interface-number.subinterface*

Parameter

Parameter	Description	Value
virtual-route-id	Specifies the global ID of a virtual router.	The value is an integer ranging from 1 to 255.
vlan-id	Specifies a VLAN ID.	The value is an integer ranging from 1 to 4094.
interface-number	Specifies a remote observation port.	The value is an integer in the range of <1-16>/<0-0>/<1-48> (For reference only. The specific value range depends on the slot number and card type).
subinterface	Specifies a sub-interface number.	The value is an integer ranging from 1 to 4094.

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

Show details of a virtual VRRP router.

```
Switch>show ip vrrp interface vlan 1 1
VRRP State                : Initial
Virtual Router ID         : 1
Role                      : normal
PriorityRun                : 100
PriorityConfig             : 100
Preempt                   : enable
Preempt Timer Delay       : 0
Holding-multiplier        : 3
Virtual Router MAC Address : 00:00:5e:00:01:01
Authentication Mode       : none
Authentication Key        : N/A
Master IP Address         : 0.0.0.0
Interface IP Address      : 0.0.0.0
Advertisement Interval     : 1
Advertisement Interval Config : 1
Associate IP Address Count : 0

Statistic of This VRRP Entry:
Master Transitions        : 0
Received Advertise        : 0
Send Priority Zero Packets : 0
Received Priority Zero Packets : 0

Switch>
```

9.3.4 show ip vrrpv3 interface

Function

The **show ip vrrpv3 interface** command displays details of the VRRPv3 router.

Format

- **show ip vrrpv3 interface vlan** *vlan-id virtual-route-id*
- **show ip vrrpv3 interface { ethernet | xgigaethernet | 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet }** *interface-number virtual-route-id*
- **show ip vrrpv3 interface { ethernet | xgigaethernet | 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet }** *interface-number.subinterface virtual-route-id*

Parameter

Parameter	Description	Value

Parameter	Description	Value
virtual-route-id	Specifies the global ID of a virtual router.	The value is an integer ranging from 1 to 255.
vlan-id	Specifies a VLAN ID.	The value is an integer ranging from 1 to 4094.
interface-number	Specifies a remote observation port.	The value is an integer in the range of <1-16>/<0-0>/<1-48> (For reference only. The specific value range depends on the slot number and card type).
subinterface	Specifies a sub-interface number.	The value is an integer ranging from 1 to 4094.

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

Show details of a virtual VRRPv3 router.

```
Switch #show ip vrrpv3 interface vlan 10 1
Virtual Router Id:1,VRRP State:Master
Row state:Active,Priority:10
Virtual Router MAC Address:00:00:5e:00:01:01
Master IP Address:1.1.1.2
Primary IP Address:1.1.1.1
Advertisement Interval:1, Preempt Mode:Enable
Virtual Router Uptime:101100, Protocol:ip
Associate IP Address Count:1
IP Address:1.1.1.2
Statistic of this VRRP entry:
Become Master:1, Advertise Received:0
Send Priority Zero Packets:104, Received Priority Zero Packets:0
Authenticate Failure:0, Invalid Authentication Type:0
Authentication Type Mismatch:0
Packet Length Errors:0, Invalid Type Packet Received:0
Advertise Interval Errors:0, IP TTL Errors:0
Switch #
```

9.3.5 show ip vrrp verbose

Function

The **show ip vrrp verbose** command displays the details of the IPv4 VRRP.

Format

show ip vrrp verbose

Parameter

NA

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

View the details of the IPv4 VRRP.

```
Switch>show ip vrrp verbose
Switch>
```

9.3.6 show ipv6 vrrp interface

Function

The **show ipv6 vrrp interface** command displays details of the VRRP router (applicable to IPv6).

Format

- **show ipv6 vrrp interface vlan** *vlan-id* *virtual-route-id*
- **show ipv6 vrrp interface vlan** *vlan-id*
- **show ipv6 vrrp interface { ethernet | xgigaethernet | 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet }** *interface-number* *virtual-route-id*
- **show ipv6 vrrp interface { ethernet | xgigaethernet | 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet }** *interface-number*
- **show ipv6 vrrp interface { ethernet | xgigaethernet | 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet }** *interface-number.subinterface* *virtual-route-id*

- **show ipv6 vrrp interface { ethernet | xgigaethernet | 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet } interface-number.subinterface**

Parameter

Parameter	Description	Value
virtual-route-id	Specifies the global ID of a virtual router.	The value is an integer ranging from 1 to 255.
vlan-id	Specifies a VLAN ID.	The value is an integer ranging from 1 to 4094.
interface-number	Specifies a remote observation port.	The value is an integer in the range of <1-16>/<0-0>/<1-48> (For reference only. The specific value range depends on the slot number and card type).
subinterface	Specifies a sub-interface number.	The value is an integer ranging from 1 to 4094.

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

Show details of a virtual VRRP router.

```
Switch>show ipv6 vrrp interface vlan 2 1
Switch>
```

9.3.7 show ipv6 vrrp binding admin-vrrp interface

Function

The **show ipv6 vrrp binding admin-vrrp interface** command displays the binding relation between the management VRRP backup group and the member VRRP backup group.

Format

- **show ipv6 vrrp binding admin-vrrp interface vlan *vlan-id* virtual-route-id**

- **show ipv6 vrrp binding admin-vrrp interface { ethernet | xgigaehternet | 10gigaehternet | 25gigaehternet | 40gigaehternet | 100gigaehternet } interface-number virtual-route-id**
- **show ipv6 vrrp binding admin-vrrp interface { ethernet | xgigaehternet | 10gigaehternet | 25gigaehternet | 40gigaehternet | 100gigaehternet } interface-number.subinterface virtual-route-id**

Parameter

Parameter	Description	Value
vlan-id	Specifies a VLANIF interface number.	The value is an integer ranging from 1 to 4094.
virtual-route-id	Specifies a member VRRP backup group ID.	The value is an integer ranging from 1 to 255.
interface-number	Specifies a remote observation port.	The value is an integer in the range of <1-16>/<0-0>/<1-48> (For reference only. The specific value range depends on the slot number and card type).
subinterface	Specifies a sub-interface number.	The value is an integer ranging from 1 to 4094.

Default Value

NA

View

Common user view

Usage Guidelines

The following table describes VRRP binding information that can be queried using this command.

Item	Description
Member-Interface	Specifies the interface type and number of the management VRRP.
Member-VRID	Specifies a member VRRP backup group ID.
VR-State	Specifies the VRRP backup group state, including Master, Backup, and Initial.

Example

Show binding relation between the management VRRP backup group and the member VRRP backup group.

```
Switch>show ipv6 vrrp binding admin-vrrp interface vlan 1 1
  Member-Interface    Member-VRID    VR-State
  vlan-20             2              Initial
Switch>
```

9.3.8 show ipv6 vrrp verbose

Function

The **show ipv6 vrrp verbose** command displays the details of the IPv6 VRRP.

Format

show ipv6 vrrp verbose

Parameter

NA

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

View the details of the IPv6 VRRP.

```
Switch>show ipv6 vrrp verbose
Switch>
```

9.4 EFM Configuration Commands

9.4.1 debug efm

Function

The **debug efm** command enables 802.3ah debugging.

The **no debug efm** command disables 802.3ah debugging.

Format

- **debug efm { error | event | fsm | timer | out | in | test | system | all }**
- **no debug efm { error | event | fsm | timer | out | in | test | system | all }**

Parameter

Parameter	Description	Value

Parameter	Description	Value
error	Specifies error messages at runtime.	-
event	Specifies special event information at runtime.	-
fsm	Specifies state machine change information.	-
timer	Specifies timer overflow information.	-
out	Specifies information about sent packets.	-
in	Specifies information about received packets.	-
test	Specifies selftest debugging information.	-
system	Specifies system debugging information.	-
all	Specifies all debugging information.	-

Default Value

By default, 802.3ah debugging is disabled.

View

Privileged user view

Usage Guidelines

NA

Example

Enable 802.3ah debugging.

```
Switch#debug efm all
Switch#
```

Disable 802.3ah debugging.

```
Switch#no debug efm all
Switch#
```

9.4.2 efm {enable|disable}

Function

The **efm {enable|disable}** command enables or disables the EFM protocol on an interface.

Format

efm { enable | disable }

Parameter

Parameter	Description	Value
enable	Enables the EFM protocol on an interface.	-

Parameter	Description	Value
disable	Disables the EFM protocol on an interface.	-

Default Value

By default, the EFM protocol is disabled on an interface.

View

Ethernet bridge interface configuration view, router interface configuration view

Usage Guidelines

After the EFM protocol is enabled on an interface, the interface uses the following default settings:

- EFM mode: Active
- Maximum EFM PDU sending rate: 10 EFM PDUs per interval
- Minimum EFM PDU sending interval: 1 second
- EFM discovery timeout duration: 5 seconds
- Loopback: unsupported
- Link detection: unsupported

Example

Enable the EFM protocol on interface xgigaethernet 1/0/1.

```
Switch(config-10ge1/0/1)#efm enable
Switch(config-10ge1/0/1)#
```

9.4.3 efm fault-logs clear all

Function

The **efm fault-logs clear all** command clears the EFM logs of the switch.

Format

efm fault-logs clear all

Parameter

NA

Default Value

NA

View

Privileged user view

Usage Guidelines

When the error logs of an EFM instance reach the maximum number, you can run this command to clear the error logs.

Example

Clear the EFM logs of the switch.

```
Switch#efm fault-logs clear all
Switch#
```

9.4.4 efm fault-logs clear

Function

The **efm fault-logs clear** command clears the EFM logs of an interface.

Format

efm fault-logs clear

Parameter

NA

Default Value

NA

View

Ethernet bridge interface configuration view, router interface configuration view

Usage Guidelines

When the error logs of an EFM instance reach the maximum number, you can run this command to clear the error logs.

Example

Clear the EFM logs of an interface.

```
Switch(config-10ge1/0/1)#efm fault-logs clear
Switch(config-10ge1/0/1)#
```

9.4.5 efm link-monitor {supported|unsupported}

Function

The **efm link-monitor {supported|unsupported}** command configures whether to support link detection.

Format

efm link-monitor { supported | unsupported }

Parameter

Parameter	Description	Value
supported	Specifies that link detection is supported.	-
unsupported	Specifies that link detection is not supported.	-

Default Value

By default, link performance detection is supported. Data is collected every 100 milliseconds.

View

Ethernet bridge interface configuration view, router interface configuration view

Usage Guidelines

NA

Example

Configure link detection support.

```
Switch(config-10ge1/0/1)#efm link-monitor supported
Switch(config-10ge1/0/1)#
```

9.4.6 efm link-monitor frame threshold window

Function

The **efm link-monitor frame threshold window** command configures a window and threshold for error frames.

The **no efm link-monitor frame** command disables error frame detection.

Format

- **efm link-monitor frame threshold** *threshold-value* **window** { *window-value* | **default** }
- **no efm link-monitor frame**

Parameter

Parameter	Description	Value
threshold-value	Specifies a threshold for error frames.	The value is an integer ranging from 1 to 65535.
window-value	Specifies a window size for error frames.	The value is an integer ranging from 10 to 600 and is a multiple of 100 milliseconds.
default	Specifies the default value.	10

Default Value

By default, error frame detection is enabled. The default window size is 1 second, and the default threshold is 1 error frame.

View

Ethernet bridge interface configuration view, router interface configuration view

Usage Guidelines

NA

Example

Set the window size to 10000 and threshold to 150 for error frame detection.

```
Switch(config-10ge1/0/1)#efm link-monitor frame threshold 10000 window 150
Switch(config-10ge1/0/1)#
```

9.4.7 efm link-monitor frame-period threshold window**Function**

The **efm link-monitor frame-period threshold window** command configures a window and threshold for the error frame detection interval.

The **no efm link-monitor frame-period** command disables the error frame detection interval.

Format

- **efm link-monitor frame-period threshold** *threshold-value* **window** { *window value-range* | **default** }
- **no efm link-monitor frame-period**

Parameter

Parameter	Description	Value
threshold-value	Specifies a threshold for the error	The value is an integer ranging from 1 to

Parameter	Description	Value
	frame detection interval.	65535.
window-value	Specifies a window size for the error frame detection interval.	The value is an integer ranging from 1 to 65535.
default	Specifies the default value.	10

Default Value

By default, the error frame detection interval is enabled. The default window size is 100000 data frames, and the default threshold is 1 error frame.

View

Ethernet bridge interface configuration view, router interface configuration view

Usage Guidelines

NA

Example

Set the window size to 10000 and threshold to 1500 for error frame detection.

```
Switch(config-10ge1/0/1)#efm link-monitor frame-period threshold 10000 window 1500
Switch(config-10ge1/0/1)#
```

9.4.8 efm link-monitor frame-seconds threshold window

Function

The **efm link-monitor frame-seconds threshold window** command configures a window and threshold for error frame seconds.

The **no efm link-monitor frame** command disables detection of error frame seconds.

Format

- **efm link-monitor frame-seconds threshold *threshold-value* window { *window-value* | default }**
- **no efm link-monitor frame-seconds**

Parameter

Parameter	Description	Value
threshold-value	Specifies a detection interval for error frame seconds.	The value is an integer ranging from 1 to 900.
window-value	Specifies a window size for detecting error frame seconds.	The value is an integer ranging from 100 to 9000 and is a multiple of 100 milliseconds.

Parameter	Description	Value
default	Specifies the default value.	The default value is 100.

Default Value

100 ms

View

Ethernet bridge interface configuration view, router interface configuration view

Usage Guidelines

NA

Example

Set the window size to 500 and threshold to 500 for detection of error frame seconds.

```
Switch(config-10ge1/0/1)#efm link-monitor frame-seconds threshold 500 window 500
Switch(config-10ge1/0/1)#
```

9.4.9 efm link-monitor high-threshold action**Function**

The **efm link-monitor high-threshold action** command configures the action to be taken upon error occurrence.

The **no efm link-monitor high-threshold action** command cancels the action to be taken upon error occurrence.

Format

- **efm link-monitor high-threshold action { disable-on-error | trap | all }**
- **no efm link-monitor high-threshold action { disable-on-error | trap | all }**

Parameter

NA

Default Value

By default, no action is taken upon error occurrence.

View

Ethernet bridge interface configuration view, router interface configuration view

Usage Guidelines

When four link faults or three critical link faults occur locally or when the switch receives a fault packet from the remote end, you can locally use the trap function of the network management system (NMS) to send an alert to the server or directly disable the interface. Alternatively, you can enable warning information debugging to view the trap information printed in a window.

Example

Configure the action of sending an alert to the server through the trap function of the NMS upon error occurrence.

```
Switch(config-10ge1/0/1)#efm link-monitor high-threshold action trap
Switch(config-10ge1/0/1)#
```

9.4.10 efm link-monitor recover-period

Function

The **efm link-monitor recover-period** command sets the linkage time of the EFM interface.

Format

efm link-monitor recover-period { *recover-time* | **default** }

Parameter

Parameter	Description	Value
recover-time	Specifies the linkage time of the EFM interface.	The value is an integer ranging from 30 to 86400, in seconds.
default	Specifies the default value.	The default value is 30 seconds.

Default Value

30 seconds

View

Ethernet bridge interface configuration view, router interface configuration view

Usage Guidelines

If the action taken upon error occurrence is configured as disabling the interface, by default, the EFM instance disables the interface for 30 seconds when a link fault is detected and then automatically enables the interface again. This allows other protocols running on the interface to detect any interface fault. Alternatively, you can configure the action of manually enabling the interface.

Example

Set the linkage time of the EFM interface to 200 seconds.

```
Switch(config-10ge1/0/1)#efm link-monitor recover-period 200
Switch(config-10ge1/0/1)#
```

9.4.11 efm link-monitor never recover

Function

The **efm link-monitor never recover** command cancels the linkage time of the EFM interface (that is, the interface is disabled permanently).

Format

efm link-monitor never recover

Parameter

NA

Default Value

NA

View

Ethernet bridge interface configuration view, router interface configuration view

Usage Guidelines

If the action taken upon error occurrence is configured as disabling the interface, by default, the EFM instance disables the interface for 30 seconds when a link fault is detected and then automatically enables the interface again. This allows other protocols running on the interface to detect any interface fault. Alternatively, you can configure the action of manually enabling the interface.

Example

Cancel the linkage time of the EFM interface.

```
Switch(config-10ge1/0/1)#efm link-monitor never recover
Switch(config-10ge1/0/1)#
```

9.4.12 efm critical-event

Function

The **efm critical-event** command configures whether an interface supports critical events.

Format

efm critical-event { **supported** | **unsupported** }

Parameter

Parameter	Description	Value
supported	Specifies that an interface supports critical events.	-
unsupported	Specifies that an interface does not support critical events.	-

Default Value

supported

View

Ethernet bridge interface configuration view, router interface configuration view

Usage Guidelines

NA

Example

Configure an interface to support critical events.

```
Switch(config-10ge1/0/1)#efm critical-event supported
Switch(config-10ge1/0/1)
```

9.4.13 efm max-rate**Function**

The **efm max-rate** command sets the maximum rate for sending EFM PDUs.

Format

efm max-rate { *rate* | **default** }

Parameter

Parameter	Description	Value
rate	Specifies the maximum rate for sending EFM PDUs.	The value is an integer ranging from 1 to 10.
default	Specifies the default value.	10

Default Value

The default maximum rate for sending EFM PDUs is 10.

View

Ethernet bridge interface configuration view, router interface configuration view

Usage Guidelines

Use this command to set the maximum sending rate to limit the EFM-occupied bandwidth, ensuring that only the specified number of EFM PDUs can be sent at most at an interval.

Example

Set the maximum rate for sending EFM PDUs to 6.

```
Switch(config-10ge1/0/1)#efm enable
Switch(config-10ge1/0/1)#efm max-rate 6
Switch(config-10ge1/0/1)#
```

9.4.14 efm min-rate

Function

The **efm min-rate** command sets the minimum interval for sending EFM PDUs.

Format

efm min-rate { *rate* | **default** }

Parameter

Parameter	Description	Value
rate	Specifies the minimum interval for sending EFM PDUs.	The value is an integer ranging from 1 to 10, in seconds.
default	Specifies the default value.	1 seconds

Default Value

The default minimum interval for sending EFM PDUs is 1 second.

View

Ethernet bridge interface configuration view, router interface configuration view

Usage Guidelines

The minimum sending interval is used to maintain the session between two EFM entities. At least one EFM PDU must be sent at the specified interval.

When testing the EFM discovery timeout duration, ensure that the minimum sending interval is smaller than the discovery timeout duration. When testing the loopback response timeout duration, ensure that the minimum sending interval is smaller than the loopback response timeout duration.

Example

Set the minimum EFM PDU sending interval to 6 seconds.

```
Switch(config-10ge1/0/1)#efm enable
Switch(config-10ge1/0/1)#efm min-rate 6
Switch(config-10ge1/0/1)#
```

9.4.15 efm mode**Function**

The **efm mode** command sets the EFM mode of an interface.

Format

efm mode { active | passive }

Parameter

Parameter	Description	Value
active	Sets the EFM mode to Active mode.	-
passive	Sets the EFM mode to Passive mode.	-

Default Value

The default EFM mode is Active.

View

Ethernet bridge interface configuration view, router interface configuration view

Usage Guidelines

You can set the EFM mode after discovery is completed to initiate discovery again. Discovery fails if the EFM mode is set to Passive on switches at both ends.

Example

Set the EFM mode to Passive on interface gigabitEthernet1/0/1.

```
Switch(config-10ge1/0/1)#efm enable
Switch(config-10ge1/0/1)#efm mode passive
Switch(config-10ge1/0/1)#
```

9.4.16 efm remote-loopback {supported|unsupported}**Function**

The **efm remote-loopback {supported|unsupported}** command configures whether an interface supports the remote loopback function.

Format

efm remote-loopback { supported | unsupported }

Parameter

Parameter	Description	Value
supported	Specifies that remote loopback is supported.	-
unsupported	Specifies that remote loopback is not supported.	-

Default Value

By default, remote loopback is supported.

View

Ethernet bridge interface configuration view, router interface configuration view

Usage Guidelines

A loopback interface allows you to ensure link quality and estimate whether links meet QoS requirements when installing Ethernet and detecting Ethernet faults. A loopback interface also helps testing of latency, jitter, and throughput.

In loopback mode, all received frames except EFM PDUs and Pause frames are sent by the source interface, which no longer runs L2 and L3 protocols. In loopback mode, EFM PDUs are still periodically exchanged to maintain the EFM session. After receiving the loopback command, the peer switch must notify the local switch of its being in loopback mode by responding to information EFM PDU set by a loopback state flag within a specified time. Otherwise, the sender determines that settings time out.

Only EFM entities in Active mode can set the peer end to be in the loopback state. If both the local and peer ends are in the Active state and one end has sent the remote loopback command but receives a remote loopback command from the peer end while waiting for a response from the peer end, the local end compares the MAC addresses of both ends. If the MAC address of the local end is smaller than that of the peer end, the local end does not process the remote loopback command from the peer end. If the MAC address of the local end is greater than that of the peer end, the local end enters loopback mode.

Example

```
# Configure interface gigabitEthernet1/0/1 not to support remote loopback.
```

```
Switch(config-10ge1/0/1)#efm enable
Switch(config-10ge1/0/1)#efm remote-loopback unsupported
Switch(config-10ge1/0/1)#
```

9.4.17 efm remote-loopback start

Function

The **efm remote-loopback start** command enables the remote loopback function.

Format

efm remote-loopback start

Parameter

NA

Default Value

By default, remote loopback is disabled.

View

Ethernet bridge interface configuration view, router interface configuration view

Usage Guidelines

To enable EFM loopback, ensure that the EFM entities at both ends support EFM remote loopback. Otherwise, configuration fails, with the error message "%Failed to get peer's loopback support status."

Only EFM entities in Active mode can send remote loopback commands. If active EFM entities are in the loopback state, remote loopback cannot be enabled or disabled on the local EFM entity even when the other active EFM entity sets the local EFM entity to remote loopback. You can only enable and disable remote loopback at the peer end.

Example

Enable remote loopback on interface gig ethernet1/0/1.

```
Switch(config-10ge1/0/1)#efm enable
Switch(config-10ge1/0/1)#efm remote-loopback start
Switch(config-10ge1/0/1)#
```

9.4.18 efm remote-loopback start holdtime

Function

The **efm remote-loopback start holdtime** command sets the remote loopback holdtime.

Format

efm remote-loopback start holdtime { *holdtime-value* | **default** }

Parameter

Parameter	Description	Value
holdtime-value	Specifies a remote loopback holdtime.	The value is an integer ranging from 0 to 1000, in minutes.
default	Specifies the default value.	20 minutes

Default Value

The default remote loopback holdtime is 20 minutes.

View

Ethernet bridge interface configuration view, router interface configuration view

Usage Guidelines

Ensure that the EFM entities at both ends support EFM remote loopback. Otherwise, configuration fails, with the error message "%Failed to get peer's loopback support status."

EFM remote loopback is automatically disabled upon timeout to avoid the case that users forget to disable EFM remote loopback, causing links fail to forward service data properly for a long time. Use this command to set the holdtime after which remote loopback is automatically disabled. To always keep a link in the remote loopback state, set the holdtime to 0, in which case you need to manually disable remote loopback.

Example

Set the remote loopback holdtime to 50 minutes.

```
Switch(config-10ge1/0/1)#efm enable
Switch(config-10ge1/0/1)#efm remote-loopback start holdtime 50
Switch(config-10ge1/0/1)#
```

9.4.19 efm remote-loopback stop

Function

The **efm remote-loopback stop** command disables the remote loopback function.

Format

efm remote-loopback stop

Parameter

NA

Default Value

By default, remote loopback is disabled.

View

Ethernet bridge interface configuration view, router interface configuration view

Usage Guidelines

Ensure that the EFM entities at both ends support EFM remote loopback. Otherwise, configuration fails, with the error message "%Failed to get peer's loopback support status."

Example

Disable remote loopback on interface gigabitEthernet1/0/1.

```
Switch(config-10ge1/0/1)#efm enable
Switch(config-10ge1/0/1)#efm remote-loopback stop
Switch(config-10ge1/0/1)#
```

9.4.20 efm remote-loopback timeout**Function**

The **efm remote-loopback timeout** command sets the remote loopback response timeout duration.

Format

efm remote-loopback timeout { *timeout-value* | **default** }

Parameter

Parameter	Description	Value
timeout-value	Specifies a remote loopback response timeout duration.	The value is an integer ranging from 1 to 10, Specifies the number of seconds.
default	Specifies the default value.	10 seconds

Default Value

By default, the response timeout duration of the remote loop is 10s.

View

Ethernet bridge interface configuration view, router interface configuration view

Usage Guidelines

EFM remote loopback is automatically disabled upon timeout to avoid the case that users forget to disable EFM remote loopback, causing links fail to forward service data properly for a long time. Use this command to set the holdtime after which remote loopback is automatically disabled. To always keep a link in the remote loopback state, set the holdtime to 0, in which case you need to manually disable remote loopback.

Example

Set the remote loopback response timeout duration to 10 seconds.

```
Switch(config-10ge1/0/1)#efm enable
Switch(config-10ge1/0/1)#efm remote-loopback timeout 10
Switch(config-10ge1/0/1)#
```

9.4.21 efm timeout

Function

The **efm timeout** command sets the EFM discovery timeout duration.

Format

efm timeout { *timeout-value* | **default** }

Parameter

Parameter	Description	Value
timeout-value	Specifies EFM discovery timeout duration.	The value is an integer ranging from 2 to 30, Specifies the number of seconds.
default	Specifies the default value.	5 seconds

Default Value

By default, the response timeout duration of the remote loop is 5s.

View

Ethernet bridge interface configuration view, router interface configuration view

Usage Guidelines

If the local EFM entity does not receive an EFM PDU from the peer end within the discovery timeout duration, it determines that discovery connection fails and restarts discovery.

Example

Set the EFM discovery timeout duration to 10 seconds.

```
Switch(config-10ge1/0/1)#efm enable
```

```
Switch(config-10ge1/0/1)#efm timeout 10
Switch(config-10ge1/0/1)#
```

9.4.22 show efm fault-logs

Function

The **show efm fault-logs** command displays the error logs of the local EFM entity.

Format

- **show efm fault-logs all**
- **show efm fault-logs interface { ethernet | xgigaethernet | 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet } interface-number**

Parameter

Parameter	Description	Value
interface-number	Specifies an Ethernet interface number.	The value is an integer in the range of <1-1> / <0-1> / <1-48> (For reference only. The specific value range depends on the slot number and card type).

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

Display the error logs of the local EFM entity.

```
Switch##show efm fault-logs all

interface xge-1/0/1 fault-logs information :
-----Remote Faults Log-----
err-type   time           window    threshold    errors    totalErr    totalEvt
critical   2019-10-10 19:38:06    ---      ---          ---        ---        ---
critical   2019-10-10 19:38:06    ---      ---          ---        ---        ---
critical   2019-10-10 19:38:07    ---      ---          ---        ---        ---
critical   2019-10-10 19:38:07    ---      ---          ---        ---        ---
```



```

Switch>show efm fault-logs interface xgigeaetherne 1/01
-----Remote Faults Log-----
err-type   time        window    threshold  errors    totalErr  totalEvt
critical   2020-10-10 19:38:06 ---        ---        ---        ---        ---
critical   2020-10-10 19:38:06 ---        ---        ---        ---        ---
critical   2020-10-10 19:38:07 ---        ---        ---        ---        ---
critical   2020-10-10 19:38:07 ---        ---        ---        ---        ---
critical   2020-10-10 19:38:07 ---        ---        ---        ---        ---
critical   2020-10-10 19:38:08 ---        ---        ---        ---        ---
critical   2020-10-10 19:38:08 ---        ---        ---        ---        ---
Switch#

```

9.4.23 show efm session

Function

The **show efm session** command displays information about the EFM OAM session between a specified interface and the peer end.

Format

- **show efm session all**
- **show efm session interface { ethernet | xgigaetherne | 10gigaetherne | 25gigaetherne | 40gigaetherne | 100gigaetherne } interface-number**

Parameter

Parameter	Description	Value
interface-number	Specifies an Ethernet interface number.	The value is an integer in the range of <1-1>/<0-1>/<1-48> (For reference only. The specific value range depends on the slot number and card type).

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

Display information about the EFM OAM session between every interface and the peer end.

```
Switch>show efm session all

interface xge-1/0/1 discovery information :
-----Local Client-----
Port status : operational
Mode : active
Pdu size : 1518
Unidirection: unsupported
Remote loopback: supported
Link monitor: supported
MIB variable: unsupported
Loopback status : no loopback
-----Remote Client-----
Mac Address : 00:04:67:98:50:26
Oui : 000467
Peer Mode : passive
Peer pdu size : 1518
Unidirection: unsupported
Remote loopback: supported
Link monitor: supported
MIB variable: unsupported
Switch#
Switch>show efm session interface xgigaethernet 1/0/1
-----Local Client-----
Port status : operational
Mode : active
Pdu size : 1518
Unidirection: unsupported
Remote loopback: supported
Link monitor: supported
MIB variable: unsupported
Loopback status : no loopback
-----Remote Client-----
Mac Address : 00:04:67:98:50:26
Oui : 000467
Peer Mode : passive
Peer pdu size : 1518
Unidirection: unsupported
Remote loopback: supported
Link monitor: supported
MIB variable: unsupported
```

```
Switch#
```

9.4.24 show efm statistic

Function

The **show efm statistic** command displays the numbers of all types of EFM PDUs sent and received by the local EFM entity and the total number of errors occurred at the local and remote ends.

Format

- **show efm statistic all**
- **show efm statistic interface { ethernet | xgigaethernet | 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet } interface-number**

Parameter

Parameter	Description	Value
interface-number	Specifies an Ethernet interface number.	The value is an integer in the range of <1-1>/<0-1>/<1-48> (For reference only. The specific value range depends on the slot number and card type).

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

Display the numbers of all types of EFM PDUs sent and received by the local EFM entity and the total number of errors occurred at the local and remote ends.

```
Switch>show efm statistic all

interface xge-1/0/1 Statistic information :
Pdu Count Statistic:
  Information OAMPDU Tx : 6755
  Information OAMPDU Rx : 6754
  Unique Event Notification OAMPDU Tx : 0
  Unique Event Notification OAMPDU Rx : 0
```

```

Duplicate Event Notification OAMPDU Tx : 0
Duplicate Event Notification OAMPDU Rx : 0
Loopback Control OAMPDU Tx : 0
Loopback Control OAMPDU Rx : 0
Org Specific OAMPDU Tx : 0
Org Specific OAMPDU Rx : 0
Unsupported OAMPDU Tx : 0
Unsupported OAMPDU Rx : 0
Frames Lost Due To Oam : 0

```

Local Faults Record:

```

0 Link Fault Record
0 Dying Gasp Record
0 Critical Event Record
0 Symbol Error Record
0 Frame Error Record
0 Frame Period Error Record
0 Frame Second Error Record

```

Remote Faults Record:

```

0 Link Fault Record
0 Dying Gasp Record
0 Critical Event Record
0 Symbol Error Record
0 Frame Error Record
0 Frame Period Error Record
0 Frame Second Error Record

```

Switch#

9.4.25 show efm status

Function

The **show efm status** command displays the configuration of the local interface.

Format

- **show efm status all**
- **show efm status interface { ethernet | xgigaethernet | 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet } interface-number**

Parameter

Parameter	Description	Value

Parameter	Description	Value
interface-number	Specifies an Ethernet interface number.	The value is an integer in the range of <1-1>/<0-1>/<1-48> (For reference only. The specific value range depends on the slot number and card type).

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

Display the configuration of the local interface.

```
Switch>show efm status all

interface xge-1/0/1 status information :
-----General-----
Mode : active
Pdu max rate : 10 packets per second
Pdu min rate : 1 packet per 1 second
Link lost timeout: 5 seconds
Loopback timeOut : 1 seconds
remote-loopback holdtime : 20min
recover period : 3
-----Link Monitor-----
Link monitor: supported
Symbol Period Error : On
    Window : 1 million symbols
    Threshold : 1 error symbol(s)
Frame Period Error : On
    Window : 10 x 10000 frames
    Threshold : 1 error frame(s)
Frame Error : On
    Window : 100 x 100 millisecond
    Threshold : 1 error frame(s)
Frame Seconds Error : On
    Window : 1000 x 100 millisecond
    Threshold : 1 error second(s)
```

```
critical event : supported
Switch#
```

9.4.26 show efm summary

Function

The **show efm summary** command displays the summary of all EFM-enabled interfaces of the local switch.

Format

show efm summary

Parameter

NA

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

Display the summary of all EFM-enabled interfaces and the summary of the remote end.

```
Switch>show efm summary

              Local                      Remote
Interface  Mode   LB-Status   MAC-Address   Vendor      Mode
-----
xge-1/0/1  Active NO_LOOPBACK 00.04.67.98.50.26  000467      Active
Switch#
```

9.5 CFM Configuration Commands

9.5.1 ccm {enable|disable}

Function

The **ccm {enable|disable}** command enables or disables CC detection for all MEPs in an MA.

Format

ccm { enable | disable }

Parameter

Parameter	Description	Value
enable	Enables CC detection for all MEPs in an MA.	-
disable	Disables CC detection for all MEPs in an MA.	-

Default Value

By default, this function is disabled.

View

MA configuration view

Usage Guidelines

NA

Example

Enable CC check for all MEPs of an MA.

```
Switch(config)#cfm
Switch(config-cfm)#md name md1 level 1
Switch(config-md-md1)#ma name ma1 vlan 1
Switch(config-md-md1-ma-ma1)#ccm enable
Switch(config-md-md1-ma-ma1)#
```

9.5.2 ccm-interval

Function

The **ccm-interval** command sets the CC packet sending interval for MEPs in the current MA.

Format

ccm-interval { 300Hz | 10ms | 100ms | 10s | 1min | 10min | default }

Parameter

NA

Default Value

The default CC packet sending interval is 1 second.

View

MA configuration view

Usage Guidelines

NA

Example

Enter the MA1 configuration view and set the CC packet sending interval to 100 milliseconds.

```
Switch(config)#cfm
Switch(config-cfm)#md name md1 level 1
Switch(config-md-md1)#ma name ma1 vlan 1
Switch(config-md-md1-ma-ma1)#ccm-interval 100ms
Switch(config-md-md1-ma-ma1)#
```

9.5.3 ccm loss-threshold**Function**

The **ccm loss-threshold** command sets the CC loss threshold for MEPs in the current MA.

Format

ccm loss-threshold { *threshold-value* | **default** }

Parameter

Parameter	Description	Value
threshold-value	Specifies a CC loss threshold.	The value is an integer ranging from 2 to 255, in the unit of CC packet sending intervals.
default	Uses the default CC loss threshold.	The default CC loss threshold is 3.5 times the CC packet sending interval.

Default Value

The default CC loss threshold is 3.5 times the CC packet sending interval.

View

MA configuration view

Usage Guidelines

Loss threshold x CC packet sending interval for local MEPs = CC packet continuous loss time. This command is invalid for switches that process received and sent CC packets through hardware, such as the 48G line card of Switch.

Example

Set the CC loss threshold to be 2 times the CC packet sending interval.


```
Switch(config)#cfm
Switch(config-cfm)#md name md1 level 1
Switch(config-md-md1)#ma name ma1 vlan 1
Switch(config-md-md1-ma-ma1)#ccm loss-threshold 2
Switch(config-md-md1-ma-ma1)#
```

9.5.4 cfm

Function

The **cfm** command switches to the CFM configuration view from the global configuration view.

Format

cfm

Parameter

NA

Default Value

NA

View

Global configuration view

Usage Guidelines

Before configuring CFM connectivity fault management, run this command to enter the CFM connectivity fault management configuration node.

Example

Switch to the CFM configuration view from the global configuration view.

```
Switch(config)#cfm
Switch(config-cfm)#
```

9.5.5 cfm mep vlan level mepid

Function

The **cfm mep vlan level mepid** command creates an MEP.

The **no cfm mep** command deletes an existing MEP.

Format

- **cfm mep vlan** *vlan-id* **level** *level* **mepid** *mep-id* { **inward** | **outward** }

- **cfm mep vlan** *vlan-id* **level** *level* **mepid** *mep-id*
- **no cfm mep vlan** *vlan-id* **level** *level* **mepid** *mep-id*

Parameter

Parameter	Description	Value
vlan-id	Specifies a VLAN ID.	The value is an integer ranging from 1 to 4094.
level	Specifies a level.	The value is an integer ranging from 0 to 7.
mep-id	Specifies a local MEP ID.	The value is an integer ranging from 1 to 8191.
inward	Specifies the up direction.	-
outward	Specifies the down direction.	-

Default Value

NA

View

Ethernet bridge interface configuration view, Ethernet routing interface configuration view

Usage Guidelines

The requirements for creating MEPs in the same MA of the same bridge are as follows:

- MEPs of the inward interface type and MEPs of the outward interface type cannot coexist.
- MEPs and RMEPs in the same MA cannot coexist on the same switch.
- MEPs and MIPs in the same MA cannot coexist on the same interface.
- An interface allows up to one MEP in the same MA.
- If Y.1731 MEPs or MIPs are configured on the same interface, MEPs of CFM cannot be configured.

Create an MD and MA before running this command. Otherwise, the system prompts "%Failed, there is no this ma".

When using this command, ensure that the **vlan** and **level** parameters are correctly mapped to the MA that corresponds to MEP.

If you do not specify a direction when configuring an MEP, the direction is set to **outward** by default. If you set the direction to **inward**, you need to configure an MIP of the same MA on another interface so that the MEP can work properly.

Example

Create an MEP of ID 1 in MA of VLAN 5 and Level 1.

```
Switch(config)#cfm
Switch(config-cfm)#md name md1 level 1
Switch(config-md-md1)#ma name ma1 vlan 5
Switch(config-md-md1-ma-ma1)#quit
Switch(config-md-md1)#quit
Switch(config-cfm)#quit
Switch(config)#interface 10gigaethernet 1/0/1
Switch(config-10ge1/0/1)#cfm mep vlan 5 level 1 mepid 1
Switch(config-10ge1/0/1)#
```

9.5.6 cfm mep vlan level mepid ccm

Function

The **cfm mep vlan level mepid ccm** command enables or disables CC detection for an MEP.

Format

- **cfm mep vlan *vlan-id* level *level* mepid *mep-id* ccm priority *priority* { enable | disable }**
- **cfm mep vlan *vlan-id* level *level* mepid *mep-id* ccm { enable | disable }**

Parameter

Parameter	Description	Value
vlan-id	Specifies a VLAN ID.	The value is an integer ranging from 1 to 4094.
level	Specifies a level.	The value is an integer ranging from 0 to 7.
mep-id	Specifies a local MEP ID.	The value is an integer ranging from 1 to 8191.
priority	Specifies a priority.	The value ranges from 0 to 7.

Default Value

NA

View

Ethernet bridge interface configuration view, Ethernet routing interface configuration view

Usage Guidelines

If do not specify the CCM priority when using this command, it is set to 6 by default.

Example

Enable CC detection for MEP of ID 2.

```
Switch(config-10ge1/0/1)#cfm mep vlan 1 level 5 mepid 2
Switch(config-10ge1/0/1)#cfm mep vlan 1 level 5 mepid 2 ccm enable
Switch(config-10ge1/0/1)#
```

9.5.7 cfm mep vlan level mepid mac

Function

The **cfm mep vlan level mepid mac** command sets the MAC address of an MEP.

Format

cfm mep vlan *vlan-id* **level** *level* **mepid** *mep-id* **mac** *mac-address*

Parameter

Parameter	Description	Value
vlan-id	Specifies a VLAN ID.	The value is an integer ranging from 1 to 4094.
level	Specifies a level.	The value is an integer ranging from 0 to 7.
mep-id	Specifies a local MEP ID.	The value is an integer ranging from 1 to 8191.
mac-address	Specifies the MAC address of an MEP.	The value is in the AA:BB:CC:DD:EE:FF format, where A to F are hexadecimal digits.

Default Value

The default MAC address of an MEP is the hardware address of the interface where the MEP is located.

View

Ethernet bridge interface configuration view, Ethernet routing interface configuration view

Usage Guidelines

Normally, this command is not required for setting the MAC address of an MEP. The configured MAC address is only used as the source MAC address in the CFM packets sent by the MEP. Received CCM packets are not matched with the MAC address, whereas received LBM and LTM packets are matched with the MAC address.

Create an MEP before running this command. Otherwise, the system prompts "%Failed, there is no this mep".

Example

Set the MAC address of an MEP to 00:00:00:00:00:01.

```
Switch(config-10ge1/0/1)#cfm mep vlan 1 level 5 mepid 2 mac 00:00:00:00:00:01
Switch(config-10ge1/0/1)#
```

9.5.8 cfm mep vlan level mepid reset counter

Function

The **cfm mep vlan level mepid reset counter** command resets the CFM packet counters of an MEP.

Format

cfm mep vlan *vlan-id* level *level* mepid *mep-id* reset counter

Parameter

Parameter	Description	Value
vlan-id	Specifies a VLAN ID.	The value is an integer ranging from 1 to 4094.
level	Specifies a level.	The value is an integer ranging from 0 to 7.
mep-id	Specifies a local MEP ID.	The value is an integer ranging from 1 to 8191.

Default Value

NA

View

Ethernet bridge interface configuration view, Ethernet routing interface configuration view

Usage Guidelines

Create an MEP before running this command. Otherwise, the system prompts "%Failed, there is no this mep".

Example

Reset the CFM packet counters of an MEP.

```
Switch(config-10ge1/0/1)#cfm mep vlan 1 level 5 mepid 2 reset counter
Switch(config-10ge1/0/1)#
```

9.5.9 cfm mip vlan level

Function

The **cfm mip vlan level** command creates an MIP.

The **no cfm mip** command deletes an MIP.

Format

- **cfm mip vlan *vlan-id* level *level***
- **no cfm mip vlan *vlan-id* level *level***

Parameter

Parameter	Description	Value
vlan-id	Specifies a VLAN ID.	The value is an integer ranging from 1 to 4094.

Parameter	Description	Value
level	Specifies a level.	The value is an integer ranging from 0 to 7.

Default Value

NA

View

Ethernet bridge interface configuration view, Ethernet routing interface configuration view

Usage Guidelines

The requirements for creating MIPs in the same MA of the same switch are as follows:

- MIPs and MEPs in the same MA cannot coexist on the same interface.
- An interface allows up to one MIP in the same MA.
- If Y.1731 MIPs or MEPs are configured on the same interface, MIPs of CFM cannot be configured.

When using this command, ensure that the **vlan** and **level** parameters are correctly mapped to the MA that corresponds to MEP.

Example

Create an MIP.

```
Switch(config-10ge1/0/1)#cfm mip vlan 1 level 5
Switch(config-10ge1/0/1)#
```

9.5.10 cfm mip vlan level mac

Function

The **cfm mip vlan level mac** command sets the MAC address of an MIP.

Format

cfm mip vlan *vlan-id* **level** *level* **mac** *mac-address*

Parameter

Parameter	Description	Value
vlan-id	Specifies a VLAN ID.	The value is an integer ranging from 1 to 4094.
level	Specifies a level.	The value is an integer ranging from 0 to 7.
mac-address	Specifies the MAC address of an MIP.	The value is in the AA:BB:CC:DD:EE:FF format, where A to F are hexadecimal digits.

Default Value

The default MAC address of an MIP is the hardware address of the interface where the MIP is located.

View

Ethernet bridge interface configuration view, Ethernet routing interface configuration view

Usage Guidelines

Normally, this command is not required for setting the MAC address of an MIP. The configured MAC address is only used as the source MAC address in the CFM packets sent by the MIP. Received CCM packets are not matched with the MAC address, whereas received LBM and LTM packets are matched with the MAC address.

Example

Set the MAC address of an MIP.

```
Switch(config-10ge1/0/1)#cfm mip vlan 1 level 5 mac 00:00:00:00:00:01
Switch(config-10ge1/0/1)#
```

9.5.11 cfm ping**Function**

The **cfm ping mac** command configures MAC address ping for locating a CFM connectivity fault.

The **cfm ping remote-mep** command configures remote MEP ping for locating a CFM connectivity fault.

Format

- **cfm ping mac** *mac-address* **mep vlan** *vlan-id* **level** *level* **mepid** *mep-id* **-c** *packet-count* **-s** *packet-size* **-t** *packet-timeout*
- **cfm ping mac** *mac-address* **mep vlan** *vlan-id* **level** *level* **mepid** *mep-id* **priority** *priority-value* **-c** *packet-count* **-s** *packet-size* **-t** *packet-timeout*
- **cfm ping mac** *mac-address* **mep vlan** *vlan-id* **level** *level* **mepid** *mep-id*
- **cfm ping remote-mep** *remote-mep-id* **mep vlan** *vlan-id* **level** *level* **mepid** *mep-id* **-c** *packet-count* **-s** *packet-size* **-t** *packet-timeout*
- **cfm ping remote-mep** *remote-mep-id* **mep vlan** *vlan-id* **level** *level* **mepid** *mep-id* **priority** *priority* **-c** *packet-count* **-s** *packet-size* **-t** *packet-timeout*

- **cfm ping remote-mep** *remote-mep-id* **mep vlan** *vlan-id* **level** *level* **mepid** *mep-id*
- **cfm ping all remote-mep vlan** *vlan-id* **level** *level* **mepid** *mep-id* **-s** *packet-size* **-t** *packet-timeout*
- **cfm ping all remote-mep vlan** *vlan-id* **level** *level* **mepid** *mep-id* **priority** *priority* **-s** *packet-size* **-t** *packet-timeout*
- **cfm ping all remote-mep vlan** *vlan-id* **level** *level* **mepid** *mep-id*

Parameter

Parameter	Description	Value
vlan-id	Specifies a VLAN ID.	The value is an integer ranging from 1 to 4094.
level	Specifies a level.	The value is an integer ranging from 0 to 7.
mac-address	Specifies the MAC address of the remote MEP or MIP.	The value is in AA:BB:CC:DD:EE:FF format, in which A to F are hexadecimal digits.
mep-id	Specifies the MEP that initiates ping in the local bridge.	The value is an integer ranging from 1 to 8191.
remote-mep-id	Specifies the MEP ID of a remote network bridge.	The value is an integer ranging from 1 to 8191.
priority-value	Specifies a priority.	The value is an integer ranging from 0 to 7.
packet-count	Specifies the times of ping.	The value is an integer ranging from 1 to 1024.
packet-size	Specifies the size of a sent ping packet, including the size of the L2 packet header.	The value is an integer ranging from 64 to 1518. The default value is 64.
packet-timeout	Specifies a wait timeout duration of response packets.	The value is an integer ranging from 1 to 60, in seconds. The default value is 5 seconds.

Default Value

NA

View

Privileged user view

Usage Guidelines

Use this command to test the connectivity between local and remote MEPs or MIPs in the current MA.

To stop sending LBM packets, press **Ctrl+C**. If a local MEP in the up direction is associated with two or more MIPs, ensure that the network to which the MIPs are connected contains only one L2 data service channel (this is typically ensured by the STP protocol or an Ethernet ring protocol). Otherwise, the CFM fault locating result is unpredictable.

When using this command, ensure that the **vlan** and **level** parameters are correctly mapped to the MA that corresponds to MEP. If remote MEP ping is used, also ensure that the remote MEP is properly connected.

Example

Configure MAC address ping for locating any CFM connectivity fault.

```
Switch#cfm ping mac 00:00:00:00:00:01 mep vlan 1 level 1 mepid 1
Pinging 00-00-00-00-00-01 with 64 bytes of data:
request time out

Ping statistics for 00-00-00-00-00-01:
    Packets: Sent = 1, Received = 0, Lost = 1 <100.00% loss>
Approximate round trip times in milliseconds:
    Minimum = 5000ms, Maximum = 5000ms, Average = 5000.00ms

Switch#
```

9.5.12 cfm reset counter

Function

The **cfm reset counter** command resets the CFM packet counters of an interface.

Format

cfm reset counter

Parameter

NA

Default Value

NA

View

Ethernet bridge interface configuration view, Ethernet routing interface configuration view

Usage Guidelines

NA

Example

Reset CFM packet counters on interface 10gigaethernet 1/0/1.

```
Switch(config-10ge1/0/1)#cfm reset counter
Switch(config-10ge1/0/1)#
```

9.5.13 cfm trace

Function

The **cfm trace mac** command configures MAC address tracing for locating any CFM connectivity fault.

The **cfm trace remote-mep** command configures remote MEP tracing for locating any CFM connectivity fault.

Format

- **cfm trace mac** *mac-address* **mep** **vlan** *vlan-id* **level** *level* **mepid** *local-mep-id*
- **cfm trace mac** *mac-address* **mep** **vlan** *vlan-id* **level** *level* **mepid** *local-mep-id* **priority** *priority*
- **cfm trace mac** *mac-address* **mep** **vlan** *vlan-id* **level** *level* **mepid** *local-mep-id* **-t** *packet-timeout*
- **cfm trace mac** *mac-address* **mep** **vlan** *vlan-id* **level** *level* **mepid** *local-mep-id* **priority** *priority* **-t** *packet-timeout* { **fdb-only** | **ccdb** }
- **cfm trace mac** *mac-address* **mep** **vlan** *vlan-id* **level** *level* **mepid** *local-mep-id* { **fdb-only** | **ccdb** }
- **cfm trace mac** *mac-address* **mep** **vlan** *vlan-id* **level** *level* **mepid** *local-mep-id* **priority** *priority* { **fdb-only** | **ccdb** }
- **cfm trace mac** *mac-address* **mep** **vlan** *vlan-id* **level** *level* **mepid** *local-mep-id* **priority** *priority* **-t** *packet-timeout*
- **cfm trace mac** *mac-address* **mep** **vlan** *vlan-id* **level** *level* **mepid** *local-mep-id* **-t** *packet-timeout* { **fdb-only** | **ccdb** }
- **cfm trace mac** *mac-address* **mep** **vlan** *vlan-id* **level** *level* **mepid** *local-mep-id* **ttl** *ttl-value*
- **cfm trace mac** *mac-address* **mep** **vlan** *vlan-id* **level** *level* **mepid** *local-mep-id* **priority** *priority* **ttl** *ttl-value*
- **cfm trace mac** *mac-address* **mep** **vlan** *vlan-id* **level** *level* **mepid** *local-mep-id* **priority** *priority* **ttl** *ttl-value* { **fdb-only** | **ccdb** }
- **cfm trace mac** *mac-address* **mep** **vlan** *vlan-id* **level** *level* **mepid** *local-mep-id* **ttl** *ttl-value* { **fdb-only** | **ccdb** }

- **cfm trace remote-mep** *remote-mep-id* **mep vlan** *vlan-id* **level** *level* **mepid** *local-mep-id*
- **cfm trace remote-mep** *remote-mep-id* **mep vlan** *vlan-id* **level** *level* **mepid** *local-mep-id* **priority** *priority*
- **cfm trace remote-mep** *remote-mep-id* **mep vlan** *vlan-id* **level** *level* **mepid** *local-mep-id* **priority** *priority* **-t** *packet-timeout*
- **cfm trace remote-mep** *remote-mep-id* **mep vlan** *vlan-id* **level** *level* **mepid** *local-mep-id* **priority** *priority* **-t** *packet-timeout* { **fdb-only** | **ccdb** }
- **cfm trace remote-mep** *remote-mep-id* **mep vlan** *vlan-id* **level** *level* **mepid** *local-mep-id* { **fdb-only** | **ccdb** }
- **cfm trace remote-mep** *remote-mep-id* **mep vlan** *vlan-id* **level** *level* **mepid** *local-mep-id* **priority** *priority* { **fdb-only** | **ccdb** }
- **cfm trace remote-mep** *remote-mep-id* **mep vlan** *vlan-id* **level** *level* **mepid** *local-mep-id* **-t** *packet-timeout*
- **cfm trace remote-mep** *remote-mep-id* **mep vlan** *vlan-id* **level** *level* **mepid** *local-mep-id* **-t** *packet-timeout* { **fdb-only** | **ccdb** }
- **cfm trace remote-mep** *remote-mep-id* **mep vlan** *vlan-id* **level** *level* **mepid** *local-mep-id* **ttl** *ttl-value*
- **cfm trace remote-mep** *remote-mep-id* **mep vlan** *vlan-id* **level** *level* **mepid** *local-mep-id* **priority** *priority* **ttl** *ttl-value*
- **cfm trace remote-mep** *remote-mep-id* **mep vlan** *vlan-id* **level** *level* **mepid** *local-mep-id* **priority** *priority* **ttl** *ttl-value* { **fdb-only** | **ccdb** }
- **cfm trace remote-mep** *remote-mep-id* **mep vlan** *vlan-id* **level** *level* **mepid** *local-mep-id* **ttl** *ttl-value* { **fdb-only** | **ccdb** }

Parameter

Parameter	Description	Value
mac-address	Specifies the MAC address of the remote MEP or MIP.	The value is in AA:BB:CC:DD:EE:FF format, where A to F are hexadecimal digits.
vlan-id	Specifies a VLAN ID.	The value is an integer ranging from 1 to 4094.
level	Specifies a level.	The value is an integer ranging from 0 to 7.
remote-mep-id	Specifies the MEP ID of a remote network bridge.	The value is an integer ranging from 1 to 8191.
local-mep-id	Specifies the MEP ID of the Trace	The value is an integer ranging from 1 to

Parameter	Description	Value
	action initiated by the local network bridge.	8191.
priority	Specifies a priority.	The value is an integer ranging from 0 to 7.
packet-timeout	Specifies the wait timeout duration of response packets.	The value is an integer ranging from 1 to 60, in seconds. The default value is 5 seconds.
ttl-value	Specifies the maximum number of hops for Trace.	The value is an integer ranging from 1 to 255. The default value is 64.
fdb-only	Specifies that only the MAC forwarding table is used for forwarding LTM packets.	-
ccdb	Specifies the use of MIP CCDB for forwarding LTM packets when they cannot be forwarded by using the forwarding table. This is the default option for tracing initiation.	-

Default Value

NA

View

Privileged user view

Usage Guidelines

Use this command to configure CFM fault locating to perform in the privileged user view of the switch. Tracing results are displayed immediately if they are correct. If tracing results are incorrect, reference results may be displayed after the set timeout duration. If you want to stop tracing, press **Ctrl+C**. If a local MEP in the up direction is associated with two or more MIPs, ensure that the network to which the MIPs are connected contains only one L2 data service channel (this is typically ensured by the STP protocol or an Ethernet ring protocol). Otherwise, the CFM fault locating result is unpredictable.

Example

Configure remote MEP tracing for locating any CFM connectivity fault.

```
Switch#cfm trace remote-mep 2 mep vlan 1 level 5 mepid 1
Info: This operation will take some time..
Tracing the route to remote mep 2 over a maximum of 64 hops:
-----
Hops Host          Mac              Ingr             IngrAct   RelayAct
```

Forwarded	Engr	EngrAct	IsMep	
1	00:04:67:00:1a:9a	10ge-1/0/1/48	IngOk	RlyFDB
Forwarded	10ge-1/0/2	EgrOk	NO	
2	00:04:67:00:1a:99	10ge-1/0/3	IngOk	RlyHit
Not Forwarded		EgrNoTlv	YES	
Switch#				

9.5.14 cross-check {enable|disable}

Function

The **cross-check {enable|disable}** command enables or disables static RMEP check.

Format

cross-check { enable | disable }

Parameter

Parameter	Description	Value
enable	Enables static RMEP check.	-
disable	Disables static RMEP check.	-

Default Value

By default, static RMEP check is disabled.



Note:

For the switch that uses hardware for sending and receiving CC packets, static RMEP check is enabled by default after an RMEP is created.

View

MA configuration view

Usage Guidelines

Static RMEP check is similar to the whitelist feature. After static RMEP check is enabled, only locally configured RMEPs can establish CC links. The CC links already established by dynamic RMEPs are automatically set to the Down state to improve CC link security.

Example

```
# Enable static RMEP check.
```

```
Switch(config-md-md1-ma-ma1)#cross-check enable
Switch(config-md-md1-ma-ma1)#
```

9.5.15 cross-check start-delay

Function

The **cross-check start-delay** command sets the RMEP start delay.

Format

cross-check start-delay { *delay-value* | **default** }

Parameter

Parameter	Description	Value
delay-value	Specifies an RMEP start delay.	The value is an integer ranging from 1 to 65535, in seconds.
default	Specifies the default value.	0s

Default Value

The default RMEP start delay is 0 seconds, indicating that an RMEP is started immediately after being configured.

View

MA configuration view

Usage Guidelines

For the switch configured with the RMEP start delay, after the function of receiving CCM packets from the RMEP is enabled at the local end, the local switch receives CCM packets after the RMEP start delay has elapsed. That is, the RMEP start delay is the time reserved for manually performing remote MEP configuration.

After the set RMEP start delay has elapsed, if the MEP of the local device does not receive any CCM packet within the CCM packet sending interval (which is several times the CC continuous loss threshold), the inter-MEP connection is faulty and an RMEP connectivity alarm is displayed on the local switch.

Example

Set the RMEP start delay to 10 seconds.

```
Switch(config-md-md1-ma-ma1)#cross-check start-delay 10
Switch(config-md-md1-ma-ma1)#
```

9.5.16 debug cfm

Function

The **debug cfm module** command enables debugging of the CFM connectivity fault management module.

The **no debug cfm module** command disables debugging of the CFM connectivity fault management module.

The **debug cfm packet** command enables CFM packet transmission debugging.

The **no debug cfm packet** command disables CFM packet transmission debugging.

Format

- **debug cfm module** { nm | main | trap | os-io | sync | pkt-out | pkt-in | hw-notify | hw-setting | ccm-out | ccm-in | lbr-out | lbr-in | lbr-out | lbr-in | ltr-in | ltr-out | ltm-in | ltm-out | ais-out | ais-in | lck-out | lck-in | all }
- **debug cfm packet** { ccm-out | ccm-in | lbr-out | lbr-in | lbr-out | lbr-in | ltr-in | ltr-out | ltm-in | ltm-out | ais-out | ais-in | lock-out | lock-in | all }
- **debug cfm packet** { ccm-out | ccm-in | lbr-out | lbr-in | lbr-out | lbr-in | ltr-in | ltr-out | ltm-in | ltm-out | ais-out | ais-in | lock-out | lock-in | all } interface { ethernet | xgigaethernet | 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet } *interface-number*
- **debug cfm packet** { ccm-out | ccm-in | lbr-out | lbr-in | lbr-out | lbr-in | ltr-in | ltr-out | ltm-in | ltm-out | ais-out | ais-in | lock-out | lock-in | all } interface eth-trunk *trunk-number*
- **no debug cfm module** { nm | main | trap | os-io | sync | pkt-out | pkt-in | hw-notify | hw-setting | ccm-out | ccm-in | lbr-out | lbr-in | lbr-out | lbr-in | ltr-in | ltr-out | ltm-in | ltm-out | ais-out | ais-in | lck-out | lck-in | all }
- **no debug cfm packet** { ccm-out | ccm-in | lbr-out | lbr-in | lbr-out | lbr-in | ltr-in | ltr-out | ltm-in | ltm-out | ais-out | ais-in | lock-out | lock-in | all }
- **no debug cfm packet** { ccm-out | ccm-in | lbr-out | lbr-in | lbr-out | lbr-in | ltr-in | ltr-out | ltm-in | ltm-out | ais-out | ais-in | lock-out | lock-in | all } interface { ethernet | xgigaethernet | 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet } *interface-number*
- **no debug cfm packet** { ccm-out | ccm-in | lbr-out | lbr-in | lbr-out | lbr-in | ltr-in | ltr-out | ltm-in | ltm-out | ais-out | ais-in | lock-out | lock-in | all } interface eth-trunk *trunk-number*

Parameter

Parameter	Description	Value
interface-number	Specifies the ID of a physical interface.	The value is an integer in the range of <1-1>/<0-1>/<1-48> (For reference only. The specific value range depends on the slot number and card type).
trunk-number	Specifies the number of a Trunk interface.	The value is an integer ranging from 1 to 128.

Default Value

By default, CFM debugging is disabled.

View

Privileged user view

Usage Guidelines

NA

Example

Enable debugging of the CFM connectivity fault management module.

```
Switch#debug cfm module all
Switch#
```

Disable debugging of the CFM connectivity fault management module.

```
Switch#no debug cfm module all
Switch#
```

9.5.17 ma name vlan**Function**

The **ma name vlan** command creates an MA and enters the MA configuration view. If the MA already exists, this command enters the MA configuration view.

The **no ma name** command deletes a specified MA. The **no ma all** command deletes all MAs.

The **ma vlan** command creates MAs in batches.

Format

- **ma name name vlan** *vlan-id*
- **ma vlan** *vlan-list*
- **no ma name** *name*

- **no ma all**

Parameter

Parameter	Description	Value
name	Specifies the name of an MA.	The value is a character string.
vlan-id	Specifies the VLAN ID to be mapped to an MA.	The value is an integer ranging from 1 to 4094.
vlan-list	Specifies the VLAN list with MAC address mapping for batch creation.	The value is an integer ranging from 1 to 4094.
level	Specifies an MA level.	The value is an integer ranging from 0 to 7.

Default Value

NA

View

MD configuration view

Usage Guidelines

The requirements for creating MAs in the same bridge are as follows:

- Each of the MAs in the same MD can be mapped to only one VLAN.
- Each of the MAs in the same MD must be named uniquely.
- MAs in different MDs can have the same name.

Because each of the MAs in the same MD can be mapped to only one VLAN, when you create MAs in batches by running the command, the system automatically names each MA in the format *MA+vlan-id* based on the mapped VLAN. This ensures that each MA has a unique ID.

When you delete MAs in batches by running the command, MAs mapped to the specified *vlan-list* and *level* are deleted, and the MEP, RMEP, MIP, MEP CCDB, and MEP ERROR DB entities in these MAs are also deleted.

Currently, the Switch series switch supports creating up to 4094 MAs.

Example

Create nine MAs in batches in MD1, with MA names automatically generated.

```
Switch(config-md-md1)#ma vlan 2-10
Switch(config-md-md1)#
```

9.5.18 md name level

Function

The **md name level** command creates an MD and enters the MD configuration view. If the MD already exists, this command enters the MD configuration view.

The **no md name** command deletes a specified MD.

The **no md all** command deletes all MDs.

Format

- **md name** *name* **level** *level*
- **no md name** *name*
- **no md all**

Parameter

Parameter	Description	Value
name	Specifies an MD name.	The value is a character string.
level	Specifies an MD level.	The value is an integer ranging from 0 to 7.

Default Value

NA

View

CFM configuration view

Usage Guidelines

An MD name must be globally unique in the local bridge. That is, each of the MD names in the same bridge must be unique. The greater the *level* value, the higher the MD priority. The 802.1ag protocol packet sent by an MD of a lower priority to an MD of a higher priority is discarded. The 802.1ag packet sent by an MD of a higher priority can pass through an MD of a lower priority. The 802.1ag packet sent by an MD cannot pass through another MD of the same priority.

To modify the name and level of an existing MD, you need to delete the MD and create an MD again.

After a specified MD or all MDs are deleted, the MA, MEP, RMEP, MIP, MEP CCDB, MIP CCDB, and MEP ERROR DB instances of the MD(s) are also deleted. This is equivalent to disabling CFM in the local bridge.

Currently, the Switch series switch supports creating up to 64 MDs.

Example

Create an MD named md1 of level 5.

```
Switch(config-cfm)#md name md1 level 5
Switch(config-md-md1)#
```

9.5.19 mip auto-config vlan**Function**

The **mip auto-config vlan** command creates a VLAN mapping table automatically generated by MIP.

The **no mip auto-config vlan** command deletes a VLAN mapping list automatically generated by an MIP.

Format

- **mip auto-config vlan** *vlan-list*
- **no mip auto-config vlan** *vlan-list*

Parameter

Parameter	Description	Value
vlan-list	Specifies a VLAN mapping list.	The value is an integer ranging from 1 to 4094.

Default Value

NA

View

CFM configuration view

Usage Guidelines

After you run this command to create a VLAN mapping table automatically generated by MIP, the interface with the specified *vlan-list* tag automatically creates MIP nodes based on the MA-mapped VLAN.

After you run this command to delete the VLAN mapping table automatically generated by MIP, the interface with the specified *vlan-list* tag automatically deletes MIP nodes based on the MA-mapped VLAN.

Example

Create a VLAN mapping list including VLAN 8 and VLAN 10 automatically generated by an MIP.

```
Switch(config-cfm)#mip auto-config vlan 8,10
Switch(config-cfm)#
```

9.5.20 mip-ccdb aging-time

Function

The **mip-ccdb aging-time** command sets the aging time of MIP CCDB.

Format

mip-ccdb aging-time { *aging-time* | **default** }

Parameter

Parameter	Description	Value
aging-time	Specifies the aging time of MIP CCDB.	The value is an integer ranging from 1 to 65535, in seconds.
default	Uses the default aging time of MIP CCDB.	1000s

Default Value

The default aging time of MIP CCDB is 1000 seconds.

View

MA configuration view

Usage Guidelines

The aging time of MIP CCDB is the same as the holdtime of the ETH-CC continuous loss state of an RMEP. The RMEP is automatically deleted after the aging time has elapsed.

Example

Set the aging time of MIP CCDB to 2000 seconds.

```
Switch(config-md-md1-ma-ma1)#mip-ccdb aging-time 2000
Switch(config-md-md1-ma-ma1)#
```

9.5.21 no mep all

Function

The **no mep all** command deletes all MEPs in a specified MA.

Format

no mep all

Parameter

NA

Default Value

NA

View

MA configuration view

Usage Guidelines

NA

Example

Delete all MEPs in MA1.

```
Switch(config-10ge1/0/1)#show cfm mep
The total number of MEPs is :2
MdName Level MaName VlanId  MepId  Interface  Direction  Mac
md1      1      ma1      5       1       ge-1/0/1   outward   aa:bb:cc:dd:ee:ff
md1      1      ma1      5       2       ge-1/0/2   outward   00:04:00:00:00:06
Switch(config-10ge1/0/1)#quit
Switch(config)#cfm
Switch(config-cfm)#md name md1 level 1
Switch(config-md-md1)#ma name ma1 vlan 5
Switch(config-md-md1-ma-ma1)#no mep all
Switch(config-md-md1-ma-ma1)#show cfm mep
The total number of MEPs is :0
Switch(config-md-md1-ma-ma1)#
```

9.5.22 no mip all

Function

The **no mip all** command deletes all MIPs in a specified MA.

Format

no mip all

Parameter

NA

Default Value

NA

View

MA configuration view

Usage Guidelines

NA

Example

Delete all MIPs in MA1.

```
Switch(config-10ge1/0/1)#show cfm mip
Index Vlan    Level  Interface    Mac
1      1        5      10ge-1/0/11  00:04:00:00:00:06
Switch(config-10ge1/0/1)#quit
Switch(config)#cfm
Switch(config-cfm)#md name md1 level 5
Switch(config-md-md1)#ma name md1_ma vlan 1
Switch(config-md-md1-ma-md1_ma)#no mip all
Switch(config-md-md1-ma-md1_ma)#show cfm mip
Switch(config-md-md1-ma-md1_ma)#
```

9.5.23 remote-mep aging-time**Function**

The **remote-mep aging-time** command sets the dynamic RMEP aging time.

Format

remote-mep aging-time { *aging-time* | **default** }

Parameter

Parameter	Description	Value
aging-time	Specifies the aging time of a dynamic RMEP.	The value is an integer ranging from 1 to 65535, in seconds.
default	Uses the default aging time.	1000s

Default Value

The default aging time of a dynamic RMEP is 1000 seconds.

View

MA configuration view

Usage Guidelines

The aging time of a dynamic RMEP is the same as the holdtime of the ETH-CC continuous loss state of the dynamic RMEP. The dynamic RMEP is automatically deleted after the aging time has elapsed.

Example

Set the dynamic RMEP aging time to 2000s.

```
Switch(config-md-md1-ma-ma1)#remote-mep aging-time 2000
Switch(config-md-md1-ma-ma1)#
```

9.5.24 remote-mep mep-id

Function

The **remote-mep mep-id mac** command creates an RMEP in the current MA.

The **remote-mep mep-id** command creates RMEPs in batches in the current MA.

The **no remote-mep all** command deletes all RMEPs in a specified MA.

The **no remote-mep mep-id** command deletes an RMEP in a specified MA.

Format

- **remote-mep mep-id** *mep-id* **mac** *mac-address*
- **remote-mep mep-id** *mep-id-list*
- **no remote-mep all**
- **no remote-mep mep-id** *mep-id-list*

Parameter

Parameter	Description	Value
mep-id	Specifies an RMEP ID.	The value is an integer ranging from 1 to 8191.
mep-id-list	Specifies a list of RMEP IDs.	The value is an integer ranging from 1 to 8191.
mac-address	Specifies the bridge MAC address of the switch where the RMEP is located.	The value is in AA:BB:CC:DD:EE:FF format, where A to F are hexadecimal digits.
all	Specifies all RMEPs in the current MA.	-

Default Value

NA

View

MA configuration view

Usage Guidelines

The default MAC addresses of batch-configured RMEPs are all 0s. To modify the bridge MAC address of an existing RMEP, delete the RMEP from the MA and configure the RMEP again.

Example

Configure an RMEP with ID 1 in MA1 and set the bridge MAC address of the RMEP to 00:10:94:00:00:01.

```
Switch(config-md-md1-ma-ma1)#remote-mep mep-id 1 mac 00:10:94:00:00:01
Switch(config-md-md1-ma-ma1)#
```

9.5.25 reset counter**Function**

The **reset counter** command resets the CFM packet counters of an MA.

Format

reset counter

Parameter

NA

Default Value

NA

View

MA configuration view

Usage Guidelines

Use this command to clear the CFM packet counters of all MEPs in an MA.

Example

Reset the CFM packet counters of an MA.

```
Switch(config)#cfm
Switch(config-cfm)#md name md1 level 1
Switch(config-md-md1)#ma name ma1 vlan 1
Switch(config-md-md1-ma-ma1)#reset counter
Switch(config-md-md1-ma-ma1)#
```


9.5.26 senderid-tlv-type

Function

The **senderid-tlv-type** command sets the sender ID TLV type of CFM packets.

Format

senderid-tlv-type { **none** | **chassis** | **manage** | **chassis-manage** | **defer** }

Parameter

Parameter	Description	Value
none	Specifies that the sender ID TLV type is not included in sent CFM packets.	-
chassis	Specifies that the chassis ID is included in sent CFM packets.	-
manage	Specifies that the management address is included in sent CFM packets.	-
chassis-manage	Specifies that the chassis ID and management address are included in sent CFM packets.	-
defer	Indicates that the Sender ID TLV content is determined by the MD management object.	-

Default Value

The default sender ID TLV type is **none**, indicating that CFM packets do not include the sender ID TLV type.

View

MD configuration view

Usage Guidelines

Currently, Switch does not support **manage**, **chassis-manage**, and **defer**.

Example

Set the sender ID TLV type to **chassis**.

```
Switch(config-md-md1)#senderid-tlv-type chassis
Switch(config-md-md1)#
```

9.5.27 show cfm

Function

The **show cfm** command displays the summary of CFM connectivity fault management.

Format

show cfm

Parameter

NA

Default Value

NA

View

Common user view

Usage Guidelines

Use this command to query the global configuration of CFM connectivity fault management.

Example

Display the summary of CFM connectivity fault management.

```
Switch>show cfm
      version CFM_VB3.00.02.00
      md default level 0.
      snmp trap   disable.
Switch>
```

9.5.28 show cfm config**Function**

The **show cfm config** command displays the CFM configuration file information.

Format

show cfm config

Parameter

NA

Default Value

NA

View

Common user view

Usage Guidelines

Use this command to query the CFM configuration file content.

Example

Display the CFM configuration file information.

```
Switch>show cfm config
cfm
  md name md1 level 1
    senderid-tlv-type chassis
  ma name ma1 vlan 1
  ma name md1_ma vlan 1
  ma name ma2 vlan 2
  ma name ma3 vlan 3
  ma name ma4 vlan 4
  ma name ma5 vlan 5
  ma name ma6 vlan 6
  ma name ma7 vlan 7
  ma name ma8 vlan 8
  ma name ma9 vlan 9
  ma name ma10 vlan 10
Switch>
```

9.5.29 show cfm error ccdb**Function**

The **show cfm error ccdb** command displays the summary or details of MEP ERROR CCDBs.

Format

- **show cfm error ccdb**
- **show cfm error ccdb** *remote-mep-id* **vlan** *vlan-id* **level** *level* **mepid** *mep-id*

Parameter

Parameter	Description	Value
remote-mep-id	Specifies a remote MEP ID.	The value is an integer ranging from 1 to 8191.
vlan-id	Specifies a VLAN ID.	The value is an integer ranging from 1 to 4094.
level	Specifies an MEP level.	The value is an integer ranging from 0 to 7.
mep-id	Specifies a local MEP ID.	The value is an integer ranging from 1 to 8191.

Default Value

NA

View

Common user view

Usage Guidelines

This command supports the following two query methods:

- If no parameters are set, this command queries the summary of all MEP ERROR CCDBs configured for the bridge.
- If parameters are set, this command queries the details of a specific MEP ERROR CCDB configured for the bridge.

Example

Display the summary of all MEP ERROR CCDBs configured for the bridge.

```
Switch>show cfm error cddb
  Index MdName  Level  MaName  Vlan  mepid  RmepId RmepErrorType  RmepMac
  1      md2      5      md2_ma1  1      1      2      unexp-mep      00:00:00:00:00:00
Switch>
```

9.5.30 show cfm ma

Function

The **show cfm ma** command displays the summary or details of an MA.

Format

- **show cfm ma**
- **show cfm ma name** *name* **vlan** *vlan-id*

Parameter

Parameter	Description	Value
name	Specifies an MA name.	The value is a character string.
vlan-id	Specifies a mapped VLAN ID.	The value is an integer ranging from 1 to 4094.

Default Value

NA

View

Common user view

Usage Guidelines

This command supports the following two query methods:

- If the MA name and VLAN ID are not set, this command queries the summary of all MAs configured for the bridge.
- If the MA name and VLAN ID are set, this command queries the details of a specific MA configured for the bridge.

Example

Display the summary of all MAs configured for the bridge.

```
Switch>show cfm ma
The total number of MAs is 3
Ma Name           :ma1
Ma Vlan           :1
CCM Interval      :100MS
AIS Interval      :1S
LCK Interval      :1S
CCM Loss Threshold :default(3.5)
AIS Loss Threshold :default(3.5)
LCK Loss Threshold :default(3.5)
Cross Check       :disable
Cross Check Start Delay :0
Remote Mep Aging Time :1000
Trace Reply Aging Time :1000
Mip Ccdb Aging Time  :1000

Ma Name           :ma2
Ma Vlan           :2
CCM Interval      :100MS
AIS Interval      :1S
LCK Interval      :1S
CCM Loss Threshold :default(3.5)
AIS Loss Threshold :default(3.5)
LCK Loss Threshold :default(3.5)
Cross Check       :disable
Cross Check Start Delay :0
Remote Mep Aging Time :1000
Trace Reply Aging Time :1000
Mip Ccdb Aging Time  :1000

Ma Name           :ma3
Ma Vlan           :3
CCM Interval      :100MS
AIS Interval      :1S
```

```

LCK Interval           :1S
CCM Loss Threshold     :default(3.5)
AIS Loss Threshold     :default(3.5)
LCK Loss Threshold     :default(3.5)
Cross Check           :disable
Cross Check Start Delay :0
Remote Mep Aging Time  :1000
Trace Reply Aging Time :1000
Mip Ccdb Aging Time    :1000

```

```
Switch>
```

Display the details of MA1.

```

Switch>show cfm ma ma1 vlan 1
Ma Name           :ma1
Ma Vlan           :1
CCM Interval      :100MS
AIS Interval      :1S
LCK Interval      :1S
CCM Loss Threshold :default(3.5)
AIS Loss Threshold :default(3.5)
LCK Loss Threshold :default(3.5)
Cross Check       :disable
Cross Check Start Delay :0
Remote Mep Aging Time  :1000
Trace Reply Aging Time :1000
Mip Ccdb Aging Time    :1000

```

```
Switch>
```

9.5.31 show cfm md

Function

The **show cfm md** command displays the summary or details of an MD.

Format

- **show cfm md**
- **show cfm md *name***

Parameter

Parameter	Description	Value
name	Specifies an MD name.	The value is a character string.

Default Value

NA

View

Common user view

Usage Guidelines

This command supports the following two query methods:

- If the MD name is not set, this command queries the summary of all MDs configured for the bridge.
- If the MD name is set, this command queries the details of a specific MD configured for the bridge.

Example

Display the summary of all MDs configured for the bridge.

```
Switch>show cfm md
The total number of MDs is : 1
Md Name           :md1
Md Level           :5
SenderID TLV-type :none
Ma List           :
Ma Name           :ma1
Ma Vlan           :1
CCM Interval       :100MS
AIS Interval       :1S
LCK Interval       :1S

Ma Name           :ma2
Ma Vlan           :2
CCM Interval       :100MS
AIS Interval       :1S
LCK Interval       :1S

Ma Name           :ma3
Ma Vlan           :3
CCM Interval       :100MS
AIS Interval       :1S
LCK Interval       :1S
Switch>
```

9.5.32 show cfm mep

Function

The **show cfm mep** command displays the summary or details of an MEP.

Format

- **show cfm mep**
- **show cfm mep vlan** *vlan-id* **level** *level* **mepid** *mep-id*

Parameter

Parameter	Description	Value
vlan-id	Specifies a VLAN ID.	The value is an integer ranging from 1 to 4094.
level	Specifies an MEP level.	The value is an integer ranging from 0 to 7.
mep-id	Specifies a local MEP ID.	The value is an integer ranging from 1 to 8191.

Default Value

NA

View

Common user view

Usage Guidelines

This command supports the following two query methods:

- If no parameters are set, this command queries the summary of all MEPs configured for the bridge.
- If parameters are set, this command queries the details of a specific MEP configured for the bridge.

Example

Display the summary of all MEPs configured for the bridge.

```
Switch>show cfm mep
The total number of MEPs is :10
  MdName Level MaName VlanId  MepId  Interface  Direction  Mac
md1      5    ma1     1    2  ge-1/0/11  outward    00:04:00:00:00:06
md1      5    ma2     2    2  ge-1/0/11  outward    00:04:00:00:00:06
md1      5    ma3     3    2  ge-1/0/11  outward    00:04:00:00:00:06
md1      5    ma4     4    2  ge-1/0/11  outward    00:04:00:00:00:06
md1      5    ma5     5    2  ge-1/0/11  outward    00:04:00:00:00:06
md1      5    ma6     6    2  ge-1/0/11  outward    00:04:00:00:00:06
```



```

md1 5 ma7 7 2 ge-1/0/11 outward 00:04:00:00:00:06
md1 5 ma8 8 2 ge-1/0/11 outward 00:04:00:00:00:06
md1 5 ma9 9 2 ge-1/0/11 outward 00:04:00:00:00:06
md1 5 ma10 10 2 ge-1/0/11 outward 00:04:00:00:00:06
Switch>

```

Display the details of the MEP of VLAN 1, level 5, and ID 2.

```

Switch>show cfm mep vlan 1 level 5 mepid 2
Mep vlan 1 level 5 mepid 2 information:
Mep interface : ge-1/0/11
Mep direction : outward
Mep mac : 00:04:00:00:00:06
Mep alarm time : 0
Mep alarm recover time : 0
Mep alarm lowest priority : 1
Mep ccm state : enable
Mep ais State : disable
Mep lock state : disable
Switch>

```

9.5.33 show cfm mep ccdb

Function

The **show cfm mep ccdb** command displays the summary or details of MEP CCDBs.

Format

- **show cfm mep ccdb**
- **show cfm mep ccdb** *remote-mep-id* **vlan** *vlan-id* **level** *level* **mepid** *mep-id*

Parameter

Parameter	Description	Value
remote-mep-id	Specifies a remote MEP ID.	The value is an integer ranging from 1 to 8191.
vlan-id	Specifies a VLAN ID.	The value is an integer ranging from 1 to 4094.
level	Specifies an MEP level.	The value is an integer ranging from 0 to 7.
mep-id	Specifies a local MEP ID.	The value is an integer ranging from 1 to 8191.

Default Value

NA

View

Common user view

Usage Guidelines

This command supports the following two query methods:

- If no parameters are set, this command queries the summary of all MEP CCDBs configured for the bridge.
- If parameters are set, this command queries the details of a specific MEP CCDB configured for the bridge.

Example

Display the summary of a specific MEP CCDB configured for the bridge.

```
Switch>show cfm mep cddb 1 vlan 1 level 5 mepid 2
Md Name                : md2
Md Level                : 5
Ma Name                 : md2_ma1
Ma Vlan                 : 1
Mep ID                  : 2
Remote Mep ID           : 1
Remote Mep State        : ok
Remote Mep Mac           : 00:04:67:90:ff:ff
Remote Mep Chassis ID   :
Remote Mep Last Service State : unknown
Remote Mep Last Forward State : forwarded
Remote Mep Last Operate State : up
Remote Mep Life Time(sec) : forever
Switch>
```

9.5.34 show cfm mip

Function

The **show cfm mip** command displays information about all MIPs configured for the bridge.

Format

show cfm mip

Parameter

NA

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

Display information about all MIPs configured for the bridge.

```
Switch>show cfm mip
Index Vlan    Level  Interface  Mac
1     1       5      10ge-1/0/10  00:04:00:00:00:06
Switch>
```

9.5.35 show cfm mip ccdb**Function**

The **show cfm mip ccdb** command displays the summary of MIP CCDBs.

Format

show cfm mip ccdb

Parameter

NA

Default Value

NA

View

Common user view

Usage Guidelines

Use this command to query the summary of all MIP CCDBs configured for the bridge.

Example

Display the summary of all MIP CCDBs configured for the bridge.

```
Switch>show cfm mip ccdb
Index Level  Vlan  RmepId Interface  Age(Sec)  Mac
1     6     1     1    10ge-1/0/1    1000     00:04:67:00:00:99
2     6     1     3    10ge-1/0/1    1000     00:04:67:00:00:99
```

```

3  6  1  5  10ge-1/0/1  1000  00:04:67:00:00:99
4  6  1  2  10ge-1/0/2  1000  00:04:67:97:db:81
5  6  1  4  10ge-1/0/2  1000  00:04:67:97:db:81
6  6  1  6  10ge-1/0/2  1000  00:04:67:97:db:81
7  5  1  1  10ge-1/0/1  1000  00:04:67:00:00:99
8  5  1  2  10ge-1/0/2  1000  00:04:67:97:db:81
Switch>

```

9.5.36 show cfm pdu-statistic

Function

The **show cfm pdu-statistic** command displays CFM packet statistics on an interface.

Format

- **show cfm pdu-statistic interface**
- **show cfm pdu-statistic interface { ethernet | xgigaethernet | 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet } interface-number**
- **show cfm pdu-statistic interface eth-trunk trunk-number**

Parameter

Parameter	Description	Value
interface-number	Specifies an Ethernet interface number.	The value is an integer in the range of <1-1>/<0-1>/<1-48> (For reference only. The specific value range depends on the slot number and card type).
trunk-number	Specifies an aggregation interface number.	The value is an integer ranging from 1 to 128.

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

Display CFM packet statistics on bridge interface 10gigaethernet 1/0/1.

```
Switch>show cfm pdu-statistic interface 10gigaethernet 1/0/1
```

```

Out Ccm Count :    0   In Ccm Count : 0
Out Lbr Count :    0   In Lbr Count : 0
Out Lbm Count :    0   In Lbm Count      : 0
Out Ltr Count :    0   In Ltr Count      : 0
Out Ltm Count :    0   In Ltm Count      : 0
Out Ais Count :    0   In Ais Count      : 0
Out Lck Count :    0   In Lck Count      : 0
Failed in Pdu Count :    0   Failed out Pdu Count      : 0
Forwarded Pdu Count : 0
Switch>

```

9.5.37 show cfm remote-mep

Function

The **show cfm remote-mep** command displays the summary or details of an RMEP.

Format

- **show cfm remote-mep**
- **show cfm remote-mep vlan** *vlan-id* **level** *level* **mepid** *mep-id*

Parameter

Parameter	Description	Value
vlan-id	Specifies a VLAN ID.	The value is an integer ranging from 1 to 4094.
level	Specifies a level.	The value is an integer ranging from 0 to 7.
mep-id	Specifies a local MEP ID.	The value is an integer ranging from 1 to 8191.

Default Value

NA

View

Common user view

Usage Guidelines

This command supports the following two query methods:

- If no parameters are set, this command queries the summary of all RMEPs configured for the bridge.
- If parameters are set, this command queries the details of a specific RMEP configured for the bridge.

Example

Display the summary of all RMEPs configured for the bridge.

```
Switch>show cfm remote-mep vlan 1 level 5 mepid 1
Md Name                : md2
Md Level                : 5
Ma Name                : md2_ma1
Ma Vlan                : 1
Remote Mep ID          : 1
Remote Mep State        : failed
Remote Mep Type         : static
Remote Mep Mac          : 00:04:67:90:ff:ff
Remote Mep Chassis ID   :
Remote Mep Interface Name :
Remote Mep Last Service State : unknown
Remote Mep Last Forward State : forwarded
Remote Mep Last Operate State : up
Remote Mep Life Time(sec) : forever
Switch>
```

9.5.38 show cfm trace-result mep vlan level mepid

Function

The **show cfm trace-result mep vlan level mepid** command displays the results of the last query about fault locating for an MEP of the bridge.

Format

show cfm trace-result mep vlan *vlan-id* **level** *level* **mepid** *mep-id*

Parameter

Parameter	Description	Value
vlan-id	Specifies a VLAN ID.	The value is an integer ranging from 1 to 4094.
level	Specifies a level.	The value is an integer ranging from 0 to 7.
mep-id	Specifies a local MEP ID.	The value is an integer ranging from 1 to 8191.

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

Display the results of the last query about fault locating for an MEP of the bridge.

```
Switch>show cfm trace-result mep vlan 1 level 5 mepid 2
```

Hops Host	Mac	Ingr	IngrAct	RelayAct
Forwarded	Engr	EngrAct	IsMep	
1	00:03:09:01:09:2a	10ge-1/0/1	IngOk	RlyHit
Not Forwarded	EgrNoTlv	YES		

```
Switch>
```

9.5.39 snmp-trap**Function**

The **snmp-trap** command enables or disables the SNMP alarm reporting function for CFM.

Format

snmp-trap { enable | disable }

Parameter

Parameter	Description	Value
enable	Enables the SNMP alarm reporting function for CFM.	-
disable	Disables the SNMP alarm reporting function for CFM.	-

Default Value

By default, the SNMP alarm reporting function is disabled for CFM.

View

CFM configuration view

Usage Guidelines

NA

Example

Enable the SNMP trap function of CFM.

```
Switch(config-cfm)#snmp-trap enable
Switch(config-cfm)#
```

9.5.40 trace-replay aging-time

Function

The **trace-replay aging-time** command sets the aging time of LTR responses.

Format

trace-replay aging-time { *aging-time* | **default** }

Parameter

Parameter	Description	Value
aging-time	Specifies the aging time of LTR response.	The value is an integer ranging from 1 to 65535, in seconds.
default	Uses the default aging time of LTR responses.	1000s

Default Value

The default aging time of LTR responses is 1000 seconds.

View

MA configuration view

Usage Guidelines

The aging time of LTR responses is the same as the link holdtime returned for the last query about fault locating for an MEP. After the aging time has elapsed, the link returned for the last query about fault locating is automatically deleted.

Example

Set the aging time of LTR responses to 600 seconds.

```
Switch(config-cfm)#md name md1 level 5
Switch(config-md-md1)#ma name ma1 vlan 1
Switch(config-md-md1-ma-ma1)#trace-reply aging-time 600
Switch(config-md-md1-ma-ma1)#
```

9.6 Y.1731 Configuration Commands

9.6.1 debug y1731 packet

Function

The **debug y1731 packet** command enables debugging of Y.1731 interface packets.

The **no debug y1731 packet** command disables debugging of Y.1731 interface packets.

Format

- **debug y1731 packet { ccm-out | ccm-in | lbr-out | lbr-in | lbrm-out | lbrm-in | ltr-in | ltr-out | ltm-in | ltm-out | ais-out | ais-in | lock-out | lock-in | tst-out | tst-in | mcc-out | mcc-in | lmr-out | lmr-in | lmm-out | lmm-in | 1dm | dmr-out | dmr-in | dmm-out | dmm-in | exp | vsp | all }**
- **debug y1731 packet { ccm-out | ccm-in | lbr-out | lbr-in | lbrm-out | lbrm-in | ltr-in | ltr-out | ltm-in | ltm-out | ais-out | ais-in | lock-out | lock-in | tst-out | tst-in | mcc-out | mcc-in | lmr-out | lmr-in | lmm-out | lmm-in | 1dm | dmr-out | dmr-in | dmm-out | dmm-in | exp | vsp | all } interface { ethernet | xgigaethernet | 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet } interface-number**
- **debug y1731 packet { ccm-out | ccm-in | lbr-out | lbr-in | lbrm-out | lbrm-in | ltr-in | ltr-out | ltm-in | ltm-out | ais-out | ais-in | lock-out | lock-in | tst-out | tst-in | mcc-out | mcc-in | lmr-out | lmr-in | lmm-out | lmm-in | 1dm | dmr-out | dmr-in | dmm-out | dmm-in | exp | vsp | all } interface eth-trunk trunk-number**
- **no debug y1731 packet { ccm-out | ccm-in | lbr-out | lbr-in | lbrm-out | lbrm-in | ltr-in | ltr-out | ltm-in | ltm-out | ais-out | ais-in | lock-out | lock-in | tst-out | tst-in | mcc-out | mcc-in | lmr-out | lmr-in | lmm-out | lmm-in | 1dm | dmr-out | dmr-in | dmm-out | dmm-in | exp | vsp | all }**
- **no debug y1731 packet { ccm-out | ccm-in | lbr-out | lbr-in | lbrm-out | lbrm-in | ltr-in | ltr-out | ltm-in | ltm-out | ais-out | ais-in | lock-out | lock-in | tst-out | tst-in | mcc-out | mcc-in | lmr-out | lmr-in | lmm-out | lmm-in | 1dm | dmr-out | dmr-in | dmm-out | dmm-in | exp | vsp | all } interface { ethernet | xgigaethernet | 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet } interface-number**
- **no debug y1731 packet { ccm-out | ccm-in | lbr-out | lbr-in | lbrm-out | lbrm-in | ltr-in | ltr-out | ltm-in | ltm-out | ais-out | ais-in | lock-out | lock-in | tst-out | tst-in | mcc-out | mcc-in | lmr-out | lmr-in | lmm-out | lmm-in | 1dm | dmr-out | dmr-in | dmm-out | dmm-in | exp | vsp | all } interface eth-trunk trunk-number**

Parameter

Parameter	Description	Value
ccm-out	Specifies packets sent for an Y.1731 continuity test.	-
ccm-in	Specifies packets received for an Y.1731 continuity test.	-
lbr-out	Specifies response packets sent for Y.1731 loopback.	-
lbr-in	Specifies response packets received for Y.1731 loopback.	-
lbrm-out	Specifies packets sent for Y.1731 loopback.	-

Parameter	Description	Value
lbm-in	Specifies packets received for Y.1731 loopback.	-
ltr-out	Specifies response packets sent for Y.1731 link tracing.	-
ltr-in	Specifies response packets received for Y.1731 link tracing.	-
ltm-out	Specifies packets sent for Y.1731 link tracing.	-
ltm-in	Specifies packets received for Y.1731 link tracing.	-
ais-out	Specifies packets sent for Y.1731 alarm indication signals.	-
ais-in	Specifies packets received for Y.1731 alarm indication signals.	-
lock-out	Specifies packets sent for Y.1731 lock signals.	-
lock-in	Specifies packets received for Y.1731 lock signals.	-
tst-out	Specifies PDUs sent for an Y.1731 test.	-
tst-in	Specifies PDUs received for an Y.1731 test.	-
mcc-out	Specifies packets sent for the Y.1731 maintenance communication channel.	-
mcc-in	Specifies packets received for the Y.1731 maintenance communication channel.	-
lmr-out	Specifies response packets sent for Y.1731 loss measurement.	-
lmr-in	Specifies response packets received for Y.1731 loss measurement.	-
lmm-out	Specifies packets sent for Y.1731 loss measurement.	-
lmm-in	Specifies packets received for Y.1731 loss measurement.	-
ldm	Specifies Y.1731 unidirectional latency measurement.	-
dmr-out	Specifies response packets sent for Y.1731 latency measurement.	-
dmr-in	Specifies response packets received for Y.1731 latency measurement.	-
dmm-out	Specifies packets sent for Y.1731 latency measurement.	-
dmm-in	Specifies packets received for Y.1731 latency measurement.	-
exp	Specifies Y.1731 experiment packets.	-
vsp	Specifies Y.1731 vendor-defined packets.	-
all	Specifies all the preceding sent and received packets.	-
interface-number	Specifies an Ethernet interface number.	The value is an integer in the range of <1-1>/<0-1>/<1-48> (For reference only. The specific value range depends on the slot number and card type).
trunk-number	Specifies a Trunk interface number.	The value is an integer ranging from 1 to 128.

Default Value

By default, debugging of Y.1731 interface packets is disabled.

View

Privileged user view

Usage Guidelines

NA

Example

Enable debugging of packets sent for Y.1731 continuity testing on interface 10gigaethernet 1/0/1.

```
Switch#debug y1731 packet ccm-out interface 10gigaethernet 1/0/1
Switch#
```

9.6.2 debug y1731 module**Function**

The **debug y1731 module** command enables Y.1731 module debugging.

The **no debug y1731 module** command disables Y.1731 module debugging.

Format

- **debug y1731 module { nm | main | trap | os-io | sync | pkt-out | pkt-in | hw-notify | hw-setting | ccm-out | ccm-in | lbr-out | lbr-in | lbr-out | lbr-in | lbr-out | lbr-in | ltr-in | ltr-out | ltm-in | ltm-out | ais-out | ais-in | lock-out | lock-in | tst | mcc | lmr | lmm | 1dm | dmr | dmm | exp | vsp | all }**
- **no debug y1731 module { nm | main | trap | os-io | sync | pkt-out | pkt-in | hw-notify | hw-setting | ccm-out | ccm-in | lbr-out | lbr-in | lbr-out | lbr-in | lbr-out | lbr-in | ltr-in | ltr-out | ltm-in | ltm-out | ais-out | ais-in | lock-out | lock-in | tst | mcc | lmr | lmm | 1dm | dmr | dmm | exp | vsp | all }**

Parameter

Parameter	Description	Value
nm	Specifies Y.1731 network management.	-
main	Specifies the Y.1731 protocol stack.	-
trap	Specifies Y.1731 SNMP trap.	-
os-io	Specifies the Y.1731 system interface.	-
sync	Specifies Y.1731 synchronization information.	-
pkt-out	Specifies the details of sent Y.1731 packets.	-

Parameter	Description	Value
pkt-in	Specifies the details of received Y.1731 packets.	-
hw-notify	Specifies Y.1731 hardware notification.	-
hw-setting	Specifies Y.1731 hardware delivery.	-
ccm-out	Specifies packets sent for an Y.1731 continuity test.	-
ccm-in	Specifies packets received for an Y.1731 continuity test.	-
lbr-out	Specifies response packets sent for Y.1731 loopback.	-
lbr-in	Specifies response packets received for Y.1731 loopback.	-
lbrm-out	Specifies packets sent for Y.1731 loopback.	-
lbrm-in	Specifies packets received for Y.1731 loopback.	-
ltr-out	Specifies response packets sent for Y.1731 link tracing.	-
ltr-in	Specifies response packets received for Y.1731 link tracing.	-
ltm-out	Specifies packets sent for Y.1731 link tracing.	-
ltm-in	Specifies packets received for Y.1731 link tracing.	-
ais-out	Specifies packets sent for Y.1731 alarm indication signals.	-
ais-in	Specifies packets received for Y.1731 alarm indication signals.	-
lock-out	Specifies packets sent for Y.1731 lock signals.	-
lock-in	Specifies packets received for Y.1731 lock signals.	-
tst	Specifies PDUs sent and received for an Y.1731 test.	-
mcc	Specifies packets sent and received for the Y.1731 maintenance communication channel.	-
lmr	Specifies response packets sent and received for Y.1731 loss measurement.	-
lmm	Specifies packets sent and received for Y.1731 loss measurement.	-
ldm	Specifies Y.1731 unidirectional latency measurement.	-
dmr	Specifies response packets sent and received for Y.1731 latency measurement.	-
dmm	Specifies packets sent and received for Y.1731 latency measurement.	-
exp	Specifies debugging of Y.1731 experiment packets.	-
vsp	Specifies debugging of Y.1731 vendor-defined packets.	-
all	Specifies all the preceding sent and received packets.	-

Default Value

By default, Y.1731 module debugging is disabled.

View

Privileged user view

Usage Guidelines

NA

Example

Enable debugging of response packets sent for Y.1731 loss measurement.

```
Switch#debug y1731 module lmr
Switch#
```

9.6.3 show y1731

Function

The **show y1731** command displays the Y.1731 global configuration.

Format

show y1731

Parameter

NA

Default Value

NA

View

Common user view

Usage Guidelines

Use this command to query the Y.1731 global configuration.

Example

Display the Y.1731 global configuration.

```
Switch>show y1731
  meg default level 0.
  remote mep aging time 0.
  trace reply aging time 0.
  snmp trap  disable.
Switch#
```

9.6.4 show y1731 ccdb

Function

The **show y1731 ccdb** command displays the summary or details of MEP CCDBs.

Format

- **show y1731 ccdb**
- **show y1731 ccdb remote-mep-id vlan vlan-id level level mepid mep-id**

Parameter

Parameter	Description	Value
remote-mep-id	Specifies a remote MEP ID.	The value is an integer ranging from 1 to 8191.
vlan-id	Specifies a VLAN ID.	The value is an integer ranging from 1 to 4094.
level	Specifies an MEP level.	The value is an integer ranging from 0 to 7.
mep-id	Specifies a local MEP ID.	The value is an integer ranging from 1 to 8191.

Default Value

NA

View

Common user view

Usage Guidelines

This command supports the following two query methods:

- If no parameters are set, this command queries the summary of all MEP CCDBs configured for the bridge.
- If parameters are set, this command queries the details of a specific MEP CCDB configured for the bridge.

Example

Display the summary of a specific MEP CCDB configured for the bridge.

```
Switch>show y1731 ccdb
Index Vlan  Level  MepId  RmepId RmepState  RmepMac
1   1    3    1    2    ok      00:04:67:59:09:09
2   1    6    1    2    ok      00:04:67:59:09:09
Switch>show y1731 ccdb 2 vlan 1 level 3 mepid 1
Meg Vlan          : 1
Meg Level         : 3
Meg Icc           : v1
Meg Umc           : fh3
Meg ID            : 1
Remote Mep ID     : 2
Remote Mep State  : ok
```

```

Remote Mep Mac      : 00:04:67:59:09:09
Remote Mep Interface Name : 10ge-1/0/1
Remote Mep Chassis ID   :
Remote Mep Last Service State : unknown
Remote Mep Last Forward State : forwarded
Remote Mep Last Operate State : up
  Index Vlan  Level  MepId  RmepId RmepState  RmepMac
  1    1    3    1    2    ok      00:04:67:59:09:09
  2    1    6    1    2    ok      00:04:67:59:09:09
Switch>

```

9.6.5 show y1731 config

Function

The **show y1731 config** command displays the Y.1731 configuration file information.

Format

show y1731 config

Parameter

NA

Default Value

NA

View

Common user view

Usage Guidelines

Use this command to query the Y.1731 configuration file content.

Example

Display the Y.1731 configuration file content.

```

Switch>show y1731 config
y1731
  meg vlan 1 level 1 icc 123 umc tst
  lmm-interval 100ms
Switch>

```

9.6.6 show y1731 error ccdb

Function

The **show y1731 error ccdb** command displays the error CCDB summary of all MEPs configured for the switch or the error CCDB details of a specified MEP.

Format

- **show y1731 error ccdb**
- **show y1731 error ccdb** *remote-mep-id* **vlan** *vlan-id* **level** *level* **mepid** *mep-id*

Parameter

Parameter	Description	Value
remote-mep-id	Specifies a remote MEP ID.	The value is an integer ranging from 1 to 8191.
vlan-id	Specifies a VLAN ID.	The value is an integer ranging from 1 to 4094.
level	Specifies an MEP level.	The value is an integer ranging from 0 to 7.
mep-id	Specifies a local MEP ID.	The value is an integer ranging from 1 to 8191.

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

Display the error CCDB summary of all MEPs configured for the switch or the error CCDB details of a specified MEP.

```
Switch>show y1731 error ccdb
Index Vlan  Level  mepid  RmepId RmepErrorType  RmepMac
1    1    3    2    2    unexp-mep    00:04:67:97:db:81
Switch>
```

9.6.7 show y1731 meg

Function

The **show y1731 meg** command displays all MEGs configured for the switch.

Format

- **show y1731 meg**
- **show y1731 meg vlan *vlan-id* level *level***

Parameter

Parameter	Description	Value
vlan-id	Specifies a VLAN ID.	The value is an integer ranging from 1 to 4094.
level	Specifies an MEP level.	The value is an integer ranging from 0 to 7.

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

Display all MEGs configured for the switch.

Switch>show y1731 meg					
Index	VlanId	Level	ICC	UMC	
1	1	1	v1	fhn1	
2	3	1	v3	fhn1	
3	5	1	v5	fhn1	
4	6	1	v6	fhn1	
5	7	1	v7	fhn1	
Switch>					

9.6.8 show y1731 mep

Function

The **show y1731 mep** command displays the summary or details of an MEP.

Format

- **show y1731 mep**
- **show y1731 mep vlan *vlan-id* level *level* mepid *mep-id***

Parameter

Parameter	Description	Value

Parameter	Description	Value
vlan-id	Specifies a VLAN ID.	The value is an integer ranging from 1 to 4094.
level	Specifies an MEP level.	The value is an integer ranging from 0 to 7.
mep-id	Specifies a local MEP ID.	The value is an integer ranging from 1 to 8191.

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

Display the summary and details of an MEP.

```
Switch>show y1731 mep
  Index   VlanId  Level  MepId  Interface  Direction  Mac
  1       1      1      1      10ge-1/0/1  outward    00:05:67:fc:c1:cb

Switch>show y1731 mep vlan 1 level 1 mepid 1
Mep vlan 1 level 1 mepid 1 information:
Mep interface : 10ge-1/0/1
Mep direction : outward
Mep mac : 00:05:67:fc:c1:cb
Mep service type : inservice
Mep ccm state : disable
Mep ais State : disable
Mep lock state : disable
Switch>
```

9.6.9 show y1731 mip

Function

The **show y1731 mip** command displays information about all MIPs configured for the switch.

Format

show y1731 mip

Parameter

NA

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

Display information about all MIPs configured for the switch.

```
Switch>show y1731 mip
Index Vlan    Level  Interface      Mac
1      5       1      10ge-1/0/11    00:04:00:00:00:06
Switch>
```

9.6.10 show y1731 pdu-statistic**Function**The **show y1731 pdu-statistic** command displays Y.1731 frame statistics on an interface.**Format**

- **show y1731 pdu-statistic interface**
- **show y1731 pdu-statistic interface { ethernet | xgigaethernet | 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet } interface-number**
- **show y1731 pdu-statistic interface eth-trunk trunk-number**

Parameter

Parameter	Description	Value
interface-number	Specifies an Ethernet interface number.	The value is an integer in the range of <1-1>/<0-1>/<1-48> (For reference only. The specific value range depends on the slot number and card type).
trunk-number	Specifies the number of a Trunk interface.	The value is an integer ranging from 1 to 128.

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

Display Y.1731 frame statistics on an interface.

```
Switch>show y1731 pdu-statistic interface 10gigaethernet 1/0/1
Mep Count :      1  Mip Count : 0
Out Ccm Count :    0  In Ccm Count : 0
Out Lbr Count :    0  In Lbr Count : 0
Out Lbm Count :    0  In Lbm Count      : 0
Out Ltr Count :    0  In Ltr Count      : 0
Out Ltm Count :    0  In Ltm Count      : 0
Out Ais Count :    0  In Ais Count      : 0
Out Lck Count :    0  In Lck Count      : 0
Out Tst Count :    0  In Tst Count      : 0
Out Mcc Count :    0  In Mcc Count      : 0
Out Lmr Count :    0  In Lmr Count      : 0
Out Lmm Count :    0  In Lmm Count      : 0
Out Idm Count :    0  In Idm Count      : 0
Out Dmr Count :    0  In Dmr Count      : 0
Out Dmm Count :    0  In Dmm Count      : 0
Out Exr Count :    0  In Exr Count      : 0
Out Exm Count :    0  In Exm Count      : 0
Out Vsr Count :    0  In Vsr Count      : 0
Out Vsm Count :    0  In Vsm Count      : 0
Out Ping Request Count :    0  In Ping Request Count      : 0
Out Ping Reply Count :    0  In Ping Reply Count      : 0
Out Trace Request Count :    0  In Trace Request Count      : 0
Out Trace Reply Count :    0  In Trace Reply Count      : 0
Failed in Pdu Count :    0  Failed out Pdu Count      : 0
Forwarded Pdu Count : 0
Switch>
```

9.6.11 show y1731 remote-mep**Function**

The **show y1731 remote-mep** command displays the summary of all remote MEPs configured for the switch or the details of a remote MEP.

Format

- **show y1731 remote-mep**
- **show y1731 remote-mep vlan *vlan-id* level *level* mepid *mep-id***

Parameter

Parameter	Description	Value
vlan-id	Specifies a VLAN ID.	The value is an integer ranging from 1 to 4094.
level	Specifies an MEP level.	The value is an integer ranging from 0 to 7.
mep-id	Specifies a local MEP ID.	The value is an integer ranging from 1 to 8191.

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

Display the summary of all remote MEPs configured for the switch or the details of a remote MEP.

```

Switch>show y1731 remote-mep
Index Vlan  Level  RmepId RmepState  RmepType  RmepMac
1    1    3    2    ok      dynamic   00:04:67:59:09:09
2    1    6    2    ok      dynamic   00:04:67:59:09:09

Switch>show y1731 remote-mep vlan 1 level 6 mepid 2
Meg Vlan          : 1
Meg Level         : 6
Meg Icc           : v1
Meg Umc           : fh6
Remote Mep ID     : 2
Remote Mep State  : ok
Remote Mep Type   : dynamic
Remote Mep Mac    : 00:04:67:59:09:09
Remote Mep Chassis ID :
Remote Mep Interface Name : 10ge-1/0/2
Remote Mep Last Service State : unknown
Remote Mep Last Forward State : forwarded
Remote Mep Last Operate State : down
Remote Mep Life Time(sec) : 1000

```

```
Switch>
```

9.6.12 show y1731 trace-result

Function

The **show y1731 trace-result** command displays the results of the last query about fault locating for an MEP configured for the switch.

Format

show y1731 trace-result mep vlan *vlan-id* level *level* mepid *mep-id*

Parameter

Parameter	Description	Value
vlan-id	Specifies a VLAN ID.	The value is an integer ranging from 1 to 4094.
level	Specifies an MEP level.	The value is an integer ranging from 0 to 7.
mep-id	Specifies a local MEP ID.	The value is an integer ranging from 1 to 8191.

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

Display the results of the last query about fault locating for an MEP configured for the switch.

```
Switch>show y1731 trace-result mep vlan 1 level 6 mepid 2
```

```
-----
Hops Host      Mac           Ingr          IngrAct  RelayAct
          Forwarded   Engr          EngrAct   IsMep
-----
1           00:04:67:97:db:81  10ge-1/0/1    IngOk    RlyHit
          Not Forwarded  10ge-1/0/2    EgrDown  YES
Switch>
```

9.6.13 y1731 ping

Function

The **y1731 ping** command tests whether an Y.1731 fault occurs.

Format

- **y1731 ping all remote-mep vlan** *vlan-id* **level** *level* **mepid** *mep-id*
- **y1731 ping all remote-mep vlan** *vlan-id* **level** *level* **mepid** *mep-id* **-s** *packet-size* **-t** *packet-timeout*
- **y1731 ping all remote-mep vlan** *vlan-id* **level** *level* **mepid** *mep-id* **priority** *priority* **-s** *packet-size* **-t** *packet-timeout*
- **y1731 ping mac** *mac-address* **mep** *vlan* *vlan-id* **level** *level* **mepid** *mep-id*
- **y1731 ping mac** *mac-address* **mep** *vlan* *vlan-id* **level** *level* **mepid** *mep-id* **-c** *packet-count* **-s** *packet-size* **-t** *packet-timeout*
- **y1731 ping mac** *mac-address* **mep** *vlan* *vlan-id* **level** *level* **mepid** *mep-id* **priority** *priority* **-c** *packet-count* **-s** *packet-size* **-t** *packet-timeout*
- **y1731 ping remote-mep** *remote-mep-id* **mep** *vlan* *vlan-id* **level** *level* **mepid** *mep-id*
- **y1731 ping remote-mep** *remote-mep-id* **mep** *vlan* *vlan-id* **level** *level* **mepid** *mep-id* **-c** *packet-count* **-s** *packet-size* **-t** *packet-timeout*
- **y1731 ping remote-mep** *remote-mep-id* **mep** *vlan* *vlan-id* **level** *level* **mepid** *mep-id* **priority** *priority* **-c** *packet-count* **-s** *packet-size* **-t** *packet-timeout*

Parameter

Parameter	Description	Value
vlan-id	Specifies the VLAN ID to be mapped to an MA.	The value is an integer ranging from 1 to 4094.
level	Specifies an MA level.	The value is an integer ranging from 0 to 7.
mep-id	Specifies an MEP ID.	The value is an integer ranging from 1 to 8191.
remote-mep-id	Specifies a remote MEP ID.	The value is an integer ranging from 1 to 8191.
priority	Specifies a priority.	The value is an integer ranging from 0 to 7.
packet-size	Specifies the size of a sent ping packet, including the size of the L2 packet header.	The value is an integer ranging from 64 to 1518.
packet-timeout	Specifies the wait timeout duration of response packets.	The value is an integer ranging from 1 to 60.
packet-count	Specifies the times of ping.	The value is an integer ranging from 1 to 1024.

Default Value

NA

View

Privileged user view

Usage Guidelines

Use this command to test whether an Y.1731 fault occurs. The test is performed on the root node of the switch. To stop sending LBM packets, press **Ctrl+C**. If a local MEP in the up direction is associated with two or more MIPs, ensure that the network to which the MIPs are connected contains only one L2 data service channel (this is typically ensured by the STP protocol or an Ethernet ring protocol). Otherwise, the Y.1731 fault locating result is unpredictable.

Example

Test whether an Y.1731 fault occurs.

```
Switch#y1731 ping mac 00:04:67:97:db:81 mep vlan 1 level 6 mepid 2 -c 1024 -s 1518 -t 1
```

```
Pinging 00-04-67-97-db-81 with 1518 bytes of data:
```

```
Reply from 00-04-67-97-db-81: bytes=1518 time<1ms
```

```
Reply from 00-04-67-97-db-81: bytes=1518 time<1ms
```

```
Reply from 00-04-67-97-db-81: bytes=1518 time<1ms
```

```
Ping statistics for 00-04-67-97-db-81:
```

```
Packets: Sent = 3, Received = 3, Lost = 0 <0.00% loss>
```

```
Approximate round trip times in milliseconds:
```

```
Minimum = 0ms, Maximum = 0ms, Average = 0.00ms
```

```
Switch#
```

9.6.14 y1731 trace**Function**

The **y1731 trace** command locates any Y.1731 fault.

Format

- **y1731 trace mac** *mac-address* **mep vlan** *vlan-id* **level** *level* **mepid** *mep-id*
- **y1731 trace mac** *mac-address* **mep vlan** *vlan-id* **level** *level* **mepid** *mep-id* **-t** *packet-timeout*
- **y1731 trace mac** *mac-address* **mep vlan** *vlan-id* **level** *level* **mepid** *mep-id* **priority** *priority*
- **y1731 trace mac** *mac-address* **mep vlan** *vlan-id* **level** *level* **mepid** *mep-id* **priority** *priority* **t** *packet-timeout*

- **y1731 trace mac** *mac-address* **mep vlan** *vlan-id* **level** *level* **mepid** *mep-id* **priority** *priority* **ttl** *ttl-value*
- **y1731 trace mac** *mac-address* **mep vlan** *vlan-id* **level** *level* **mepid** *mep-id* **-ttl** *ttl-value*
- **y1731 trace remote-mep** *remote-mep-id* **mep vlan** *vlan-id* **level** *level* **mepid** *mep-id*
- **y1731 trace remote-mep** *remote-mep-id* **mep vlan** *vlan-id* **level** *level* **mepid** *mep-id* **-t** *packet-timeout*
- **y1731 trace remote-mep** *remote-mep-id* **mep vlan** *vlan-id* **level** *level* **mepid** *mep-id* **priority** *priority*
- **y1731 trace remote-mep** *remote-mep-id* **mep vlan** *vlan-id* **level** *level* **mepid** *mep-id* **priority** *priority* **-t** *packet-timeout*
- **y1731 trace remote-mep** *remote-mep-id* **mep vlan** *vlan-id* **level** *level* **mepid** *mep-id* **priority** *priority* **ttl** *ttl-value*
- **y1731 trace remote-mep** *remote-mep-id* **mep vlan** *vlan-id* **level** *level* **mepid** *mep-id* **ttl** *ttl-value*

Parameter

Parameter	Description	Value
mac-address	Specifies the MAC address of the remote MEP or MIP.	The value is in AA:BB:CC:DD:EE:FF format, where A to F are hexadecimal digits.
vlan-id	Specifies a VLAN ID.	The value is an integer ranging from 1 to 4094.
level	Specifies a level.	The value is an integer ranging from 0 to 7.
remote-mep-id	Specifies the MEP ID of a remote network bridge.	The value is an integer ranging from 1 to 8191.
mep-id	Specifies the MEP ID of the Trace action initiated by the local network bridge.	The value is an integer ranging from 1 to 8191.
priority	Specifies a priority.	The value is an integer ranging from 0 to 7.
packet-timeout	Specifies a wait timeout duration of response packets.	The value is an integer ranging from 1 to 60, in seconds. The default value is 5 seconds.
ttl-value	Specifies the maximum number of hops for Trace.	The value is an integer ranging from 1 to 255. The default value is 64.

Default Value

NA

View

Privileged user view

Usage Guidelines

Configure the Y.1731 fault locating to be performed on the root node of the device, and the trace result to be automatically displayed after the timeout interval is set. To terminate the trace operation in advance, press Ctrl+C. To associate with two or more local UP MEPs, ensure that the network connecting the MIP has only one L2 data service channel, which is generally guaranteed by the spanning tree or Ethernet ring protocol. Otherwise, the Y.1731 fault locating result is unpredictable.

Example

Locate the Y.1731 fault.

```
Switch#y1731 trace mac 00:04:67:97:db:81 mep vlan 1 level 6 mepid 2
Info: This operation will take some time.
Tracing the route to remote mep 0 over a maximum of 64 hops:
-----
Hops Host                Mac                Ingr                IngrAct  RelayAct
          Forwarded          Engr                EngrAct  IsMep
-----
1          00:04:67:97:db:81 10ge-1/0/1          IngOk     RlyHit
          Not Forwarded      10ge-1/0/2          EgrDown   YES
Switch#
```

9.6.15 y1731

Function

The **y1731** command allows access to the Y.1731 configuration view from the global configuration view.

Format

y1731

Parameter

NA

Default Value

NA

View

Global configuration view

Usage Guidelines

To configure the Y.1731 fault management, you must first run this command to enter the Y.1731 fault management configuration node.

Example

Access the Y.1731 configuration view from the global configuration view.

```
Switch#configure
    %Enter configuration commands.End with Ctrl+Z or command "quit" & "end"
Switch(config)#y1731
Switch(config-y1731)#
```

9.6.16 meg vlan level

Function

The **meg vlan level** command creates an MEG and access the MEG configuration view.

The **no meg vlan level** command deletes MEGs.

Format

- **meg vlan** *vlan-id* **level** *level* **icc** *icc-string* **umc** *umc-string*
- **no meg vlan** *vlan-id* **level** *level*

Parameter

Parameter	Description	Value
vlan-id	Specifies the VLAN ID corresponding to a single created MEG.	The value is an integer ranging from 1 to 4094.
level	Specifies an MEG level. A total of 8 levels are supported.	The value is an integer ranging from 0 to 7. By default, MEG levels are classified as follows: Three MEG levels are allocated for the customer role: 7, 6, and 5. Two MEG levels are allocated for the supplier role: 4 and 3. Three MEG levels are allocated for the carrier role: 2, 1, and 0.
icc-string	Specifies the International Telecommunication Union (ITU) carrier code (ICC).	The value is a string of less than six characters.
umc-string	Specifies the unique MEG ID code.	The value is a string of less than six characters.

Default Value

By default, no MEG is created in the system.

View

Y1731 configuration view

Usage Guidelines

For batch created MEGs, a pair of VLAN and level can map the unique MEG ID. Therefore, MEG ICCs and UMCs of the batch created MEGs can be automatically generated according to the VLAN and level, so as to determine the unique MEG ID. ICCs are automatically named in *v+vlan-id* format, while UMCs are automatically named in *fhn+level* format.

Example

Enable CC check for all MEPs of an MA.

```
Switch(config-y1731)#meg vlan 2 level 3 icc fhn1 umc fhn2
Switch(config-meg-fhn1-fhn2)#
```

9.6.17 no meg all**Function**

The **no meg all** command deletes all MEGs.

Format

no meg all

Parameter

NA

Default Value

NA

View

Y.1731 configuration view and MEG configuration view

Usage Guidelines

NA

Example

Delete all MEGs.

```
Switch(config-meg-fhn1-fhn2)#no meg all
Switch(config-meg-fhn1-fhn2)#
```

9.6.18 mip auto-config vlan

Function

The **mip auto-config vlan** command creates a VLAN mapping table automatically generated by MIP.

The **no mip auto-config vlan** command deletes the VLAN mapping table automatically created by the MIP.

Format

- **mip auto-config vlan** *vlan-list*
- **no mip auto-config vlan** *vlan-list*

Parameter

Parameter	Description	Value
vlan-list	Specifies the VLAN ID mapping the MEG.	The value is an integer ranging from 1 to 4094.

Default Value

NA

View

Y1731 configuration view

Usage Guidelines

Before running this command, run the **meg vlan level** command to create the MEG and the corresponding VLAN.

After running this command, the interface (the interface has been added to the VLAN specified by the VLANLIST) that specifies the VLANLIST label automatically creates or deletes the MIP node according to the VLAN mapping the MEG.

Switch series switches do not support automatic creation of Y.1731 and CFM MIPs at the same time.

Example

The VLAN mapping tables automatically generated during MIP creation are VLAN3, VLAN5, and VLAN6.

```
Switch(config)#y1731
Switch(config-y1731)#meg vlan 1,3,5-7 level 1
Switch(config-y1731)#mip auto-config vlan 3,5,6
Switch(config-y1731)#
```

9.6.19 snmp-trap

Function

The **snmp-trap** command enables or disables the SNMP alarm reporting function of Y.1731.

Format

snmp-trap { enable | disable }

Parameter

Parameter	Description	Value
enable	Enables the SNMP alarm reporting function of Y.1731.	-
disable	Disables the SNMP alarm reporting function of Y.1731.	-

Default Value

By default, the SNMP alarm reporting function of Y.1731 is disabled.

View

Y1731 configuration view

Usage Guidelines

NA

Example

Enable the SNMP alarm reporting function of Y.1731.

```
Switch(config)#y1731
Switch(config-y1731)#snmp-trap enable
Switch(config-y1731)#
```

9.6.20 y1731 mep vlan level mepid

Function

The **y1731 mep vlan level mepid** command creates MEPs.

The **no y1731 mep vlan level mepid** command deletes MEPs.

Format

- **y1731 mep vlan *vlan-id* level *level* mepid *mepid-id***
- **y1731 mep vlan *vlan-id* level *level* mepid *mepid-id* { inward | outward }**
- **no y1731 mep vlan *vlan-id* level *level* mepid *mepid-id***

Parameter

Parameter	Description	Value
vlan-id	Specifies the VLAN ID mapping the MEG.	The value is an integer ranging from 1 to 4094.
level	Specifies an MEG level.	The value is an integer ranging from 0 to 7.
inward	Specifies the MEP direction, which is the upper interface for Ethernet business flows.	-
outward	Specifies the MEP direction, which is the lower interface for Ethernet business flows.	The default MEP direction is outward.
mepid-id	Specifies a local MEP ID.	The value is an integer ranging from 1 to 8191.

Default Value

The default MEP direction is outward.

View

Interface configuration view (Trunk), Ethernet bridge interface configuration view, Ethernet routing interface configuration view

Usage Guidelines

The VLAN and level must be correctly mapping the MEG corresponding to the MEP. The default MEP direction is outward.

- The MIP and MEP in the same MEG cannot coexist in an interface.
- Only one MIP in the same MEG can exist in an interface.
- If the MIP or MEP of the CFM is configured in an interface, the MIP of Y.1731 cannot be configured in the interface any more.

Example

Create a MEP.

```
Switch(config-10ge1/0/1)#y1731 mep vlan 2 level 1 mepid 10 outward
Switch(config-10ge1/0/1)#
```

9.6.21 y1731 mep vlan level mepid ais

Function

The **y1731 mep vlan level mepid ais** command enables or disables the AIS function of the MEP.

Format

- **y1731 mep vlan *vlan-id* level *level* mepid *mep-id* ais { enable | disable }**
- **y1731 mep vlan *vlan-id* level *level* mepid *mep-id* ais priority *priority* { enable | disable }**

Parameter

Parameter	Description	Value
vlan-id	Specifies the VLAN ID mapping the MEG.	The value is an integer ranging from 1 to 4094.
level	Specifies an MEG level.	The value is an integer ranging from 0 to 7.
mep-id	Specifies a local MEP ID.	The value is an integer ranging from 1 to 8191.
priority	Specifies an AIS priority.	The value is an integer ranging from 0 to 7.

Default Value

By default, the AIS function of the MEP is disabled.

View

Interface configuration view (Trunk), Ethernet bridge interface configuration view, Ethernet routing interface configuration view

Usage Guidelines

The ETH-AIS Ethernet alarm indication signal uses a class-1 multicast MAC address to suppress alarms (Traps) after the service layer (sublayer) detects a connectivity fault. Transmission of the Y.1731 frame with ETH-AIS information is sent at the customer's MEG level when the MEP (or server MEP) detects a fault. The MEL of ETH-AIS is always higher than that of the MEP that sends the ETH-AIS information.

The general faults include:

- Abnormal signal in the case of ETH-CC execution in an MEG;
- AIS or LCK when ETH-CC is turned off in an MEG;

The first fault mainly includes:

- Loss of continuity (LOC) between any pair of MEPs in a MEG;
- Undesired connectivity between two MEGs (with error contained and different MEG IDs);
- Undesired connectivity between an MEG and an unrequired MEP (undesired MEP);
- Undesired MEG level (the local MEP detects a lower MEL for ETH-CC);
- Unexpected cycles (cycles of the local MEP and remote MEP in an MEG are inconsistent);

- ETH-CC hysteresis (the local MEP in an MEG receives its own ETH-CC information);

When ETH-CC is turned off in an MEG, the AIS or LCK generally needs to be triggered by other Ethernet link detection protocols. Currently, AIS can be triggered only after the IEEE 802.3ah discovery function fails.



Caution

For the two faults mentioned above, to meet the ETH-AIS transmission requirements, ensure that the interface of the MEP transmitting AIS is configured with an MIP with a level higher than the MEP level.

Before running this command, run the `meg vlan level` and `y1731 mep vlan level` commands to create an MEG and the corresponding MEP.

Example

Enable the AIS function of the MEP by using the gigabitEthernet 1/0/1 port.

```
Switch(config-10ge1/0/1)#y1731 mep vlan 3 level 1 mepid 1
Switch(config-10ge1/0/1)#y1731 mep vlan 3 level 1 mepid 1 ais priority 1 enable
Switch(config-10ge1/0/1)#
```

9.6.22 y1731 mep vlan level mepid ccm

Function

The **y1731 mep vlan level mepid ccm** command enables or disables the CCM detection of the MEP.

Format

- **y1731 mep vlan *vlan-id* level *level* mepid *mepid-id* ccm { enable | disable }**
- **y1731 mep vlan *vlan-id* level *level* mepid *mepid-id* ccm priority *priority* { enable | disable }**

Parameter

Parameter	Description	Value
vlan-id	Specifies the VLAN ID mapping the MEG.	The value is an integer ranging from 1 to 4094.
level	Specifies an MEG level.	The value is an integer ranging from 0 to 7.
mepid-id	Specifies a local MEP ID.	The value is an integer ranging from 1 to 8191.
enable	Enables the CCM detection of the MEP.	-

Parameter	Description	Value
disable	Disables the CCM detection of the MEP.	-
priority	Specifies a CCM priority.	The value is an integer ranging from 0 to 7.

Default Value

The default CCM priority is 6.

View

Interface configuration view (Trunk), Ethernet bridge interface configuration view, Ethernet routing interface configuration view

Usage Guidelines

NA

Example

Enable the CCM detection of the MEP, and configure the CCM detection priority to 2.

```
Switch(config-10ge1/0/1)#y1731 mep vlan 1 level 1 mepid 20 ccm priority 2 enable
Switch(config-10ge1/0/1)#
```

9.6.23 y1731 mep vlan level mepid mac

Function

The **y1731 mep vlan level mepid mac** command configures the MAC address of an MEP.

Format

y1731 mep vlan *vlan-id* **level** *level* **mepid** *mepid-id* **mac** *mac-address*

Parameter

Parameter	Description	Value
vlan-id	Specifies the VLAN ID mapping the MEG.	The value is an integer ranging from 1 to 4094.
level	Specifies an MEG level.	The value is an integer ranging from 0 to 7.
mepid-id	Specifies a local MEP ID.	The value is an integer ranging from 1 to 8191.
mac-address	Specifies the MAC address of an MEP.	The value is in AA:BB:CC:DD:EE:FF format, where A to F are hexadecimal digits.

Default Value

The default MEP direction is outward.

View

Interface configuration view (trunk) and Ethernet bridge interface configuration view

Usage Guidelines

NA

Example

Configure the MAC address of the MEP to 00:00:00:ee:ff:ab.

```
Switch(config-10ge1/0/1)#y1731 mep vlan 2 level 1 mepid 10 mac 00:00:00:ee:ff:ab
Switch(config-10ge1/0/1)#
```

9.6.24 y1731 mep vlan level mepid reset counter

Function

The **y1731 mep vlan level mepid reset counter** command clears the Y.1731 frame count of an MEG.

Format

y1731 mep vlan *vlan-id* **level** *level* **mepid** *mepid-id* **reset counter**

Parameter

Parameter	Description	Value
vlan-id	Specifies the VLAN ID mapping the MEG.	The value is an integer ranging from 1 to 4094.
level	Specifies an MEG level.	The value is an integer ranging from 0 to 7.
mepid-id	Specifies a local MEP ID.	The value is an integer ranging from 1 to 8191.

Default Value

NA

View

Interface configuration view (trunk) and Ethernet bridge interface configuration view

Usage Guidelines

The VLAN and level must be correctly mapping the MEG corresponding to the MEP. The default MEP direction is outward.

- The MIP and MEP in the same MEG cannot coexist in an interface.
- Only one MIP in the same MEG can exist in an interface.
- If the MIP or MEP of the CFM is configured in an interface, the MIP of Y.1731 cannot be configured in the interface any more.

Example

Clear the Y.1731 frame count of an MEG.

```
Switch(config-10ge1/0/1)#y1731 mep vlan 2 level 1 mepid 10 reset counter
Switch(config-10ge1/0/1)#
```

9.6.25 y1731 mep vlan level mepid service-type**Function**

The **y1731 mep vlan level mepid service-type** command configures the service mode of the MEP.

Format

y1731 mep vlan *vlan-id* **level** *level* **mepid** *mepid-id* **service-type** { **outofservice** | **inservice** }

Parameter

Parameter	Description	Value
outofservice	Specifies the out-of-service mode.	-
inservice	Specifies the in-service mode.	-
vlan-id	Specifies the VLAN ID mapping the MEG.	The value is an integer ranging from 1 to 4094.
level	Specifies an MEG level.	The value is an integer ranging from 0 to 7.
mepid-id	Specifies a local MEP ID.	The value is an integer ranging from 1 to 8191.

Default Value

Inservice

View

Interface configuration view (Trunk), Ethernet bridge interface configuration view, Ethernet routing interface configuration view

Usage Guidelines

NA

Example

Configure the service mode of the MEP to the out-of-service mode.

```
Switch(config-10ge1/0/1)#y1731 mep vlan 2 level 1 mepid 10 service-type outofservice
Switch(config-10ge1/0/1)#
```

9.6.26 y1731 mip vlan level**Function**

The **y1731 mip vlan level** command creates MIPs.

The **no y1731 mip vlan level** command deletes MIPs.

Format

- **y1731 mip vlan *vlan-id* level *level***
- **no y1731 mip vlan *vlan-id* level *level***

Parameter

Parameter	Description	Value
vlan-id	Specifies the VLAN ID to be mapped to an MA.	The value is an integer ranging from 1 to 4094.
level	Specifies an MEG level.	The value is an integer ranging from 0 to 7.

Default Value

NA

View

Interface configuration view (Trunk), Ethernet bridge interface configuration view, Ethernet routing interface configuration view

Usage Guidelines

The VLAN and level must be correctly mapping the MEG corresponding to the MEP.

- The MIP and MEP in the same MEG cannot coexist in an interface.
- Only one MIP in the same MEG can exist in an interface.
- If the MIP or MEP of the CFM is configured in an interface, the MIP of Y.1731 cannot be configured in the interface any more.

Example

Create an MIP.

```
Switch(config-10ge1/0/1)#y1731 mip vlan 2 level 3
Switch(config-10ge1/0/1)#
```

9.6.27 y1731 mip vlan level mac

Function

The **y1731 mip vlan level mac** command configures the MAC address of the MIP.

Format

y1731 mip vlan *vlan-id* **level** *level* **mac** *mac-address*

Parameter

Parameter	Description	Value
vlan-id	Specifies the VLAN ID mapping the MEG.	The value is an integer ranging from 1 to 4094.
level	Specifies an MEG level.	The value is an integer ranging from 0 to 7.
mac-address	Specifies the MAC address of an MEP.	The value is in AA:BB:CC:DD:EE:FF format, where A to F are hexadecimal digits.

Default Value

NA

View

Interface configuration view (Trunk), Ethernet bridge interface configuration view, Ethernet routing interface configuration view

Usage Guidelines

NA

Example

Configure the MAC address of the MIP to 00:00:00:ee:ff:ab.

```
Switch(config-10ge1/0/1)#y1731 mip vlan 2 level 3 mac 00:00:00:ee:ff:ab
Switch(config-10ge1/0/1)#
```

9.6.28 y1731 reset counter

Function

The **y1731 reset counter** command clears the Y.1731 frame count of the interface.

Format

y1731 reset counter

Parameter

NA

Default Value

NA

View

Interface configuration view (Trunk), Ethernet bridge interface configuration view, Ethernet routing interface configuration view

Usage Guidelines

NA

Example

Clear the Y.1731 frame count of the 10gigaethernet 1/0/1 interface.

```
Switch(config)#interface 10gigaethernet 1/0/1
Switch(config-10ge1/0/1)#y1731 reset counter
Switch(config-10ge1/0/1)#
```

9.6.29 ais {enable|disable}

Function

The **ais {enable|disable}** command enables or disables the AIS function of an MEG.

Format

ais { enable | disable }

Parameter

Parameter	Description	Value
enable	Enables the AIS function.	-
disable	Disables the AIS function.	-

Default Value

By default, the AIS function is not enabled in the system.

View

MEG configuration view

Usage Guidelines

NA

Example

Enable the AIS function.

```
Switch(config-meg-fhn1-fhn2)#ais enable
Switch(config-meg-fhn1-fhn2)#
```

9.6.30 ais loss-threshold

Function

The **ais loss-threshold** command configures the AIS loss threshold of the MEP.

Format

ais loss-threshold { *loss-threshold* | **default** }

Parameter

Parameter	Description	Value
loss-threshold	Specifies an AIS loss threshold.	The value is an integer ranging from 2 to 255.
default	Specifies the default AIS loss threshold.	3.5

Default Value

The default value is 3.5.

View

MEG configuration view

Usage Guidelines

For Y.1731, if the default MEP does not receive AIS (alarm indication signal) in 3.5 times the AIS transmission period, it is deemed that the AIS status disappears. If the default value is not used, the product of the threshold value and the AIS period received by the local MEP is the AIS loss time.

Example

Configure the AIS loss threshold of the MEP to 20.

```
Switch(config-meg-fhn1-fhn2)#ais loss-threshold 20
Switch(config-meg-fhn1-fhn2)#
```

9.6.31 ais-interval

Function

The **ais-interval** command configures the AIS transmission period of the MEP.

Format

ais-interval { **1s** | **1min** }

Parameter

Parameter	Description	Value
ais-interval	Specifies an AIS transmission period.	1s or 1 minute

Default Value

NA

View

MEG configuration view

Usage Guidelines

NA

Example

Configure the AIS transmission period of the MEP to 1 minute.

```
Switch(config-meg-fhn1-fhn2)#ais-interval 1min
Switch(config-meg-fhn1-fhn2)#
```

9.6.32 ccm {enable|disable}**Function**The **ccm {enable|disable}** command enables or disables the CCM function.**Format****ccm { enable | disable }****Parameter**

Parameter	Description	Value
enable	Enables the CCM function.	-
disable	Disables the CCM function.	-

Default Value

By default, the CCM function is not enabled in the system.

View

MEG configuration view

Usage Guidelines

NA

Example

Enable the CCM function.

```
Switch(config-meg-fhn1-fhn2)#ccm enable
```

```
Switch(config-meg-fhn1-fhn2)#
```

9.6.33 ccm loss-threshold

Function

The **ccm loss-threshold** command configures the CCM loss threshold of the MEP.

Format

ccm loss-threshold { *loss-threshold* | **default** }

Parameter

Parameter	Description	Value
loss-threshold	Specifies a CCM loss threshold.	The value is an integer ranging from 2 to 255.
default	Specifies the default CCM loss threshold.	3.5

Default Value

The default value is 3.5.

View

MEG configuration view

Usage Guidelines

NA

Example

Configure the CCM loss threshold of the MEP to 20.

```
Switch(config-meg-fhn1-fhn2)#ccm loss-threshold 20
Switch(config-meg-fhn1-fhn2)#
```

9.6.34 ccm-interval

Function

The **ccm-interval** command configures the CCM transmission period of the MEP.

Format

ccm-interval { **300Hz** | **10ms** | **100ms** | **1s** | **10s** | **1min** | **10min** | **default** }

Parameter

NA

Default Value

By default, the CCM transmission period is 1s.

View

MEG configuration view

Usage Guidelines

NA

Example

Configure the CCM transmission period of the MEP to 1 minute.

```
Switch(config-meg-fhn1-fhn2)#ccm-interval 1min
Switch(config-meg-fhn1-fhn2)#
```

9.6.35 cross-check {enable|disable}

Function

The **cross-check {enable|disable}** command enables or disables static RMEP verification.

Format

cross-check { enable | disable }

Parameter

Parameter	Description	Value
enable	Enables static RMEP verification.	-
disable	Disables static RMEP verification.	-

Default Value

NA

View

MEG configuration view

Usage Guidelines

NA

Example

Enable static RMEP verification.

```
Switch(config-meg-fhn1-fhn2)#cross-check enable
Switch(config-meg-fhn1-fhn2)#
```

9.6.36 cross-check start-delay

Function

The **cross-check start-delay** command configures the activation time of a static RMEP.

Format

cross-check start-delay { *start-delay-time* | **default** }

Parameter

Parameter	Description	Value
start-delay-time	Specifies the activation time of a static RMEP.	The value is an integer ranging from 1 to 65535, in seconds.
default	Specifies the default activation time.	0s

Default Value

By default, the activation time of a static RMEP is 0s.

View

MEG configuration view

Usage Guidelines

The default activation time of a static RMEP is 0s, indicating that it is immediately activated upon configuration.

Example

Configure the activation time of a static RMEP to 10s.

```
Switch(config-meg-fhn1-fhn2)#cross-check start-delay 10
Switch(config-meg-fhn1-fhn2)#
```

9.6.37 lock {enable|disable}

Function

The **lock {enable|disable}** command enables or disables the LCK function of an MEG.

Format

lock { **enable** | **disable** }

Parameter

Parameter	Description	Value
enable	Enables the LCK function of the MEG.	-

Parameter	Description	Value
disable	Disables the LCK function of the MEG.	-

Default Value

NA

View

MEG configuration view

Usage Guidelines

NA

Example

Enable the LCK function of the MEG.

```
Switch(config-meg-fhn1-fhn2)#lock enable
Switch(config-meg-fhn1-fhn2)#
```

9.6.38 lock loss-threshold**Function**The **lock loss-threshold** command configures the LCK loss threshold of the MEP.**Format****lock loss-threshold** { *loss-threshold* | **default** }**Parameter**

Parameter	Description	Value
loss-threshold	Specifies the LCK loss threshold.	The value is an integer ranging from 2 to 255.
default	Specifies the default LCK loss threshold.	3.5

Default Value

The default value is 3.5.

View

MEG configuration view

Usage Guidelines

NA

Example

Configure the LCK loss threshold of the MEP to 20.

```
Switch(config-meg-fhn1-fhn2)#lock loss-threshold 20
Switch(config-meg-fhn1-fhn2)#
```

9.6.39 lock-interval

Function

The **lock-interval** command configures the LCK transmission period of the MEP.

Format

lock-interval { **1s** | **1min** }

Parameter

NA

Default Value

NA

View

MEG configuration view

Usage Guidelines

NA

Example

Configure the LCK transmission period of the MEP to 1s.

```
Switch(config-meg-fhn1-fhn2)#lock-interval 1s
Switch(config-meg-fhn1-fhn2)#
```

9.6.40 no remote-mep all

Function

The **no remote-mep all** command deletes all RMEPs of an MEG.

Format

- **no remote-mep all**
- **no remote-mep mep-id *id-list* all**

Parameter

Parameter	Description	Value
id-list	Specifies the values of batch created RMEPs.	Each value is an integer. Multiple values are separated by hyphens (-).

Default Value

NA

View

MEG configuration view

Usage Guidelines

NA

Example

Delete all RMEPs of an MEG.

```
Switch(config-meg-fhn1-fhn2)#no remote-mep all
Switch(config-meg-fhn1-fhn2)#
```

9.6.41 no y1731 mep all**Function**The **no y1731 mep all** command deletes all MEPs of an MEG.**Format****no y1731 mep all****Parameter**

NA

Default Value

NA

View

MEG configuration view

Usage Guidelines

NA

Example

Delete all MEPs of an MEG.

```
Switch(config-meg-fhn1-fhn2)#no y1731 mep all
Switch(config-meg-fhn1-fhn2)#
```

9.6.42 no y1731 mip all

Function

The **no y1731 mip all** command deletes all MIPs of a specified MEG.

Format

no y1731 mip all

Parameter

NA

Default Value

NA

View

MEG configuration view

Usage Guidelines

NA

Example

Delete all MIPs of an MEG.

```
Switch(config-meg-fhn1-fhn2)#no y1731 mip all
Switch(config-meg-fhn1-fhn2)#
```

9.6.43 remote-mep aging-time

Function

The **remote-mep aging-time** command sets the dynamic RMEP aging time.

Format

remote-mep aging-time { *aging-time* | **default** }

Parameter

Parameter	Description	Value
aging-time	Specifies the aging time of a dynamic RMEP.	The value is an integer ranging from 1 to 65535, in seconds.

Parameter	Description	Value
default	Specifies the default value.	1000s

Default Value

The default value is 1000 seconds.

View

MEG configuration view

Usage Guidelines

NA

Example

Set the dynamic RMEP aging time to 3000s.

```
Switch(config-meg-fhn1-fhn2)#remote-mep aging-time 3000
Switch(config-meg-fhn1-fhn2)#
```

9.6.44 remote-mep mep-id mac

Function

The **remote-mep mep-id mac** command creates an RMEP.

Format

remote-mep mep-id *mep-id* **mac** *mac-address*

Parameter

Parameter	Description	Value
mep-id	Specifies an RMEP ID.	The value is an integer ranging from 1 to 8191.
mac-address	Specifies the MAC address of an RMEP.	The value is in dotted decimal notation, for example, AA:BB:CC:DD:EE:FF, where A to F are hexadecimal digits, ranging from 0 to 255.

Default Value

NA

View

MEG configuration view

Usage Guidelines

The MAC address is not used as a matching condition for ETH-CC to receive packets.

One RMEP or the list of RMEPs can be deleted as prompted.

Example

Create an RMEP.

```
Switch(config-meg-fhn1-f22)#remote-mep mep-id 2000-3000
Switch(config-meg-fhn1-f22)#
```

9.6.45 remote-mep mep-id

Function

The **remote-mep mep-id** command creates batch RMEPs.

The **no remote-mep mep-id** command deletes batch created RMEPs.

Format

- **remote-mep mep-id** *id-list*
- **no remote-mep mep-id** *id-list*

Parameter

Parameter	Description	Value
id-list	Specifies the values of batch created RMEPs.	Each value is an integer. Multiple values are separated by hyphens (-).

Default Value

NA

View

MEG configuration view

Usage Guidelines

Create RMEPs in batches according to the specified RMEP list. Theoretically, the number of RMEPs that can be created for an MEG in batches is equal to the maximum number (8190) of RMEPs supported by Y.1731, and the final number of RMEPs created will be equal to the number of entries in the input RMEP list as memory allows.

Example

Create RMEP 2000 to RMEP 3000 in batches

```
Switch(config-meg-fhn1-f22)#remote-mep mep-id 2000-3000
Switch(config-meg-fhn1-f22)#
```

9.6.46 reset counter

Function

The **reset counter** command clears the Y.1731 frame count of MEGs.

Format

reset counter

Parameter

NA

Default Value

NA

View

MEG configuration view

Usage Guidelines

You can run this command to clear the Y.1731 frame count of all MEGs.

Example

Clear the Y.1731 frame count of all MEGs.

```
Switch(config-y1731)#meg vlan 3 level 1 icc v3 umc fh1
Switch(config-meg-v3-fh1)#reset counter
Switch(config-meg-v3-fh1)#
```

9.6.47 senderid-tlv-type

Function

The **senderid-tlv-type** command configures the Sender ID TLV type of Y.1731 packets.

Format

senderid-tlv-type { **none** | **chassis** | **manage** | **chassis-manage** | **defer** }

Parameter

Parameter	Description	Value
none	Specifies that the sent Y.1731 packet does not contain the Sender ID TLV type.	-
chassis	Specifies that the sent Y.1731 packet contains Chassis ID information.	-
manage	Specifies that the sent Y.1731 packet contains address management information.	-
chassis-manage	Specifies that the sent Y.1731 packet contains the Chassis ID and address	-

Parameter	Description	Value
	management information.	
defer	Indicates that the Sender ID TLV content is determined by the MD management object.	-

Default Value

By default, the Sender ID TLV type is **none**, indicating that the Y.1731 packet does not contain the Sender ID TLV type.

View

MEG configuration view

Usage Guidelines

Currently, Switch does not support **manage**, **chassis-manage**, and **defer**.



Note

After the network management is configured to chassis-manage, the device adds the chassis field to the corresponding packet but does not add the manage field.

Example

Configure the Sender ID TLV type of the Y.1731 packet to **chassis**.

```
Switch(config-y1731)#meg vlan 3 level 1 icc v3 umc fh1
Switch(config-meg-v3-fh1)#senderid-tlv-type chassis
Switch(config-meg-v3-fh1)#
```

9.6.48 service-type

Function

The **service-type** command configure the service mode.

Format

service-type { **outofservice** | **inservice** }

Parameter

Parameter	Description	Value
outofservice	Specifies the out-of-service mode.	-
inservice	Specifies the in-service mode.	-

Default Value

Inservice

View

MEG configuration view

Usage Guidelines

NA

Example

Configure the service mode to the out-of-service mode.

```
Switch(config)#y1731
Switch(config-y1731)#meg vlan 3 level 1 icc v3 umc fh1
Switch(config-meg-v3-fh1)#service-type outofservice
Switch(config-meg-v3-fh1)#
```

9.6.49 trace-reply aging-time**Function**

The **trace-reply aging-time** command configures the aging time of the LTR reply.

Format

trace-reply aging-time { *aging-time* | **default** }

Parameter

Parameter	Description	Value
aging-time	Specifies the aging time of LTR response.	The value is an integer ranging from 1 to 65535.
default	Specifies the default aging time of the LTR reply.	1000s

Default Value

The default aging time of the LTR reply is 1000s.

View

MEG configuration view

Usage Guidelines

The aging time of the LTR reply is the holding time of the link path queried during last fault locating by an MEP. When the aging time arrives, the link path queried during last fault locating is automatically deleted.

Example

Configure the aging time of the LTR reply to 2000s.

```
Switch(config)#y1731
Switch(config-y1731)#meg vlan 3 level 1 icc v3 umc fh1
Switch(config-meg-v3-fh1)#trace-reply aging-time 2000
Switch(config-meg-v3-fh1)#
```

9.7 G.8032 Configuration Commands

9.7.1 debug g8032

Function

The **debug g8032** command enables G8032 debugging.

The **no debug g8032** command disables G8032 debugging.

Format

- **debug g8032 { in | out | packet | sm | timer | event | all }**
- **no debug g8032 { in | out | packet | sm | timer | event | all }**

Parameter

Parameter	Description	Value
timer	Indicates debugging information on the timer.	-
in	Indicates debugging information on packets received by the protocol.	-
out	Indicates debugging information on packets sent by the protocol.	-
packet	Indicates protocol packet debugging information.	-
event	Indicates debugging information on the event.	-
all	Indicates debugging information on preceding types.	-
sm	Specifies status machine debugging information.	

Default Value

By default, the G8032 debugging function is disabled.

View

Privileged user view

Usage Guidelines

NA

Example

Enable G8032 debugging.

```
Switch#debug g8032 in
Switch#
```

Disable G8032 debugging.

```
Switch#no debug g8032 out
Switch#
```

9.7.2 g8032**Function**

The **g8032** command allows access to the G8032 configuration view from the global configuration view.

Format**g8032****Parameter**

NA

Default Value

NA

View

Global configuration view

Usage Guidelines

NA

Example

Access the G8032 configuration view from the global configuration view.

```
Switch(config)#g8032
Switch(config-g8032)#
```

9.7.3 g8032 instance mip-port

Function

The **g8032 instance mip-port** command configures the interface as the MIP port of the virtual channel UP MEP of a G8032 instance.

Format

- **g8032 instance** *instance-num* **mip-port**
- **no g8032 instance** *instance-num* **mip-port**

Parameter

Parameter	Description	Value
instance-num	Specifies a G8032 instance number.	The value is an integer ranging from 1 to 128.

Default Value

NA

View

Ethernet bridge interface configuration view, Ethernet route interface configuration view, and Eth-trunk configuration view

Usage Guidelines

NA

Example

Configure the interface as the MIP port of the virtual channel UP MEP of the G8032 instance.

```
Switch(config-10ge1/0/1)#g8032 instance 1 mip-port
Switch(config-10ge1/0/1)#
```

9.7.4 g8032 instance {port1|port2}[Interface Configuration View]

Function

The **g8032 instance {port1|port2}** command configures the interface as port1 and port2 of the G8032 instance.

Format

- **g8032 instance** *instance-num* { **port1** | **port2** }
- **no g8032 instance** *instance-num* { **port1** | **port2** }

Parameter

Parameter	Description	Value
instance-num	Specifies a G8032 instance number.	The value is an integer ranging from 1 to 128.

Default Value

NA

View

Ethernet bridge interface configuration view, Ethernet route interface configuration view, and Eth-trunk configuration view

Usage Guidelines

NA

Example

Configure the interface as port1 of the G8032 instance.

```
Switch(config-10ge1/0/1)#g8032 instance 1 port1
Switch(config-10ge1/0/1)#
```

9.7.5 g8032 instance {add|remove} mip-port**Function**

The **g8032 instance add mip-port** command adds the MIP port of the virtual channel UP MEP of the G8032 instance.

The **g8032 instance remove mip-port** command deletes the MIP port of the virtual channel UP MEP of the G8032 instance.

Format

- **g8032 instance** *instance-num* **add mip-port** { **ethernet** | **xgigaethernet** | **10gigaethernet** | **25gigaethernet** | **40gigaethernet** | **100gigaethernet** } *mip-port-number*
- **g8032 instance** *instance-num* **add mip-port eth-trunk** *trunk-number*
- **g8032 instance** *instance-num* **remove mip-port** { **ethernet** | **xgigaethernet** | **10gigaethernet** | **25gigaethernet** | **40gigaethernet** | **100gigaethernet** } *mip-port-number*
- **g8032 instance** *instance-num* **remove mip-port eth-trunk** *trunk-number*

Parameter

Parameter	Description	Value
instance-num	Specifies a G8032 instance number.	The value is an integer ranging from 1 to 128.
mip-port -number	Specifies an Ethernet interface number.	The value is an integer in the range of <1-1>/<0-1>/<1-48> (For reference only. The specific value range depends on the slot number and card type).
trunk-number	Specifies the number of an aggregation interface.	The value is an integer ranging from 1 to 128.

Default Value

NA

View

G8032 configuration view

Usage Guidelines

NA

Example

Add the MIP port 10gigaethernet 1/01 of the virtual channel UP MEP of the G8032 instance.

```
Switch(config-g8032)#g8032 instance 1 add mip-port 10gigaethernet 1/01
Switch(config-g8032)#
```

9.7.6 g8032 instance {port1|port2}[G8032 Configuration View]

Function

The **g8032 instance {port1|port2}** command configures port1 and port2 of the G8032 instance.

The **no g8032 instance {port1|port2}** command deletes port1 and port2 of the G8032 instance.

Format

- **g8032 instance** *instance-num* { **port1** | **port2** } { **xgigaethernet** } *interface-number*
- **g8032 instance** *instance-num* { **port1** | **port2** } **eth-trunk** *trunk-number*
- **no g8032 instance** *instance-num* { **port1** | **port2** }

Parameter

Parameter	Description	Value
instance-num	Specifies a G8032 instance number.	The value is an integer ranging from 1 to 128.
interface-number	Specifies an Ethernet interface	The value is an integer in the range of

Parameter	Description	Value
	number.	<1-1>/<0-1>/<1-48> (For reference only. The specific value range depends on the slot number and card type).
trunk-number	Specifies the number of an aggregation interface.	The value is an integer ranging from 1 to 128.

Default Value

NA

View

G8032 configuration view

Usage Guidelines

NA

Example

Configure port1 of the G8032 instance.

```
Switch(config-g8032)#g8032 instance 1 port1 gigabernet 1/0/1
Switch(config-g8032)#
```

9.7.7 g8032 instance {port1|port2} fs**Function**The **g8032 instance {port1|port2} fs** command forces exchange for a port in the G8032 instance.**Format****g8032 instance** *instance-number* { **port1** | **port2** } **fs****Parameter**

Parameter	Description	Value
instance-number	Specifies a G8032 instance number.	The value is an integer ranging from 1 to 128.

Default Value

NA

View

G8032 configuration view

Usage Guidelines

NA

Example

Configure forced exchange for the G8032 instance.

```
Switch(config)#g8032
Switch(config-g8032)#g8032 instance 1 channel 1
Switch(config-g8032)#g8032 instance 1 port1 10gigaethernet 1/0/1
Switch(config-g8032)#g8032 instance 1 port1 fs
Switch(config-g8032)#
```

9.7.8 g8032 instance {port1|port2} ms

Function

The **g8032 instance {port1|port2} ms** command implements manual exchange for a port in the G8032 instance.

Format

g8032 instance *instance-number* { **port1** | **port2** } **ms**

Parameter

Parameter	Description	Value
instance-number	Specifies an instance number.	The value is an integer ranging from 1 to 128.

Default Value

NA

View

G8032 configuration view

Usage Guidelines

NA

Example

Configure manual exchange for the G8032 instance.

```
Switch(config-g8032)#g8032 instance 2 port1 ms
Switch(config-g8032)#
```

9.7.9 g8032 instance channel

Function

The **g8032 instance channel** command configures the control channel of the G8032 instance.

Format

g8032 instance *instance-number* **channel** *channel-number*

Parameter

Parameter	Description	Value
instance-number	Specifies an instance number.	The value is an integer ranging from 1 to 128.
channel-number	Specifies a control channel number.	The value is an integer ranging from 1 to 4094.

Default Value

NA

View

G8032 configuration view

Usage Guidelines

NA

Example

Configure the control channel number of the G8032 instance to 1.

```
Switch(config-g8032)#g8032 instance 1 channel 1
Switch(config-g8032)#
```

9.7.10 g8032 instance clear

Function

The **g8032 instance clear** command clears the G8032 instance status.

Format

g8032 instance *instance-number* **clear**

Parameter

Parameter	Description	Value
instance-num	Specifies a G8032 instance number.	The value is an integer ranging from 1 to 128.

Default Value

NA

View

G8032 configuration view

Usage Guidelines

NA

Example

Clear the status of G8032 instance 1.

```
Switch(config-g8032)#g8032 instance 1 clear
Switch(config-g8032)#
```

9.7.11 g8032 instance mel

Function

The **g8032 instance mel** command configures the protocol channel level of the G8032 instance.

Format

g8032 instance *instance-num* **mel** *mel-num*

Parameter

Parameter	Description	Value
instance-num	Specifies a G8032 instance number.	The value is an integer ranging from 1 to 128.
mel-num	Specifies the protocol channel level of a G8032 instance.	The value is an integer ranging from 0 to 7.

Default Value

NA

View

G8032 configuration view

Usage Guidelines

NA

Example

Configure the protocol channel level of the G8032 instance to level 6.

```
Switch(config-g8032)#g8032 instance 1 mel 6
Switch(config-g8032)#
```

9.7.12 g8032 instance mode

Function

The **g8032 instance mode** command configures the node mode of the G8032 instance to recoverable or unrecoverable.

Format

g8032 instance *instance-number* **mode** { **revertive** | **non-revertive** }

Parameter

Parameter	Description	Value
instance-number	Specifies an instance number.	The value is an integer ranging from 1 to 128.
(revertive non-revertive)	Specifies the node mode of the G8032 instance, which can be recoverable or unrecoverable.	-

Default Value

revertive

View

G8032 configuration view

Usage Guidelines

NA

Example

View the login information and configure device user information.

```
Switch(config-g8032)#g8032 instance 1 mode revertive
Switch(config-g8032)#
```

9.7.13 g8032 instance role

Function

The **g8032 instance role** command configures the node role of the G8032 instance.

Format

g8032 instance *instance-number* **role** { **rpl-owner-node** | **neighbor** | **none** }

Parameter

Parameter	Description	Value

Parameter	Description	Value
instance-number	Specifies an instance number.	The value is an integer ranging from 1 to 128.
(rpl-owner-node neighbor none)	Specifies the node role of the G8032 instance.	-

Default Value

NA

View

G8032 configuration view

Usage Guidelines

NA

Example

Configure the node role of the G8032 instance to rpl-owner-node.

```
Switch(config-g8032)#g8032 instance 1 role rpl-owner-node
Switch(config-g8032)#
```

9.7.14 g8032 instance rpl**Function**The **g8032 instance rpl** command configures the RPL port of the G8032 instance.**Format****g8032 instance** *instance-number* **rpl** { **port1** | **port2** | **none** }**Parameter**

Parameter	Description	Value
instance-number	Specifies an instance number.	The value is an integer ranging from 1 to 128.
(port1 port2 none)	Specifies the RPL port of the G8032 instance.	-

Default Value

NA

View

G8032 configuration view

Usage Guidelines

NA

Example

Configure the RPL port of the G8032 instance to port1.

```
Switch(config-g8032)#g8032 instance 1 rpl port1
Switch(config-g8032)#
```

9.7.15 g8032 instance vc-holdoff-timer**Function**

The **g8032 instance vc-holdoff-timer** command configures the time (in milliseconds) of the holdoff timer for the G8032 instance virtual channel.

Format

g8032 instance *instance-num* **vc-holdoff-timer** { *vc-holdoff-timer* | **default** }

Parameter

Parameter	Description	Value
instance-num	Specifies a G8032 instance number.	The value is an integer ranging from 1 to 128.
vc-holdoff-timer	Specifies the time of the holdoff timer, in milliseconds.	The value is an integer ranging from 0 to 10000.
default	Specifies the default value.	0 ms

Default Value

0 ms

View

G8032 configuration view

Usage Guidelines

NA

Example

Configure the time of the holdoff timer for the G8032 instance virtual channel to 100 ms.

```
Switch(config-g8032)#g8032 instance 1 vc-holdoff-timer 100
Switch(config-g8032)#
```

9.7.16 g8032 instance vc-mel

Function

The **g8032 instance vc-mel** command configures the virtual channel level of the G8032 instance.

Format

g8032 instance *instance-num* **vc-mel** *vc -mel-num*

Parameter

Parameter	Description	Value
instance-num	Specifies a G8032 instance number.	The value is an integer ranging from 1 to 128.
vc-mel-num	Specifies the virtual channel level of a G8032 instance.	The value is an integer ranging from 0 to 7.

Default Value

NA

View

G8032 configuration view

Usage Guidelines

NA

Example

Configure the virtual channel level of the G8032 instance to level 1.

```
Switch(config-g8032)#g8032 instance 1 vc-mel 1
Switch(config-g8032)#
```

9.7.17 g8032 instance vc-mep {port1|port2|none}

Function

The **g8032 instance vc-mep {port1|port2|none}** command configures the MEP port of the G8032 instance virtual channel.

Format

g8032 instance *instance-num* **vc-mep** { **port1** | **port2** | **none** }

Parameter

Parameter	Description	Value
instance-num	Specifies a G8032 instance number.	The value is an integer ranging from 1 to 128.

Default Value

NA

View

G8032 configuration view

Usage Guidelines

NA

Example

Configure the MEP port of the G8032 instance virtual channel to port1.

```
Switch(config-g8032)#g8032 instance 1 vc-mep port1
Switch(config-g8032)#
```

9.7.18 g8032 instance version**Function**The **g8032 instance version** command configures the version number of the G8032 instance.**Format****g8032 instance** *instance-number* **version** { **v1** | **v2** }**Parameter**

Parameter	Description	Value
instance-number	Specifies an instance number.	The value is an integer ranging from 1 to 128.

Default Value

v2

View

G8032 configuration view

Usage Guidelines

NA

Example

Configure the version number of the G8032 instance to v1.

```
Switch(config-g8032)#g8032 instance 4 version v1
Switch(config-g8032)#
```

9.7.19 g8032 instance virtual-channel

Function

The **g8032 instance virtual-channel** command configures the virtual channel of the G8032 instance.

Format

g8032 instance *instance-number* **virtual-channel** *virtual-channel-number*

Parameter

Parameter	Description	Value
instance-number	Specifies an instance number.	The value is an integer ranging from 1 to 128.
virtual-channel-number	Specifies the virtual channel number of the G8032 instance.	The value is an integer ranging from 0 to 4094.

Default Value

NA

View

G8032 configuration view

Usage Guidelines

This command configures 0 to delete the virtual channel.

Example

Configure the virtual channel number of the G8032 instance to 1.

```
Switch(config-g8032)#g8032 instance 1 virtual-channel 1
Switch(config-g8032)#
```

9.7.20 g8032 instance vlan

Function

The **g8032 instance vlan** command configures the VLAN list mapping the G8032 instance.

The **no g8032 instance vlan** command deletes the VLAN list mapping the G8032 instance.

Format

- **g8032 instance** *instance-number* **vlan** *vlan-list*
- **no g8032 instance** *instance-number* **vlan** *vlan-list*

Parameter

Parameter	Description	Value
instance-number	Specifies an instance number.	The value is an integer ranging from 1 to 128.
vlan-list	Specifies a VLAN list.	The value is a character string, for example, 1, 3, and 5-10.

Default Value

NA

View

G8032 configuration view

Usage Guidelines

NA

Example

Configure the VLAN list mapping the G8032 instance.

```
Switch(config-g8032)#g8032 instance 1 vlan 1,3,5-10
Switch(config-g8032)#
```

Delete the VLAN list mapping the G8032 instance.

```
Switch(config-g8032)#no g8032 instance 1 vlan 1,3,5-10
Switch(config-g8032)#
```

9.7.21 g8032 instance wtr-timer

Function

The **g8032 instance wtr-timer** command configures the WTR timer period of the G8032 instance.

Format

g8032 instance *instance-number* **wtr-timer** { *wtr-timer* | **default** }

Parameter

Parameter	Description	Value
instance-number	Specifies an instance number.	The value is an integer ranging from 1 to 128.
wtr-timer	Specifies the WTR timer period of a G8032 instance.	The value is an integer ranging from 1 to 12, in minutes.
default	Specifies the default value.	5 minutes

Default Value

By default, the WTR timer period of the G8032 instance is 5 minutes.

View

G8032 configuration view

Usage Guidelines

NA

Example

Configure the WTR timer period of the G8032 instance to 10 minutes.

```
Switch(config-g8032)#g8032 instance 1 wtr-timer 10
Switch(config-g8032)#
```

9.7.22 g8032 instance guard-timer**Function**

The **g8032 instance guard-timer** command configures the Guard-Timer period of the G8032 instance.

Format

g8032 instance *instance-number* **guard-timer** { *guard-timer* | **default** }

Parameter

Parameter	Description	Value
instance-number	Specifies an instance number.	The value is an integer ranging from 1 to 128.
guard-timer	Specifies the period of the Guard-Timer.	The value is an integer ranging from 10 to 2000, in milliseconds.
default	Specifies the default value of the timer.	500 ms

Default Value

By default, the Guard-Timer period of the G8032 instance is 500 ms.

View

G8032 configuration view

Usage Guidelines

NA

Example

Configure the Guard-Timer period of the G8032 instance to 1000 ms.

```
Switch(config-g8032)#g8032 instance 1 guard-timer 1000
Switch(config-g8032)#
```

9.7.23 g8032 instance hold-off-timer

Function

The **g8032 instance hold-off-timer** command configures the Hold-off-Timer period of the G8032 instance.

Format

g8032 instance *instance-number* **hold-off-timer** { *hold-off-timer* | **default** }

Parameter

Parameter	Description	Value
instance-number	Specifies an instance number.	The value is an integer ranging from 1 to 128.
hold-off-timer	Specifies the period of the Hold-off-Timer.	The value is an integer ranging from 0 to 10000, in milliseconds.
default	Specifies the default value.	0 ms

Default Value

By default, the Hold-off-Timer period of the G8032 instance is 0 ms.

View

G8032 configuration view

Usage Guidelines

NA

Example

Configure the Hold-off-Timer period of the G8032 instance to 2000 ms.

```
Switch(config-g8032)#g8032 instance 1 hold-off-timer 2000
Switch(config-g8032)#
```

9.7.24 g8032 trap {enable|disable}

Function

The **g8032 trap {enable|disable}** command enables or disables the G8032 alarm function.

Format

g8032 trap { **enable** | **disable** }

Parameter

Parameter	Description	Value
enable	Enables the G8032 alarm function.	-
disable	Disables the G8032 alarm function.	-

Default Value

Disable

View

G8032 configuration view

Usage Guidelines

NA

Example

Enable the G8032 alarm function.

```
Switch(config-g8032)#g8032 trap enable
Switch(config-g8032)#
```

9.7.25 g8032 vs-switch {enable|disable}**Function**

The **g8032 vs-switch {enable|disable}** command enables or disables the virtual link switchover switch.

Format

g8032 vs-switch { enable | disable }

Parameter

Parameter	Description	Value
enable	Enables the virtual link switchover switch.	-
disable	Disables the virtual link switchover switch.	-

Default Value

NA

View

G8032 configuration view

Usage Guidelines

The value `disable` is recommended when the topology consists of multiple loops. It is not configured when the topology consists of only one loop.

Example

Enable the virtual link switchover switch.

```
Switch(config-g8032)#g8032 vs-switch enable
Switch(config-g8032)#
```

9.7.26 no g8032 instance

Function

The **no g8032 instance** command deletes G8032 instances.

Format

no g8032 instance *instance-num*

Parameter

Parameter	Description	Value
instance-num	Specifies a G8032 instance number.	The value is an integer ranging from 1 to 128.

Default Value

NA

View

G8032 configuration view

Usage Guidelines

NA

Example

Delete the G8032 instance 1.

```
Switch(config-g8032)#no g8032 instance 1
Switch(config-g8032)#
```

9.7.27 show g8032

Function

The **show g8032** command displays all information about the G8032 instance.

Format

show g8032**Parameter**

NA

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

Display all information about the G8032 instance.

```
Switch>show g8032
g8032 trap:enable
g8032 vs-switch:disable
Switch>
```

9.7.28 show g8032 instance**Function**The **show g8032 instance** command displays information about a G8032 instance or all instances.**Format**

- **show g8032 instance** *instance-num*
- **show g8032 instance**

Parameter

Parameter	Description	Value
instance-num	Specifies a G8032 instance number.	The value is an integer ranging from 1 to 128.

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

Display information about the G8032 instance 1.

```
Switch>show g8032 instance 1
g8032 trap:enable
g8032 vs-switch:disable
      g8032 instance is not exist.
Switch>
```

Display information about all G8032 instances.

```
Switch>show g8032 instance
g8032 trap:enable
g8032 vs-switch:disable
Switch>
```

9.7.29 show g8032 instance interface**Function**The **show g8032 instance** command displays interface information on G8032 instances.**Format**

- **show g8032 instance** *instance-num* **interface**
- **show g8032 instance interface**

Parameter

Parameter	Description	Value
instance-num	Specifies a G8032 instance number.	The value is an integer ranging from 1 to 128.

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

Display interface information on G8032 instances.

```
Switch>show g8032 instance interface
Instance Interface      Type      Operate   Forward   Rx-Count  Tx-Count
1      [1]10ge-1/0/2      rpl       working   blocking   0          50
1      [2]10ge-1/0/2      normal    working   forwarding 0          50
Switch>
```

9.7.30 show g8032 interface

Function

The **show g8032 interface** command displays interface information on G8032 instances.

Format

show g8032 interface

Parameter

NA

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

Display interface information on G8032 instances.

```
Switch>show g8032 interface
Instance Interface      Type      Operate   Forward   Rx-Count  Tx-Count
1      [1]10ge-1/0/1      normal    working   forwarding 0          0
Switch>
```

9.8 UDLD Configuration Commands

9.8.1 debug udld

Function

The **debug udld** command enables the UDLD debugging function.

The **no debug udld** command disables the UDLD debugging function.

Format

- **debug udld { config | rx | tx | pkt | timer | all }**

Parameter

NA

Default Value

Disable

View

Privileged user view

Usage Guidelines

NA

Example

Enable UDLD debugging.

```
Switch#debug udld all
Switch#
```

9.8.2 udld work-mode

Function

The **udld work-mode** command configures the working mode of the one-way link detection.

Format

- **udld work-mode { normal | aggressive }**

Parameter

Parameter	Description	Value
normal	Specifies the normal mode.	-
aggressive	Specifies the aggressive mode.	-

Default Value

By default, the working mode is normal.

View

Global configuration view

Usage Guidelines

NA

Example

Configure the working mode of the one-way link detection.

```
Switch(config)#udld work-mode aggressive
Switch(config)#
```

9.8.3 udld uni-shutdown

Function

The **udld uni-shutdown** command configures the shutdown mode of one-way channel interface.

Format

- **udld uni-shutdown { manual | auto }**

Parameter

Parameter	Description	Value
manual	Specifies the manual closing mode.	-
auto	Specifies the automatic closing mode.	-

Default Value

By default, the closing mode is auto.

View

Global configuration view

Usage Guidelines

NA

Example

Configure the closing mode of one-way channel interface.

```
Switch(config)#udld uni-shutdown manual
Switch(config)#
```

9.8.4 udld advertise-interval

Function

The **udld advertise-interval** command configures the sending interval of advertisement packets.

Format

- **udld advertise-interval** { *adver-interval* | **default** }

Parameter

Parameter	Description	Value
adver-interval	Specifies the sending interval of advertisement packets.	The value is an integer ranging from 2 to 15, in seconds.
default	Specifies the default sending interval of advertisement packets.	7 seconds

Default Value

7 seconds

View

Global configuration view

Usage Guidelines

NA

Example

Configure the sending interval of advertisement packets.

```
Switch(config)#udld advertise-interval 8
```

```
Switch(config)#
```

9.8.5 udld {enable|disable}

Function

The **udld {enable|disable}** command enables or disables the UDLD protocol of an interface.

Format

- **udld** { **enable** | **disable** }

Parameter

Parameter	Description	Value
enable	Enables the UDLD protocol of an interface.	-
disable	Disables the UDLD protocol of an interface.	-

Default Value

By default, the UDLD protocol of an interface is disabled.

View

Interface configuration view (Ethernet), interface group configuration view

Usage Guidelines

NA

Example

Enable the UDLD protocol of an interface.

```
Switch(config-10ge1/0/1)#udld enable
Switch(config-10ge1/0/1)#
```

9.8.6 udld aggressive {enable|disable}

Function

The **udld aggressive {enable|disable}** command enables or disables the UDLD aggressive mode of an interface.

Format

- **udld aggressive { enable | disable }**

Parameter

Parameter	Description	Value
enable	Enables the UDLD aggressive mode of an interface.	-
disable	Disables the UDLD aggressive mode of an interface.	-

Default Value

By default, the UDLD aggressive mode of an interface is disabled.

View

Interface configuration view (Ethernet), interface group configuration view

Usage Guidelines

NA

Example

Enable the UDLD aggressive mode of an interface.

```
Switch(config-10ge1/0/1)#udld aggressive enable
Switch(config-10ge1/0/1)#
```


9.8.7 udld cisco-checksum {enable|disable}

Function

The **udld cisco-checksum {enable|disable}** command enables or disables the verification code type of an interface.

Format

- **udld cisco-checksum { enable | disable }**

Parameter

Parameter	Description	Value
enable	Enables the UDLD aggressive mode of an interface.	-
disable	Disables the UDLD aggressive mode of an interface.	-

Default Value

By default, the verification code type of an interface is disabled.

View

Interface configuration view (Ethernet), interface group configuration view

Usage Guidelines

NA

Example

Disable the verification code type of an interface.

```
Switch(config-10ge1/0/1)#udld cisco-checksum enable
Switch(config-10ge1/0/1)#
```

9.8.8 show udld local

Function

The **show udld local** command shows UDLD local information.

Format

- **show udld local**

Parameter

NA

Default Value

NA

View

Common user view, privileged user view, global configuration view

Usage Guidelines

NA

Example

Display the UDLD local information.

```
Switch(config)#show udld local
Switch(config)#
```

9.8.9 show udld interface**Function**The **show udld interface** command shows UDLD interface information.**Format**

- **show udld interface**

Parameter

NA

Default Value

NA

View

Common user view, privileged user view, global configuration view

Usage Guidelines

NA

Example

Display the UDLD interface information.

```
Switch(config)#show udld interface
Switch(config)#
```

9.8.10 show udld peer

Function

The **show udld peer** command shows UDLD peer information.

Format

- **show udld peer**

Parameter

NA

Default Value

NA

View

Common user view, privileged user view, global configuration view

Usage Guidelines

NA

Example

Display the UDLD peer information.

```
Switch(config)#show udld peer
UDLD Peer information:
  Interface : ge-1/0/2
  Mac address: 0000:0102:5666
  Peer State : bidirectional
  Peer Device Id : 000001025666
  Peer Port Id : GigabitEthernet1/0/2
  Peer Device Name :
  Peer Message Interval : 7
  Peer Timeout Interval : 5
  Peer Expire Time : 17
Switch(config)#
```

9.8.11 show udld config

Function

The **show udld config** command shows UDLD configuration information.

Format

- **show udld config**

Parameter

NA

Default Value

NA

View

Common user view, privileged user view, global configuration view

Usage Guidelines

NA

Example

Display UDLD configuration on the switch.

```
Switch(config)#show udld config
Version                               :UDLD_VB3.00.05.00
  udld uni-shutdown manual
  udld advertise-interval 8
  interface ge-1/0/1
  udld enable
Switch(config)#
```

Chapter 10 Device Management Commands

Introduces the commands used for device management.

10.1 Hardware Configuration Commands

10.1.1 debug fan

Function

The **debug fan** command turns on the fan debugging switch.

The **no debug fan** command turns off the fan debugging switch.

Format

- **debug fan**
- **no debug fan**

Parameter

NA

Default Value

NA

View

Privileged user view

Usage Guidelines

NA

Example

Turn on the fan debugging switch.

```
Switch#debug fan
Switch#
```

10.1.2 cpu low-threshold high-threshold

Function

The **cpu low-threshold high-threshold** command configures the upper and lower thresholds of the CPU utilization.

Format

cpu { *slot-number/cpu-number* | **all** } **low-threshold** { *low-threshold* | **default** } **high-threshold** { *high-threshold* | **default** }

Parameter

Parameter	Description	Value
slot-number	Specifies a slot number.	The value is an integer ranging from 1 to 1.
cpu-number	Specifies a CPU number.	The value is an integer ranging from 1 to 1.
all	Indicates all CPUs.	-
low-threshold	Specifies the lower threshold of the CPU utilization.	The value is an integer ranging from 0 to 100.
high-threshold	Specifies the upper threshold of the CPU utilization.	The value is an integer ranging from 1 to 100.

Default Value

The default upper limit of CPU usage is 80.

View

Global configuration view

Usage Guidelines

When the CPU usage is below the lower limit, the switch triggers a monitoring alarm if monitoring and alarm reporting are enabled.

The default value is recommended. If the lower limit is too high, the system frequently reports alarms. If the lower limit is too low, you cannot learn the CPU usage in a timely manner.

Example

Configure the upper and lower thresholds of the CPU utilization to 70 and 50 respectively.

```
Switch(config)#cpu all low-threshold 50 high-threshold 70
Switch(config)#
```

10.1.3 cpu trap

Function

The **cpu trap** command enables or disables CPU alarm reporting.

Format

cpu { *cpu-number* | **all** } **trap** { **enable** | **disable** }

Parameter

Parameter	Description	Value
cpu-number	Specifies a CPU number.	<1-1>/<1-1> indicates the slot number and CPU number.
all	Indicates all CPUs.	-
enable	Enables the CPU alarm reporting function.	-
disable	Disables the CPU alarm reporting function.	-

Default Value

By default, the CPU alarm reporting function is enabled.

View

Global configuration view

Usage Guidelines

Generally, this command is used together with the **cpu monitor** command.

Example

Enable CPU alarm reporting.

```
Switch(config)#cpu all trap enable
Switch(config)#
```

10.1.4 cpu monitor

Function

The **cpu monitor** command enables or disables the CPU monitoring function.

Format

cpu monitor { **enable** | **disable** }

Parameter

Parameter	Description	Value

Parameter	Description	Value
enable	Enables the CPU monitoring function.	-
disable	Disables the CPU monitoring function.	-

Default Value

By default, CPU monitoring is enabled.

View

Global configuration view

Usage Guidelines

NA

Example

Disable the CPU monitoring function.

```
Switch(config)#cpu monitor disable
Switch(config)#
```

10.1.5 fanctrl level

Function

The **fanctrl level** command configures the fan control levels of the device.

Format

fanctrl { *fan-number* | **all** } **level** { *fan-level* | **default** }

Parameter

Parameter	Description	Value
fan-number	Specifies a fan number.	The value is an integer ranging from 1 to 2.
fan-level	Specifies a fan level range.	The value is an integer ranging from 1 to 7.

Default Value

By default, the fan level of the device is 4.

View

Global configuration view

Usage Guidelines

NA

Example

Configure the fan control level of the device to 2.

```
Switch(config)#fanctrl all level 2
Switch(config)#
```

10.1.6 fanctrl low-threshold high-threshold**Function**

The **fanctrl low-threshold high-threshold** command configures the thresholds of the fan rotation speed.

Format

fanctrl { *fan-number* | **all** } **low-threshold** { *low-threshold* | **default** } **high-threshold** { *high-threshold* | **default** }

Parameter

Parameter	Description	Value
fan-number	Specifies a fan number.	The value is an integer ranging from 1 to 2.
all	Specifies all fans.	-
low-threshold	Specifies the lower threshold of the fan rotation speed.	The value is an integer ranging from 1000 to 8000.
high-threshold	Specifies the upper threshold of the fan rotation speed.	The value is an integer ranging from 8000 to 25000.

Default Value

By default, the upper threshold of temperature is set to 25000, and the lower threshold is set to 1000.

View

Global configuration view

Usage Guidelines

When the fan rotation speed is higher than the upper threshold or lower than the lower threshold specified by this command, the system triggers a monitoring alarm upon monitoring and alarm reporting enabled. The default value is recommended.

Example

Configure the lower threshold of the fan rotation speed to 1500 and the upper threshold to 8000.

```
Switch(config)#fanctrl all low-threshold 1500 high-threshold 8000
```

```
Switch(config)#
```

10.1.7 fanctrl mode

Function

The **fanctrl mode** command configures the fan control mode of a device.

Format

fanctrl { *fan-number* | **all** } **mode** { **speed-level** | **standard-temperature-control** }

Parameter

Parameter	Description	Value
speed-level	Specifies a fixed rotation speed.	-
standard-temperature-control	Specifies a temperature control.	-
fan-number	Specifies a fan number.	The value is an integer ranging from 1 to 2.
all	Specifies all fans.	-

Default Value

standard-temperature-control

View

Global configuration view

Usage Guidelines

NA

Example

Configure the fan control mode of the device to rotation at a fixed speed.

```
Switch(config)#fanctrl all mode speed-level
Switch(config)#
```

10.1.8 fanctrl trap

Function

The **fanctrl tap** command enables or disables the alarm reporting function for fan control.

Format

fanctrl { *fan-number* | **all** } **trap** { **enable** | **disable** }

Parameter

Parameter	Description	Value
fan-number	Specifies a fan number.	The value is an integer ranging from 1 to 2.
all	Specifies all fans.	-
enable	Enables the alarm reporting function for fan control.	-
disable	Disables the alarm reporting function for fan control.	-

Default Value

By default, the fan alarm reporting function is enabled.

View

Global configuration view

Usage Guidelines

Generally, this command is used together with the `fanctrl monitor` command.

Example

Disable the alarm reporting function for fan control.

```
Switch(config)#fanctrl all trap disable
Switch(config)
```

10.1.9 fanctrl monitor**Function**

The **fanctrl monitor** command enables or disables the fan control monitoring function of a device.

Format

fanctrl monitor { enable | disable }

Parameter

Parameter	Description	Value
enable	Enables the fan control monitoring function of a device.	-
disable	Disables the fan control monitoring function of a device.	-

Default Value

By default, the fan control monitoring function of a device is enabled.

View

Global configuration view

Usage Guidelines

This command is generally used with the `fanctrl trap` command to implement the device fan monitoring function for users.

Example

Disable the fan control monitoring function of a device.

```
Switch(config)#fanctrl monitor disable
Switch(config)
```

10.1.10 power trap

Function

The **power trap** command enables or disables the power alarm reporting function.

Format

power { *power-number* | **all** } **trap** { **enable** | **disable** }

Parameter

Parameter	Description	Value
power-number	Specifies a power number.	The value is an integer in the range of 1-1/1-2.
all	Specifies all power supplies.	-
enable	Enables the power alarm reporting function.	-
disable	Disables the power alarm reporting function.	-

Default Value

By default, power alarm reporting is enabled.

View

Global configuration view

Usage Guidelines

This command is used with the **power monitor** command.

Example

Disable the power alarm reporting function.

```
Switch(config)#power all trap disable
```

```
Switch(config)
```

10.1.11 power monitor

Function

The **power monitor** command enables or disables the power monitoring function.

Format

power monitor { **enable** | **disable** }

Parameter

Parameter	Description	Value
enable	Enables power monitoring.	-
disable	Disables power monitoring.	-

Default Value

By default, power monitoring is enabled.

View

Global configuration view

Usage Guidelines

NA

Example

Disable power monitoring.

```
Switch(config)#power monitor disable
Switch(config)
```

10.1.12 memory low-threshold high-threshold

Function

The **memory high-threshold** command configures the upper and lower thresholds of the device memory usage.

Format

memory { *memory-pool-number* | **all** } **low-threshold** { *low-threshold* | **default** } **high-threshold** { *high-threshold* | **default** }

Parameter

Parameter	Description	Value
memory-pool-number	Specifies the slot number of a service cable.	The value is an integer in the range of <1-1>/<1-2>.
high-threshold	Specifies the upper threshold of the memory usage.	The value is an integer ranging from 1 to 100.
low-threshold	Specifies the lower threshold of the memory usage.	The value is an integer ranging from 0 to 100.

Default Value

By default, the upper and lower thresholds of the memory usage are 90 and 1 respectively.

View

Global configuration view

Usage Guidelines

When the memory usage is higher than the upper threshold or lower than the lower threshold specified by this command, the system triggers a monitoring alarm upon monitoring and alarm reporting enabled. The default value is recommended.

Example

Configure the upper and lower thresholds of the memory usage to 70 and 50 respectively.

```
Switch(config)# memory 1/1 low-threshold 50 high-threshold 70
Switch(config)#
```

10.1.13 memory trap

Function

The **memory tap** command enables or disables the memory alarm reporting function of a device.

Format

memory { *memory-pool-number* | **all** } **trap** { **enable** | **disable** }

Parameter

Parameter	Description	Value
memory-pool-number	Specifies the slot number of a service cable.	<1-1> and <1-2> indicate the slot number and memory pool number respectively.
all	Specifies all memory pools.	-
enable	Enables power alarm reporting.	-
disable	Disables power alarm reporting.	-

Default Value

By default, the memory alarm reporting function is enabled.

View

Global configuration view

Usage Guidelines

Generally, this command is used together with the memory monitor command.

Example

Disable the memory alarm reporting function.

```
Switch(config)#memory 1/1 trap enable
Switch(config)#
```

10.1.14 memory monitor**Function**

The **memory monitor** command enables or disables the memory monitoring function of a device.

Format

memory monitor { **enable** | **disable** }

Parameter

Parameter	Description	Value
enable	Enables the memory monitoring function of a device.	-
disable	Disables the memory monitoring function of a device.	-

Default Value

By default, the memory monitoring function of a device is enabled.

View

Global configuration view

Usage Guidelines

This command is generally used with the memory trap command to implement the memory usage monitoring function of a device for users.

Example

Disable the memory monitoring function of a device.

```
Switch(config)#memory monitor disable
Switch(config)#
```

10.1.15 show cpu configure

Function

The **show cpu configure** command displays the current CPU configuration on the switch.

Format

show cpu configure

Parameter

NA

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

Display the current CPU configuration.

```
Switch>show cpu configure
!
cpu monitor disable
Switch>
```

10.1.16 show cpu statistic

Function

The **show cpu statistic** command displays CPU usage statistics.

Format

show cpu statistic

Parameter

NA

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

Display CPU usage statistics.

```
Switch> show cpu statistic
CPU statistics information:
  CPU monitor: enable
  CPU index: Cpu-1/1
  CPU current usage: 3.20%
  CPU utilization last-5sec: 3.20%, last-1min: 3.31%, last-5min :3.37%
  Max CPU usage: 33.00%
  Max CPU usage stat time: 2018-04-09 10:52:32
  State: normal
  High threshold: 80%, Low threshold : 0%
Service Name      UseRate      MaxUseRate      MaxUseTime
(uspdriver)       2.14%        2.44%           2018-04-09 11:23:44
(uspuienet)       0.24%        0.94%           2018-04-09 11:22:24
(uspdevm)         0.24%        0.34%           2018-04-09 11:24:34
(uspdevice)       0.24%        0.64%           2018-04-09 11:22:24
(uspnmagent)      0.09%        0.44%           2018-04-09 11:24:29
(uspmam)          0.04%        0.09%           2018-04-09 11:22:24
(uspmstp)         0.04%        0.09%           2018-04-09 11:24:59
(uspdot1x)        0.04%        0.04%           2018-04-09 11:25:09
Switch>
```

10.1.17 show fan

Function

The **show fan** command displays the fan state.

Format

show fan

Parameter

NA

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

Display the fan state.

Switch> show fan										
Fan information:										
Fan monitor: enable										
Mode:(FS: fixed-speed, TC: temperature-control, ETC: enhance-temperature-control										
STC: standard-temperature-control, SL: speed-level, AUTO: auto-mode										
Ctrl	Module	Fan	LT	HT	Mode	Speed	Level	Trap	Present	Descr
1			1000	25000	STC	--	--	enable	--	--
	1/1		--	--	--	4592	1	--	YES	FAN-1/1
		1/1/1	--	--	--	--	--	--	--	--
2			1000	25000	STC	--	--	enable	--	--
	2/1		--	--	--	3936	1	--	YES	FAN-2/1
		2/1/1	--	--	--	--	--	--	--	--
Switch>										

10.1.18 show memory pool

Function

The **show memory pool** command displays the memory usage of the currently used cards.

Format

show memory pool

Parameter

NA

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

View the CLI module memory usage on this card of the device.

Switch>show memory pool

Memory pool information:

Memory pool monitor: enable

Memory pool: Memory-1/1

Memory description: memory-1/1

Memory type: Ram

Total memory : 3784760 KB

Total memory used: 1746636 KB

Current usage : 46.20%

Max usage : 46.21%

Trap state : enable

Status : normal

High threshold : 90%, Low threshold : 1%

ServiceName	MemUsage(Kb)	MaxMemUsage(Kb)	MaxMemUseTime
uspdriver	266752	266752	2000-02-10 20:52:28
uspuinet	216076	216076	2000-02-10 22:12:33
usphwrt	83560	83560	2000-02-10 20:51:38
uspmam	64156	64156	2000-02-10 20:51:38
uspnmagent	49412	49412	2000-02-11 05:00:37
uspospfv3	30192	30192	2000-02-10 20:51:38
usparpprobe	27436	27436	2000-02-10 20:51:38
uspl3vpn	23352	23352	2000-02-10 20:51:38
uspacl	22584	22584	2000-02-10 20:51:37
uspnnetconf	20792	20792	2000-02-10 20:51:37
uspmvrp	20192	20192	2000-02-10 20:51:37
uspmstp	15228	15228	2000-02-10 20:51:37
uspdevice	14740	14740	2000-02-10 20:51:37
uspdevm	13784	13784	2000-02-10 20:51:37
uspportisolate	13424	13424	2000-02-10 20:51:37

uspvlanmapping	13088	13088	2000-02-10 20:51:37
usproutepolicy	12776	12776	2000-02-10 20:51:37
uspstormcontrol	12644	12644	2000-02-10 20:51:37
uspvrrp	12232	12232	2000-02-10 20:51:37
usplldp	12200	12200	2000-02-10 20:51:47
uspbpdutunnel	12156	12156	2000-02-10 20:51:37
usptelemetry	12036	12036	2000-02-10 20:51:37
uspqinq	12016	12016	2000-02-10 20:51:37
uspdhcpsnooping	11924	11924	2000-02-10 20:51:37
uspdhcpclient	11644	11644	2000-02-10 20:51:37
usptimerange	11620	11620	2000-02-10 20:51:37
usplacp	11548	11548	2000-02-10 20:51:37
usphwmc	11492	11492	2000-02-10 20:51:37
usprlink	11480	11480	2000-02-10 20:51:37
uspppoeplus	11468	11468	2000-02-10 20:51:37
uspbgp	10892	10892	2000-02-10 20:51:37
uspdropbear	10852	10852	2000-02-10 20:51:38
uspdhcpv6	10844	10844	2000-02-10 20:51:38
uspqueue	10828	10828	2000-02-10 20:51:38
uspmldsnooping	10828	10828	2000-02-10 20:51:38
uspdiffserv	10816	10816	2000-02-10 20:51:38
uspmirror	10812	10812	2000-02-10 20:51:38
usntp	10812	10812	2000-02-10 20:51:38
uspigmp	10796	10796	2000-02-10 20:51:38
usppolicyroute	10784	10784	2000-02-10 20:51:38
usrip	10784	10784	2000-02-10 20:51:38
uspsis	10784	10784	2000-02-10 20:51:38
uspsmartinstall	10776	10776	2000-02-10 20:51:38
uspigmpsnooping	10772	10772	2000-02-10 20:51:38
uspddm	10768	10768	2000-02-10 20:51:38
uspwred	10760	10760	2000-02-10 20:51:38
uspsoa	10760	10760	2000-02-10 20:51:38
usppim	10756	10756	2000-02-10 20:51:38
uspprotovlan	10748	10748	2000-02-10 20:51:38
uspiptsg	10744	10744	2000-02-10 20:51:38
uspstormsuppres	10740	10740	2000-02-10 20:51:38
usphwvp	10736	10736	2000-02-10 20:51:38
uspudd	10732	10732	2000-02-10 20:51:38
uspdot1ag	10732	10732	2000-02-10 20:51:38
uspy1731	10732	10732	2000-02-10 20:51:37
uspdot3ah	10732	10732	2000-02-10 20:51:37
uspospfv2	10732	10732	2000-02-10 20:51:37
uspdosantiattac	10728	10728	2000-02-10 20:51:37

uspflush	10728	10728	2000-02-10 20:51:37
uspalb	10728	10728	2000-02-10 20:51:37
uspmad	10724	10724	2000-02-10 20:51:37
usplinkflap	10716	10716	2000-02-10 20:51:37
uspiss	10716	10716	2000-02-10 20:51:37
uspscheduleprof	10712	10712	2000-02-10 20:51:37
uspmacvlan	10712	10712	2000-02-10 20:51:37
uspdot1x	10712	10712	2000-02-10 20:51:37
uspg8032	10704	10704	2000-02-10 20:51:37
uspmld	10692	10692	2000-02-10 20:51:37
usppim6	10688	10688	2000-02-10 20:51:37
uspvct	10684	10684	2000-02-10 20:51:37
uspbfd	10684	10684	2000-02-10 20:51:37
uspvtp	10676	10676	2000-02-10 20:51:37
uspaaa	10676	10676	2000-02-10 20:51:37
uspdid	10676	10676	2000-02-10 20:51:37
uspdhcp	10672	10672	2000-02-10 20:51:37
uspevpn	10668	10668	2000-02-10 20:51:37
uspmلاغ	10664	10664	2000-02-10 20:51:37
uspbshell	10664	10664	2000-02-10 20:51:38
usppatch	10660	10660	2000-02-10 20:51:38
uspmلاغ	10660	10660	2000-02-10 20:51:38
uspipvlan	10644	10644	2000-02-10 20:51:38
uspcfx	10608	10608	2000-02-10 20:51:38
system	31304	33960	2000-02-10 21:01:28

Memory pool: Memory-1/2

Memory description: Flash-1/1

Memory type: Flash

Total memory : 3392564 KB

Total memory used: 1318616 KB

Current usage : 38.89%

Max usage : 38.89%

Trap state : enable

Status : normal

High threshold : 95%, Low threshold : 1%

Switch>

10.1.19 show temperature

Function

The **show temperature** command displays temperature of all cards.

Format

show temperature

Parameter

NA

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

Display temperature of all cards.

```
Switch>show temperature
Temperature information:
Temperature monitor: enable
  Index          CurrValue L-Threshold H-Threshold  Status  Trap      Descr
*  Temper-1/0/1    54      -10         82       normal  enable    Sensor Temperature
Switch>
```

10.1.20 show temperature config

Function

The **show temperature config** command displays temperature configuration of the switch in the configuration file.

Format

show temperature config

Parameter

NA

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

Display the temperature configuration of the switch in the configuration file.

```
Switch>show temperature config
!
temperature 1/0/1 low-threshold -40 high-threshold 100
Switch>
```

10.1.21 temperature low-threshold high-threshold

Function

The **temperature low-threshold high-threshold** command configures the upper and lower thresholds of the switch temperature.

Format

temperature { *temperature-number* | **all** } **low-threshold** { *low-threshold* | **default** }
high-threshold { *high-threshold* | **default** }

Parameter

Parameter	Description	Value
temperature-number	Specifies a temperature number.	The value is an integer in the range of <1-1>/<0-0>/<1-1>.
all	Indicates all temperature.	-
low-threshold	Specifies the lower threshold of the temperature.	The value is an integer ranging from -60 to 30.
high-threshold	Specifies the upper threshold of the temperature.	The value is an integer ranging from 30 to 150.

Default Value

By default, the lower temperature threshold is -10°C, and the upper temperature threshold is 68°C.

View

Global configuration view

Usage Guidelines

When the temperature is higher than the upper threshold or lower than the lower threshold specified by this command, the system triggers device restart.

Example

Configure the upper and lower thresholds of the switch temperature to 58°C and 20°C respectively.

```
Switch(config)#temperature all low-threshold 20 high-threshold 58
Switch(config)#
```

10.1.22 temperature trap

Function

The **temperature trap** command enables or disables the temperature alarm reporting function of a device.

Format

temperature { *temperature-number* | **all** } **trap** { **enable** | **disable** }

Parameter

Parameter	Description	Value
temperature-number	Specifies a temperature number.	<1-1>/<0-0>/<1-1> indicates the slot number, daughter card number, and temperature controller number.
all	Indicates all temperature.	-
enable	Enables temperature alarm reporting.	-
disable	Disables temperature alarm reporting.	-

Default Value

By default, the temperature alarm reporting function of a device is enabled.

View

Global configuration view

Usage Guidelines

Generally, this command is used together with the temperature monitor command.

Example

Disable temperature alarm reporting.

```
Switch(config)#temperature all trap disable
Switch(config)#
```


10.1.23 temperature monitor

Function

The **temperature monitor** command enables or disables temperature monitoring.

Format

temperature monitor { enable | disable }

Parameter

Parameter	Description	Value
enable	Enables temperature monitoring.	-
disable	Disables temperature monitoring.	-

Default Value

By default, temperature monitoring is enabled.

View

Global configuration view

Usage Guidelines

Generally, this command is used together with the temperature trap command to monitor the switch temperature.

Example

Disable temperature monitoring.

```
Switch(config)#temperature monitor disable
Switch(config)#
```

10.1.24 show cpu

Function

The **show cpu** command displays CPU usage statistics and configuration.

Format

show cpu

Parameter

NA

Default Value

NA

View

Common user view

Usage Guidelines

You can use this command to check the usage and configuration of CPUs on the main control board and all line cards of the switch.

Example

Display CPU usage statistics and configuration.

Switch>show cpu								
CPU information:								
CPU monitor: enable								
Index	CurrUse	MaxUse	L-Threshold	H-Threshold	Status	Trap	Descr	
* Cpu-1/1	3.55%	26.80%	0%	80%	normal	enable	CPU-1/1	
Switch>								

10.1.25 show fanctrl config

Function

The **show fanctrl config** command displays the fan control configuration information.

Format

show fanctrl config

Parameter

NA

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

Display the fan control configuration information.

```
Switch>show fanctrl config
Switch>
```

10.1.26 show power

Function

The **show power** command shows the power status of a switch.

The **show power config** command shows the power configuration information on a switch.

Format

- **show power**
- **show power config**

Parameter

NA

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

View the power status of a switch.

```
Switch>show power
Power information:
  Power monitor: enable
  Present: YES(power supply in) or NO(power out of position)
  Mode: DC(dc power) or AC(ac power) or N/A(power not available)
-----
-----
      Index      Status      Trap      Fuse      Present(Volt)  Mode(Ampere)  Voltage(Watts)
Current(Watts)  ActualPower  RatedPower  Descr      Serial
-----
-----
```

* Power-1/1	underflow	enable	normal	YES	DC	0	0	0
550	PWR-1/1							
* Power-1/2	normal	enable	normal	YES	DC	12	11	143
550	PWR-1/2							
Switch>								

10.1.27 show system chassis

Function
The show system chassis command shows the system chassis information.
Format
show system chassis
Parameter
NA
Default Value
NA
View
Common user view
Usage Guidelines
NA
Example
View the system chassis information.
Switch>show system chassis
Switch>

10.1.28 show hwmc l2 forwarding-table

Function
The show hwmc l2 forwarding-table command shows the HWMC management level-2 forwarding table.
Format
● show hwmc l2 forwarding-table ● show hwmc l2 forwarding-table vlan <i>vlan-id</i>

Parameter

Parameter	Description	Value
vlan-id	Specifies a VLAN ID.	The value is an integer ranging from 1 to 4094.

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

View the HWMC management level-2 forwarding table.

```
Switch>show hwmc l2 forwarding-table
L2 Current Number: 0
L2 Max Number:    2048
Switch>
```

10.1.29 show hwmc l3 forwarding-table**Function**

The **show hwmc l3 forwarding-table** command displays the HWMC management level-3 forwarding table.

Format

- **show hwmc l3 forwarding-table**
- **show hwmc l2 forwarding-table vpn-instance *name***

Parameter

Parameter	Description	Value
name	VPN instance name	The value is a character string.

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

View the HWMC management level-3 forwarding table.

```
Switch>show hwmc l3 forwarding-table
L3 Current Number: 0
L3 Max Number:    2048
Switch>
```

10.2 Mirror Configuration Commands

10.2.1 debug mirror

Function

The **debug mirror** command enables mirroring debugging.

The **no debug mirror** command disables mirroring debugging.

Format

- **debug mirror**
- **no debug mirror**

Parameter

NA

Default Value

By default, mirroring debugging is disabled.

View

Privileged user view

Usage Guidelines

You can use this command to debug mirroring functions and identify mirroring faults.

Example

Enable mirroring debugging.

```
Switch#debug mirror
Switch#
```

Disable mirroring debugging.

```
Switch#no debug mirror
Switch#
```

10.2.2 mirror group (Local Mirror)

Function

The **mirror group** command configures a local mirror group and an observing interface.

The **no mirror group** command deletes a local mirror group and an observing interface.

Format

- **mirror group** *groupnum* { **ethernet** | **xgigaethernet** | **10xgigaethernet** | **25gigaethernet** | **40gigaethernet** | **100gigaethernet** } *interface-number*
- **mirror group** *groupnum* **eth-trunk** *trunk-number*
- **no mirror group** *groupnum* { **ethernet** | **xgigaethernet** | **10xgigaethernet** | **25gigaethernet** | **40gigaethernet** | **100gigaethernet** } *interface-number*
- **no mirror group** *groupnum* **eth-trunk** *trunk-number*
- **no mirror group** [*groupnum1*]

Parameter

Parameter	Description	Value
groupnum	Specifies a mirror group ID.	The value is an integer ranging from 1 to 4.
interface-number	Specifies the number of the Ethernet interface used as an observation port.	The value is an integer in the range of <1-1>/<0-1>/<1-48>.
trunk-number	Specifies the number of the aggregation port used as an observation port.	The value is an integer ranging from 1 to 128.

Default Value

By default, the local observing group and observing interface are not configured.

View

Global configuration view

Usage Guidelines

When the observing interface and observed interface (source interface of mirroring) are on the same device, you can use this command to configure a local mirror group and observing interface.

If an interface is designated as an observing interface, do not make other configurations on this interface. Otherwise, the mirror function may be affected.

To change a local observing interface to a remote observing interface, you must delete the original configuration and then configure the interface again.

Example

Configure the local mirror group and its observation port to 25gigaethernet1/0/1.

```
Switch(config)#mirror group 1 25gigaethernet 1/0/1
Switch(config)#
```

10.2.3 mirror group (Remote Mirror)

Function

The **mirror group** command configures the remote mirror group and its observation port.

The **no mirror group** command deletes the configured remote mirror group and its observation port.

Format

- **mirror group** *groupnum* { **ethernet** | **xgigaethernet** | **10gigaethernet** | **25gigaethernet** | **40gigaethernet** | **100gigaethernet** } *interface-number* **rspan** *vlan-id*
- **mirror group** *groupnum* { **ethernet** | **xgigaethernet** | **10gigaethernet** | **25gigaethernet** | **40gigaethernet** | **100gigaethernet** } *interface-number* **rspan** *vlan-id* **tpid** { **standard** | *protocol-id* }
- **mirror group** *groupnum* **eth-trunk** *trunk-number* **rspan** *vlan-id*
- **mirror group** *groupnum* **eth-trunk** *trunk-number* **rspan** *vlan-id* **tpid** { **standard** | *protocol-id* }
- **no mirror group** [*groupnum1*]

Parameter

Parameter	Description	Value
groupnum	Specifies a mirror group ID.	The value is an integer ranging from 1 to 4.
interface-number	Specifies a remote observation port.	The value is an integer in the range of <1-1>/<0-1>/<1-48>.
vlan-id	Specifies a VLAN ID.	The value is an integer ranging from 1

Parameter	Description	Value
		to 4094.
protocol-id	Indicates the label protocol identifier of the outer tag of the current interface.	The value is a hexadecimal number ranging from 0x0 to 0xffff.
standard	Specifies a standard value.	0x8100
trunk-number	Specifies the number of a Trunk interface.	The value is an integer ranging from 1 to 128.

Default Value

By default, the remote mirror group and its observation port are not configured for the system.

View

Global configuration view

Usage Guidelines

When the observation port and the observed port (mirror source port) are not on the same device but are connected over the network (level-2 or level-3 network), you can run this command to configure the remote mirror group and its observation port.

The remote observation port can be connected by a VLAN. The command contains the **rspan** keyword, which is applicable to monitor the connection between the host and the device of the observation port over the level-2 network.

To modify the observation port, run the **no mirror group** command to delete the configuration and then reconfigure it.

Example

Configure the VLAN-based remote observation port to gigabitEthernet1/0/1 and the mirror VLAN to 100.

```
Switch(config)#mirror group 3 gigabitEthernet 1/0/1 rspan 100
Switch(config)#
```

10.2.4 mirror {ingress|egress|both} group

Function

The **mirror {ingress|egress|both} group** command sets the mirroring function on an interface.

The **no mirror {ingress|egress|both} group** command cancels the mirroring function on an interface.

Format

- **mirror** { **ingress** | **egress** | **both** } **group** *group-id*
- **no mirror** { **ingress** | **egress** | **both** } **group** *group-id*

Parameter

Parameter	Description	Value
ingress	Mirrors the inbound packets in the interface.	-
egress	Mirrors the outbound packets in the interface.	-
both	Mirrors the outbound and inbound packets in the interface.	-
group-id	Specifies the serial number in the mirror group list.	The value is an integer ranging from 1 to 4.

Default Value

By default, the mirroring function is disabled on an interface.

View

Ethernet bridge interface configuration view, Ethernet route interface configuration view, interface configuration view (trunk), and Peerlink configuration view

Usage Guidelines

After an interface is configured as the source interface of mirroring, packets passing through this interface are mirrored to the observing interface specified by the mirror group. To prevent packet loss, you are advised to configure the same type and bandwidth for the observing interface and observed interface.

Example

Mirror inbound packets in the 10gigaethernet1/0/1 interface.

```
Switch(config)#interface 10gigaethernet 1/0/1
Switch(config-10ge1/0/1)#mirror ingress group 3
Switch(config-10ge1/0/1)#
```

10.2.5 show mirror config

Function

The **show mirror config** command displays the mirroring configuration on the switch.

Format

show mirror config

Parameter

NA

Default Value

NA

View

Common user view

Usage Guidelines

This command does not show L2, L3, and local mirroring information simultaneously. The initialized information is 0.

Example

Display mirroring configuration.

```
Switch>show mirror config
Version : MIRROR_VX2.10.00.00
  mirror group 1 gigabitEthernet 1/0/1
interface ge-1/0/5
  mirror ingress group 1
Switch>
```

10.2.6 show mirror group**Function**

The **show mirror group** command displays mirror group information on the switch.

Format

show mirror group

Parameter

NA

Default Value

NA

View

Common user view

Usage Guidelines

This command does not show L2, L3, and local mirroring information simultaneously. The initialized information is 0.

Example

Display mirror group information.

```
Switch>show mirror group
Mirror group 1 is set to interface ge-1/0/1
Mirror group type: Local

Switch>
```

10.2.7 show mirror interface

Function

The **show mirror interface** command displays interface mirroring usage on the switch.

Format

show mirror interface

Parameter

NA

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

Display interface mirroring usage.

```
Switch>show mirror interface

Interface   Mac-address/Mask   Mirror-group   Direction
-----
ge-1/0/5    ----              1              ingress

Switch>
```

10.3 Log Management Commands

10.3.1 show syslog

Function

The **show syslog config** command displays the syslog server configuration file.

The **show syslog server** command displays syslog server information.

Format

- **show syslog config**
- **show syslog server**

Parameter

NA

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

View the configuration file information on the syslog server.

```
Switch>show syslog config
!
syslog server 223.1.10.206
Switch>
```

10.3.2 syslog facility

Function

The **syslog facility** command specifies the system function log protocol.

Format

syslog facility { kernel | user | mail | system-daemons | security-authorization1 | syslogd | line-printer | network-news | uucp | clock-daemon | security-authorization2 | ftp | ntp | log-audit | log-alert | note2 | local0 | local1 | local2 | local3 | local4 | local5 | local6 | local7 }

Parameter

Parameter	Description	Value
kernel	Specifies the kernel message.	-
user	Specifies the user-level message.	-
mail	Specifies the main system.	-
system-daemons	Specifies the system program.	-
security-authorization1	Specifies the security or authorization message.	-
syslogd	Specifies the system log generation message.	-
Line-printrt	Specifies the queued printing subsystem.	-
network-news	Specifies the network news subsystem.	-
uucp	Specifies the UUCP subsystem.	-
clock-daemon	Specifies the clock program.	-
security-authorization2	Specifies the security or authorization message.	-
ftp	Specifies the FTP program.	-
ntp	Specifies the NTP subsystem.	-
log-audit	Specifies log auditing.	-
log-alert	Specifies log alerting.	-
note2	Specifies the clock program.	-
local0	Specifies the local use 0.	-
local1	Specifies the local use 1.	-
Local2	Specifies the local use 2.	-
Local3	Specifies the local use 3.	-
Local4	Specifies the local use 4.	-
Local5	Specifies the local use 5.	-
Local6	Specifies the local use 6.	-
Local7	Specifies the local use 7.	-

Default Value

By default, the user-level message is used.

View

Global configuration view

Usage Guidelines

This command can specify a function log protocol of a system.

Example

Specify the kernel message log protocol of the syslog server.

```
Switch(config)#syslog facility kernel
Switch(config)#
```

10.3.3 syslog server

Function

The **syslog server** command configures a syslog server.

The **no syslog server** command deletes a syslog server.

Format

- **syslog server** *ipv4-address* [**vpn-instance** *instance-name*]
- **syslog server** *ipv4-address server-port* [**vpn-instance** *instance-name*]
- **syslog6 server** *ipv6-address* [**vpn-instance** *instance-name*]
- **syslog6 server** *ipv6-address server-port* [**vpn-instance** *instance-name*]
- **no syslog server** *ipv4-address* [**vpn-instance** *instance-name*]
- **no syslog6 server** *ipv6-address* [**vpn-instance** *instance-name*]
- **syslog server** *ipv4-address source-ip src-ipv4-address*
- **syslog6 server** *ipv6-address source-ip src-ipv6-address*
- **syslog server** *ipv4-address source-ip src-ipv4-address server-port*
- **syslog6 server** *ipv6-address source-ip src-ipv6-address server-port*

Parameter

Parameter	Description	Value
instance-name	Specifies a VPN instance name.	The value is a string of up to 64 characters.
ipv4-address	Specifies the IPv4 address of a syslog server.	The value is in dotted decimal notation.
ipv6-address	Specifies the IPv6 address of a syslog server.	In this format, a 128-digit IP address is divided into 8 segments. Each segment consists of 16 digits and is represented by 4 hexadecimal characters (0-9 and A-F). Segments are separated by colons (:). Every "X" represents a group of hexadecimal digits.

Parameter	Description	Value
server-port	Specifies the port number of a syslog server.	The value is an integer ranging from 1 to 65535.
src-ipv4-address	Specifies a source IPv4 address.	The value is in dotted decimal notation.
src-ipv6-address	Specifies a source IPv6 address.	-

Default Value

NA

View

Global configuration view

Usage Guidelines

You can use this command to configure a syslog server. The syslog server receives logs from the clients. In this manner, you can uniformly manage and view the logs, facilitating device monitoring.

Example

Set the IP address of the syslog source server to 1.1.1.1.

```
Switch(config)#syslog server 1.1.1.1
Switch(config)#
```

10.3.4 clear abnormal-log**Function**

The **clear abnormal-log** command clears abnormal logs.

Format

clear abnormal-log

Parameter

NA

Default Value

NA

View

Privileged user view

Usage Guidelines

NA

Example

Clear abnormal logs.

```
Switch#clear abnormal-log
Switch#
```

10.3.5 clear logging {logbuffer|trapbuffer}

Function

The **clear logging {logbuffer|trapbuffer}** command clears the log buffer.

Format

clear logging { logbuffer | trapbuffer }

Parameter

NA

Default Value

NA

View

Global configuration view

Usage Guidelines

NA

Example

Clear the log buffer.

```
Switch(config)#clear logging logbuffer
Switch(config)#
```

10.3.6 clear logging logfile

Function

The **clear logging logfile all** command clears all the content in a log file.

The **clear logging logfile default** command clears the default content in a log file.

Format

- **clear logging logfile all**
- **clear logging logfile default**

Parameter

NA

Default Value

NA

View

Global configuration view

Usage Guidelines

NA

Example

Clear all the content of a log file.

```
Switch(config)#clear logging logfile all
Switch(config)#
```

10.3.7 clear logging source**Function**The **clear logging source** command clears log information on a specified module.**Format**

```
clear logging source { aaa | acl | antiattack | arp | arp-antiattack | arp-probe | bfd | bgp | cli |
counter | cpu | cpu-defend | ddm | default | devcomm | dhcp | dhcp-client | did | diffserv | dot1x |
dos-antiattack | evpn | fan | hwbd | hwroute | hwvp | hwvrf | icmp | icmp6 | ifm | igmp |
igmp-snooping | ip | ipsg | ip-subnet-vlan | ipv6 | isis | iss | lacp | link-flap | llt | lldp | loopcheck |
l3vpn | mac-vlan | mad | mam | memory | mirror | mlag | mld | mld-snooping | mlink | mvrp |
nd-snooping | ndp | ntp | ospf | ospf6 | patch | pim | port-isolate | power | pppoeplus |
protocol-vlan | policy-route | rawip | rawip6 | rip | rlink | route | route-policy | scheduleprofile |
snmp | soa | ssh | stg | stp | storm-control | storm-suppression | system | temperature | tcp | tcp6 |
time-range | udp | udp6 | udr | uinetsck | virtual-cable-test | vlan-mapping | vlan-stacking | vtp |
vxlan | slot }
```

Parameter

NA

Default Value

NA

View

Global configuration view

Usage Guidelines

NA

Example

Clear log information on a specified module.

```
Switch(config)#clear logging source mlag
Switch(config)#
```

10.3.8 logging import {log|trap|debug}**Function**

The **logging import {log|trap|debug}** command sends a custom log.

Format

logging import { log | trap | debug } log-buffer-value

Parameter

Parameter	Description	Value
log-buffer-value	Specifies the log content.	The length of the value is less than 150 bytes.
log trap debug	Specifies a log type.	-

Default Value

NA

View

Global configuration view

Usage Guidelines

In a sent customized log, the log type must be specified, and the source is the default source.

Example

Send a customized log.

```
Switch(config)#logging import log log
Switch(config)#
```

10.3.9 logging logfile path**Function**

The **logging logfile path** command configures the storage path of log files.

Format

logging logfile path { **flash** | **ram** }

Parameter

NA

Default Value

NA

View

Global configuration view

Usage Guidelines

NA

Example

Configure the storage path of log files.

```
Switch(config)#logging logfile path flash
Switch(config)#
```

10.3.10 logging logfile max-number**Function**

The **logging logfile max-number** command configures the maximum number of log files.

Format

logging logfile max-number { *max-value* | **default** }

Parameter

Parameter	Description	Value
max-value	Specifies the maximum number of logs.	The value is an integer ranging from 1 to 16.
default	Specifies the default value.	16

Default Value

16

View

Global configuration view

Usage Guidelines

NA

Example

Set the maximum number of logs to 5.

```
Switch(config)#logging logfile max-number 5
Switch(config)#
```

10.3.11 logging logfile size

Function

The **logging logfile size** command configures the size of a log file.

Format

logging logfile size kbytes { *size-value* | **default** }

Parameter

Parameter	Description	Value
size-value	Specifies the log file size, in KBs.	The value is an integer ranging from 32 to 16384.
default	Specifies the default value.	16384

Default Value

3072 KB

View

Global configuration view

Usage Guidelines

NA

Example

Configure the size of a log file to 8192 KB.

```
Switch(config)#logging logfile size kbytes 8192
Switch(config)#
```

10.3.12 logging source action**Function**

The **logging source action** command configures the priority threshold for a specified type of logs for a specified action of a specified module.

The **no logging source action** command cancels the priority threshold for a specified type of logs for a specified action of a specified module.

Format

- **logging source** { aaa | acl | antiattack | arp | arp-antiattack | arp-probe | bfd | bgp | cli | counter | cpu | cpu-defend | ddm | default | devcomm | dhcp | dhcp-client | did | diffserv | dot1x | evpn | fan | hwbd | hwroute | hwvp | hwvrf | icmp | icmp6 | ifm | igmp | igmp-snooping | ip | ipsg | ip-subnet-vlan | ipv6 | isis | iss | lacp | link-flap | llc | lldp | loopcheck | l3vpn | mac-vlan | mad | mam | memory | mirror | mlag | mld | mld-snooping | mlink | mvrp | nd-snooping | ndp | ntp | ospf | ospf6 | patch | pim | port-isolate | power | pppoeplus | protocol-vlan | policy-route | rawip | rawip6 | rip | rlink | route | route-policy | scheduleprofile | snmp | soa | ssh | stg | stp | storm-control | storm-suppression | system | temperature | tcp | tcp6 | time-range | udp | udp6 | udr | uinetsck | virtual-cable-test | vlan-mapping | vlan-stacking | vtp | vxlan | slot } **action** { console | monitor | logfile | logbuffer | trap | trapbuffer | syslog | smtp } { log | debug | trap } **level** { emergencies | alert | critical | error | warning | notification | information | debugging | default }
- **logging source** { aaa | acl | antiattack | arp | arp-antiattack | arp-probe | bfd | bgp | cli | counter | cpu | cpu-defend | ddm | default | devcomm | dhcp | dhcp-client | did | diffserv | dot1x | evpn | fan | hwbd | hwroute | hwvp | hwvrf | icmp | icmp6 | ifm | igmp | igmp-snooping | ip | ipsg | ip-subnet-vlan | ipv6 | isis | iss | lacp | link-flap | llc | lldp | loopcheck | l3vpn | mac-vlan | mad | mam | memory | mirror | mlag | mld | mld-snooping | mlink | mvrp | nd-snooping | ndp | ntp | ospf | ospf6 | patch | pim | port-isolate | power | pppoeplus | protocol-vlan | policy-route | rawip | rawip6 | rip | rlink | route | route-policy | scheduleprofile | snmp | soa | ssh | stg | stp | storm-control | storm-suppression | system |

temperature | tcp | tcp6 | time-range | udp | udp6 | udr | uinetsck | virtual-cable-test |
vlan-mapping | vlan-stacking | vtp | vxlan | slot } action { console | monitor | logfile |
logbuffer | trap | trapbuffer | syslog | smtp } { log | debug | trap } state { enable | disable |
default }

- **logging source** { aaa | acl | antiattack | arp | arp-antiattack | arp-probe | bfd | bgp | cli |
counter | cpu | cpu-defend | ddm | default | devcomm | dhcp | dhcp-client | did | diffserv |
dot1x | evpn | fan | hwbd | hwroute | hwvp | hwvrf | icmp | icmp6 | ifm | igmp |
igmp-snooping | ip | ipsg | ip-subnet-vlan | ipv6 | isis | iss | lacp | link-flap | llt | lldp |
loopcheck | l3vpn | mac-vlan | mad | mam | memory | mirror | mlag | mld | mld-snooping |
mlink | mvrp | nd-snooping | ndp | ntp | ospf | ospf6 | patch | pim | port-isolate | power |
pppoeplus | protocol-vlan | policy-route | rawip | rawip6 | rip | rlink | route | route-policy |
scheduleprofile | snmp | soa | ssh | stg | stp | storm-control | storm-suppression | system |
temperature | tcp | tcp6 | time-range | udp | udp6 | udr | uinetsck | virtual-cable-test |
vlan-mapping | vlan-stacking | vtp | vxlan | slot } action { console | monitor | logfile |
logbuffer | trap | trapbuffer | syslog | smtp } { log | debug | trap } state { enable | disable |
default } level { emergencies | alert | critical | error | warning | notification | information |
debugging | default }
- **no logging source** { aaa | acl | antiattack | arp | arp-antiattack | arp-probe | bfd | bgp | cli |
counter | cpu | cpu-defend | ddm | default | devcomm | dhcp | dhcp-client | did | diffserv |
dot1x | evpn | fan | hwbd | hwroute | hwvp | hwvrf | icmp | icmp6 | ifm | igmp |
igmp-snooping | ip | ipsg | ip-subnet-vlan | ipv6 | isis | iss | lacp | link-flap | llt | lldp |
loopcheck | l3vpn | mac-vlan | mad | mam | memory | mirror | mlag | mld | mld-snooping |
mlink | mvrp | nd-snooping | ndp | ntp | ospf | ospf6 | patch | pim | port-isolate | power |
pppoeplus | protocol-vlan | policy-route | rawip | rawip6 | rip | rlink | route | route-policy |
scheduleprofile | snmp | soa | ssh | stg | stp | storm-control | storm-suppression | system |
temperature | tcp | tcp6 | time-range | udp | udp6 | udr | uinetsck | virtual-cable-test |
vlan-mapping | vlan-stacking | vtp | vxlan | slot } action { console | monitor | logfile |
logbuffer | trap | trapbuffer | syslog | smtp }

Parameter

Parameter	Description	Value

aaa acl antiattack arp arp-antiattack arp-probe bfd bgp cli counter cpu cpu-defend ddm default diffserv dot1x evpn fan hwroute icmp icmp6 ifm igmp igmp-snooping ip ipsg ip-subnet-vlan ipv6 isis iss lacp link-flap lldp loopcheck l3vpn mac-vlan mad mam memory mirror mlag mld mld-snooping mlink mvrp nd-snooping ndp ntp ospf ospf6 patch pim port-isolate power pppoeplus protocol-vlan policy-route rawip rawip6 rip rlink route-policy scheduleprofile snmp soa ssh stg stp storm-control storm-suppression system temperature tcp tcp6 time-range udp udp6 udr uinetsck virtual-cable-test vlan-mapping vlan-stacking vtp vxlan slot	Specifies the functional module name.	-
console monitor logfile logbuffer trap trapbuffer syslog smtp	Specifies the action to be performed for a log.	-
emergencies alert critical error warning notification information debugging default	Specifies a log priority or restores the default value.	-

Default Value

NA

View

Global configuration view

Usage Guidelines

The log action takes effect when the priority of a sent log is higher than this threshold.

	A	B	C	D	E	F	G	H	I	J	K
1	logging action state default(1:enable.0:disable)										
2	logging action										
3		console	monitor	logfile	logbuffer	trap	trapbuffer	syslog	smtp		
4	type str	log	1	1	1	1	0	0	1		0
5		debug	1	1	0	0	0	0	0		0
6		trap	0	0	1	1	0	0	1		0
7											
8											
9	logging action										
10	leveldefault(Emergencies:0,Alert:1,Critical:2,Error:3,Warning:4,Notification:5,Information:6,Debugging:7)										
11		console	monitor	logfile	logbuffer	trap	trapbuffer	syslog	smtp		
12	type str	log	4	4	7	7	6	6	6		4
13		debug	7	7	7	7	7	7	7		4
14		trap	7	7	7	7	7	7	7		4
15											
16											

Example

Configure log management for the ACL module.

```
Switch(config)#logging source acl action smtp log state enable
Switch(config)#
```

10.3.13 logging source logfile size kbytes

Function

The **logging source logfile size kbytes** command configures the size of log files of each module.

Format

logging source { aaa | acl | antiattack | arp | arp-antiattack | arp-probe | bfd | bgp | counter | cpu | cpu-defend | ddm | default | devcomm | did | diffserv | dos-antiattack | dot1x | evpn | fan | hwroute | hwvp | hwvrf | icmp | icmp6 | ifm | igmp | igmp-snooping | ip | ipsg | ip-subnet-vlan | ipv6 | isis | iss | l3vpn | lacp | link-flap | lldp | llt | loopcheck | mac-vlan | mad | mam | memory | mirror | mlag | mld | mld-snooping | mlink | mvrp | ndp | nd-snooping | ntp | ospf | ospf6 | patch | pim | port-isolate | power | pppoeplus | protocol-vlan | rawip | rawip6 | rip | rlink | route-policy | scheduleprofile | slot | snmp | soa | ssh | stg | stp | system | tcp | tcp6 | temperature | time-range | uddld | udp | udp6 | udr | uinetsck | virtual-cable-test | vlan-mapping | vlan-stacking | vrrp | vtp | vxlan } **logfile size kbytes** { *file_size* | **default** }

Parameter

Parameter	Description	Value
file_size	Specifies a file size.	The value ranges from 32 to 16384, in KB.
default	Specifies the default value.	The default value is 16384 KB.

Default Value

By default, the log function is enabled.

View

Global configuration view

Usage Guidelines

NA

Example

Configure the size of log files of the aaa module to the default value.

```
Switch(config)#logging source aaa logfile size kbytes default
Switch(config)#
```

10.3.14 logging source max-number

Function

The **logging source max-number** command configures the maximum number of log files of each module.

Format

logging source { aaa | acl | antiattack | arp | arp-antiattack | arp-probe | bfd | bgp | counter | cpu | cpu-defend | ddm | default | devcomm | did | diffserv | dos_antiattack | dot1x | evpn | fan | hwroute | hwvp | hwvrf | icmp | icmp6 | ifm | igmp | igmp-snooping | ip | ipsg | ip-subnet-vlan | ipv6 | isis | iss | lacp | link-flap | lldp | llt | mac-vlan | mad | mam | memory | mirror | mlag | mld | mld-snooping | mlink | mvrp | ndp | nd-snooping | ntp | ospf6 | patch | pim | port-isolate | power | pppoeplus | protocol-vlan | rawip | rawip6 | rip | rlink | route-policy | scheduleprofile | slot | snmp | soa | ssh | stg | stp | system | tcp | tcp6 | temperature | time-range | udld | udp | udp6 | udr | uinetsck | virtual-cable-test | vlan-mapping | vlan-stacking | vrrp | vtp | vxlan } **max-number** { *file_num* | **default** }

Parameter

Parameter	Description	Value
file_num	Specifies the number of files.	The value is an integer ranging from 1 to 16.
default	Specifies the default value.	16

Default Value

16

View

Global configuration view

Usage Guidelines

NA

Example

Configure the maximum number of log files of the aaa module to the default value.

```
Switch(config)#logging source aaa max-number default
Switch(config)#
```

10.3.15 logging on

Function

The **logging on** command enables the log function of the system.

The **no logging on** command disables the log function of the system.

Format

- **logging on**
- **no logging on**

Parameter

NA

Default Value

By default, the log function is enabled.

View

Global configuration view

Usage Guidelines

To monitor system operation and status, you can enable the log function. Then you can obtain the system status by checking logs and take appropriate actions. The log file can save 2000 consecutive records. When the number of records exceeds 2000, the system automatically deletes the earliest records. To prevent loss of log records, you are advised to export the log file regularly.

Example

Disable the log function of the system.

```
Switch(config)#no logging on
Switch(config)#
```

10.3.16 save logging logfile

Function

The **save logging logfile** command enables you to manually save log files.

Format

save logging logfile

Parameter

NA

Default Value

NA

View

Global configuration view

Usage Guidelines

You can use this command to save logs in the log buffer to log files.

Example

Manually save log files.

```
Switch(config)#save logging logfile
Switch(config)#
```

10.3.17 show {logbuffer|trapbuffer} module**Function**

The **show {logbuffer|trapbuffer} module** command displays log information on a specified module in the log buffer or alarm buffer.

Format

show { logbuffer | trapbuffer } module { aaa | acl | antiattack | arp | arp-antiattack | arp-probe | bfd | bgp | cli | counter | cpu | cpu-defend | ddm | default | devcomm | dhcp | dhcp-client | did | diffserv | dot1x | evpn | fan | hwbd | hwroute | hwvp | hwvrf | icmp | icmp6 | ifm | igmp | igmp-snooping | ip | ipsg | ip-subnet-vlan | ipv6 | isis | iss | lacp | link-flap | llt | lldp | loopcheck | l3vpn | mac-vlan | mad | mam | memory | mirror | mlag | mld | mld-snooping | mlink | mvrp | nd-snooping | ndp | ntp | ospf | ospf6 | patch | pim | port-isolate | power | pppoeplus | protocol-vlan | rawip | rawip6 | rip | rlink | route | route-policy | scheduleprofile | snmp | soa | ssh | stg | stp | storm-control | storm-suppression | system | temperature | tcp | tcp6 | time-range | udp | udp6 | udr | virtual-cable-test | vlan-mapping | vlan-stacking | vtp | vxlan | dos-antiattack | uinetsck | slot }

Parameter

Parameter	Description	Value
logbuffer	Specifies the log buffer.	-
trapbuffer	Specifies the alarm buffer.	-

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

Display log information on a specified module in the log buffer.

```
Switch>show logbuffer module default
2019/10/16 05:15:58 Switch %01-6- default -INFO(l):[telnet] Host(192.168.11.54) successfully log on
2019/10/16 04:35:35 Switch %01-7- default -INFO(l):vty->timeout:fd is 14,line is 32
2019/10/16 04:25:28 Switch %01-6- default -INFO(l):card 1/1/2 up
2019/10/16 04:25:28 Switch %01-6- default -INFO(l):card 1/1/1 up
2019/10/16 4:25:27 AM Switch %01-6- default -INFO(l):card 1/1/0 up
2019/10/16 04:25:27 Switch %01-6- default -INFO(l):slot 1/1 up
Switch>
```

10.3.18 show (logbuffer|trapbuffer) module policy-route

Function

The **show (logbuffer|trapbuffer) module policy-route** command displays the log buffer and alarm buffer of the system running information.

Format

show { logbuffer | trapbuffer } module policy-route

Parameter

NA

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

View the log buffer and alarm buffer of the system running information.

```
Switch>show logbuffer module policy-route
Switch>
```

10.3.19 show {logbuffer|trapbuffer}**Function**

The **show {logbuffer|trapbuffer}** command displays log information on the log buffer or the alarm log buffer.

Format

- **show { logbuffer | trapbuffer }**
- **show { logbuffer | trapbuffer } { include | exclude | begin } substring *string***

Parameter

Parameter	Description	Value
string	Specifies a matching character string.	The value is a character string.

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

Display log information in logs.

```

Switch>show logbuffer
2019/11/30 00:38:19 Switch %01-6- default -INFO(l):10.166.18.7 User=admin:show abn
2019/11/30 00:38:06 Switch %01-6- default -INFO(l):10.166.18.7 User=admin:exit
2019/11/30 00:38:04 Switch %01-6- default -INFO(l):10.166.18.7 User=admin:eit
2019/11/30 00:32:33 Switch %01-6- default -INFO(l):10.166.18.7 User=admin:logging import log log
2019/11/30 00:32:33 Switch %01-0- default -INFO(l):log
2019/11/30 00:32:20 Switch %01-6- default -INFO(l):10.166.18.7
2019/11/30 00:00:00 Switch %01-7- default -INFO(l):[trap]system 1 slot 1 card 1 up
2019/01/01 00:00:12 Switch %01-7- default -INFO(l):[trap]system 1 slot 1 card 0 up
2019/01/01 00:00:12 Switch %01-7- default -INFO(l):[trap]system 1 slot 1 up

Switch#

```

10.3.20 show {logbuffer|trapbuffer} size

Function

The **show {logbuffer|trapbuffer}** command displays the number of logs in the log buffer or the alarm log buffer.

Format

- **show { logbuffer | trapbuffer } size size-value**
- **show { logbuffer | trapbuffer } size size-value { include | exclude | begin } substring string**

Parameter

Parameter	Description	Value
string	Specifies a matching character string.	Specifies a character string.
size-value	Specifies the number of logs.	The value is an integer ranging from 1 to 2000.

View

Common user view

Usage Guidelines

NA

Example

View that the number of logs in the logbuffer is 2.

```
Switch>show logbuffer size 2
2019/11/30 12:47:08 AM Switch %01-6- default -INFO(l):10.166.18.7 User=admin:2019/01/01 00:00:12
Switch %01-7- default -INFO(l):[trap]system 1 slot 1 card 0 up
2019/11/30 12:47:08 AM Switch %01-6- default -INFO(l):10.166.18.7 User=admin:2019/11/30 00:00:00
Switch %01-7- default -INFO(l):[trap]system 1 slot 1 card 1 up

Switch>
```

10.3.21 show {logbuffer|trapbuffer} start-time

Function

The **show {logbuffer|trapbuffer} start-time** command displays log information on a specified time.

Format

- **show { logbuffer | trapbuffer } YY/MM/DD hh:mm:ss**
- **show { logbuffer | trapbuffer } start-time YY/MM/DD hh:mm:ss end-time YY/MM/DD hh:mm:ss**

Parameter

Parameter	Description	Value
YY/MM/DD	Specifies the start or end time, in the format of yy:mm:dd.	The value is an integer in the range of <2001-2099>:<1-12>:<1-31>.
hh:mm:ss	Specifies the start or end time, in the format of hh:mm:ss.	The value is an integer in the range of <0-23>:<0-59>:<0-59>.

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

Display log information on a specified time.

```
Switch>show logbuffer start-time 2019/1/1 13:20:15
Switch(config)#
```


10.3.22 show abnormal-log

Function

The **show abnormal-log** command displays abnormal log information.

Format

show abnormal-log

Parameter

Description	Description	Value
string	Specifies a matching character string.	The value is a character string.

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

Display abnormal log information.

```
Switch>show abnormal-log
pid:115 signal:11 address:0xa ip:0x631d44
/usr/lib/libusposl.so[0x2ac1ba5c]
/lib/libc.so.0[0x3287e3d0]
/usr/bin/uspnmagent(nm_acl_allow+0x1d2)[0x631d46]
/usr/bin/uspnmagent(cliCfgFileProcess+0x1740)[0x678f1c]
/usr/bin/uspnmagent(cliCfgFileServer+0x210)[0x67953c]
/usr/bin/uspnmagent(cli_process_ipc_config+0x130)[0x67a030]
/lib/libpthread.so.0[0x2aacc028]
Switch>
```

10.3.23 show logfile

Function

The **show logfile** command displays a log file in the log buffer.

Format

- **show logfile** *file-name*
- **show logfile** *file-name* { **include** | **exclude** | **begin** } **substring** *string*

Parameter

Parameter	Description	Value
string	Specifies a matching character string.	The value is a character string.
file-name	Specifies the file name that includes a path.	The value is a character string.

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

Display log files in the logbuffer.

```

Switch>ls
  attr    link uid      gid      size    date  time  name
-----
-rw-r--r--    1 root    root      16301 Oct 17 04:34 log.log

          available space: 302886912 bytes.

Switch>show logfile log.log
2019/10/17 04:34:15 Switch %01-5-MAM-EVENT(l):LoopBack0 add ip address
2019/10/17 04:34:15 Switch %01-5-MAM-EVENT(l):LoopBack0 add ip address, end not vlan
2019/10/17 04:34:15 Switch %01-5-MAM-EVENT(l):LoopBack0 add ip address
2019/10/17 04:34:15 Switch %01-5-MAM-EVENT(l):LoopBack0 add ip address, end not vlan
2019/10/17 04:34:15 Switch %01-7-SNMP-TRAP(t):system 1 slot 1 up
2019/10/17 04:34:15 Switch %01-6- default -INFO(l):slot 1/1 up
2019/10/17 04:34:15 Switch %01-7-SNMP-TRAP(t):system 1 slot 1 card 0 up.
2019/10/17 04:34:15 Switch %01-6- default -INFO(l):card 1/1/0 up
Switch>

```

10.3.24 show logfile module

Function

The **show logfile module** command displays log file information on different modules.

Format

show logfile *file-name* **module** { **aaa** | **acl** | **antiattack** | **arp** | **arp-antiattack** | **arp-probe** | **bfd** | **bgp** | **cli** | **counter** | **cpu** | **cpu-defend** | **ddm** | **default** | **devcomm** | **dhcp** | **dhcp-client** | **did** | **diffserv** | **dot1x** | **evpn** | **fan** | **hwbd** | **hwroute** | **hwvp** | **hwvrf** | **icmp** | **icmp6** | **ifm** | **igmp** | **igmp-snooping** | **ip** | **ipsg** | **ip-subnet-vlan** | **ipv6** | **isis** | **iss** | **lacp** | **link-flap** | **llt** | **lldp** | **loopcheck** | **l3vpn** | **mac-vlan** | **mad** | **mam** | **memory** | **mirror** | **mlag** | **mld** | **mld-snooping** | **mlink** | **mvrp** | **dos-antiattack** | **nd-snooping** | **ndp** | **ntp** | **ospf** | **ospf6** | **patch** | **pim** | **port-isolate** | **power** | **pppoeplus** | **protocol-vlan** | **policy-route** | **rawip** | **rawip6** | **rip** | **rlink** | **route** | **route-polic** | **y** | **scheduleprofile** | **snmp** | **soa** | **ssh** | **stg** | **stp** | **storm-control** | **storm-suppression** | **system** | **temperature** | **tcp** | **tcp6** | **time-range** | **udp** | **udp6** | **udr** | **uinetsck** | **virtual-cable-test** | **vlan-mapping** | **vlan-stacking** | **vtp** | **vxlan** | **slot** }

Parameter

Parameter	Description	Value
file-name	Specifies the file name that includes a path.	The value is a character string.
default	By default, the basic configuration log file information is initialized.	-

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

Display log file information on module AAA.

```
Switch>show logfile log1 module aaa
Switch>
```

10.3.25 show logfile start-time

Function

The **show logfile start-time** command displays log file information on a specified time.

Format

- **show logfile start-time** *YY/MM/DD hh:mm:ss*
- **show logfile start-time** *YY/MM/DD hh:mm:ss end-time YY/MM/DD hh:mm:ss*

Parameter

Parameter	Description	Value
YY/MM/DD	Specifies the start to end date (year/month/day).	The value is an integer in the range of <2001-2099>/<1-12>/<1-31>.
hh:mm:ss	Specifies the start or end time (hour:minute:second)	The value is an integer in the range of <0-23>:<0-59>:<0-59>.

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

Display log file information on a specified time.

```
Switch>show logbuffer start-time 2020/01/12 00:59:53
2020/01/12 00:59:53 Switch-10 %01-6-CLI-CMDRECORD(1):Console User=admin:show logbuffer start-time
2008
Switch(config)#
```

10.3.26 show logging

Function

The **show logging** command displays system logs, including the log information on a specified entry and log information including or excluding a specified string of characters.

Format

show logging

Parameter

NA

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

Display the content of a system log.

```
Switch>show logging
Logging                :enable
Source number          :107
Logfile path           :"/tmp/ram/log"
Logfile max size       :16384 Kb
Logfile max number     :16
Logbuffer Max number   :16000
Logbuffer Current number :550
Logbuffer history number :550
Switch>
```

10.3.27 show logging action

Function

The **show logging action** command displays logging action for each module.

Format

- **show logging action**
- **show logging action { console | monitor | logfile | logbuffer | trap | syslog | smtp }**

Parameter

Parameter	Description	Value
console monitor logfile logbuffer	Specifies the action to be performed for a log.	-

Parameter	Description	Value
trap syslog smtp		

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

Display logging action for each module.

```

Switch>show logging action
  Action:console
  Source      Log      Level      Debug  Level      Trap      Level
  DEFAULT     enable  warning    enable  debugging  disable  debugging
  IFM         enable  warning    disable debugging  disable debugging

  Action:monitor
  Source      Log      Level      Debug  Level      Trap      Level
  DEFAULT     disable warning    disable debugging  disable debugging

  Action:logfile
  Source      Log      Level      Debug  Level      Trap      Level
  DEFAULT     disable debugging  disable debugging  disable debugging
  CLI         enable  debugging  disable debugging  disable debugging

  Action:logbuffer
  Source      Log      Level      Debug  Level      Trap      Level
  DEFAULT     disable debugging  disable debugging  disable debugging
  CLI         enable  debugging  disable debugging  disable debugging

  Action:trap
  Source      Log      Level      Debug  Level      Trap      Level
  DEFAULT     disable information  disable debugging  disable debugging

  Action:syslog
  Source      Log      Level      Debug  Level      Trap      Level
  DEFAULT     disable information  disable debugging  disable debugging

```

```

Action:smtp
Source      Log      Level      Debug  Level      Trap      Level
DEFAULT    disable warning    disable warning    disable warning

Switch>

```

10.3.28 show logging source

Function

The **show logging source** command displays details of each module.

Format

- **show logging source**
- **show logging source { aaa | acl | antiattack | arp | arp-antiattack | arp-probe | bfd | bgp | cli | counter | cpu | cpu-defend | ddm | default | devcomm | dhcp | dhcp-client | did | diffserv | dot1x | dos-antiattack | evpn | fan | hwbd | hwroute | hwvp | hwvrf | icmp | icmp6 | ifm | igmp | igmp-snooping | ip | ipsg | ip-subnet-vlan | ipv6 | isis | iss | lacp | link-flap | llt | lldp | loopcheck | l3vpn | mac-vlan | mad | mam | memory | mirror | mlag | mld | mld-snooping | mlink | mvrp | nd-snooping | ndp | ntp | ospf | ospf6 | patch | pim | port-isolate | power | pppoeplus | protocol-vlan | policy-route | rawip | rawip6 | rip | rlink | route | route-policy | scheduleprofile | snmp | soa | ssh | stg | stp | storm-control | storm-suppression | system | temperature | tcp | tcp6 | time-range | udp | udp6 | udr | uinetsck | virtual-cable-test | vlan-mapping | vlan-stacking | vtp | vxlan | slot }**

Parameter

Parameter	Description	Value
{ aaa acl antiattack arp arp-antiattack arp-probe bfd bgp cli counter cpu cpu-defend ddm default devcomm dhcp dhcp-client did diffserv dot1x evpn fan hwbd hwroute hwvp hwvrf icmp icmp6 ifm igmp igmp-snooping ip ipsg ip-subnet-vlan ipv6 isis iss lacp link-flap llt lldp loopcheck l3vpn mac-vlan mad mam memory mirror mlag mld mld-snooping mlink mvrp nd-snooping ndp ntp ospf ospf6 patch pim port-isolate power pppoeplus protocol-vlan rawip rawip6 rip rlink route route-policy scheduleprofile snmp }	Specifies a protocol name.	-

Parameter	Description	Value
soa ssh stg stp storm-control storm-suppression system temperature tcp tcp6 time-range udp udp6 udr virtual-cable-test vlan-mapping vlan-stacking vtp vxlan slot }		
default	Shows initialized configuration information.	-

Default Value

By default, this command shows initialized configuration information.

View

Common user view

Usage Guidelines

NA

Example

Display the detailed information about the default module

```
Switch>show logging source default
```

```
Source name      :default
```

```
Statistic
```

```
Log total number      :35
```

```
Log lost number       :0
```

```
Debug total number    :0
```

```
Debug lost number     :0
```

```
Trap total number     :1
```

```
Trap lost number      :0
```

Source	Action	Log	Level	Debug	Level	Trap	Level
default	console	enable	warning	enable	debugging	enable	debugging
default	monitor	enable	warning	enable	debugging	enable	debugging
default	logfile	enable	debugging	disable	debugging	enable	debugging
default	logbuffer	enable	debugging	disable	debugging	enable	debugging
default	trap	disable	debugging	disable	debugging	disable	debugging
default	trapbuffer	disable	information	disable	debugging	enable	debugging
default	syslog	enable	information	disable	debugging	enable	debugging
default	smtp	disable	warning	disable	warning	disable	warning

```
Switch>
```


10.3.29 show logging statistics

Function

The **show logging statistics** command displays log statistics information on all modules.

Format

show logging statistics

Parameter

NA

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

Display log statistics information on all modules.

Switch>show logging statistics			
Logfile max size	:16384 Kb		
Logfile max number	:16		
Logbuffer Max number	:16000		
Logbuffer Current number	:554		
Logbuffer history number	:554		
Receiving Messages	:0/224733		
Length errors	:0		
Source mismatch	:0		
Send errors	:0		
Receive errors	:0		
Malloc errors	:0		
File operation errors	:0		
Miss Messages	:5		
General errors	:0		
Source number	:107		
Source	Log(Total/Lost)	Debug(Total/Lost)	Trap(Total/Lost)
aaa	0/0	0/0	0/0
acl	0/0	0/0	0/0

antiattack	0/0	0/0	0/0
arp	0/0	0/0	0/0
arp-antiattack	0/0	0/0	0/0
arp-probe	31/0	0/0	0/0
auto-config	0/0	0/0	0/0
bfd	0/0	0/0	0/0
bgp	0/0	0/0	0/0
bpdu-tunnel	0/0	0/0	0/0
cli	55/0	0/0	1/0
counter	0/0	0/0	0/0
cpu	0/0	0/0	0/0
cpu-defend	0/0	0/0	0/0
ddm	0/0	0/0	2081/0
default	35/0	0/0	1/0
devcomm	3/0	0/0	0/0
dhcp	0/0	0/0	0/0
dhcp-client	0/0	0/0	0/0
dhcp-snooping	0/0	0/0	0/0
dhcpv6	0/0	0/0	0/0
did	0/0	0/0	0/0
diffserv	0/0	0/0	0/0
dos-antiattack	0/0	0/0	0/0
dot1x	0/0	0/0	0/0
evpn	0/0	0/0	0/0
fan	10/0	0/0	0/0
g8032	0/0	0/0	0/0
hwroute	33238/0	0/0	0/0
hwvp	0/0	0/0	0/0
hwvrf	0/0	0/0	0/0
icmp	0/0	0/0	0/0
icmp6	0/0	0/0	0/0
if-ref	0/0	0/0	0/0
ifm	194/0	0/0	38/0
igmp	0/0	0/0	0/0
igmp-snooping	0/0	0/0	0/0
inp	0/0	0/0	0/0
ip	0/0	0/0	0/0
ip-subnet-vlan	10/0	0/0	0/0
ipsg	0/0	0/0	0/0
ipv6	6/0	0/0	0/0
isis	0/0	0/0	0/0
iss	0/0	0/0	0/0
l2tftpc	0/0	0/0	0/0

l2ftpd	0/0	0/0	0/0
l3vpn	0/0	0/0	0/0
lacp	7370/0	0/0	0/0
link-flap	1/0	0/0	0/0
lldp	0/0	0/0	0/0
lle-lock	0/0	0/0	0/0
llt	99235/0	0/0	0/0
loopcheck	0/0	0/0	0/0
mac-vlan	3/0	0/0	0/0
mad	0/0	0/0	0/0
mam	194/0	0/0	0/0
memory	0/0	0/0	0/0
mirror	7/0	0/0	0/0
mlag	100/0	0/0	0/0
mld	0/0	0/0	0/0
mld-snooping	0/0	0/0	0/0
mlink	50/0	0/0	0/0
mvrp	0/0	0/0	0/0
nd-snooping	0/0	0/0	0/0
ndp	0/0	0/0	0/0
ntp	18/0	0/0	2/0
ospf	0/0	0/0	0/0
ospf6	24/0	12/0	0/0
patch	0/0	0/0	0/0
pim	0/0	0/0	0/0
policy-route	6/0	0/0	0/0
port-isolate	3/0	0/0	0/0
power	0/0	0/0	0/0
pppoePlus	0/0	0/0	0/0
protocol-vlan	0/0	0/0	0/0
rawip	0/0	0/0	0/0
rawip6	0/0	0/0	0/0
rip	0/0	0/0	0/0
rlink	0/0	0/0	0/0
route	0/0	0/0	0/0
route-lock	0/0	0/0	0/0
route-policy	0/0	0/0	0/0
scheduleprofile	8/0	0/0	0/0
slot	31/0	0/0	0/0
snmp	0/0	0/0	15/0
soa	11/0	0/0	0/0
ssh	0/0	0/0	0/0
stg	77/0	0/0	0/0

storm-control	0/0	0/0	0/0
storm-suppression	0/0	0/0	0/0
stp	426/0	0/0	0/0
system	38963/0	0/0	0/0
tcp	0/0	0/0	0/0
tcp6	0/0	0/0	0/0
temperature	0/0	0/0	0/0
time-range	0/0	0/0	0/0
udld	0/0	0/0	0/0
udp	227/0	0/0	0/0
udp6	0/0	0/0	0/0
udr	42034/0	0/0	0/0
uinetsck	0/0	0/0	0/0
virtual-cable-test	0/0	0/0	0/0
vlan-mapping	0/0	0/0	0/0
vlan-stacking	3/0	0/0	0/0
vrrp	161/0	0/0	0/0
vtp	0/0	0/0	0/0
vxlan	49/0	0/0	0/0
Switch>			

10.3.30 show logging config

Function
The show logging config command displays log configuration information.
Format
show logging config
Parameter
NA
Default Value
NA
View
Common user view
Usage Guidelines
NA
Example

Display log configuration information.

```
Switch>show logging config
Switch>
```

10.3.31 show logging error

Function

The **show logging error** command displays error log information.

Format

show logging error

Parameter

NA

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

Display error log information.

```
Switch>show logging error
Switch>
```

10.3.32 show logging event

Function

The **show logging event** command displays event logs.

Format

show logging event

Parameter

NA

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

Display event logs.

```
Switch>show logging event
```

Source	Event-ID	Log(Total/Current)	Debug(Total/Current)	Trap(Total/Current)
aaa	4240000	0/0	0/0	0/0
acl	3ea0000	0/0	0/0	0/0
acl	3ea0001	0/0	0/0	0/0
acl	3ea0002	0/0	0/0	0/0
acl	3ea0003	0/0	0/0	0/0
acl	3ea0004	0/0	0/0	0/0
acl	3ea0005	0/0	0/0	0/0
acl	3ea0006	0/0	0/0	0/0
acl	3ea0007	0/0	0/0	0/0
arp	43d0000	0/0	0/0	0/0
arp	43d0001	0/0	0/0	0/0
arp	43d0002	0/0	0/0	0/0
arp	43d0003	0/0	0/0	0/0
arp	43d0004	0/0	0/0	0/0
arp	43d0005	0/0	0/0	0/0
arp	43d0006	0/0	0/0	0/0
arp	43d0007	0/0	0/0	0/0
arp-antiattack	48d0000	0/0	0/0	0/0
arp-probe	44e0000	0/0	0/0	0/0
arp-probe	44e0001	0/0	0/0	0/0
arp-probe	44e0002	0/0	0/0	0/0

```
Switch>
```

10.4 DDM Configuration Commands

10.4.1 ddm {enable|disable}

Function

The **ddm {enable|disable}** command globally enables or disables the DDM function.

Format

ddm { enable | disable }

Parameter

Parameter	Description	Value
enable	Globally enables the DDM function.	-
disable	Globally disables the DDM function.	-

Default Value

Disable

View

Global configuration view

Usage Guidelines

NA

Example

Globally enable the DDM function.

```
Switch(config)#ddm enable
Switch(config)#
```

10.4.2 ddm interval

Function

The **ddm interval** command sets the polling interval.

Format

ddm interval { interval-time | default }

Parameter

Parameter	Description	Value

Parameter	Description	Value
interval-time	Sets an interval.	The value is an integer ranging from 60 to 7200, in seconds.
default	Sets the default interval.	60 seconds

Default Value

60 seconds

View

Global configuration view

Usage Guidelines

NA

Example

Set the polling interval to 400s.

```
Switch(config)#ddm interval 400
Switch(config)#
```

10.4.3 show ddm config**Function**

The **show ddm config** command displays Digital Diagnostics Monitoring (DDM) information on optical interfaces, including upper and lower thresholds of current, voltage, and other attributes of optical transceivers on the interfaces.

Format

show ddm config

Parameter

NA

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

Display the DDM information configured on the optical port.

```
Switch>show ddm config
!
interface 10gigaethernet 1/0/5
  laser voltage-threshold 2 8
  laser rx-power-threshold -20 5
Switch>
```

10.4.4 show laser hardware

Function

The **show laser hardware** command displays general transceiver hardware information on all the interfaces with optical transceivers installed.

Format

show laser hardware

Parameter

NA

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

Display general hardware information about all the modules where the ports of optical modules are inserted.

```
Switch> show laser hardware
Interface:100ge1/0/20
Common information:
  Transceiver Type      :100GBASE-CR4
  Identifier Type       :QSFP28
  Connector Type        :No Separable connector
  Wavelength(nm)        :64
  Linklength(m)         :0
  Encoding              :Unspecified
  DDM support           :NO
Manufacture information:
  Vendor Name           :LUXSHARE-TECH
  Vendor Part Num       :LWUQF002-SD-R
  Vendor Serial Num     :WUQF00209B0063
  Vendor in Num         :A
  Manufacturing Date    :20200911
  PEC Code              :
Switch>
```

10.4.5 show laser hardware detailed

Function
The show laser hardware detailed command displays detailed transceiver hardware information on all the interfaces with optical transceivers installed.
Format
show laser hardware detailed
Parameter
NA
Default Value
NA
View
Common user view
Usage Guidelines
NA
Example

Display detailed hardware information about all the modules where the ports of optical modules are inserted.

```
Switch>show laser hardware detailed
Interface:gigaethernet 1/0/25
Common information:
  Transceiver Type      :1000BASE-CX_SFP
  Connector Type        :LC
  Wavelength(nm)       :1310
  Linklength(m)        :5000
  Encoding              :NRZ
  Nominal BR(mbps)     :25
  Min BR(mbps)         :23.25
  Max BR(mbps)         :26.0275
  DDM support          :Yes
Manufacture information:
  Vendor Name           :etech
  Vendor Part Num       :OP6E-S05-13-CM
  Vendor Serial Num     :8225259025
  Vendor rev Num        :0000
  Manufacturing Date    :080223
Diagnostic information:
  Current temperature(°C) :42
  Temperature threshold(°C) :-10/10 (User set)
  Current rx power(dBM)   : -18.18
  Rx Power threshold(dBM) :-15.00/-10.00 (User set)
  Current tx power(dBM)   : -6.36
  Tx Power threshold(dBM) :-11.45/-1.44 (Auto)
  Current voltage(V)      :3.29
  Voltage threshold(V)    :2.75/3.75 (Auto)
  Bias current(mA)        :4.36
  Bias current threshold(mA) :25.00/25.00 (User set)

Switch>
```

10.4.6 show laser hardware

{ethernet|xgigaethernet|10gigaethernet|25gigaethernet|40gigaethernet|100gigaethernet}

Function

The **show laser hardware**

{ethernet|xgigaethernet|10gigaethernet|25gigaethernet|40gigaethernet|100gigaethernet}

command displays general hardware information about a module where the port of an optical module is inserted.

Format

show laser hardware { ethernet | xgigaethernet | 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet } interface-number

Parameter

Parameter	Description	Value
interface-number	Specifies an interface number.	The value is an integer in the range of <1-1>/<0-1>/<1-48>.

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

Display the general hardware information about a module where the gigaethernet 1/0/25 port of an optical module is inserted.

```

Switch>show laser hardware ethernet 1/0/25
Interface:gigaethernet 1/0/25
  Common information:
    Transceiver Type      :1000BASE-CX_SFP
    Connector Type        :LC
    Wavelength(nm)        :1310
    Linklength(m)         :5000
    Encoding              :NRZ
    Nominal BR(mbps)       :25
    Min BR(mbps)          :23.25
    Max BR(mbps)          :26.0275
    DDM support           :Yes
  Manufacture information:
    Vendor Name           :etech
    Vendor Part Num       :OP6E-S05-13-CM
    Vendor Serial Num     :8225259025
    Vendor rev Num        :0000
    Manufacturing Date    :080223

Switch>

```

10.4.7 show laser hardware

{ethernet|xgigaethernet|10gigaethernet|25gigaethernet|40gigaethernet|100gigaethernet} detailed

Function

The **show laser hardware**

{ethernet|xgigaethernet|10gigaethernet|25gigaethernet|40gigaethernet|100gigaethernet}

detailed command displays detailed hardware information about a module where the port of an optical module is inserted.

Format

show laser hardware { ethernet | xgigaethernet | 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet } interface-number detailed

Parameter

Parameter	Description	Value
interface-number	Specifies an interface number.	The value is an integer in the range of <1-1>/<0-1>/<1-48>.

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

Display the detailed hardware information about a module where the gigabitEthernet 1/0/25 port of an optical module is inserted.

```
Switch>show laser hardware gigabitEthernet 1/0/25 detailed
Interface:gigabitEthernet 1/0/1
Common information:
  Transceiver Type      :1000BASE-CX_SFP
  Connector Type        :LC
  Wavelength(nm)       :1310
  Linklength(m)         :5000
  Encoding              :NRZ
  Nominal BR(mbps)      :25
  Min BR(mbps)          :23.25
  Max BR(mbps)          :26.0275
  DDM support           :Yes
Manufacture information:
  Vendor Name           :etech
  Vendor Part Num       :OP6E-S05-13-CM
  Vendor Serial Num     :8225259025
  Vendor rev Num        :0000
  Manufacturing Date    :080223
Diagnostic information:
  Current temperature(°C) :42
  Temperature threshold(°C) :-10/30 (User set)
  Current rx power(dBM)   : -18.18
  Rx Power threshold(dBM) :-15.00/-10.00 (User set)
  Current tx power(dBM)   : -6.33
  Tx Power threshold(dBM) :-15.00/5.00 (User set)
  Current voltage(V)      :3.29
  Voltage threshold(V)    :2.75/3.75 (Auto)
  Bias current(mA)        :4.38
  Bias current threshold(mA) :25.00/25.00 (User set)

Switch>
```

10.4.8 debug ddm

Function

The **debug ddm** command enables the DDM debugging function.

The **no debug ddm** command disables the DDM debugging function.

Format

- **debug ddm { poll | event | all }**
- **no debug ddm { poll | event | all }**

Parameter

NA

Default Value

NA

View

Privileged user view

Usage Guidelines

NA

Example

Enable the DDM debugging function.

```
Switch#debug ddm all
Switch#
```

10.4.9 error-down auto-recovery cause transceiver-power-low interval

Function

The **error-down auto-recovery cause transceiver-power-low interval** command configures the time of automatic recovery link up after the optical power of the port is too low and the status changes to down.

The **no error-down auto-recovery cause transceiver-power-low** command disables the operation.

Format

- **error-down auto-recovery cause transceiver-power-low interval *interval***

- **no error-down auto-recovery cause transceiver-power-low**

Parameter

Parameter	Description	Value
interval	Specifies a delay for automatically restoring a port to up state.	The value is an integer ranging from 30 to 86400, in seconds.

Default Value

Enables the synchronization function.

View

Global configuration view

Usage Guidelines

NA

Example

Configure the time of automatic recovery link up to 50s after the optical power of the port is too low and the status changes to down.

```
Switch(config)#error-down auto-recovery cause transceiver-power-low interval 50
Switch(config)#
```

10.4.10 laser bias-current-threshold**Function**

The **laser bias-current-threshold** command configures the bias current thresholds of an optical module port.

Format

laser bias-current-threshold *low-threshold high-threshold*

Parameter

Parameter	Description	Value
low-threshold	Specifies the lower threshold of bias current of an optical module port.	The value is an integer ranging from 0 to 500.
high-threshold	Specifies the upper threshold of bias current of an optical module port.	The value is an integer ranging from 0 to 500.

Default Value

NA

View

Ethernet bridge interface configuration view, Ethernet routing interface configuration view

Usage Guidelines

NA

Example

Configure the bias current thresholds of the optical module port to 25 and 15 respectively.

```
Switch(config-10ge1/0/25)#laser bias-current-threshold 15 25
Switch(config-10ge1/0/25)#
```

10.4.11 laser bias-current-threshold auto

Function

The **laser bias-current-threshold auto** command configures to automatically obtain the bias current thresholds of an optical module port.

Format

laser bias-current-threshold auto

Parameter

By default, the device automatically obtains the bias current thresholds of the optical module port.

Default Value

NA

View

Ethernet bridge interface configuration view, Ethernet routing interface configuration view

Usage Guidelines

NA

Example

Configure to automatically obtain the bias current thresholds of an optical module of the 10gigaethernet 1/0/25 port.

```
Switch(config-10ge1/0/25)#laser bias-current-threshold auto
```

```
Switch(config-10ge1/0/25)#
```

10.4.12 laser rx-power-threshold

Function

The **laser rx-power-threshold** command configures the thresholds for receiving optical power of an optical module port.

Format

laser rx-power-threshold *rx-low-threshold rx-high-threshold*

Parameter

Parameter	Description	Value
rx-low-threshold	Specifies the lower threshold for sending optical power of an optical module port.	The value is an integer ranging from -25 to 5.
rx-high-threshold	Specifies the upper threshold for sending optical power of an optical module port.	The value is an integer ranging from -25 to 5.

Default Value

NA

View

Ethernet bridge interface configuration view, Ethernet routing interface configuration view

Usage Guidelines

NA

Example

Configure the thresholds for receiving optical power of an optical module port.

```
Switch(config-10ge1/0/25)#laser rx-power-threshold -15 -10
Switch(config-10ge1/0/25)#
```

10.4.13 laser rx-power-threshold auto

Function

The **laser rx-power-threshold auto** command configures to automatically obtain the thresholds for receiving optical power of an optical module port.

Format

laser rx-power-threshold auto**Parameter**

NA

Default Value

By default, the device automatically obtains the thresholds for receiving optical power of an optical module port.

View

Ethernet bridge interface configuration view, Ethernet routing interface configuration view

Usage Guidelines

NA

Example

Configure to automatically obtain the thresholds for receiving optical power of an optical module port.

```
Switch(config-10ge1/0/25)#laser rx-power-threshold auto
Switch(config-10ge1/0/25)#
```

10.4.14 laser temperature-threshold**Function**

The **laser temperature-threshold** command configures the temperature threshold of an optical module port.

Format

laser temperature-threshold *low-threshold high-threshold*

Parameter

Parameter	Description	Value
low-threshold	Specifies the lower temperature threshold of an optical module port.	The value is an integer ranging from -50 to 120.
high-threshold	Specifies the upper temperature threshold of an optical module port.	The value is an integer ranging from -50 to 120.

Default Value

NA

View

Ethernet bridge interface configuration view, Ethernet routing interface configuration view

Usage Guidelines

NA

Example

Configure the temperature thresholds of the optical module port to -10 and 30 respectively.

```
Switch(config-10ge1/0/25)#laser temperature-threshold -10 30
Switch(config-10ge1/0/25)#
```

10.4.15 laser temperature-threshold auto**Function**

The **laser temperature-threshold auto** command configures to automatically obtain the temperature thresholds of an optical module port.

Format

laser temperature-threshold auto

Parameter

NA

Default Value

By default, the device automatically obtains the temperature thresholds of the optical module port.

View

Ethernet bridge interface configuration view, Ethernet routing interface configuration view

Usage Guidelines

NA

Example

Configure to automatically obtain the temperature thresholds of an optical module port.

```
Switch(config-10ge1/0/25)#laser temperature-threshold auto
Switch(config-10ge1/0/25)#
```

10.4.16 laser trap {enable|disable}

Function

The **laser trap {enable|disable}** command enables or disables the trap reporting function of the optical module.

Format

laser trap { enable | disable }

Parameter

Parameter	Description	Value
enable	Enables the trap reporting function of the optical module.	-
disable	Disables the trap reporting function of the optical module.	-

Default Value

Disable

View

Ethernet bridge interface configuration view, Ethernet routing interface configuration view

Usage Guidelines

This command is applicable to optical ports.

Example

Enable the trap reporting function of the optical module.

```
Switch(config-10ge1/0/25)#laser trap enable
Switch(config-10ge1/0/25)#
```

10.4.17 laser tx-power-threshold

Function

The **laser tx-power-threshold** command configures the thresholds for sending optical power of an optical module port.

Format

laser tx-power-threshold *tx-low-threshold tx-high-threshold*

Parameter

Parameter	Description	Value

Parameter	Description	Value
tx-low-threshold	Specifies the lower threshold for sending optical power of an optical module port.	The value is an integer ranging from -7 to 5.
tx-high-threshold	Specifies the upper threshold for sending optical power of an optical module port.	The value is an integer ranging from -7 to 5.

Default Value

NA

View

Ethernet bridge interface configuration view, Ethernet routing interface configuration view

Usage Guidelines

NA

Example

Configure the thresholds for sending optical power of an optical module port to 5 and -7 respectively.

```
Switch(config-10ge1/0/25)#laser tx-power-threshold -7 5
Switch(config-10ge1/0/25)#
```

10.4.18 laser tx-power-threshold auto**Function**

The **laser tx-power-threshold auto** command configures to automatically obtain the thresholds for sending optical power of an optical module port.

Format**laser tx-power-threshold auto****Parameter**

NA

Default Value

By default, the device automatically obtains the thresholds for sending optical power of an optical module port.

View

Ethernet bridge interface configuration view, Ethernet routing interface configuration view

Usage Guidelines

NA

Example

Configure to automatically obtain the thresholds for sending optical power of the optical module port.

```
Switch(config-10ge1/0/25)#laser tx-power-threshold auto
Switch(config-10ge1/0/25)#
```

10.4.19 laser voltage-threshold

Function

The **laser voltage-threshold** command configures the voltage threshold of an optical module port.

Format

laser voltage-threshold *low-threshold high-threshold*

Parameter

Parameter	Description	Value
low-threshold	Specifies the lower threshold of voltage of an optical module port.	The value is an integer ranging from 0 to 10.
high-threshold	Specifies the upper threshold of voltage of an optical module port.	The value is an integer ranging from 0 to 10.

Default Value

NA

View

Ethernet bridge interface configuration view, Ethernet routing interface configuration view

Usage Guidelines

NA

Example

Configure the voltage thresholds of the optical module port to 6 and 1 respectively.

```
Switch(config-10ge1/0/25)#laser voltage-threshold 1 6
```

```
Switch(config-10ge1/0/25)#
```

10.4.20 laser voltage-threshold auto

Function

The **laser voltage-threshold auto** command configures to automatically obtain the voltage thresholds of an optical module port.

Format

laser voltage-threshold auto

Parameter

NA

Default Value

By default, the device automatically obtains the voltage thresholds of the optical module port.

View

Ethernet bridge interface configuration view, Ethernet routing interface configuration view

Usage Guidelines

NA

Example

Configure to automatically obtain the voltage thresholds of an optical module port.

```
Switch(config-10ge1/0/25)#laser voltage-threshold auto
Switch(config-10ge1/0/25)#
```

10.4.21 transceiver power low trigger error-down {enable|disable}

Function

The **transceiver power low trigger error-down {enable|disable}** command configures to enable or disable the Error-Down function triggered when the optical power received by the specified Ethernet optical port is too low.

Format

transceiver power low trigger error-down { enable | disable }

Parameter

Parameter	Description	Value
enable	Enables the Error-Down function triggered when the optical power received by the specified Ethernet optical port is too low.	-
disable	Disables the Error-Down function triggered when the optical power received by the specified Ethernet optical port is too low.	-

Default Value

Disable

View

Ethernet bridge interface configuration view, Ethernet routing interface configuration view

Usage Guidelines

When the device encounters a too low optical power, services will be intermittent. To ensure normal service running, users want to trigger the Error-Down function when the switch optical power is too low, so as to switch services upon faults.

Example

Enable the Error-Down function triggered when the optical power received by the specified Ethernet optical port is too low.

```
Switch(config-10ge1/0/1)#transceiver power low trigger error-down enable
Switch(config-10ge1/0/1)#
```

10.4.22 ddm report interval

Function

The **ddm report interval** command configures the DDM reporting polling interval.

Format

ddm report interval { *value* | **default** }

Parameter

Parameter	Description	Value
value	Specifies the DDM reporting polling interval.	The value is an integer ranging from 60 to 7200, in seconds.
default	Specifies the default DDM reporting polling interval.	300 seconds

Default Value

300 seconds

View

Global configuration view

Usage Guidelines

NA

Example

Configure the DDM reporting polling interval.

```
Switch(config)#ddm report interval 500
Switch(config)#
```

10.5 Patch Configuration Commands

10.5.1 debug patch

Function

The **debug patch** command enables the patch debugging function.

The **no debug patch** command disables the patch debugging function.

Format

- **debug patch { error | event | all }**
- **no debug patch { error | event | all }**

Parameter

Parameter	Description	Value
error	Debugs error information.	-
event	Displays debugging information about events.	-
all	Displays all the preceding information.	-

Default Value

NA

View

Privileged user view

Usage Guidelines

NA

Example

Enable the patch debugging function.

```
Switch#debug patch all
Switch#
```

10.5.2 patch load**Function**

The **patch load** command downloads patch files.

Format

patch *patch-number* **load** *file-name*

Parameter

Parameter	Description	Value
patch-number	Specifies a patch number.	The value is an integer ranging from 1 to 100.
file-name	Specifies a patch file name.	The value is a character string.

Default Value

NA

View

Global configuration view

Usage Guidelines

Before loading patches, the system needs to parse the patch package, check whether the patch files in the package are valid, and obtain the patch file attributes, including the patch type, board type, and version information.

When patches are loaded during registration of the standby master control board (not registered), the system prompts a message asking you whether to continue patch loading.

Example

Download patch files.

```
Switch(config)#patch 1 load abc
Switch(config)#
```

10.5.3 patch active

Function

The **patch active** command activates patches and configures whether patches are activated permanently or temporarily.

Format

patch *patch-number* **active** { **permanent** | **temporary** }

Parameter

Parameter	Description	Value
patch-number	Specifies a patch number.	The value is an integer ranging from 1 to 100.
permanent temporary	Specifies whether patches are activated permanently or temporarily.	-

Default Value

NA

View

Global configuration view

Usage Guidelines

Run this command to activate the specified patches loaded on the present board.

The current patch function can load patches for software on the master control board and line card. As long as the master control software system is started, patches can be loaded or activated. Only when the line card is online, can patches be loaded and the slot number of the line card be specified in the command.

Example

Permanently activate the patch 1.

```
Switch(config)#patch 1 active permanent
Switch(config)#
```

10.5.4 patch deactivate

Function

The **patch deactivate** command deactivates patches.

Format

patch *patch-number* **deactive**

Parameter

Parameter	Description	Value
patch-number	Specifies a patch number.	The value is an integer ranging from 1 to 100.

Default Value

NA

View

Global configuration view

Usage Guidelines

When you run this command to deactivate patches, the patches must exist and be activated.

Example

Deactivate the patch 1.

```
Switch(config)#patch 1 deactive
Switch(config)#
```

10.5.5 patch delete**Function**

The **patch delete** command deletes patches. Activated patches will be automatically deactivated before being deleted.

Format

patch *patch-number* **delete**

Parameter

Parameter	Description	Value
patch-number	Specifies a patch number.	The value is an integer ranging from 1 to 100.

Default Value

NA

View

Global configuration view

Usage Guidelines

After you run this command, all patches in any state will be deleted (patch files are deleted and activated patches are deactivated).

Example

Delete the patch 1.

```
Switch(config)#patch 1 delete
Switch(config)#
```

10.5.6 show patch information

Function

The **show patch information** command displays all patch information in the system.

Format

show patch information

Parameter

NA

Default Value

NA

View

Common user view

Usage Guidelines

You can run this command to check the system patch information, including the patch unit number, patch file name, patch function, and patch status.

Example

View patch information in the Switch system.

```
Switch>show patch information
Patch max number      : 100
Patch current number  : 0
Patch permanent number : 0
Switch>
```

10.6 STG Configuration Commands

10.6.1 debug stg

Function

The **debug stg** command enables the STG debugging function.

The **no debug hwroute** command disables the STG debugging function.

Format

- **debug stg { error | event | notification | sync | all }**
- **no debug stg { error | event | notification | sync | all }**

Parameter

Parameter	Description	Value
error	Specifies error packet information.	-
event	Specifies event packet information.	-
notification	Specifies alarm packet information.	-
sync	Specifies synchronous packet information.	-
all	Specifies all packet information.	-

Default Value

Disable

View

Privileged user view

Usage Guidelines

NA

Example

Enable STG debugging.

```
Switch#debug stg all
Switch#
```

10.6.2 reset stg error

Function

The **reset stg error** command clears the STG error packet function.

Format

reset stg error

Parameter

NA

Default Value

NA

View

Privileged user view

Usage Guidelines

NA

Example

Clear the STG error packet function.

```
Switch#reset stg error
Switch#
```

10.6.3 show stg

Function

The **show stg** command shows the STG function information.

Format

show stg { all | brief | error | memory }

Parameter

Parameter	Description	Value
all	Displays all the preceding information.	-
brief	Specifies global information.	-
error	Specifies running error information.	-
memory	Specifies memory information.	-

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

view the STG function information.

```
Switch>show stg all
Switch>
```

10.6.4 show stg instance**Function**The **show stg instance** command shows the STG instance information.**Format****show stg instance** { *instance-id* | **all** }**Parameter**

Parameter	Description	Value
instance-id	Specifies an instance number.	The value is an integer ranging from 1 to 1024.
all	Specifies all instances.	-

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

View the STG instance information.

```
Switch>show stg instance all
Switch>
```

10.6.5 show stg interface**Function**The **show stg interface** command shows the STG interface information.

Format

- **show stg interface { ethernet | xgigaethernet | 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet } interface-number**
- **show stg interface all**

Parameter

Parameter	Description	Value
interface-number	Specifies an Ethernet interface number.	The value is an integer in the range of <1-1>/<0-1>/<1-48>.

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

View the STG interface information.

```
Switch>show stg interface xgigaethernet 1/0/1
Switch>
```

10.6.6 show stg protocol**Function**The **show stg protocol** command shows the STG protocol information.**Format****show stg protocol { all | stp | alb | cfm | g8032 | lacp | mad | mlink | rlink | y1731 }****Parameter**

Parameter	Description	Value
all	Specifies all protocol information.	-
stp	Specifies STP protocol information.	-
alb	Specifies loopback detection protocol information.	-
cfm	Specifies CFM protocol information.	-
g8032	Specifies G.8032 protocol information.	-

Parameter	Description	Value
lacp	Specifies link aggregation protocol information.	-
mad	Specifies MAD protocol information.	-
mlink	Specifies MLINK protocol information.	-
rlink	Specifies RLINK protocol information.	-
y1731	Specifies Y.1731 protocol information.	-

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

View the STG protocol information.

```
Switch>show stg protocol all
Switch>
```

Chapter 11 O&M Commands

This chapter mainly describes configuration commands related to O&M and network management.

11.1 NTP Configuration Commands

11.1.1 debug ntp

Function

The **debug ntp** command enables NTP debugging.

The **no debug ntp** command disables NTP debugging.

Format

- **debug ntp { error | pkt | warning | event | auth | all }**
- **no debug ntp { error | pkt | warning | event | auth | all }**

Parameter

Parameter	Description	Value
error	Displays debugging information about errors.	-
pkt	Displays debugging information about packets.	-
warning	Displays warning information.	-
event	Displays debugging information about events.	-
auth	Displays debugging information about MD5 authentication.	-
all	Displays all debugging information.	-

Default Value

By default, NTP debugging is disabled.

View

Privileged user view

Usage Guidelines

You can use this command to view the NTP process and packet sending and receiving situations. This command is used to maintain and debug the NTP function of the switch.

Example

Enable NTP debugging.

```
Switch#debug ntp all
```

```
Switch#
```

Disable NTP debugging.

```
Switch#no debug ntp all
Switch#
```

11.1.2 ntp

Function

The **ntp** command displays the NTP configuration view.

Format

ntp

Parameter

NA

Default Value

NA

View

Global configuration view

Usage Guidelines

This command is a prerequisite for configuring other NTP parameters in the NTP configuration view.

Example

Switch to the NTP configuration view from the global configuration view.

```
Switch(config)#ntp
Switch(config-ntp)#
```

11.1.3 ntp broadcast-client

Function

The **ntp broadcast-client** command adds or modifies an NTP broadcast client.

The **no ntp broadcast-client** command deletes an NTP broadcast client.

Format

- **ntp broadcast-client**

- **ntp broadcast-client** *ipv4-address*
- **no ntp broadcast-client**
- **no ntp broadcast-client** *ipv4-address*

Parameter

Parameter	Description	Value
ipv4-address	Specifies a broadcast IP address.	The default value is 255.255.255.255.

Default Value

The default value is 255.255.255.255.

View

VLANIF configuration view, Ethernet route interface configuration view, and Outband management interface configuration view

Usage Guidelines

You can use this command to enable the switch to automatically run in client mode after the current interface receives an NTP broadcast packet or a multicast message.

Example

Add an NTP broadcast client.

```
Switch(config-vlanif-4002)#ntp broadcast-client
Switch(config-vlanif-4002)#
```

11.1.4 ntp multicast-client

Function

The **ntp multicast-client** command adds or modifies an NTP multicast client.

The **no ntp multicast-client** command deletes an NTP multicast client.

Format

- **ntp multicast-client**
- **ntp multicast-client** *ipv4-address*
- **no ntp multicast-client** *ipv4-address*
- **no ntp multicast-client**

Parameter

Parameter	Description	Value
ipv4-address	Specifies a multicast IP address.	The value is in dotted decimal notation. The default value is 224.0.1.1.

Default Value

The default multicast IP address is 224.0.1.1.

View

VLANIF configuration view, Ethernet route interface configuration view, and Outband management interface configuration view

Usage Guidelines

You must enter a multicast IP address in the command.

Example

Add an NTP multicast client with IP address 239.255.255.255.

```
Switch(config-vlanif-4002)#ntp multicast-client 239.255.255.255
Switch(config-vlanif-4002)#
```

11.1.5 ntp broadcast-server**Function**

The **ntp broadcast-server** command adds or modifies an NTP broadcast server.

The **no ntp broadcast-server** command deletes an NTP broadcast server.

Format

- **ntp broadcast-server**
- **ntp broadcast-server** *ipv4-address*
- **ntp broadcast-server authentication-keyid** *key-id*
- **ntp broadcast-server authentication-keyid** *key-id* *ipv4-address*
- **ntp broadcast-server version** { **1** | **2** | **3** | **4** }
- **ntp broadcast-server version** { **1** | **2** | **3** | **4** } *ipv4-address*
- **ntp broadcast-server authentication-keyid** *key-id* **version** { **1** | **2** | **3** | **4** }
- **ntp broadcast-server authentication-keyid** *key-id* **version** { **1** | **2** | **3** | **4** } *ipv4-address*

- **no ntp broadcast-server**
- **no ntp broadcast-server *ipv4-address***

Parameter

Parameter	Description	Value
key-id	Specifies a key ID used when sending messages to the remote server.	The value is an integer ranging from 1 to 4294967295.
version { 1 2 3 4 }	Specifies an NTP version.	The default value is 3.
ipv4-address	Specifies a broadcast IP address.	The value is in dotted decimal notation. The default value is 255.255.255.0.

Default Value

The default NTP service version is 3.

View

VLANIF configuration view, Ethernet route interface configuration view, and Outband management interface configuration view

Usage Guidelines

You can use this command to enable an interface of a local switch to send NTP broadcast packets. When the local switch runs in server mode, it periodically sends, as a broadcast or multicast server, broadcast packets to broadcast or multicast clients. The client and server ends must be configured in the same mode, that is, broadcast or multicast mode.

Example

Add an NTP broadcast server.

```
Switch(config-vlanif-1)#ntp broadcast-server authentication-keyid 1 version 1
Switch(config-vlanif-1)#
```

11.1.6 ntp multicast-server

Function

The **ntp multicast-server** command adds or modifies an NTP multicast server.

The **no ntp multicast-server** command deletes an NTP multicast server.

Format

- **ntp multicast-server**
- **ntp multicast-server *ipv4-address***

- **ntp multicast-server authentication-keyid** *key-id*
- **ntp multicast-server authentication-keyid** *key-id ipv4-address*
- **ntp multicast-server version** { 1 | 2 | 3 | 4 }
- **ntp multicast-server version** { 1 | 2 | 3 | 4 } *ipv4-address*
- **ntp multicast-server ttl** *ttl-value*
- **ntp multicast-server ttl** *ttl-value ipv4-address*
- **ntp multicast-server version** { 1 | 2 | 3 | 4 } **ttl** *ttl-value*
- **ntp multicast-server version** { 1 | 2 | 3 | 4 } **ttl** *ttl-value ipv4-address*
- **ntp multicast-server authentication-keyid** *key-id version* { 1 | 2 | 3 | 4 } **ttl** *ttl-value*
- **ntp multicast-server authentication-keyid** *key-id version* { 1 | 2 | 3 | 4 } **ttl** *ttl-value ipv4-address*
- **no ntp multicast-server**
- **no ntp multicast-server** *ipv4-address*

Parameter

Parameter	Description	Value
keyid	Specifies a key ID used when sending messages to the remote server.	The value is an integer ranging from 1 to 4294967295.
ipv4-address	Specifies a multicast IPv4 address.	The value is in dotted decimal notation.
version { 1 2 3 4 }	Specifies an NTP version.	The default value is 3.
ttl-value	Specifies the TTL of the multicast packets.	The value is an integer ranging from 1 to 255. The default value is 8.

Default Value

The default multicast IP address is 224.0.1.1.

View

VLANIF configuration view, Ethernet route interface configuration view, and Outband management interface configuration view

Usage Guidelines

You must enter a multicast IP address in the command.

Example

Add an NTP multicast server.

```
Switch(config-vlanif-4002)#ntp multicast-server version 2 ttl 254
Switch(config-vlanif-4002)#
```

11.1.7 show ntp

Function

The **show ntp** command displays global NTP configuration information.

Format

show ntp

Parameter

NA

Default Value

NA

View

Common user view

Usage Guidelines

You can use this command to check the NTP configuration information in the configuration file.

Example

Check the global NTP configuration.

```
Switch>show ntp
Version                : NTP_VB3.00.00.00
ntp once sync          : disable
ntp client update-interval : 64s
ntp server broadcast-interval : 64s
ntp stratum             : 16
ntp master              : false
ntp authentication      : disable
Switch>
```

11.1.8 show ntp service

Function

The **show ntp service** command displays the NTP service information.

Format**show ntp service****Parameter**

NA

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

Display the NTP service information.

Switch>show ntp service

Mode	Source	Version	key-id	Offset(s)	Delay(s)	Disper(s)
unicast-peer	::	2	2	0.000000	0.000000	16.000000
unicast-peer	192.168.2.202	3	4294927694	0.000000	0.000000	16.000000
unicast-client	::	1	1	0.000000	0.000000	16.000000
unicast-client	192.168.1.202	4	4294927695	0.000000	0.000000	16.000000

Switch>

11.1.9 show ntp service verbose**Function**The **show ntp service verbose** command displays detailed information about the NTP service.**Format****show ntp service verbose****Parameter**

NA

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

Display detailed information about the NTP service.

```
Switch>show ntp service verbose
clock source: ::
  clock stratum: 16
  reference clock ID: ::
  local mode: active, local poll: 4
  peer mode: passive, peer poll: 0
  offset: 0.000000s, delay: 0.000000s, disper: The default value is 16.000000 seconds.
  root delay: 0.000000s, root disper: The default value is 0.000000 seconds.
  precision: -18, version: 2
  reftime: 00:00:00 UTC Jan 00 1900 (0.0)
  orgtime: 00:00:00 UTC Jan 00 1900 (0.0)
  rcvtime: 00:00:00 UTC Jan 00 1900 (0.0)
  xmttime: 00:00:00 UTC Jan 00 1900 (0.0)

clock source: 192.168.2.202
  clock stratum: 16
  reference clock ID: 192.168.2.202
  local mode: active, local poll: 4
  peer mode: passive, peer poll: 0
  offset: 0.000000s, delay: 0.000000s, disper: The default value is 16.000000 seconds.
  root delay: 0.000000s, root disper: The default value is 0.000000 seconds.
  precision: -18, version: 3
  reftime: 00:00:00 UTC Jan 00 1900 (0.0)
  orgtime: 00:00:00 UTC Jan 00 1900 (0.0)
  rcvtime: 00:00:00 UTC Jan 00 1900 (0.0)
  xmttime: 04:54:21 UTC Nov 01 2006 (c8f2a6fd.2666664c)

clock source: ::
  clock stratum: 16
  reference clock ID: ::
  local mode: client, local poll: 4
  peer mode: server, peer poll: 0
  offset: 0.000000s, delay: 0.000000s, disper: The default value is 16.000000 seconds.
  root delay: 0.000000s, root disper: The default value is 0.000000 seconds.
  precision: -18, version: 1
```

```
reftime: 00:00:00 UTC Jan 00 1900 (0.0)
orgtime: 00:00:00 UTC Jan 00 1900 (0.0)
rcvtime: 00:00:00 UTC Jan 00 1900 (0.0)
xmttime: 00:00:00 UTC Jan 00 1900 (0.0)

clock source: 192.168.1.202
clock stratum: 16
reference clock ID: 192.168.1.202
local mode: client, local poll: 4
peer mode: server, peer poll: 0
offset: 0.000000s, delay: 0.000000s, disper: The default value is 16.000000 seconds.
root delay: 0.000000s, root disper: The default value is 0.000000 seconds.
precision: -18, version: 4
reftime: 00:00:00 UTC Jan 00 1900 (0.0)
orgtime: 00:00:00 UTC Jan 00 1900 (0.0)
rcvtime: 00:00:00 UTC Jan 00 1900 (0.0)
xmttime: 04:54:22 UTC Nov 01 2006 (c8f2a6fe.2666664c)

clock source: ::
clock stratum: 16
reference clock ID: ::
local mode: server, local poll: 5
peer mode: client, peer poll: 0
offset: 0.000000s, delay: 0.000000s, disper: The default value is 16.000000 seconds.
root delay: 0.000000s, root disper: The default value is 0.000000 seconds.
precision: -18, version: 1
reftime: 00:00:00 UTC Jan 00 1900 (0.0)
orgtime: 00:00:00 UTC Jan 00 1900 (0.0)
rcvtime: 00:00:00 UTC Jan 00 1900 (0.0)
xmttime: 04:54:19 UTC Nov 01 2006 (c8f2a6fb.2666664c)

clock source: 0.0.0.0
clock stratum: 16
reference clock ID: 0.0.0.0
local mode: server, local poll: 5
peer mode: client, peer poll: 0
offset: 0.000000s, delay: 0.000000s, disper: The default value is 16.000000 seconds.
root delay: 0.000000s, root disper: The default value is 0.000000 seconds.
precision: -18, version: 4
reftime: 00:00:00 UTC Jan 00 1900 (0.0)
orgtime: 00:00:00 UTC Jan 00 1900 (0.0)
rcvtime: 00:00:00 UTC Jan 00 1900 (0.0)
xmttime: 04:54:19 UTC Nov 01 2006 (c8f2a6fb.2666664c)
```

```

clock source: 0.0.0.0
clock stratum: 16
reference clock ID: 0.0.0.0
local mode: server, local poll: 5
peer mode: client, peer poll: 0
offset: 0.000000s, delay: 0.000000s, disper: The default value is 16.000000 seconds.
root delay: 0.000000s, root disper: The default value is 0.000000 seconds.
precision: -18, version: 4
reftime: 00:00:00 UTC Jan 00 1900 (0.0)
orgtime: 00:00:00 UTC Jan 00 1900 (0.0)
rcvtime: 00:00:00 UTC Jan 00 1900 (0.0)
xmttime: 04:54:19 UTC Nov 01 2006 (c8f2a6fb.2666664c)
Switch>

```

11.1.10 show ntp config

Function

The **show ntp config** command displays NTP configuration information.

Format

show ntp config

Parameter

NA

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

View the NTP configuration.

```

Switch>show ntp config
!
ntp
client update-interval 10

```

```
stratum 9
authentication enable
ntp unicast-peer 201.1.1.1 version 4
Switch>
```

11.1.11 authentication {enable|disable}

Function

The **authentication {enable|disable}** command globally enables or disables MD5 authentication.

Format

authentication { enable | disable }

Parameter

Parameter	Description	Value
enable	Enables MD5 authentication.	-
disable	Disables MD5 authentication.	-

Default Value

By default, the MD5 authentication is disabled globally.

View

NTP configuration view

Usage Guidelines

For networks requiring high security, you can use this command to enable MD5 authentication globally.

Example

Enable MD5 authentication.

```
Switch(config-ntp)#authentication enable
Switch(config-ntp)#
```

Disable MD5 authentication.

```
Switch(config-ntp)#authentication disable
Switch(config-ntp)#
```

11.1.12 authentication-keyid

Function

The **authentication-keyid** command configures an NTP authentication key.

The **no authentication-keyid** command deletes an NTP authentication key.

Format

- **authentication-keyid** *key-id* **md5 key** *key-string*
- **authentication-keyid** *key-id* **md5 key { cipher | plain }** *key-string*
- **no authentication-keyid** *key-id*

Parameter

Parameter	Description	Value
key-id	Specifies a key ID.	The value is an integer ranging from 1 to 4294967295.
key-string	Indicates the key word.	The value is a string of no more than 16 characters.
{ cipher plain }	Displays the password in cipher text or plain text.	-

Default Value

By default, no authentication key is configured.

View

NTP configuration view

Usage Guidelines

You can use this command to configure the NTP authentication key. The switch supports only MD5 authentication.

Example

Set the MD5 authentication key ID to 100 and key content to FHNtestkey.

```
Switch(config-ntp)#authentication-keyid 100 md5 key FHNtestkey
Switch(config-ntp)#
```

Delete a configured authentication key.

```
Switch(config-ntp)#no authentication-keyid 100
Switch(config-ntp)#
```

11.1.13 client update-interval

Function

The **client update-interval** command configures the interval for updating the NTP client.

Format

client update-interval { *update-interval-time* | **default** }

Parameter

Parameter	Description	Value
update-interval-time	Specifies an interval for updating the NTP client.	The value is an integer ranging from 4 to 17 (a power of 2), in seconds.
default	Specifies the default interval for updating the NTP client.	The value is a character string.

Default Value

The default value of update-interval-time is 2, that is the default interval for updating the NTP client is 2⁶ seconds.

View

NTP configuration view

Usage Guidelines

2ⁿ seconds

Example

Set the interval for updating the NTP client to 2⁸ seconds.

```
Switch(config-ntp)#client update-interval 8
Switch(config-ntp)#show ntp
ntp client update-interval      : 256s
ntp server broadcast-interval : 64s
ntp stratum                     : 16
ntp master                     : false
ntp authentication              : disable
Switch(config-ntp)#
```

11.1.14 master

Function

The **master** command configures the switch as the primary clock.

The **no master** command cancels the primary clock configuration.

Format

- **master**
- **no master**

Parameter

NA

Default Value

By default, the device is not a primary clock.

View

NTP configuration view

Usage Guidelines

You can use this command to configure the switch as the primary clock. The primary clock can be used as a server to synchronize time of other devices.

Example

Configure the switch as the primary clock.

```
Switch(config-ntp)#master
Switch(config-ntp)#
```

11.1.15 ntp unicast-peer

Function

The **ntp unicast-peer** command creates or modifies an IPv4 NTP active peer. The command supports peer configuration in VPN instances.

The **no ntp unicast-peer** command deletes an IPv4 NTP active peer.

Format

- **ntp unicast-peer** *ipv4-address*
- **ntp unicast-peer** *ipv4-address authentication-keyid key-id*
- **ntp unicast-peer** *ipv4-address authentication-keyid key-id source-interface loopback loopback-number*
- **ntp unicast-peer** *ipv4-address authentication-keyid key-id source-interface vlan vlan-id*
- **ntp unicast-peer** *ipv4-address authentication-keyid key-id vpn-instance vpn-instance-name*

- **ntp unicast-peer** *ipv4-address authentication-keyid key-id vpn-instance vpn-instance-name source-interface loopback loopback-number*
- **ntp unicast-peer** *ipv4-address authentication-keyid key-id vpn-instance vpn-instance-name source-interface vlan vlan-id*
- **ntp unicast-peer** *ipv4-address authentication-keyid key-id vpn-instance vpn-instance-name source-interface { ethernet | xgigaethernet | 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet } interface-number*
- **ntp unicast-peer** *ipv4-address authentication-keyid key-id source-interface { ethernet | xgigaethernet | 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet } interface-number*
-
- **ntp unicast-peer** *ipv4-address source-interface loopback loopback-number*
- **ntp unicast-peer** *ipv4-address source-interface vlan vlan-id*
- **ntp unicast-peer** *ipv4-address source-interface { ethernet | xgigaethernet | 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet } interface-number*
- **ntp unicast-peer** *ipv4-address version version-value*
- **ntp unicast-peer** *ipv4-address version version-value authentication-keyid key-id*
- **ntp unicast-peer** *ipv4-address version version-value authentication-keyid key-id source-interface loopback loopback-number*
- **ntp unicast-peer** *ipv4-address version version-value authentication-keyid key-id source-interface vlan vlan-id*
- **ntp unicast-peer** *ipv4-address version version-value authentication-keyid key-id vpn-instance vpn-instance-name*
- **ntp unicast-peer** *ipv4-address version version-value authentication-keyid key-id vpn-instance vpn-instance-name source-interface loopback loopback-number*
- **ntp unicast-peer** *ipv4-address version version-value authentication-keyid key-id vpn-instance vpn-instance-name source-interface vlan vlan-id*
- **ntp unicast-peer** *ipv4-address version version-value authentication-keyid key-id source-interface { ethernet | xgigaethernet | 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet } interface-number*

- **ntp unicast-peer** *ipv4-address* **version** *version-value* **authentication-keyid** *key-id*
vpn-instance *vpn-instance-name* **source-interface** { **ethernet** | **xgigaethernet** | **10gigaethernet** | **25gigaethernet** | **40gigaethernet** | **100gigaethernet** } *interface-number*
- **ntp unicast-peer** *ipv4-address* **version** *version-value* **source-interface** **loopback** *loopback-number*
- **ntp unicast-peer** *ipv4-address* **version** *version-value* **source-interface** **vlan** *vlan-id*
- **ntp unicast-peer** *ipv4-address* **version** *version-value* **source-interface** { **ethernet** | **xgigaethernet** | **10gigaethernet** | **25gigaethernet** | **40gigaethernet** | **100gigaethernet** } *interface-number*
- **ntp unicast-peer** *ipv4-address* **version** *version-value* **vpn-instance** *vpn-instance-name*
- **ntp unicast-peer** *ipv4-address* **version** *version-value* **vpn-instance** *vpn-instance-name* **source-interface** **loopback** *loopback-number*
- **ntp unicast-peer** *ipv4-address* **version** *version-value* **vpn-instance** *vpn-instance-name* **source-interface** **vlan** *vlan-id*
- **ntp unicast-peer** *ipv4-address* **version** *version-value* **vpn-instance** *vpn-instance-name* **source-interface** { **ethernet** | **xgigaethernet** | **10gigaethernet** | **25gigaethernet** | **40gigaethernet** | **100gigaethernet** } *interface-number*
- **ntp unicast-peer** *ipv4-address* **vpn-instance** *vpn-instance-name*
- **ntp unicast-peer** *ipv4-address* **vpn-instance** *vpn-instance-name* **source-interface** **loopback** *loopback-number*
- **ntp unicast-peer** *ipv4-address* **vpn-instance** *vpn-instance-name* **source-interface** **vlan** *vlan-id*
- **ntp unicast-peer** *ipv4-address* **vpn-instance** *vpn-instance-name* **source-interface** { **ethernet** | **xgigaethernet** | **10gigaethernet** | **25gigaethernet** | **40gigaethernet** | **100gigaethernet** } *interface-number*
- **no ntp unicast-peer** *ipv4-address*

Parameter

Parameter	Description	Value
ipv4-address	Specifies an IP address in the static ARP entry.	The value is in dotted decimal notation.
version-value	Specifies an NTP version.	The value is an integer ranging from 1 to 4.
key-id	Specifies an NTP verification key.	The value is an integer ranging from 1 to 4294967295.

Parameter	Description	Value
vpn-instance-name	Specifies a VPN instance name.	The value is a string of up to 64 characters.
loopback-number	Specifies a loopback interface number.	The value is an integer ranging from 1 to 127.
vlan-id	Specifies a VLAN ID.	The value is an integer ranging from 1 to 4094.
interface-number	Specifies an Ethernet interface number.	The value is an integer in the range of <1-1>/<0-1>/<1-48>.

Default Value

The default NTP service version is 3.

View

NTP configuration view

Usage Guidelines

You can run this command to specify or not specify an IPv4 peer pair for a device. The specified IP address is the IP address of the peer device, and the version refers to the key configured for the NTP protocol version number.

Example

Add an IPv4 NTP active peer.

```
Switch(config-ntp)#ntp unicast-peer 1.1.1.1 version 3 authentication-keyid 100
Switch(config-ntp)#
```

Add an IPv4 NTP active peer for VPN instance 1.

```
Switch(config-ntp)#ntp unicast-peer 192.168.2.202 version 1 authentication-keyid 4294967295 vpn-instance
vpn1
Switch(config-ntp)#
```

11.1.16 ntp unicast-server

Function

The **ntp unicast-server** command designates a unicast IPv4 NTP server for the switch. The command supports configuration in VPN instances.

The **no ntp unicast-server** command cancels a unicast IPv4 NTP server for the device.

Format

- **ntp unicast-server** *ipv4-address*
- **ntp unicast-server** *ipv4-address authentication-keyid key-id*

- **ntp unicast-server** *ipv4-address authentication-keyid key-id source-interface loopback loopback-number*
- **ntp unicast-server** *ipv4-address authentication-keyid key-id source-interface vlan vlan-id*
- **ntp unicast-server** *ipv4-address authentication-keyid key-id source-interface { ethernet | xgigaethernet | 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet } interface-number*
- **ntp unicast-server** *ipv4-address authentication-keyid key-id vpn-instance vpn-instance-name*
- **ntp unicast-server** *ipv4-address authentication-keyid key-id vpn-instance vpn-instance-name source-interface loopback loopback-number*
- **ntp unicast-server** *ipv4-address authentication-keyid key-id vpn-instance vpn-instance-name source-interface vlan vlan-id*
- **ntp unicast-server** *ipv4-address authentication-keyid key-id vpn-instance vpn-instance-name source-interface { ethernet | xgigaethernet | 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet } interface-number*
- **ntp unicast-server** *ipv4-address source-interface loopback loopback-number*
- **ntp unicast-server** *ipv4-address source-interface vlan vlan-id*
- **ntp unicast-server** *ipv4-address source-interface { ethernet | xgigaethernet | 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet } interface-number*
- **ntp unicast-server** *ipv4-address burst { enable | disable }*
- **ntp unicast-server** *ipv4-address preference { enable | disable }*
- **ntp unicast-server** *ipv4-address version version-value*
- **ntp unicast-server** *ipv4-address version version-value authentication-keyid key-id*
- **ntp unicast-server** *ipv4-address version version-value authentication-keyid key-id source-interface loopback loopback-number*
- **ntp unicast-server** *ipv4-address version version-value authentication-keyid key-id source-interface vlan vlan-id*
- **ntp unicast-server** *ipv4-address version version-value authentication-keyid key-id source-interface { ethernet | xgigaethernet | 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet } interface-number*

- **ntp unicast-server** *ipv4-address* **version** *version-value* **authentication-keyid** *key-id*
vpn-instance *vpn-instance-name*
- **ntp unicast-server** *ipv4-address* **version** *version-value* **authentication-keyid** *key-id*
vpn-instance *vpn-instance-name* **source-interface loopback** *loopback-number*
- **ntp unicast-server** *ipv4-address* **version** *version-value* **authentication-keyid** *key-id*
vpn-instance *vpn-instance-name* **source-interface vlan** *vlan-id*
- **ntp unicast-server** *ipv4-address* **version** *version-value* **authentication-keyid** *key-id*
vpn-instance *vpn-instance-name* **source-interface** { **ethernet** | **xgigaethernet** |
10gigaethernet | **25gigaethernet** | **40gigaethernet** | **100gigaethernet** } *interface-number*
- **ntp unicast-server** *ipv4-address* **version** *version-value* **source-interface** { **ethernet** |
xgigaethernet | **10gigaethernet** | **25gigaethernet** | **40gigaethernet** | **100gigaethernet** }
interface-number
- **ntp unicast-server** *ipv4-address* **version** *version-value* **source-interface loopback**
loopback-number
- **ntp unicast-server** *ipv4-address* **version** *version-value* **source-interface vlan** *vlan-id*
- **ntp unicast-server** *ipv4-address* **version** *version-value* **vpn-instance** *vpn-instance-name*
- **ntp unicast-server** *ipv4-address* **version** *version-value* **vpn-instance** *vpn-instance-name*
source-interface loopback *loopback-number*
- **ntp unicast-server** *ipv4-address* **version** *version-value* **vpn-instance** *vpn-instance-name*
source-interface vlan *vlan-id*
- **ntp unicast-server** *ipv4-address* **version** *version-value* **vpn-instance** *vpn-instance-name*
source-interface { **ethernet** | **xgigaethernet** | **10gigaethernet** | **25gigaethernet** |
40gigaethernet | **100gigaethernet** } *interface-number*
- **ntp unicast-server** *ipv4-address* **vpn-instance** *vpn-instance-name*
- **ntp unicast-server** *ipv4-address* **vpn-instance** *vpn-instance-name* **source-interface loopback**
loopback-number
- **ntp unicast-server** *ipv4-address* **vpn-instance** *vpn-instance-name* **source-interface vlan**
vlan-id
- **ntp unicast-server** *ipv4-address* **vpn-instance** *vpn-instance-name* **source-interface** { **ethernet**
| **xgigaethernet** | **10gigaethernet** | **25gigaethernet** | **40gigaethernet** | **100gigaethernet** }
interface-number

- **no ntp unicast-server** *ipv4-address*

Parameter

Parameter	Description	Value
ipv4-address	Indicates an IP address of the peer unicast NTP server.	The value is in dotted decimal notation.
version-value	Specifies an NTP version.	The value is an integer ranging from 1 to 4. The default version number is 3.
key-id	Specifies an NTP verification key.	The value is an integer ranging from 1 to 4294967295.
vpn-instance-name	Specifies a VPN instance name.	The value is a string of up to 64 characters.
loopback-number	Specifies a loopback interface number.	The value is an integer ranging from 1 to 127.
vlan-id	Specifies a VLAN ID.	The value is an integer ranging from 1 to 4094.
interface-number	Specifies an Ethernet interface number.	The value is an integer in the range of <1-1>/<0-1>/<1-48>.

Default Value

The default NTP service version is 3.

View

NTP configuration view

Usage Guidelines

NA

Example

Configure a unicast IPv4 NTP server.

```
Switch(config-ntp)#ntp unicast-server 1.1.1.1 version 4 authentication-keyid 100
Switch(config-ntp)#
```

Configure a unicast IPv4 NTP server in VPN instance 1.

```
Switch(config-ntp)#ntp unicast-server 192.168.1.205 vpn-instance vpn1
Switch(config-ntp)#
```

11.1.17 oncesync

Function

The **oncesync** command enables or disables a synchronization operation.

Format

oncesync { enable | disable }

Parameter

Parameter	Description	Value
enable	Enables a synchronization operation.	-
disable	Disables a synchronization operation.	-

Default Value

Disable

View

NTP configuration view

Usage Guidelines

You can use this command to enable or disable the concurrency mechanism in the process of synchronizing packet interaction.

Example

Enable a synchronization operation.

```
Switch(config-ntp)#oncesync enable
Switch(config-ntp)#
```

11.1.18 server broadcast-interval

Function

The **server broadcast-interval** command configures the broadcast interval of the NTP server.

Format

server broadcast-interval { interval | default }

Parameter

Parameter	Description	Value
interval	Indicates a broadcast interval of the NTP server.	The value is an integer ranging from 4 to 17, in seconds.
default	Specifies the default value.	6

Default Value

2⁶ seconds

View

NTP configuration view

Usage Guidelines

You can use this command to configure the broadcast interval of the NTP server, so that the NTP server can periodically broadcast its own time.

Example

Set the broadcast interval of the NTP server to 2^{10} seconds.

```
Switch(config-ntp)#server broadcast-interval 10
Switch(config-ntp)#
```

11.1.19 stratum

Function

The **stratum** command configures the NTP clock hierarchy.

Format

stratum { *layer-number* | **default** }

Parameter

Parameter	Description	Value
layer-number	Specifies the number of system clock layers.	The value is an integer ranging from 1 to 16.

Default Value

16

View

NTP configuration view

Usage Guidelines

NA

Example

Set the number of NTP layers to 2^{10} .

```
Switch(config-ntp)#stratum 10
Switch(config-ntp)#
```

11.1.20 trusted-keyid {enable|disable}

Function

The **trusted-keyid {enable|disable}** command enables or disables trusting of any MD5 authentication key.

Format

trusted-keyid *trusted-keyid-time* { **enable** | **disable** }

Parameter

Parameter	Description	Value
trusted-keyid-time	Indicates an MD5 authentication key.	The value is an integer ranging from 1 to 4294967295.
enable	Enables MD5 authentication.	-
disable	Disables MD5 authentication.	-

Default Value

By default, the NTP MD5 authentication key is not trusted.

View

NTP configuration view

Usage Guidelines

NA

Example

Enable trusting of any MD5 authentication key

```
Switch(config-ntp)#trusted-keyid 1 enable
Switch(config-ntp)#
```

11.1.21 ntp6 multicast-client

Function

The **ntp6 multicast-client** command adds or modifies an NTPv6 multicast client.

The **no ntp6 multicast-client** command deletes an NTPv6 multicast client.

Format

- **ntp6 multicast-client**
- **ntp6 multicast-client** *ipv6-address*

- **ntp6 multicast-client authentication-keyid** *key-id*
- **ntp6 multicast-client authentication-keyid** *key-id* *ipv6-address*
- **no ntp6 multicast-client** *ipv6-address*
- **no ntp6 multicast-client**

Parameter

Parameter	Description	Value
ipv6-address	Specifies a multicast IPv6 address.	FF1x::/32 and FF2x::/32
key-id	Specifies a key ID used when sending messages to the remote server.	The value is an integer ranging from 1 to 4294967295.

Default Value

NA

View

VLANIF configuration view, Ethernet route interface configuration view, Ethernet sub-interface configuration view, Trunk sub-interface configuration view, and Outband management interface configuration view

Usage Guidelines

You must enter a multicast IP address in the command.

Example

Add an NTP multicast client address of FF01::1111:1.

```
Switch(config-vlanif-4002)#ntp6 multicast-client FF01::1111:1
Switch(config-vlanif-4002)#
```

11.1.22 ntp6 multicast-server

Function

The **ntp6 multicast-server** command adds or modifies an NTPv6 multicast server.

The **no ntp6 multicast-server** command deletes an NTPv6 multicast server.

Format

- **ntp6 multicast-server**
- **ntp6 multicast-server** *ipv6-address*
- **ntp6 multicast-server authentication-keyid** *key-id*

- **ntp6 multicast-server authentication-keyid** *key-id* *ipv6-address*
- **ntp6 multicast-server authentication-keyid** *key-id* **version** { 1 | 2 | 3 | 4 } **ttl** *ttl-value*
- **ntp6 multicast-server authentication-keyid** *key-id* **version** { 1 | 2 | 3 | 4 } **ttl** *ttl-value* *ipv6-address*
- **ntp6 multicast-server ttl** *ttl-value*
- **ntp6 multicast-server ttl** *ttl-value* *ipv6-address*
- **ntp6 multicast-server version** { 1 | 2 | 3 | 4 }
- **ntp6 multicast-server version** { 1 | 2 | 3 | 4 } *ipv6-address*
- **ntp6 multicast-server version** { 1 | 2 | 3 | 4 } **ttl** *ttl-value*
- **ntp6 multicast-server version** { 1 | 2 | 3 | 4 } **ttl** *ttl-value* *ipv6-address*
- **no ntp6 multicast-server**
- **no ntp6 multicast-server** *ipv6-address*

Parameter

Parameter	Description	Value
key-id	Specifies a key ID used when sending messages to the remote server.	The value is an integer in the range 1 to 4294967295.
ipv6-address	Specifies a multicast IPv6 address.	FF1x::/32 and FF2x::/32
version { 1 2 3 4 }	Specifies an NTP version.	The default value is 3.
ttl-value	Specifies the TTL of the multicast packets.	The value is an integer ranging from 1 to 255. The default value is 8.

Default Value

NA

View

VLANIF configuration view, Ethernet route interface configuration view, Ethernet sub-interface configuration view, Trunk sub-interface configuration view, and Outband management interface configuration view

Usage Guidelines

You must enter a multicast IP address in the command.

Example

Add an NTP multicast server.

```
Switch(config-vlanif-4002)#ntp6 multicast-server version 2 ttl 254
Switch(config-vlanif-4002)#
```

11.1.23 ntp6 unicast-peer

Function

The **ntp6 unicast-peer** command adds or modifies an IPv6 NTP active peer pair and supports configuration of multi-instance VPNs.

The **no ntp6 unicast-peer** command deletes an IPv6 NTP active peer pair.

Format

- **ntp6 unicast-peer** *ipv6-address*
- **ntp6 unicast-peer** *ipv6-address authentication-keyid key-id*
- **ntp6 unicast-peer** *ipv6-address authentication-keyid key-id source-interface { ethernet | xgigaethernet | 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet } interface-number*
- **ntp6 unicast-peer** *ipv6-address authentication-keyid key-id source-interface loopback loopback-number*
- **ntp6 unicast-peer** *ipv6-address authentication-keyid key-id source-interface vlan vlan-id*
- **ntp6 unicast-peer** *ipv6-address authentication-keyid key-id vpn-instance vpn-instance-name*
- **ntp6 unicast-peer** *ipv6-address authentication-keyid key-id vpn-instance vpn-instance-name source-interface { ethernet | xgigaethernet | 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet } interface-number*
- **ntp6 unicast-peer** *ipv6-address authentication-keyid key-id vpn-instance vpn-instance-name source-interface loopback loopback-number*
- **ntp6 unicast-peer** *ipv6-address authentication-keyid key-id vpn-instance vpn-instance-name source-interface vlan vlan-id*
- **ntp6 unicast-peer** *ipv6-address source-interface { ethernet | xgigaethernet | 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet } interface-number*
- **ntp6 unicast-peer** *ipv6-address source-interface loopback loopback-number*
- **ntp6 unicast-peer** *ipv6-address source-interface vlan vlan-id*

- **ntp6 unicast-peer** *ipv6-address version version-value*
- **ntp6 unicast-peer** *ipv6-address version version-value authentication-keyid key-id*
- **ntp6 unicast-peer** *ipv6-address version version-value authentication-keyid key-id*
source-interface { **ethernet** | **xgigaethernet** | **10gigaethernet** | **25gigaethernet** |
40gigaethernet | **100gigaethernet** } *interface-number*
- **ntp6 unicast-peer** *ipv6-address version version-value authentication-keyid key-id*
source-interface loopback *loopback-number*
- **ntp6 unicast-peer** *ipv6-address version version-value authentication-keyid key-id*
source-interface vlan *vlan-id*
- **ntp6 unicast-peer** *ipv6-address version version-value authentication-keyid key-id*
vpn-instance *vpn-instance-name*
- **ntp6 unicast-peer** *ipv6-address version version-value authentication-keyid key-id*
vpn-instance *vpn-instance-name source-interface* { **ethernet** | **xgigaethernet** |
10gigaethernet | **25gigaethernet** | **40gigaethernet** | **100gigaethernet** } *interface-number*
- **ntp6 unicast-peer** *ipv6-address version version-value authentication-keyid key-id*
vpn-instance *vpn-instance-name source-interface loopback* *loopback-number*
- **ntp6 unicast-peer** *ipv6-address version version-value authentication-keyid key-id*
vpn-instance *vpn-instance-name source-interface vlan* *vlan-id*
- **ntp6 unicast-peer** *ipv6-address version version-value source-interface* { **ethernet** |
xgigaethernet | **10gigaethernet** | **25gigaethernet** | **40gigaethernet** | **100gigaethernet** }
interface-number
- **ntp6 unicast-peer** *ipv6-address version version-value source-interface loopback*
loopback-number
- **ntp6 unicast-peer** *ipv6-address version version-value source-interface vlan* *vlan-id*
- **ntp6 unicast-peer** *ipv6-address version version-value vpn-instance* *vpn-instance-name*
- **ntp6 unicast-peer** *ipv6-address version version-value vpn-instance* *vpn-instance-name*
source-interface { **ethernet** | **xgigaethernet** | **10gigaethernet** | **25gigaethernet** |
40gigaethernet | **100gigaethernet** } *interface-number*
- **ntp6 unicast-peer** *ipv6-address version version-value vpn-instance* *vpn-instance-name*
source-interface loopback *loopback-number*
- **ntp6 unicast-peer** *ipv6-address version version-value vpn-instance* *vpn-instance-name*

source-interface *vlan* *vlan-id*

- **ntp6 unicast-peer** *ipv6-address* **vpn-instance** *vpn-instance-name*
- **ntp6 unicast-peer** *ipv6-address* **vpn-instance** *vpn-instance-name* **source-interface** { **ethernet** | **xgigaethernet** | **10gigaethernet** | **25gigaethernet** | **40gigaethernet** | **100gigaethernet** } *interface-number*
- **ntp6 unicast-peer** *ipv6-address* **vpn-instance** *vpn-instance-name* **source-interface** **loopback** *loopback-number*
- **ntp6 unicast-peer** *ipv6-address* **vpn-instance** *vpn-instance-name* **source-interface** **vlan** *vlan-id*
- **no ntp6 unicast-peer** *ipv6-address*

Parameter

Parameter	Description	Value
ipv6-address	Specifies an IPv6 address.	-
version-value	Specifies an NTP version.	The value is an integer ranging from 1 to 4.
key-id	Specifies an NTP verification key.	The value is an integer ranging from 1 to 4294967295.
vpn-instance-name	Specifies a VPN instance name.	The value is a string of up to 64 characters.
loopback-number	Specifies a loopback interface number.	The value is an integer ranging from 1 to 127.
vlan-id	Specifies a VLAN ID.	The value is an integer ranging from 1 to 4094.
interface-number	Specifies an Ethernet interface number.	The value is an integer in the range of <1-1>/<0-1>/<1-48>.

Default Value

The default NTP service version is 3.

View

NTP configuration view

Usage Guidelines

You can run this command to specify or not specify an IPv6 peer pair for a device. The specified IPv6 address is the IPv6 address of the peer device, and the version refers to the key configured for the NTP protocol version number.

Example

Add an IPv6 NTP active peer.

```
Switch(config-ntp)#ntp6 unicast-peer 2000::1 version 3 authentication-keyid 100
Switch(config-ntp)#
```

Add an IPv6 NTP active peer for VPN instance 1.

```
Switch(config-ntp)#ntp6 unicast-peer 2001::1 version 1 authentication-keyid 4294967295 vpn-instance vpn1
Switch(config-ntp)#
```

11.1.24 ntp6 unicast-server

Function

The **ntp6 unicast-server** command specifies a unicast IPv6 NTP server for a device and supports NTP unicast VPN configuration with multiple instances.

The **no ntp6 unicast-server** command cancels the unicast IPv6 NTP server specified for a device.

Format

- **ntp6 unicast-server** *ipv6-address*
- **ntp6 unicast-server** *ipv6-address authentication-keyid key-id*
- **ntp6 unicast-server** *ipv6-address authentication-keyid key-id source-interface { ethernet | xgigaethernet | 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet } interface-number*
- **ntp6 unicast-server** *ipv6-address authentication-keyid key-id source-interface loopback loopback-number*
- **ntp6 unicast-server** *ipv6-address authentication-keyid key-id source-interface vlan vlan-id*
- **ntp6 unicast-server** *ipv6-address authentication-keyid key-id vpn-instance vpn-instance-name*
- **ntp6 unicast-server** *ipv6-address authentication-keyid key-id vpn-instance vpn-instance-name source-interface { ethernet | xgigaethernet | 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet } interface-number*
- **ntp6 unicast-server** *ipv6-address authentication-keyid key-id vpn-instance vpn-instance-name source-interface loopback loopback-number*
- **ntp6 unicast-server** *ipv6-address authentication-keyid key-id vpn-instance vpn-instance-name source-interface vlan vlan-id*

- **ntp6 unicast-server** *ipv6-address* **source-interface** { **ethernet** | **xgigaethernet** | **10gigaethernet** | **25gigaethernet** | **40gigaethernet** | **100gigaethernet** } *interface-number*
- **ntp6 unicast-server** *ipv6-address* **source-interface loopback** *loopback-number*
- **ntp6 unicast-server** *ipv6-address* **source-interface vlan** *vlan-id*
- **ntp6 unicast-server** *ipv6-address* **version** *version-value*
- **ntp6 unicast-server** *ipv6-address* **version** *version-value* **authentication-keyid** *key-id*
- **ntp6 unicast-server** *ipv6-address* **version** *version-value* **authentication-keyid** *key-id* **source-interface** { **ethernet** | **xgigaethernet** | **10gigaethernet** | **25gigaethernet** | **40gigaethernet** | **100gigaethernet** } *interface-number*
- **ntp6 unicast-server** *ipv6-address* **version** *version-value* **authentication-keyid** *key-id* **source-interface loopback** *loopback-number*
- **ntp6 unicast-server** *ipv6-address* **version** *version-value* **authentication-keyid** *key-id* **source-interface vlan** *vlan-id*
- **ntp6 unicast-server** *ipv6-address* **version** *version-value* **authentication-keyid** *key-id* **vpn-instance** *vpn-instance-name*
- **ntp6 unicast-server** *ipv6-address* **version** *version-value* **authentication-keyid** *key-id* **vpn-instance** *vpn-instance-name* **source-interface** { **ethernet** | **xgigaethernet** | **10gigaethernet** | **25gigaethernet** | **40gigaethernet** | **100gigaethernet** } *interface-number*
- **ntp6 unicast-server** *ipv6-address* **version** *version-value* **authentication-keyid** *key-id* **vpn-instance** *vpn-instance-name* **source-interface loopback** *loopback-number*
- **ntp6 unicast-server** *ipv6-address* **version** *version-value* **authentication-keyid** *key-id* **vpn-instance** *vpn-instance-name* **source-interface vlan** *vlan-id*
- **ntp6 unicast-server** *ipv6-address* **version** *version-value* **source-interface** { **ethernet** | **xgigaethernet** | **10gigaethernet** | **25gigaethernet** | **40gigaethernet** | **100gigaethernet** } *interface-number*
- **ntp6 unicast-server** *ipv6-address* **version** *version-value* **source-interface loopback** *loopback-number*
- **ntp6 unicast-server** *ipv6-address* **version** *version-value* **source-interface vlan** *vlan-id*
- **ntp6 unicast-server** *ipv6-address* **version** *version-value* **vpn-instance** *vpn-instance-name*

- **ntp6 unicast-server** *ipv6-address* **version** *version-value* **vpn-instance** *vpn-instance-name*
source-interface { **ethernet** | **xgigaethernet** | **10gigaethernet** | **25gigaethernet** |
40gigaethernet | **100gigaethernet** } *interface-number*
- **ntp6 unicast-server** *ipv6-address* **version** *version-value* **vpn-instance** *vpn-instance-name*
source-interface loopback *loopback-number*
- **ntp6 unicast-server** *ipv6-address* **version** *version-value* **vpn-instance** *vpn-instance-name*
source-interface vlan *vlan-id*
- **ntp6 unicast-server** *ipv6-address* **vpn-instance** *vpn-instance-name*
- **ntp6 unicast-server** *ipv6-address* **vpn-instance** *vpn-instance-name* **source-interface**
{ **ethernet** | **xgigaethernet** | **10gigaethernet** | **25gigaethernet** | **40gigaethernet** |
100gigaethernet } *interface-number*
- **ntp6 unicast-server** *ipv6-address* **vpn-instance** *vpn-instance-name* **source-interface loopback**
loopback-number
- **ntp6 unicast-server** *ipv6-address* **vpn-instance** *vpn-instance-name* **source-interface vlan**
vlan-id
- **no ntp6 unicast-server** *ipv6-address*

Parameter

Parameter	Description	Value
ipv6-address	Specifies the IPv6 address of the peer unicast server.	-
version-value	Specifies an NTP version.	The value is an integer ranging from 1 to 4. The default version number is 3.
key-id	Specifies an NTP verification key.	The value is an integer ranging from 1 to 4294967295.
vpn-instance-name	Specifies a VPN instance name.	The value is a string of up to 64 characters.
loopback-number	Specifies a loopback interface number.	The value is an integer ranging from 1 to 127.
vlan-id	Specifies a VLAN ID.	The value is an integer ranging from 1 to 4094.
interface-number	Specifies an Ethernet interface number.	The value is an integer in the range of <1-1>/<0-1>/<1-48>.

Default Value

The default NTP service version is 3.

View

NTP configuration view

Usage Guidelines

NA

Example

Configure a unicast IPv6 NTP server.

```
Switch(config-ntp)#ntp6 unicast-server 2000::1 version 4 authentication-keyid 100
Switch(config-ntp)#
```

Configure a unicast IPv6 NTP server in VPN instance 1.

```
Switch(config-ntp)#ntp6 unicast-server 2002::1 vpn-instance vpn1
Switch(config-ntp)#
```

11.1.25 timestamp precision-time

Function

The **timestamp precision-time** command configures the time precision of the timestamp.

Format

timestamp precision-time { second | millisecond | default }

Parameter

Parameter	Description	Value
second	Specifies second as the time precision.	-
millisecond	Specifies millisecond as the time precision.	-
default	Specifies the default time precision.	second

Default Value

Specifies the number of seconds.

View

Global configuration view

Usage Guidelines

NA

Example

Configure the time precision of the timestamp.

```
Switch(config)#timestamp precision-time millisecond
```

```
Switch(config)#
```

11.1.26 icmp timestamp to-cpu

Function

The **icmp timestamp to-cpu** command enables or disables adding timestamps to ICMP packets sent to the CPU.

Format

icmp timestamp to-cpu { enable | disable }

Parameter

NA

Default Value

By default, ICMP packets sent to the CPU do not carry timestamps.

View

Global configuration view

Usage Guidelines

NA

Example

Enable a port to add timestamps to ICMP packets sent to the CPU.

```
Switch(config)#icmp timestamp to-cpu enable
Switch(config)#
```

11.2 RMON Configuration Commands

11.2.1 rmon history

Function

The **rmon history** command configures a RMON historical record control entry.

The **no rmon history** command deletes a RMON historical record control entry.

Format

Ethernet bridge interface configuration view, Ethernet route interface configuration view, and Trunk interface configuration view

- **rmon history** *history-id sampling-interval sample-number* [owner]

Ethernet route interface configuration view:

- **no rmon history** *history-id*

Parameter

Parameter	Description	Value
history-id	Specifies the ID of an RMON history record control entry.	The value is an integer ranging from 1 to 65535.
sampling-interval	Specifies the interval for sampling.	The value is an integer ranging from 1 to 3600, in seconds.
sample-number	Specifies the number of saved samples.	The value is an integer ranging from 1 to 65535.
[owner]	Specifies a user requesting for RMON information (optional).	The value is a character string.

Default Value

NA

View

The view is specified in the command.

Usage Guidelines

You can use this command to set the sampling interval and quantity of saved samples. If the quantity of saved samples is too large, the switch allocates the samples according to the resource situation. The RMON periodically collect data on interfaces for storage and checking.

Example

Configure a RMON historical record control entry and set the sampling interval to 10s and quantity of saved samples to 30.

```
Switch(config-10ge1/0/1)#rmon history 1 10 30
Switch(config-10ge1/0/1)#
```

11.2.2 rmon statistics

Function

The **rmon statistics** command configures control for the RMON statistics record.

The **no rmon statistics** command deletes control for the RMON statistics record.

Format

- **rmon statistics** *statistics-id* [*owner*]
- **no rmon statistics** *statistics-id*

Parameter

Parameter	Description	Value
statistics-id	Specifies an RMON statistics control entry.	The value is an integer ranging from 1 to 65535.
[owner]	Specifies a user requesting for RMON information (optional).	The value is a character string.

Default Value

NA

View

Ethernet bridge interface configuration view, Ethernet routing interface configuration view, Trunk interface configuration view

Usage Guidelines

You can use this command to configure RMON statistics measurement and enable the switch to measure errors of the monitoring interfaces.

Example

Configure a RMON statistics record control entry.

```
Switch(config-10ge1/0/1)#rmon statistics 1
Switch(config-10ge1/0/1)#
```

11.2.3 show rmon alarm

Function

The **show rmon alarm** command displays configuration of RMON alarm control entries.

Format

show rmon alarm

Parameter

NA

Default Value

NA

View

Common user view

Usage Guidelines

You can use this command to view configuration information on a RMON alarm control entry, including the alarm ID, alarm query interval, rising threshold, and falling threshold.

Example

Display the configuration of RMON alarm control entries.

```
Switch>show rmon alarm
RMON Event 1 log successedarm
  RMON Alarm:1
    Interval:2
    Source OID:1.3.6.1.2.1.2.2.1.8.2
    Sample Type:absolute value
    Alarm Value:2
    Startup Alarm:risingOrFallingAlarm
    Rising Threshold:1
    Rising Event:1
    Falling Threshold:2
    Falling Event:1
    Owner:CLI
    Status:valid
Switch>
```

11.2.4 show rmon config**Function**

The **show rmon config** command displays configuration of RMON events.

Format

show rmon config

Parameter

NA

Default Value

NA

View

Common user view

Usage Guidelines

You can use this command to view configuration information on a RMON event.

Example

Display configuration of RMON events.

```
Switch>show rmon config
!
!Rmon configuration
  rmon event 1 log
  rmon event 2 both

Switch>
```

11.2.5 show rmon event

Function

The **show rmon event** command displays configuration of RMON event control entries.

Format

show rmon event

Parameter

NA

Default Value

NA

View

Common user view

Usage Guidelines

You can use this command to view configuration information on the RMON event control entry, including the event control entry ID, description information, type, and last transmit time.

Example

Display configuration of RMON event control entries.

```
Switch>show rmon event
```

```

RMON Event:1
  Type:log
  Status:valid
  Lastsent time:0 days 0 hours 0 minutes 0 seconds
  Description:N/A
  Owner:N/A
RMON Event:2
  Type:trap&log
  Status:valid
  Lastsent time:0 days 0 hours 0 minutes 0 seconds
  Description:N/A
  Owner:N/A
Switch>

```

11.2.6 show rmon history

Function

The **show rmon history** command displays configuration information about RMON history control entries.

Format

show rmon history [*history-id*]

Parameter

Parameter	Description	Value
history-id	Specifies the ID of an RMON history record control entry.	The value is an integer ranging from 1 to 65535.

Default Value

NA

View

Common user view

Usage Guidelines

You can run this command to check configuration information about RMON history record control entries. If information does not contain the history-id parameter, configuration information about all history record control entries are displayed. Otherwise, that only of the specified ID is displayed.

Example

Display configuration of RMON event control entries.

```

Switch>show rmon history
  'BR' means 'Buckets Requested'
  'BG' means 'Buckets Granted'
  'DS' means 'Data Source'
  'ACT' means 'Active'
  'UC' means 'Undercreation'
RMON ethernet statistics
Index BR    BG    Interval State DS
1      20    20    300     ACT  ifIndex.2
Switch#

Switch>show rmon history 1
RMON history control:1
  History Data Source ifIndex.2
  Buckets Requested : 20
  Buckets Granted : 20
  Interval : 300
  Owner : cli
  Status : valid
Switch#

```

11.2.7 show rmon history statistics

Function

The **show rmon history statistics** command displays statistics on RMON historical record control entries.

Format

show rmon history statistics

Parameter

NA

Default Value

NA

View

Common user view

Usage Guidelines

You can use this command to view the statistics on the RMON historical record control entry.

Example

Display statistics on historical record control entries.

```
Switch>show rmon history statistics
  RMON History statistics:1/1
    Interval Start:0 days 0 hours 52 minutes 59 seconds
    Utilization:0
    Rx statistics:
      Drop Events:0
      Octets:0
      Pkts:0
      Broadcast:0
      Multicast:0
      Jabbers:0
    Error statistics:
      CRC Errors:0
      Undersize:0
      Oversize:0
      Fragments:0
      Collisions:0

Switch>
```

11.2.8 show rmon log**Function**

The **show rmon log** command displays logs of RMON events.

Format

show rmon log

Parameter

NA

Default Value

NA

View

Common user view

Usage Guidelines

You can use this command to view log information on a RMON event, including the event ID, log ID, log recording time, and log description.

Example

Display logs of RMON events.

```
Switch>show rmon log
  RMON Log:1/38
    Time:0 days 1 hours 35 minutes 23 seconds
    Description:alarm rising  1,1.3.6.1.2.1.2.2.1.8.2,1,2,1
  RMON Log:1/39
    Time:0 days 1 hours 35 minutes 25 seconds
    Description:alarm rising  1,1.3.6.1.2.1.2.2.1.8.2,1,2,1
  RMON Log:1/40
    Time:0 days 1 hours 35 minutes 27 seconds
    Description:alarm rising  1,1.3.6.1.2.1.2.2.1.8.2,1,2,1
  RMON Log:1/41
    Time:0 days 1 hours 35 minutes 29 seconds
    Description:alarm rising  1,1.3.6.1.2.1.2.2.1.8.2,1,2,1
  RMON Log:1/42
    Time:0 days 1 hours 35 minutes 31 seconds
    Description:alarm rising  1,1.3.6.1.2.1.2.2.1.8.2,1,2,1
  RMON Log:1/43
    Time:0 days 1 hours 35 minutes 33 seconds
    Description:alarm rising  1,1.3.6.1.2.1.2.2.1.8.2,1,2,1
  RMON Log:1/44
    Time:0 days 1 hours 35 minutes 35 seconds
    Description:alarm rising  1,1.3.6.1.2.1.2.2.1.8.2,1,2,1
  RMON Log:1/45
    Time:0 days 1 hours 35 minutes 37 seconds
    Description:alarm rising  1,1.3.6.1.2.1.2.2.1.8.2,1,2,1
  RMON Log:1/46
    Time:0 days 1 hours 35 minutes 39 seconds
    Description:alarm rising  1,1.3.6.1.2.1.2.2.1.8.2,1,2,1
  RMON Log:1/47
    Time:0 days 1 hours 35 minutes 41 seconds
    Description:alarm rising  1,1.3.6.1.2.1.2.2.1.8.2,1,2,1
Switch>
```

11.2.9 show rmon statistics

Function

The **show rmon statistics** command displays RMON statistics.

Format

show rmon statistics

Parameter

NA

Default Value

NA

View

Common user view

Usage Guidelines

You can use this command to view RMON statistics report, including the data source, Rx packets, all packets, and error packets.

Example

Display RMON statistics.

```
Switch>show rmon statistics
RMON Ethernet statistics 1
  Data Source:ifIndex.2
  Owner: N/A
  Status: valid
  Rx statistics:
    Drop Events: 0
    Octets: 62067
    Pkts: 396
    Broadcast: 19
    Multicast: 11
  Packets statistics:
    64 Octets: 506
    65-127 Octets: 216
    128-255 Octets: 8
    256-511 Octets: 0
    512-1023 Octets: 20
    1024-1518 Octets: 42
    Jabbers: 0
  Error statistics:
    CRC Errors: 0
```

```

        Undersize: 0
        Oversize: 0
        Fragments: 0
        Collisions: 0
Switch>

```

11.2.10 rmon event

Function

The **rmon event** command configures a RMON event control entry.

The **no rmon event** command deletes a RMON event control entry.

Format

- **rmon event** *event-id* { **log** | **trap** | **both** }
- **rmon event** *event-id* { **log** | **trap** | **both** } *description* [*owner*]
- **no rmon event** *event-id*

Parameter

Parameter	Description	Value
<i>event-id</i>	Specifies an RMON event control entry.	The value is an integer ranging from 1 to 65535.
{ <i>log</i> <i>trap</i> <i>both</i> }	Specifies an event type. log: The switch generates event logs. trap: The switch generates event alarms. both: The switch generates both event logs and alarms.	-
[<i>description</i>]	Specifies event description (optional).	The value is a character string.

Default Value

NA

View

Global configuration view

Usage Guidelines

You can use this command to configure the event ID and event processing mode, so that the switch can handle the alarm events accordingly.

Example

Configure a RMON event control entry.

```
Switch(config)#rmon event 1 both CLI
Switch(config)
```

11.2.11 rmon alarm

Function

The **rmon alarm** configures RMON alarm entries.

The **no rmon alarm** deletes RMON alarm entries.

Format

- **rmon alarm** *alarm-id object-id query-interval* { **absolute** | **delta** } *rising-threshold falling-threshold rising-event falling-event* [*owner*]
- **no rmon alarm** *alarm-id*

Parameter

Parameter	Description	Value
alarm-id	Specifies the ID of an RMON alarm entry.	The value is an integer ranging from 1 to 65535.
object-id	Specifies the alarm object ID (only a variable that can be resolved to the integer data type in ASN.1 can be used as the alarm object ID).	The value is in character string format, which is the dotted format of the node OID, for example, 1.3.6.1.2.1.2.2.1.8.2.
query-interval	Specifies the interval for alarm query.	The value is an integer ranging from 2 to 2000000, in seconds.
absolute delta	Indicates an absolute value or a relative value (increment).	-
rising-threshold	Indicates the rising threshold.	The value is an integer ranging from 0 to 4294967295.
falling-threshold	Indicates the falling threshold.	The value is an integer ranging from 0 to 65535.
rising-event	Indicates the rising event entry number.	The value is an integer ranging from 0 to 4294967295.
falling-event	Indicates the falling event entry number.	The value is an integer ranging from 0 to 65535.
owner	Defines an RMON alarm user (optional).	The value is an integer ranging from 0 to 127, in character string format.

Default Value

NA

View

Global configuration view

Usage Guidelines

When adding an alarm table entry using this command, configure the source object ID, query interval, alarm sample type, alarm generation type, and the corresponding time. In this way, the system can determine whether to record an alarm event in a log or send a trap message to the NMS in case of alarm events.

The sample types can be obtained in the following methods: Compare the difference between the relative value (currently sample value) minus the last sample value with the threshold; compare the absolute value (current sample value) with the threshold. The comparison result is used to generate the rising or falling event.

Example

Configure a RMON alarm entry.

```
Switch(config)#rmon alarm 1 1.3.6.1.2.1.2.2.1.8.2 2 absolute 1 1 2 1
Switch(config)#
```

11.3 SNMP Configuration Commands

11.3.1 snmp trap-history {enable|disable}

Function

The **snmp trap-history {enable|disable}** command enables or disables the SNMP historical alarm function.

Format

snmp trap-history { enable | disable }

Parameter

Parameter	Description	Value
enable	Enables the SNMP historical alarm function.	-
disable	Disables the SNMP historical alarm function.	-

Default Value

Disable

View

Global configuration view

Usage Guidelines

NA

Example

Enable the SNMP historical alarm function.

```
Switch(config)#snmp trap-history enable
Switch(config)#
```

11.3.2 snmp trap-history**Function**

The **snmp trap-history** command configures the size of the SNMP alarm history table.

Format

snmp trap-history { *value* | **default** }

Parameter

Parameter	Description	Value
value	Configures the size of an SNMP alarm history table.	The value is an integer ranging from 1 to 65535.

Default Value

The default size is 1024.

View

Global configuration view

Usage Guidelines

NA

Example

Configure the size of an SNMP alarm history table.

```
Switch(config)# snmp trap-history 1024
Switch(config)#
```

11.3.3 snmp rich-trap {enable|disable}

Function

The **snmp rich-trap {enable|disable}** command enables or disables the SNMP rich alarm function.

Format

snmp rich-trap { enable | disable }

Parameter

Parameter	Description	Value
enable	Enables the SNMP rich alarm function.	-
disable	Disables the SNMP rich alarm function.	-

Default Value

NA

View

Global configuration view

Usage Guidelines

NA

Example

Enable the SNMP rich alarm function.

```
Switch(config)# snmp rich-trap enable
Switch(config)#
```

11.3.4 show snmp trap-history

Function

Run the **show snmp trap-history** command to display the SNMP alarm history.

Format

show snmp trap-history

Parameter

NA

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

Display the SNMP historical alarm information.

```
Switch> show snmp trap-history
Index      Descr-ID Time(H:M:S)      value
1          119      0:00:42              30:5e:02:01:01:04:06:70:75:62:6c:69:63:a7:51:02
2          123      0:00:42              30:5f:02:01:01:04:06:70:75:62:6c:69:63:a7:52:0
Switch>
```

11.3.5 show snmp trap-description**Function**

The **show snmp trap-description** command displays SNMP alarm description information.

Format

show snmp trap-description

Parameter

NA

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

Display the SNMP alarm description information.

```
Switch>show snmp group
ID      Trap-OID              description              Grade
1       1.3.6.1.4.1.3807.1.8012.1.1.2.3  subCardUp              2
```

2	1.3.6.1.4.1.3807.1.8012.1.1.2.4	subCardDown	2
3	1.3.6.1.4.1.3807.2.308.0.1	cfmCcLoop	2
4	1.3.6.1.4.1.3807.2.308.0.2	cfmCcUnexpectedLevel	
Switch>			

11.3.6 snmp|snmp6 trap-server

Function

The **snmp|snmp6 trap-server** command specifies the address for receiving SNMP trap information.

The **no snmp|snmp6 trap-server** command deletes the specified receiver.

Format

- **snmp trap-server** *ipv4-address security-name { v1 | v2 | v3 } [vpn-instance name]*
- **snmp trap-server** *ipv4-address port security-name { v1 | v2 | v3 } [vpn-instance name]*
- **snmp trap-server** *ipv4-address security-name v3 { auth | priv } [vpn-instance name]*
- **snmp trap-server** *ipv4-address port security-name v3 { auth | priv } [vpn-instance name]*
- **snmp6 trap-server** *ipv6-address security-name { v1 | v2 | v3 } [vpn-instance name]*
- **snmp6 trap-server** *ipv6-address port security-name { v1 | v2 | v3 } [vpn-instance name]*
- **snmp6 trap-server** *ipv6-address security-name v3 { auth | priv } [vpn-instance name]*
- **snmp6 trap-server** *ipv6-address port security-name v3 { auth | priv } [vpn-instance name]*
- **no snmp trap-server** *ipv4-address [vpn-instance name]*
- **no snmp trap-server** *ipv4-address security-name [vpn-instance name]*
- **no snmp6 trap-server** *ipv6-address [vpn-instance name]*
- **no snmp6 trap-server** *ipv6-address security-name [vpn-instance name]*

Parameter

Parameter	Description	Value
ipv4-address	Specifies the host IPv4 address for receiving trap information.	The value is in dotted decimal notation.
ipv6-address	Specifies the host IPv6 address for receiving trap information.	-
{ v1 v2 v3 }	Specifies the trap version number sent by the SNMP.	-
security-name	Specifies a community name.	The value is a character string.
{ auth priv }	Specifies an authentication or privacy	-

Parameter	Description	Value
	mode.	
port	Specifies the port number for sending trap information.	The value is an integer ranging from 1 to 65535. The default value is 162.
name	Specifies a VPN instance name.	The value is a character string.

Default Value

NA

View

Global configuration view

Usage Guidelines

You can use this command to configure the IP address of the host that receives trap messages, so that you can manage faults of the switch remotely.

Example

Configure the switch to send trap messages to the host with IP address 10.5.6.8 and running SNMP version v2.

```
Switch(config)#snmp trap-server 10.5.6.8 name123 v2
Switch(config)#
```

11.3.7 snmp view

Function

The **snmp view** command configures the SNMP view.

The **no snmp view** command deletes a configured SNMP view.

Format

- **snmp view** *view-name old-tree* { **included** | **excluded** }
- **snmp view** *view-name old-tree* { **included** | **excluded** } **mask** *subtreemask*
- **no snmp view** *view-name*
- **no snmp view** *view-name oid-tree*

Parameter

Parameter	Description	Value
view-name	Specifies a view name.	The value is a string of no more than

Parameter	Description	Value
		32 characters.
oid-tree	Specifies an OID character string, used to identify the view range.	The value is a character string.
included excluded	Indicates the including or excluding relation.	-
subtreemask	Specifies a mask OID character string.	The value is a character string.

Default Value

NA

View

Global configuration view

Usage Guidelines

You can use this command to configure the SNMP view. It is applicable to SNMPv3. Specifying the access range of a view can improve the security and controllability.

Example

Set the access range of SNMP view v3view to 1.3.6.1MIB.

```
Switch(config)#snmp view v3view 1.3.6.1 include
Switch(config)#
```

11.3.8 snmp version

Function

The **snmp version** command configures the SNMP version.

The **no snmp version** command cancels the configured SNMP version.

Format

- **snmp version** { v1 | v2 | v3 | all }
- **no snmp version** { v1 | v2 | v3 | all }

Parameter

Parameter	Description	Value
v1 v2 v3 all	Indicates v1, v2, v3, or all versions.	-

Default Value

By default, the device supports SNMP of all versions.

View

Global configuration view

Usage Guidelines

NA

Example

Set the supported SNMP version to v3.

```
Switch(config)#snmp version v3
Switch(config)#
```

11.3.9 snmp user

Function

The **snmp user** command creates an SNMP user.

The **no snmp user** command deletes an SNMP user.

Format

- **snmp user** *user-name* **group** *group-name* **no-auth-no-priv**
- **snmp user** *user-name* **group** *group-name* **no-auth-no-priv filter-list** *acl-number*
- **snmp user** *user-name* **group** *group-name* **auth** { **md5** | **sha** } *authkey* **priv no-priv**
- **snmp user** *user-name* **group** *group-name* **auth** { **md5** | **sha** } *authkey* **priv** { **des** | **aes** } *privkey*
- **no snmp user** *user-name*

Parameter

Parameter	Description	Value
user-name	Specifies a user name.	The value is a character string consisting of a maximum of 32 characters.
group-name	Specifies a group name.	The value is a character string consisting of a maximum of 32 characters.
md5 sha	Sets the authentication mode to MD5 or SHA.	-
authkey	Specifies an authentication key.	The value is a character string consisting of a maximum of 32 characters.
privkey	Specifies an encryption key.	The value is a character string consisting of

Parameter	Description	Value
		a maximum of 32 characters.
no-priv	Disables encryption.	-
no-auth-no-priv	Disables authentication and encryption	-
acl-number	Specifies an ACL number.	The value is an integer ranging from 1 to 4000.

Default Value

NA

View

Global configuration view

Usage Guidelines

You can use this command to configure the SNMP user information, including the user name, group, authentication mode and encryption mode (authentication and encryption, authentication but no encryption, and no authentication and no encryption).

Example

Create user named sun1. Set the group to group 1 and authentication mode to MD5.

Set the authentication key to 0x1df745c352cc24781465.

Set the encryption key to 0xaaaf45e7357c629b97b7.

```
Switch(config)#snmp user sun1 group 1 auth md5 0x1df745c352cc24781465 priv des
0xaaaf45e7357c629b97b7
Switch(config)#
```

11.3.10 snmp trap-source

Function

The **snmp trap-source** command sets the IP address of the Ethernet interface, Eth-Trunk interface, loopback interface or VLAN interface as the release address of SNMP trap messages.

The **no snmp trap-source** command deletes the configuration.

Format

- **snmp trap-source** { **ethernet** | **xgigaethernet** | **10gigaethernet** | **25gigaethernet** | **40gigaethernet** | **100gigaethernet** } *interface-number*

- **snmp trap-source { ethernet | xgigaethernet | 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet } interface-number.subinterface**
- **snmp trap-source eth-trunk trunk-number**
- **snmp trap-source loopback loopback-number**
- **snmp trap-source vlan vlan-id**
- **no snmp trap-source**

Parameter

Description	Description	Value
loopback-number	Specifies a loopback interface.	The value is an integer ranging from 1 to 127.
vlan-id	Specifies a VLAN interface.	The value is an integer ranging from 1 to 4094.
interface-number	Specifies an Ethernet interface number.	The value is an integer in the range of <1-1>/<0-1>/<1-48>.
trunk-number	Specifies the number of a Trunk interface.	The value is an integer ranging from 1 to 128.
subinterface	Specifies a sub-interface number.	The value is an integer ranging from 1 to 4094.

Default Value

NA

View

Global configuration view

Usage Guidelines

You can specify the source IP address for sending SNMP trap messages as needed. The IP address can be the IP address of the Ethernet interface, Eth-Trunk interface, loopback interface, or VLAN interface.

Example

Set the SNMP trap source port.

```
Switch(config)#snmp trap-source 25gigaethernet 1/0/1
Switch(config)#
```

11.3.11 snmp rw-community

Function

The **snmp rw-community** command enables or disables the function of writing the SNMP community name.

Format

snmp rw-community { enable | disable }

Parameter

Parameter	Description	Value
enable	Enables the function of writing a community name.	-
disable	Disables the function of writing a community name.	-

Default Value

By default, the function of writing a community name is enabled.

View

Global configuration view

Usage Guidelines

NA

Example

Disable the function of writing a community name.

```
Switch(config)#snmp rw-community disable
Switch(config)#
```

11.3.12 snmp reply-source-ip {enable|disable}

Function

The **snmp reply-source-ip {enable|disable}** command configures the input IP address to the source IP address of the response.

Format

snmp reply-source-ip { enable | disable }

Parameter

Parameter	Description	Value
enable	Configures the input IP address to the source IP address of the response.	-
disable	Cancels configuring the input IP address to the source IP address of	-

Parameter	Description	Value
	the response.	

Default Value

NA

View

Global configuration view

Usage Guidelines

NA

Example

Enable the snmp reply-source-ip command.

```
Switch(config)# snmp reply-source-ip enable
Switch(config)#
```

11.3.13 snmp contact**Function**The **snmp contact** command configures the contact.**Format****snmp contact** *contact-info***Parameter**

Parameter	Description	Value
contact-info	Specifies a contact method for system maintenance.	The value is a string consisting of up to 128 bytes.

Default Value

NA

View

Global configuration view

Usage Guidelines

You can use this command to configure the SNMP contact information, so that users can easily contact the device supplier.

Example

Configure the contact to 888888888.

```
Switch(config)#snmp contact 888888888
Switch(config)#
```

11.3.14 snmp fail-count**Function**

The **snmp fail-count** command configures the number of SNMP authentication failures.

Format

snmp fail-count *count*

Parameter

Parameter	Description	Value
count	Specifies the number of SNMP authentication failures.	The value is an integer ranging from 0 to 30.

Default Value

By default, the number of SNMP authentication failures is 0, indicating that the number of authentication attempts is not limited.

View

Global configuration view

Usage Guidelines

This command allows the number of consecutive SNMP login failures. If the number of consecutive device login failures reaches the set value, the device enters the silent state. During the silent state, SNMP-based login to the device fails and will be successful only when the silent state ends.

Example

Configure the number of SNMP authentication failures to 6.

```
Switch(config)#snmp fail-count 6
Switch(config)#
```

11.3.15 snmp group**Function**

The **snmp group** command configures the SNMP group information.

The **no snmp group** command deletes the SNMP group information.

Format

- **snmp group** *group-name* **read-view** *read-view* **write-view** *write-view* **notify-view** *notify-view*
- **no snmp group** *group-name*

Parameter

Parameter	Description	Value
group-name	Specifies an SNMP group name.	The value is a string of no more than 32 characters.
read-view	Specifies a read-only view name.	The value is a character string.
write-view	Specifies a write-only view name.	The value is a character string.
notify-view	Specifies a notification view name.	The value is a character string.

Default Value

NA

View

Global configuration view

Usage Guidelines

You can use this command to configure the SNMP group information, including the group name and name of the read, write, or notification view. Different SNMP users in the group are mapped to different views, so that these SNMP users are assigned with different access permissions.

Example

Configure the SNMP group information, with the group name to **1**, read-only view name to **sun333**, read-write view name to **sun333**, and notification view name to **sun333**.

```
Switch(config)#snmp group 1 read-view sun333 write-view sun333 notify-view sun333
Switch(config)#
```

11.3.16 snmp location

Function

The **snmp location** command configures the device location information.

Format

snmp location *location-info***Parameter**

Parameter	Description	Value
location-info	Specifies device location information.	The value is a string consisting of up to 128 bytes.

Default Value

By default, the device location information is Wuhan-China.

View

Global configuration view

Usage Guidelines

You can use this command to configure the current location information on the device.

Example

Configure the current address information on a device to **wuhan-gaoxin**.

```
Switch(config)#snmp location wuhan-gaoxin
Switch(config)#
```

11.3.17 snmp reauth-interval**Function**

The **snmp reauth-interval** command configures the SNMP re-authentication interval.

Format

snmp reauth-interval *interval*

Parameter

Parameter	Description	Value
interval	Specifies re-authentication time.	The value is an integer ranging from 0 to 1440, in minutes.

Default Value

By default, the SNMP re-authentication interval is 0 minutes, indicating no silence time.

View

Global configuration view

Usage Guidelines

This command allows the number of consecutive SNMP login failures. If the number of consecutive device login failures reaches the set value, the device enters the silent state. During the silent state, SNMP-based login to the device fails and will be successful only when the silent state ends.

Example

Set the SNMP re-authentication interval to 10 minutes.

```
Switch(config)#snmp reauth-interval 10
Switch(config)#
```

11.3.18 snmp reply-auth-fail {enable|disable}

Function

The **snmp reply-auth-fail {enable|disable}** command configures whether to send an SNMP response upon an authentication failure.

Format

snmp reply-auth-fail { enable | disable }

Parameter

Parameter	Description	Value
enable	Sends an SNMP response upon an authentication failure.	-
disable	Sends no SNMP response upon an authentication failure.	-

Default Value

NA

View

Global configuration view

Usage Guidelines

NA

Example

Configure to send an SNMP response upon an authentication failure.

```
Switch(config)#snmp reply-auth-fail enable
Switch(config)#
```


11.3.19 snmp community

Function

The **snmp community** command configures an SNMP community name.

The **no snmp community** command deletes an SNMP community name.

Format

- **snmp community** *community-name* { **ro** | **rw** }
- **snmp community** *community-name* { **ro** | **rw** } { **cipher** | **plain** }
- **snmp community** *community-name* { **ro** | **rw** } { **cipher** | **plain** } **filter-list** *acl-number*
- **snmp community** *community-name* { **ro** | **rw** } { **cipher** | **plain** } **filter-list** **name** *filter-list-name*
- **snmp community** *community-name* { **ro** | **rw** } { **cipher** | **plain** } **view** *view-name*
- **snmp community** *community-name* { **ro** | **rw** } { **cipher** | **plain** } **view** *view-name* **filter-list** *filter-list-name*
- **snmp community** *community-name* { **ro** | **rw** } { **cipher** | **plain** } **view** *view-name* **filter-list** **name** *filter-list-name*
- **snmp community** *community-name* { **ro** | **rw** } **filter-list** *acl-number*
- **snmp community** *community-name* { **ro** | **rw** } **filter-list** **name** *community-name*
- **snmp community** *community-name* { **ro** | **rw** } **view** *view-name*
- **snmp community** *community-name* { **ro** | **rw** } **view** *view-name* **filter-list** *acl-number*
- **snmp community** *community-name* { **ro** | **rw** } **view** *view-name* **filter-list** **name** *filter-list-name*
- **no snmp community** *community-name*

Parameter

Parameter	Description	Value
community-name	Specifies a community name.	The value is a string of no more than 32 characters.
ro rw	Specifies permissions of the group name in a specified view, where ro indicates the read-only permission and rw indicates the read-write permission.	-
view-name	Specifies the name of the view	The value is a character string.

Parameter	Description	Value
	corresponding to the community name.	
acl-number	Specifies an ACL number.	The value is an integer ranging from 1 to 4000.
filter-list-name	Specifies an ACL name.	The value is a character string.

Default Value

By default, the SNMP community names are public and NETMAN.

View

Global configuration view

Usage Guidelines

To remotely manage the switch using an SNMP NMS, you must set a community name. You can access the MIB information on the device only after the community name passes the verification. If *view-name* is not specified, the system starts the access from the Internet node by default.

Example

Create a readable community name **public**.

```
Switch(config)#snmp community public ro
Switch(config)#
```

11.3.20 snmp auth-trap

Function

The **snmp auth-trap** command enables or disables the authentication trap function.

Format

snmp auth-trap { enable | disable }

Parameter

Parameter	Description	Value
enable	Enables the authentication trap function.	-
disable	Disables the authentication trap function.	-

Default Value

By default, the authentication trap function is enabled.

View

Global configuration view

Usage Guidelines

After the authentication trap function is enabled, the switch sends a trap message if authentication fails.

Example

Disable the authentication trap function.

```
Switch(config)#snmp auth-trap disable
Switch(config)#
```

11.3.21 snmp bulk max-varbind

Function

The **snmp bulk max-varbind** command configures the maximum number of variable bindings in an SNMP Get Bulk request.

Format

snmp bulk max-varbind { *max-number* | **default** }

Parameter

Parameter	Description	Value
max-number	Specifies the maximum number of Varbinds in the SNMPGetBulk request.	The value is an integer ranging from 100 to 4000.
default	Specifies the default value.	512

Default Value

512

View

Global configuration view

Usage Guidelines

The number of variables collected by an SNMP Get Bulk message is $N + (M \times R)$, where N is the smaller one between the value of non-repeaters and the number of request variables, M is the value of max-repetitions, and R is the larger one between the number of request variables - N and 0.

Example

Configure the maximum number of variable bindings in an SNMP Get Bulk request.

```
Switch(config)#snmp bulk max-varbind 400
Switch>show snmp config
snmp bulk max-varbind 400
Switch(config)#
```

11.3.22 show snmp agent

Function

The **show snmp agent** command displays the SNMP agent information on the switch.

Format

show snmp agent

Parameter

NA

Default Value

NA

View

Common user view

Usage Guidelines

You can use this command to view SNMP agent information, including the contact information on the current device node, physical position of the current device node, interval for reporting trap messages, and whether trap reporting is enabled.

Example

Display the SNMP agent information on the switch.

```
Switch>show snmp agent
SNMP agent:
  location is WuHan-China
  contact is WuHan-China
  auth-failure trap is enable
  Local EngineID:80000EDF030005670A6910
  sysObjectID:1.3.6.1.4.1.3807.1.695401
Switch>
```

11.3.23 show snmp community

Function

The **show snmp community** command displays the SNMP community configuration.

Format

show snmp community

Parameter

NA

Default Value

NA

View

Common user view

Usage Guidelines

You can use this command to view SNMP community configuration information, including the community name, access permissions, and state.

Example

Display the SNMP community configuration.

```
Switch>show snmp community
Community
Privilege  Status  Filter View
$9$T49x$0586b9484e80088b (The default encryption method of the device is cipher text)
rw          VALID   N/A    internet
Switch>
```

11.3.24 show snmp config

Function

The **show snmp config** command displays the SNMP configuration information.

Format

show snmp config

Parameter

NA

Default Value

NA

View

Common user view

Usage Guidelines

You can use this command to view SNMP configuration information in the configuration file.

Example

Display the SNMP configuration information.

```
Switch>show snmp config
Software Version           : SNMP_VB3.00.00.00
!
snmp view fh 1.3.6.1.3 excluded
snmp community $9$R56t$8c2e98f72954da45 rw cipher view internet
snmp trap-server 223.1.10.206 162 $9$R56t$8c2e98f72954da45 v2
snmp group fs read-view internet write-view internet notify-view internet
snmp user admin group fs no-auth-no-priv
!
snmp view fh 1.3.6.1.3 excluded
snmp community $9$D129$158d74d6610ac08b rw cipher view internet
Switch>
```

11.3.25 show snmp group**Function**

The **show snmp group** command displays the SNMP group information.

Format

show snmp group

Parameter

NA

Default Value

NA

View

Common user view

Usage Guidelines

You can use this command to view SNMP group information, including the group name, readable view, writable view.

Example

Display the SNMP group information.

```
Switch>show snmp group
Group          ReadView      WriteView      NotifyView
1              sun333        sun333        sun333
Switch>
```

11.3.26 show snmp statistic

Function

The **show snmp statistic** command displays statistics on SNMP packet processing.

Format

show snmp statistic

Parameter

NA

Default Value

NA

View

Common user view

Usage Guidelines

You can use this command to analyze packet statistics and obtain information about communication between the switch and the NMS, facilitating fault identification.

Example

Display the statistics on SNMP packet processing.

```
Switch>show snmp statistic
snmpInPkts : 120766
snmpInBadVersions : 0
```

```
snmpInBadCommunityNames : 3
snmpInBadCommunityUses : 0
snmpInASNParseErrs : 0
snmpInBadTypes : 0
snmpInTooBigs : 0
snmpInNoSuchNames : 0
snmpInBadValues : 0
snmpInReadOnlys : 0
snmpInGenErrs : 0
snmpInTotalReqVars : 120730
snmpInTotalSetVars : 0
snmpInGetRequests : 0
snmpInGetNexts : 120741
snmpInSetRequests : 0
snmpInGetResponses : 0
snmpInTraps : 0
snmpOutPkts : 120766
snmpOutTooBigs : 0
snmpOutNoSuchNames : 0
snmpOutBadValues : 0
snmpOutReadOnlys : 0
snmpOutGenErrs : 11
snmpOutGetRequests : 0
snmpOutGetNexts : 0
snmpOutSetRequests : 0
snmpOutGetResponses : 120744
snmpOutTraps : 0
snmpUnknownSecurityModels : 0
snmpInvalidMsgs : 0
snmpUnknownPDUHandlers : 0
snmpUnavailableContexts : 0
snmpUnknownContexts : 0
usmStatsUnsupportedSecLevels : 0
usmStatsNotInTimeWindows : 16
usmStatsUnknownUserNames : 0
usmStatsUnknownEngineIDs : 5
usmStatsWrongDigests : 1
usmStatsDecryptionErrors : 0
```

```
Switch>
```

11.3.27 show snmp trap-server

Function

The **show snmp trap-server** command displays the host that receives trap messages and its version and type.

Format

show snmp trap-server

Parameter

NA

Default Value

NA

View

Common user view

Usage Guidelines

You can use this command to check the host receiving trap messages and its version. Output of the command includes the host IP address, port number, version, and status.

Example

View the host that receives the trap message as well as the host version and type.

```
Switch>show snmp trap-server
IP-Address      Port  Ver  Status  Level Name  VPN
223.1.10.206    162   V2   active  None        $9$da2E$48da821d5d951e9c
Switch>
```

11.3.28 show snmp trap state

Function

The **show snmp trap state** command displays the alarm information state of the network management protocol.

Format

show snmp trap state

Parameter

NA

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

View the alarm information state of the network management protocol.

```
Switch>show snmp trap state
moduleName          trapstate
bfd                  disable
g8032                enable
g8031                enable
I3vpn                disable
rip                  disable
udld                 disable
vrrp                 enable
Switch>
```

11.3.29 show snmp user**Function**The **show snmp user** command displays the SNMP user information.**Format****show snmp user****Parameter**

NA

Default Value

NA

View

Common user view

Usage Guidelines

You can use this command to view SNMP user information, including the user name, group name, and authentication status.

Example

Display the SNMP user information.

```
Switch>show snmp user
User          Group          Auth          Priv          Filter
admin         fs             no-auth       no-priv       N/A
Switch>
```

11.3.30 show snmp view

Function

The **show snmp view** command displays the SNMP view information.

Format

show snmp view

Parameter

NA

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

Display the SNMP view information.

```
Switch>show snmp view
View          Type          OIDTree          Mask
sun333        included      1.3.6.1.2.1.4.1  all-1
internet      included      1.3.6             all-1
internet      excluded     1.3.6.1.6.3.15   all-1
internet      excluded     1.3.6.1.6.3.16   all-1
Switch>
```

11.3.31 debug snmp

Function

The **debug snmp** command enables SNMP debugging.

The **no debug snmp** command disables SNMP debugging.

Format

- **debug snmp** { rx | tx | idb | rxpkt | txpkt | trap | error | eb | all }
- **no debug snmp** { rx | tx | idb | rxpkt | txpkt | trap | error | eb | all }

Parameter

NA

Default Value

NA

View

Privileged user view

Usage Guidelines

This command is applicable to debugging SNMP functions under IPv4 and IPv6.

Example

Enable the SNMP debugging function.

```
Switch#debug snmp all
Switch#
```

11.3.32 snmp|snmp6 port

Function

The **snmp|snmp6 port** command configures the SNMP port number.

Format

- **snmp port** { *port-number* | **default** }
- **snmp6 port** { *port-number* | **default** }

Parameter

Parameter	Description	Value

Parameter	Description	Value
port-number	Specifies an SNMP port number.	The value is an integer ranging from 1024 to 65535.
default	Specifies the default value.	The value is 161.

Default Value

The default SNMP port number is 161.

View

Global configuration view

Usage Guidelines

NA

Example

Set the SNMP port number to 1024.

```
Switch(config)#snmp port 1024
Switch(config)#
```

11.4 LLDP Configuration Commands

11.4.1 debug lldp

Function

The **debug lldp** command enables Link Layer Discovery Protocol (LLDP) debugging.

The **no debug lldp** command disables LLDP debugging.

Format

- **debug lldp { config | rxstate | txstate | rxpkt | event | sync | all }**
- **no debug lldp { config | rxstate | txstate | rxpkt | event | sync | all }**

Parameter

Parameter	Description	Value
config	Displays LLDP configuration information.	-
rxstate	Displays the packet receiving state.	-
txstate	Displays the packet sending state.	-
rxpkt	Displays debugging information about egress packets.	-
event	Displays debugging information about events.	-
sync	Displays debugging information about synchronization.	-

Parameter	Description	Value
all	Displays all the preceding debugging information.	-

Default Value

NA

View

Privileged user view

Usage Guidelines

NA

Example

Enable debugging of LLDP packet receiving.

```
Switch#debug lldp rxpkt
Switch#
```

11.4.2 lldp faststart-count

Function

The **lldp faststart-count** command sets the number of fast transmitted LLDP MED packets.

Format

lldp faststart-count { *faststart-count* | **default** }

Parameter

Parameter	Description	Value
faststart-count	Specifies the number of fast transmitted LLDP MED packets.	The value is an integer ranging from 1 to 10.
default	Specifies the default size.	3

Default Value

3

View

Global configuration view

Usage Guidelines

NA

Example

Set the number of fast transmitted LLDP MED packets to 5.

```
Switch(config)#lldp faststart-count 5
Switch(config)#
```

11.4.3 lldp admin-status**Function**

The **lldp admin-status** command enables LLDP and sets its administrative status or disables LLDP on an interface.

Format

lldp admin-status { tx-only | rx-only | rx-tx | disable }

Parameter

Parameter	Description	Value
tx-only	Sends LLDP packets only.	-
rx-only	Receives LLDP packets only.	-
rx-tx	Sends and receives LLDP packets.	-
disable	Neither sends nor receives LLDP packets.	-

Default Value

NA

View

Ethernet bridge interface configuration view, Ethernet routing interface configuration view

Usage Guidelines

NA

Example

Set the LLDP administrative status.

```
Switch(config-10ge1/0/1)#lldp admin-status tx-only
Switch(config-10ge1/0/1)#
```

11.4.4 lldp basic-tlv-tx**Function**

The **lldp basic-tlv-tx** command sets the basic LLDP type-length-value (TLV) on an interface.

Format

**lldp basic-tlv-tx { port-description | system-name | system-description | system-capability | all }
{ enable | disable }**

Parameter

Parameter	Description	Value
port-description	Specifies port description.	-
system-name	Specifies a system name.	-
system-description	Indicates system description.	-
system-capability	Indicates a system capability.	-
all	Specifies all the preceding items.	
enable	Enables the synchronization function.	-
disable	Disable the synchronization function.	-

Default Value

NA

View

Ethernet bridge interface configuration view, Ethernet routing interface configuration view

Usage Guidelines

NA

Example

Configure the basic LLDP TLV.

```
Switch(config-10ge1/0/1)#lldp basic-tlv-tx port-description enable
Switch(config-10ge1/0/1)#
```

11.4.5 lldp dot1-tlv-tx port-vid

Function

The **lldp dot1-tlv-tx port-vid** command enables or disables the port VLAN ID (VID) field in optional IEEE 802.1 TLVs.

Format

lldp dot1-tlv-tx port-vid { enable | disable }

Parameter

Parameter	Description	Value
enable	Enables the port VLAN ID function of the IEEE802.1 optional TLV.	-
disable	Disables the port VLAN ID function of the IEEE802.1 optional TLV.	-

Default Value

NA

View

Ethernet bridge interface configuration view, Ethernet routing interface configuration view

Usage Guidelines

NA

Example

Configure the port VLAN ID function of the IEEE802.1 optional TLV.

```
Switch(config-10ge1/0/1)#lldp dot1-tlv-tx port-vid enable
Switch(config-10ge1/0/1)#
```

11.4.6 lldp dot1-tlv-tx protocol-vid|protocol-id

Function

The **lldp dot1-tlv-tx protocol-vid|protocol-id** command enables or disables the protocol VLAN ID field in optional IEEE 802.1 TLVs.

Format

- **lldp dot1-tlv-tx protocol-id { enable | disable }**
- **lldp dot1-tlv-tx protocol-vid *vlan-list* { enable | disable }**

Parameter

Parameter	Description	Value
vlan-list	Specifies a VLAN ID.	The value is an integer ranging from 1 to 4094.
enable	Enables the protocol VLAN ID field in optional IEEE 802.1 TLVs.	-
disable	Disables the protocol VLAN ID field in optional IEEE 802.1 TLVs.	-

Default Value

NA

View

Ethernet bridge interface configuration view, Ethernet routing interface configuration view

Usage Guidelines

NA

Example

Enable the protocol VLAN ID field in optional IEEE 802.1 TLVs.

```
Switch(config-10ge1/0/1)#lldp dot1-tlv-tx protocol-vid 12 enable
Switch(config-10ge1/0/1)#
```

11.4.7 lldp dot1-tlv-tx vlan-name**Function**

The **lldp dot1-tlv-tx vlan-name** command enables or disables the VLAN name field in optional IEEE 802.1 TLVs.

Format

lldp dot1-tlv-tx vlan-name *vlan-list* { **enable** | **disable** }

Parameter

Parameter	Description	Value
vlan-list	Specifies a VLAN ID.	The value is an integer ranging from 1 to 4094.
enable	Enables the VLAN name field in optional IEEE 802.1 TLVs.	-
disable	Disables the VLAN name field in optional IEEE 802.1 TLVs.	-

Default Value

NA

View

Ethernet bridge interface configuration view, Ethernet routing interface configuration view

Usage Guidelines

NA

Example

Enable the VLAN name field in optional IEEE 802.1 TLVs.

```
Switch(config-10ge1/0/1)#lldp dot1-tlv-tx vlan-name 122 enable
Switch(config-10ge1/0/1)#
```

11.4.8 lldp dot3-tlv-tx

Function

The **lldp dot3-tlv-tx** command sets TLV information defined in IEEE 802.3.

Format

lldp dot3-tlv-tx { **mac-phy** | **power** | **link-aggregation** | **max-frame-size** | **all** } { **enable** | **disable** }

Parameter

Parameter	Description	Value
mac-phy	Specifies a port rate.	-
power	Specifies the power supply capability of a port.	-
link-aggregation	Indicates link aggregation.	-
max-frame-size	Specifies the maximum frame size.	-
all	Specifies all the preceding items.	-
enable	Enables the protocol VLAN ID field in optional IEEE 802.1 TLVs.	-
disable	Disables the protocol VLAN ID field in optional IEEE 802.1 TLVs.	-

Default Value

NA

View

Ethernet bridge interface configuration view, Ethernet routing interface configuration view

Usage Guidelines

NA

Example

Set TLV information defined in IEEE 802.3.

```
Switch(config-10ge1/0/1)#lldp dot3-tlv-tx all enable
Switch(config-10ge1/0/1)#
```

11.4.9 lldp location-id civic-address|elin-address

Function

The **lldp location-id civic-address|elin-address** command configures the location information on a device.

Format

- **lldp location-id civic-address** *CIVIC-ADDRESS country-code ca-type ca-value*
- **lldp location-id civic-address** *CIVIC-ADDRESS country-code ca-type ca-value ca-type ca-value*
- **lldp location-id civic-address** *CIVIC-ADDRESS country-code ca-type ca-value ca-type ca-value ca-type ca-value*
- **lldp location-id civic-address** *CIVIC-ADDRESS country-code ca-type ca-value ca-type ca-value ca-type ca-value ca-type ca-value*
- **lldp location-id civic-address** *CIVIC-ADDRESS country-code ca-type ca-value ca-type ca-value ca-type ca-value ca-type ca-value ca-type ca-value*
- **lldp location-id civic-address** *CIVIC-ADDRESS country-code ca-type ca-value ca-type ca-value ca-type ca-value ca-type ca-value ca-type ca-value ca-type ca-value*
- **lldp location-id civic-address** *CIVIC-ADDRESS country-code ca-type ca-value ca-type ca-value ca-type ca-value ca-type ca-value ca-type ca-value ca-type ca-value ca-type ca-value*
- **lldp location-id civic-address** *CIVIC-ADDRESS country-code ca-type ca-value ca-type ca-value ca-type ca-value ca-type ca-value ca-type ca-value ca-type ca-value ca-type ca-value*
- **lldp location-id civic-address** *CIVIC-ADDRESS country-code ca-type ca-value ca-type ca-value ca-type ca-value ca-type ca-value ca-type ca-value ca-type ca-value ca-type ca-value*
- **lldp location-id elin-address** *number*
- **no lldp location-id { elin-address | civic-address }**

Parameter

Parameter	Description	Value
CIVIC-ADDRESS	Specifies a civic address LCI.	The value is an integer ranging from 0 to 2. The value 0 indicates the position of the DHCP

Parameter	Description	Value
		server. The value 1 indicates the position of the network element that is the closest to the client. The value 2 indicates the client position.
country-code	Specifies an ISO 3166 country code, consisting of two upper-case letters.	The two letters are ASCII characters, such as DE or US.
ca-type	Specifies data description of the civic address value.	The value is an integer ranging from 0 to 255.
ca-value	Specifies a civic address value.	The value is an integer consisting of 0 to 250 bytes.
number	Specifies an ELIN identifier of an emergency contact service.	-

Default Value

NA

View

Ethernet bridge interface configuration view, Ethernet routing interface configuration view

Usage Guidelines

NA

Example

Configure the position information on a device.

```
Switch(config-10ge1/0/1)#lldp location-id civic-address 0 CH 1 1
Switch(config-10ge1/0/1)#
```

11.4.10 lldp management-address

Function

The **lldp management-address** command configures the LLDP management IP address.

Format

- **lldp management-address** *ip-address* { **enable** | **disable** }
- **lldp management-address** *mac-address* { **enable** | **disable** }

Parameter

Parameter	Description	Value

Parameter	Description	Value
ip-address	Specifies an IP address in the static ARP entry.	The value is in dotted decimal notation.
mac-address	Specifies a MAC address.	The value is in AA:BB:CC:DD:EE:FF format, where A to F are hexadecimal digits.
enable	Enables the LLDP management IP address.	-
disable	Disables the LLDP management IP address.	-

Default Value

NA

View

Ethernet bridge interface configuration view, Ethernet routing interface configuration view

Usage Guidelines

NA

Example

Set the LLDP management IP address.

```
Switch(config-10ge1/0/1)#lldp management-address 1.2.3.1 enable
Switch(config-10ge1/0/1)#
Switch(config-10ge1/0/1)#lldp management-address 00:00:00:ee:ff:ab enable
Switch(config-10ge1/0/1)#
```

11.4.11 lldp med-notification

Function

The **lldp med-notification** command enables or disables the LLDP MED alarm function of a port.

Format

lldp med-notification { enable | disable }

Parameter

Parameter	Description	Value
enable	Disables the LLDP MED alarm function on an interface.	-
disable	Disables the LLDP MED alarm function on an interface.	-

Default Value

NA

View

Ethernet bridge interface configuration view, Ethernet routing interface configuration view

Usage Guidelines

NA

Example

Enable the LLDP MED alarm function.

```
Switch(config-10ge1/0/1)#lldp med-notification enable
Switch(config-10ge1/0/1)#
```

11.4.12 lldp med-tlv-tx**Function**The **lldp med-tlv-tx** command configures MED attributes on an interface.**Format**

lldp med-tlv-tx { **capabilities** | **network-policy** | **location** | **extended-pse** | **extended-pd** | **inventory** | **all** } { **enable** | **disable** }

Parameter

Parameter	Description	Value
capabilities	Specifies a capability set.	-
network-policy	Indicates the supported application.	-
location	Specifies location identifier information on a port.	-
extended-pse	Specifies the power supply capability.	-
inventory	Indicates a specific directory.	-
all	Specifies all the preceding items.	-
enable	Enables MED-associated information on the port.	-
disable	Disables MED-associated information on the port.	-

Default Value

NA

View

Ethernet bridge interface configuration view, Ethernet routing interface configuration view

Usage Guidelines



Note:

Switch hardware does not support the command function.

Example

Configure MED-related information under a port.

```
Switch(config-10ge1/0/1)#lldp med-tlv-tx all enable
Switch(config-10ge1/0/1)#
```

11.4.13 lldp trap {enable|disable}

Function

The **lldp trap {enable|disable}** command enables or disables the LLDP alarm function of a port.

Format

lldp trap { enable | disable }

Parameter

Parameter	Description	Value
enable	Enables the LLDP alarm function on an interface.	-
disable	Disables the LLDP alarm function on an interface.	-

Default Value

By default, the LLDP alarm function is disabled.

View

Ethernet bridge interface configuration view, Ethernet routing interface configuration view

Usage Guidelines

NA

Example

Enable the LLDP alarm function on an interface.

```
Switch(config-10ge1/0/1)#lldp trap enable
Switch(config-10ge1/0/1)#
```


11.4.14 lldp notification-interval

Function

The **lldp notification-interval** command sets the global trap transmission interval.

Format

lldp notification-interval { *notification-interval-value* | **default** }

Parameter

Parameter	Description	Value
notification-interval-value	Specifies a trap transmission interval.	The value is an integer ranging from 5 to 3600.
default	Specifies the default size.	5s

Default Value

The default value is 5 seconds.

View

Global configuration view

Usage Guidelines

Upon frequently triggered alarms on a device, alarms are sent only when the interval between two alarms is greater than the alarm sending interval.

Example

Configure the notification sending interval to 6s.

```
Switch(config)# lldp notification-interval 6
Switch(config)#
```

11.4.15 lldp reinit-delay

Function

The **lldp reinit-delay** command sets a delay in re-initiating LLDP interface status.

Format

lldp reinit-delay { *reinit-delay-value* | **default** }

Parameter

Parameter	Description	Value
reinit-delay-value	Specifies a delay in re-initiating LLDP	The value is an integer ranging from 1

Parameter	Description	Value
	interface status.	to 10.
default	Specifies the default size.	2s

Default Value

The default value is 2 seconds.

View

Global configuration view

Usage Guidelines

NA

Example

Set a delay in re-initiating LLDP interface status to 5 seconds.

```
Switch(config)# lldp reinit-delay 5
Switch(config)#
```

11.4.16 lldp tx-delay

Function

The **lldp tx-delay** command sets a delay in sending LLDP packets.

Format

lldp tx-delay { *tx-delay-value* | **default** }

Parameter

Parameter	Description	Value
tx-delay	Specifies a delay in sending LLDP packets.	The value is an integer ranging from 1 to 8192.
default	Specifies the default size.	2s

Default Value

The default value is 2 seconds.

View

Global configuration view

Usage Guidelines

This command sets the minimum delay before an interface module sends LLDP packets to the neighbor when the LLDP status of the switch changes frequently.

Example

Set a delay in sending LLDP packets to 5 seconds.

```
Switch(config)# lldp tx-delay 5
Switch(config)#
```

11.4.17 lldp tx-hold

Function

The **lldp tx-hold** command sets the multiplier of LLDP frame transmission interval.

Format

lldp tx-hold { *tx-hold-value* | **default** }

Parameter

Parameter	Description	Value
tx-hold-value	Specifies the multiplier of LLDP frame transmission interval.	The value is an integer ranging from 2 to 10.
default	Specifies the default size.	4

Default Value

4

View

Global configuration view

Usage Guidelines

NA

Example

Set the multiplier of LLDP frame transmission interval to 5.

```
Switch(config)# lldp tx-hold 5
Switch(config)#
```

11.4.18 lldp tx-interval

Function

The **lldp tx-interval** command sets the LLDP frame transmission interval.

Format

lldp tx-interval { *tx-interval-value* | **default** }

Parameter

Parameter	Description	Value
tx-interval-value	Specifies an LLDP frame transmission interval, in seconds.	The value is an integer ranging from 5 to 32768.
default	Specifies the default size.	30s

Default Value

The default value is 30 seconds.

View

Global configuration view

Usage Guidelines

NA

Example

Set the LLDP frame transmission interval to 10 seconds.

```
Switch(config)# lldp tx-interval 10
Switch(config)#
```

11.4.19 show lldp config interface**Function**

The **show lldp config interface** command displays the LLDP configuration on a specified interface.

Format

show lldp config interface { **ethernet** | **xgigaethernet** | **10gigaethernet** | **25gigaethernet** | **40gigaethernet** | **100gigaethernet** } *interface-number*

Parameter

Parameter	Description	Value
interface-number	Specifies an Ethernet interface number.	The value is an integer in the range of <1-1> / <0-1> / <1-48>.

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

Display the LLDP configuration on an interface.

```
Switch>show lldp config interface xgigaethernet 1/0/1
interface xgigaethernet 1/0/1
lldp med-notification enable
Switch>
```

11.4.20 show lldp config**Function**

The **show lldp config** command displays the LLDP configuration.

Format

show lldp config

Description

NA

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

Display the LLDP configuration.

```
Switch>show lldp config
Version                               :LLDP_VB3.00.04.00
!
lldp tx-interval 10
```

```
lldp faststart-count 5
Switch>
```

11.4.21 show lldp interface

Function

The **show lldp interface** command displays LLDP interface information.

The **show lldp interface verbose** command displays detailed LLDP interface information.

Format

- **show lldp interface**
- **show lldp interface { ethernet | xgigaethernet | 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet } interface-number**
- **show lldp interface verbose**

Parameter

Parameter	Description	Value
interface-number	Specifies an Ethernet interface number.	The value is an integer in the range of <1-1>/<0-1>/<1-48>.

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

Display LLDP interface information.

```
Switch>show lldp interface 100gigaethernet 1/0/2
Port 100ge1/0/2:
  Admin status:TxRx
  Trap enable:no
  Support tlv:port-description,system-name,system-description,system-capability
  Enabled tlv:port-description,system-name,system-description,system-capability
  Port type:interface name
  Port ID:100GigaEthernet1/0/2
```

```

Port description:100GigaEthernet1/0/2 SNMP-Index:142671873
Tx Total frames:3515
Rx Total discard frames:0
Rx Error frames:0
Rx total frames:3511
Rx tlv discard total frames:0
Rx tlv unrecognized total frames:0
Rx ageout frames total frame:1

Dot1 support tlv:port-vid,protocol-vid,vlan-name,protocol-id
Dot1 enable tlv:N/A
Dot1 port VLAN ID(PVID):1
Port protocol enabled:LACP LLDP

Dot3 support tlv:mac-phy,power,link-aggregation,max-frame-size
Dot3 enable tlv:mac-phy,power,link-aggregation,max-frame-size
Dot3 auto-negotiation supported:no
Dot3 auto-negotiation enabled:no
Dot3 MAU type:unknown
Dot3 power port class:PSE
Dot3 power supported:no
Dot3 power enabled:no
Dot3 power pairs control ability:no
Dot3 power pairs:signal
Dot3 power class:class1
Dot3 link aggregation supported:yes
Dot3 link aggregation enabled:yes
Dot3 link aggregation ID:268435457
Dot3 maximum frame size:9216

Med support tlv:capabilities,network-policy,location,extended-pse
Med trap-enable:no
Med PSE power available (watts):3.3
Med PSE power source:critical

Number of remote system:1
Number of MED remote system:0

```

Switch>

11.4.22 show lldp local

Function

The **show lldp local** command displays local LLDP device information.

Format**show lldp local****Description**

NA

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

Display the local device information.

```

Switch> show lldp local
  LLDP local:
    Message tx-interval:30(s)
    Message tx-hold:4
    Reinit delay:2(s)
    Tx delay:2(s)
    Notification interval:10(s)
    Chassis type:MAC Address
    Chassis ID:0004:6790:ffff
    System name:Switch
    System desc: Routing Switch
    System supported:Bridge/Switch,Router
    System capenabled:Bridge/Switch,Router

    Med information:
    Device class:Network Connectivity Device
    Faststart repeat-count:1
    Hardware revision:1.0
    Firmware revision:0.1
    Software revision:V210R230
    Serial number:-
    Manufacturer name: Switch
    Model name:LLDP

```



```

Asset ID:N/A
POE type:pse
Switch>

```

11.4.23 show lldp local interface

Function

The **show lldp local interface** command displays information about a local LLDP interface.

Format

show lldp local interface { ethernet | xgigaethernet | 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet } interface-number

Parameter

Parameter	Description	Value
interface-number	Specifies an Ethernet interface number.	The value is an integer in the range of <1-1>/<0-1>/<1-48>.

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

Display information about a local LLDP interface.

```

Switch>show lldp local interface 100gigaethernet 1/0/2
Port 100ge1/0/2:
  Admin status:TxRx
  Trap enable:no
  Support tlv:port-description,system-name,system-description,system-capability
  Enabled tlv:port-description,system-name,system-description,system-capability
  Port type:interface name
  Port ID:100GigaEthernet1/0/2
  Port description:100GigaEthernet1/0/2 SNMP-Index:142671873

  Dot1 support tlv:port-vid,protocol-vid,vlan-name,protocol-id
  Dot1 enable tlv:N/A

```

```

Dot1 port VLAN ID(PVID):1
Port protocol enabled:LACP LLDP

Dot3 support tlv:mac-phy,power,link-aggregation,max-frame-size
Dot3 enable tlv:mac-phy,power,link-aggregation,max-frame-size
Dot3 auto-negotiation supported:no
Dot3 auto-negotiation enabled:no
Dot3 MAU type:unknown
Dot3 power port class:PSE
Dot3 power supported:no
Dot3 power enabled:no
Dot3 power pairs control ability:no
Dot3 power pairs:signal
Dot3 power class:class1
Dot3 link aggregation supported:yes
Dot3 link aggregation enabled:yes
Dot3 link aggregation ID:268435457
Dot3 maximum frame size:9216

Med support tlv:capabilities,network-policy,location,extended-pse,inventory
Med trap-enable:no
Med PSE power available (watts):3.3
Med PSE power source:critical

Number of remote system:1
Number of MED remote system:0

```

11.4.24 show lldp remote interface

Function

The **show lldp remote interface** command displays the neighbor information on a specified interface.

Format

show lldp remote interface { ethernet | xgigaethernet | 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet } interface-number

Parameter

Parameter	Description	Value
interface-number	Specifies an Ethernet interface number.	The value is an integer in the range of <1-1>/<0-1>/<1-48>.

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

Display the LLDP configuration on an interface.

```
Switch>show lldp remote interface gigabitEthernet 1/0/1
Switch>
```

11.4.25 show lldp remote**Function**The **show lldp remote** command displays information about all neighbors or a specified neighbor.**Format**

- **show lldp remote**
- **show lldp remote verbose**
- **show lldp remote *remote-number***

Parameter

Parameter	Description	Value
remote-number	Specifies a neighbor ID.	The value is an integer ranging from 1 to 2147483647.

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

Display information about all neighbors.

```
Switch>show lldp remote
Switch>
```

11.4.26 show lldp statistic

Function

The **show lldp statistic** command displays the LLDP statistics information.

The **show lldp statistic interface** command displays the LLDP statistics information on an interface.

Format

- **show lldp statistic**
- **show lldp statistic interface { ethernet | xgigaethernet | 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet } interface-number**

Parameter

Parameter	Description	Value
interface-number	Specifies an Ethernet interface number.	The value is an integer in the range of <1-1>/<0-1>/<1-48>.

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

Display LLDP statistics.

```
Switch>show lldp statistic
LLDP statistic:
  LLDP Msap statistic:
    Last change-time: 0 days 0 hours 4 minutes 38 seconds
    Inserts:11
    Deletes:3
    Drops:0
    Ageouts:0(s)
```

```

Max number of management address:832(s)
Number of management address:0(s)

LLDP port statistic:
Port 100ge1/0/1:
    Tx Total frames:0
    Rx Total discard frames:0
    Rx Error frames:0
    Rx total frames:0
    Rx tlv discard total frames:0
    Rx tlv unrecognized total frames:0
    Rx ageout frames total frame:0
    Number of remote system:0
    Number of MED remote system:0
    ...
Switch>

```

11.5 Packet Capturing Configuration Commands

11.5.1 capture cpupkt interface

Function

The **capture cpupkt interface** command configures the continuous duration for capturing the packets sent and received by the CPU in the current interface.

Format

- **capture cpupkt interface** { ethernet | xgigaethernet | 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet } *interface-number* { arp | lldp | loopback | dot3ah | lacp | dot1x | cfm | y1731 | g8032 | g8031 | eaps | dlip | mlag | mpls | stp | isis | iss | bfd | sync | arp | ip | ospf | igmp | icmp | udp | dhcp | ldp-hello | bfd-udp | tcp | bgp | ldp-tcp | ipv6 | icmpv6 | icmpv6-echo-request | icmpv6-echo-reply | icmpv6-rs | icmpv6-ra | icmpv6-ns | icmpv6-na | icmpv6-redirect | ospfv3 | all | other } { enable | disable }
- **capture cpupkt interface** { ethernet | xgigaethernet | 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet } *interface-number* **time** *time-value*
- **capture cpupkt interface eth-trunk** *trunk-number* { arp | lldp | loopback | dot3ah | lacp | dot1x | cfm | y1731 | g8032 | g8031 | eaps | dlip | mlag | mpls | stp | isis | iss | bfd | sync | arp | ip | ospf | igmp | icmp | udp | dhcp | ldp-hello | bfd-udp | tcp | bgp | ldp-tcp | ipv6 | icmpv6 |

icmpv6-echo-request | icmpv6-echo-reply | icmpv6-rs | icmpv6-ra | icmpv6-ns | icmpv6-na | icmpv6-redirect | ospfv3 | all | other } { enable | disable }

- **capture cpupkt interface eth-trunk trunk-number time time-value**
- **capture cpupkt interface mgt-eth mgt-eth-number { arp | lldp | loopback | dot3ah | lacp | dot1x | cfm | y1731 | g8032 | g8031 | eaps | dlip | mlag | mpls | stp | isis | iss | bfd | sync | arp | ip | ospf | igmp | icmp | udp | dhcp | ldp-hello | bfd-udp | tcp | bgp | ldp-tcp | ipv6 | icmpv6 | icmpv6-echo-request | icmpv6-echo-reply | icmpv6-rs | icmpv6-ra | icmpv6-ns | icmpv6-na | icmpv6-redirect | ospfv3 | all | other } { enable | disable }**
- **capture cpupkt interface mgt-eth mgt-eth-number time time-value**
- **capture cpupkt interface stack-port iss-group-id { arp | lldp | loopback | dot3ah | lacp | dot1x | cfm | y1731 | g8032 | g8031 | eaps | dlip | mlag | mpls | stp | isis | iss | bfd | sync | arp | ip | ospf | igmp | icmp | udp | dhcp | ldp-hello | bfd-udp | tcp | bgp | ldp-tcp | ipv6 | icmpv6 | icmpv6-echo-request | icmpv6-echo-reply | icmpv6-rs | icmpv6-ra | icmpv6-ns | icmpv6-na | icmpv6-redirect | ospfv3 | all | other } { enable | disable }**
- **capture cpupkt interface stack-port iss-group-id time time-value**
- **no capture cpupkt interface { ethernet | xgigaethernet | 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet } interface-number**
- **no capture cpupkt interface eth-trunk trunk-number**
- **no capture cpupkt interface mgt-eth mgt-eth-number**
- **no capture cpupkt interface stack-port iss-group-id**

Parameter

Parameter	Description	Value
interface-number	Specifies an Ethernet interface number.	The value is an integer in the range of <1-1>/<0-1>/<1-48>.
trunk-number	Specifies the number of a Trunk interface.	The value is an integer ranging from 1 to 128.
iss-group-id	Specifies an ISS group ID.	The value is an integer ranging from 1 to 2.
time-value	Specifies the packet capturing time.	The value is an integer ranging from 1 to 1800.
mgt-eth-number	Specifies an out-of-band interface.	The value is an integer in the range of <0-0>/<0-0>/<0-0>.

Default Value

NA

View

Privileged user view

Usage Guidelines

NA

Example

Configure the continuous duration for capturing the packets sent and received by the CPU in the current interface.

```
Switch#capture cpupkt interface xgigaethernet 1/0/1 time 30
Switch#
```

11.5.2 debug cpupkt interface**Function**

The **debug cpupkt interface** command debugs configurations of the interface for the CPU to send and receive packets.

Format

- **debug cpupkt interface** { ethernet | xgigaethernet | 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet } *interface-number* { arp | lldp | loopback | dot3ah | lacp | dot1x | cfm | y1731 | g8032 | g8031 | eaps | dlip | mlag | mpls | stp | isis | iss | bfd | sync | arp | ip | ospf | igmp | icmp | udp | dhcp | ldp-hello | bfd-udp | tcp | bgp | ldp-tcp | ipv6 | icmpv6 | icmpv6-echo-request | icmpv6-echo-reply | icmpv6-rs | icmpv6-ra | icmpv6-ns | icmpv6-na | icmpv6-redirect | ospfv3 | all | other } { in | out | both | none }
- **debug cpupkt interface eth-trunk** *trunk-number* { arp | lldp | loopback | dot3ah | lacp | dot1x | cfm | y1731 | g8032 | g8031 | eaps | dlip | mlag | mpls | stp | isis | iss | bfd | sync | arp | ip | ospf | igmp | icmp | udp | dhcp | ldp-hello | bfd-udp | tcp | bgp | ldp-tcp | ipv6 | icmpv6 | icmpv6-echo-request | icmpv6-echo-reply | icmpv6-rs | icmpv6-ra | icmpv6-ns | icmpv6-na | icmpv6-redirect | ospfv3 | all | other } { in | out | both | none }
- **debug cpupkt interface mgt-eth** *mgt-eth-number* { arp | lldp | loopback | dot3ah | lacp | dot1x | cfm | y1731 | g8032 | g8031 | eaps | dlip | mlag | mpls | stp | isis | iss | bfd | sync | arp | ip | ospf | igmp | icmp | udp | dhcp | ldp-hello | bfd-udp | tcp | bgp | ldp-tcp | ipv6 | icmpv6 | icmpv6-echo-request | icmpv6-echo-reply | icmpv6-rs | icmpv6-ra | icmpv6-ns | icmpv6-na | icmpv6-redirect | ospfv3 | all | other } { in | out | both | none }

Parameter

Parameter	Description	Value
interface-number	Specifies an Ethernet interface number.	The value is an integer in the range of <1-1>/<0-1>/<1-48>.
trunk-number	Specifies the number of a Trunk interface.	The value is an integer ranging from 1 to 128.
mgt-eth-number	Specifies an out-of-band interface.	The value is an integer in the range of <0-0>/<0-0>/<0-0>.

Default Value

NA

View

Privileged user view

Usage Guidelines

You can run this command to debug configurations of the interface for the CPU to send and receive packets.

Example

Debug configurations of the interface for the CPU to send and receive packets.

```
Switch#debug cpupkt interface xgigaethernet 1/0/1 iss none
Switch#
```

11.5.3 show cpupkt interface statistic

Function

The **show cpupkt interface statistic** command displays the statistics information on the interface for the CPU to send and receive packets.

Format

- **show cpupkt interface** { ethernet | xgigaethernet | 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet } *interface-number* { arp | lldp | loopback | dot3ah | lacp | dot1x | cfm | y1731 | g8032 | g8031 | eaps | dlip | mlag | mpls | stp | isis | iss | bfd | sync | arp | ip | ospf | igmp | icmp | udp | dhcp | ldp-hello | bfd-udp | tcp | bgp | ldp-tcp | ipv6 | icmpv6 | icmpv6-echo-request | icmpv6-echo-reply | icmpv6-rs | icmpv6-ra | icmpv6-ns | icmpv6-na | icmpv6-redirect | ospfv3 | all | other } **statistic**
- **show cpupkt interface eth-trunk** *trunk-number* { arp | lldp | loopback | dot3ah | lacp | dot1x | cfm | y1731 | g8032 | g8031 | eaps | dlip | mlag | mpls | stp | isis | iss | bfd | sync | arp | ip |

ospf | igmp | icmp | udp | dhcp | ldp-hello | bfd-udp | tcp | bgp | ldp-tcp | ipv6 | icmpv6 | icmpv6-echo-request | icmpv6-echo-reply | icmpv6-rs | icmpv6-ra | icmpv6-ns | icmpv6-na | icmpv6-redirect | ospfv3 | all | other } statistic

- **show cpupkt interface mgt-eth *mgt-eth-number* { arp | lldp | loopback | dot3ah | lacp | dot1x | cfm | y1731 | g8032 | g8031 | eaps | dlip | mlag | mpls | stp | isis | iss | bfd | sync | arp | ip | ospf | igmp | icmp | udp | dhcp | ldp-hello | bfd-udp | tcp | bgp | ldp-tcp | ipv6 | icmpv6 | icmpv6-echo-request | icmpv6-echo-reply | icmpv6-rs | icmpv6-ra | icmpv6-ns | icmpv6-na | icmpv6-redirect | ospfv3 | all | other } statistic**

Parameter

Parameter	Description	Value
interface-number	Specifies an Ethernet interface number.	The value is an integer in the range of <1-1>/<0-1>/<1-48>.
trunk-number	Specifies the number of a Trunk interface.	The value is an integer ranging from 1 to 128.
mgt-eth-number	Specifies a management Ethernet port.	The value is an integer in the range of <0-0>/<0-0>/<0-0>.

Default Value

NA

View

Common user view

Usage Guidelines

This command is run to display the statistics information on an interface for the CPU to send and receive packets.

Example

Display the statistics information on an interface for the CPU to send and receive packets.

```
Switch>show cpupkt interface 25gigaethernet 1/0/1 all statistic
-----
Receive Packet      : 0          SendOut Packet      : 0
Receive Byte        : 0          SendOut Byte        : 0
Switch>
```

11.5.4 reset cpupkt interface statistic

Function

The **reset cpupkt interface statistic** command resets the CPU packet capturing information on the current interface.

Format

- **reset cpupkt interface** { ethernet | xgigaethernet | 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet } *interface-number* { arp | lldp | loopback | dot3ah | lacp | dot1x | cfm | y1731 | g8032 | g8031 | eaps | dlip | mlag | mpls | stp | isis | iss | bfd | sync | arp | ip | ospf | igmp | icmp | udp | dhcp | ldp-hello | bfd-udp | tcp | bgp | ldp-tcp | ipv6 | icmpv6 | icmpv6-echo-request | icmpv6-echo-reply | icmpv6-rs | icmpv6-ra | icmpv6-ns | icmpv6-na | icmpv6-redirect | ospfv3 | all | other } **statistic**
- **reset cpupkt interface eth-trunk** *trunk-number* { arp | lldp | loopback | dot3ah | lacp | dot1x | cfm | y1731 | g8032 | g8031 | eaps | dlip | mlag | mpls | stp | isis | iss | bfd | sync | arp | ip | ospf | igmp | icmp | udp | dhcp | ldp-hello | bfd-udp | tcp | bgp | ldp-tcp | ipv6 | icmpv6 | icmpv6-echo-request | icmpv6-echo-reply | icmpv6-rs | icmpv6-ra | icmpv6-ns | icmpv6-na | icmpv6-redirect | ospfv3 | all | other } **statistic**
- **reset cpupkt interface mgt-eth** *mgt-eth-number* { arp | lldp | loopback | dot3ah | lacp | dot1x | cfm | y1731 | g8032 | g8031 | eaps | dlip | mlag | mpls | stp | isis | iss | bfd | sync | arp | ip | ospf | igmp | icmp | udp | dhcp | ldp-hello | bfd-udp | tcp | bgp | ldp-tcp | ipv6 | icmpv6 | icmpv6-echo-request | icmpv6-echo-reply | icmpv6-rs | icmpv6-ra | icmpv6-ns | icmpv6-na | icmpv6-redirect | ospfv3 | all | other } **statistic**

Parameter

Parameter	Description	Value
interface-number	Specifies an Ethernet interface number.	The value is an integer in the range of <1-1>/<0-1>/<1-48>.
trunk-number	Specifies the number of a Trunk interface.	The value is an integer ranging from 1 to 128.
mgt-eth-number	Specifies an out-of-band interface.	The value is an integer in the range of <0-0>/<0-0>/<0-0>.

Default Value

NA

View

Privileged user view

Usage Guidelines

NA

Example

Reset the CPU packet capturing information on the current interface.

```
Switch#reset cpupkt interface xgigaethernet 1/0/1 iss statistic
Switch#
```

11.6 Telemetry Configuration Commands

11.6.1 ip address port|ipv6 address port

Function

The **ip address port** command configures the IP address, port number, protocol, and encryption mode of the upstream destination collector.

The **no ip address port** command deletes the IP address, port number, protocol, and encryption mode of the upstream destination collector.

Format

- **ip address** *ipv4-address* **port** *port-number* **protocol** **grpc**
- **ip address** *ipv4-address* **port** *port-number* **vpn-instance** *name* **protocol** **grpc**
- **no ip address** *ipv4-address* **port** *port-number*
- **no ip address** *ipv4-address* **port** *port-number* **vpn-instance** *name*

Parameter

Parameter	Description	Value
ipv4-address	Specifies an upstream destination IP address.	The value is in dotted decimal notation.
port-number	Specifies an upstream destination port number.	The value is an integer ranging from 1 to 65535.
name	Specifies an upstream destination VPN instance name.	The value is a character string.
grpc	Specifies that the data reporting protocol is GRPC.	-

Default Value

NA

View

Destination-group configuration view

Usage Guidelines

NA

Example

Configure the IP address to 10.1.1.1, port number to 10001, and data reporting protocol to GRPC for the upstream destination collector.

```
Switch(config)#telemetry destination-group group1
Switch(config-telemetry-destination-group-group1)#ip address 10.1.1.1 port 10001 protocol grpc
Switch(config-telemetry-destination-group-group1)#
```

11.6.2 sensor-path**Function**

The **sensor-path** command configures the sampling path of the Telemetry sensor.

The **no sensor-path** command deletes the sampling path of the Telemetry sensor.

Format

- **sensor-path** *name*
- **no sensor-path** *name*

Parameter

Parameter	Description	Value
name	Specifies a sampling path name.	The value is a character string.

Default Value

NA

View

Sensor-group configuration view

Usage Guidelines

NA

Example

Configure the path of the Telemetry sampling sensor.

```
Switch(config)#telemetry sensor-group group1
Switch(config-telemetry sensor-group-1)#sensor-path devm:devm/cpuInfos
```

11.6.3 destination-group

Function

The **destination-group** command configures the associated upstream destination group.

The **no destination-group** command deletes the configured associated upstream destination group.

Format

- **destination-group** *name*
- **no destination-group** *name*

Parameter

Parameter	Description	Value
name	Specifies an upstream destination group name.	The value is a character string.

Default Value

NA

View

Subscription configuration view

Usage Guidelines

NA

Example

Create the upstream destination group named a in the Telemetry view, and associate the destination group in the Subscription view.

```
Switch(config)#telemetry destination-group aa
Switch(config-telemetry-destination-group-aa)#quit
Switch(config)#telemetry subscription group1
Switch(config-telemetry-subscription-group1)#destination-group aa
Switch(config-telemetry-subscription-group1)#
```

11.6.4 sensor-group

Function

The **sensor-group** command associates a sampling sensor group and configures the sampling period of the group.

The **no sensor-group** command cancels association of a sampling sensor group.

Format

- **sensor-group** *name* **sample-interval** *interval-value*
- **no sensor-group** *name*

Parameter

Parameter	Description	Value
name	Specifies an associated sampling sensor group name.	The value is a character string.
interval-value	Specifies a sampling interval.	The value is an integer ranging from 100 to 1800000, in milliseconds.

Default Value

NA

View

Subscription configuration view

Usage Guidelines

NA

Example

Associate a sampling sensor group and configure the sampling period of the group.

```
Switch(config)#telemetry sensor-group 1
Switch(config-telemetry sensor-group-1)#quit
Switch(config)#telemetry subscription group1
Switch(config-telemetry-subscription-group1)#sensor-group 1 sample-interval 100
Switch(config-telemetry-subscription-group1)#
```

11.6.5 telemetry {enable|disable}

Function

The **telemetry {enable|disable}** command enables or disables the data collection function.

Format

telemetry { enable | disable }

Parameter

NA

Default Value

NA

View

Global configuration view

Usage Guidelines

NA

Example

Enable the data collection function.

```
Switch(config)#telemetry enable
Switch(config)#
```

11.6.6 telemetry destination-group**Function**

The **telemetry destination-group** command configures an upstream destination group of sampled data and enters the Destination-group view.

The **no telemetry destination-group** command deletes the upstream destination group used to create sampling data.

Format

- **telemetry destination-group** *name*
- **no telemetry destination-group** *name*

Parameter

Parameter	Description	Value
name	Specifies an upstream destination group name.	The value is a character string.

Default Value

NA

View

Global configuration view

Usage Guidelines

NA

Example

Configure an upstream destination group for data collection.

```
Switch(config)#telemetry destination-group group1
Switch(config-telemetry-destination-group-group1)#
```

11.6.7 telemetry sensor-group**Function**

The **telemetry sensor-group** command creates a sampling sensor group and enters the Sensor-group view.

The **no telemetry sensor-group** command deletes the created sampling sensor group.

Format

- **telemetry sensor-group** *name*
- **no telemetry sensor-group** *name*

Parameter

Parameter	Description	Value
name	Specifies the name of a sampling sensor group.	The value is a character string.

Default Value

NA

View

Global configuration view

Usage Guidelines

NA

Example

Create a sampling sensor group and enter the Sensor-group view.

```
Switch(config)#telemetry sensor-group group1
Switch(config-telemetry sensor-group-1)#
```


11.6.8 telemetry subscription

Function

The **telemetry subscription** command creates subscription to associate an upstream destination group and a sampling sensor group and enters the Subscription view.

The **no telemetry subscription** command deletes the created subscription.

Format

- **telemetry subscription** *name*
- **no telemetry subscription** *name*

Parameter

Parameter	Description	Value
name	Specifies a subscription name.	The value is a character string.

Default Value

NA

View

Global configuration view

Usage Guidelines

NA

Example

Create subscription to associate an upstream destination group and a sampling sensor group and enter the Subscription view.

```
Switch(config)#telemetry subscription group1
Switch(config-telemetry-subscription-group1)#
```

11.6.9 show telemetry

Function

The **show telemetry config** command shows Telemetry sensor configuration information.

The **show telemetry destination config** command shows upstream destination group information.

The **show telemetry sensor config** command shows sampling sensor group information.

The **show telemetry config** command shows Telemetry sensor subscription information.

Format

show telemetry config

show telemetry destination config

show telemetry sensor config

show telemetry subscription config

Parameter

NA

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

View Telemetry sensor configuration information.

```
Switch>show telemetry config
Switch>
```

11.7 NQA Configuration Commands

11.7.1 nqa {start|stop}

Function

The **nqa start** command enables the NQA globally.

The **nqa stop** command disables the NQA globally.

Format

nqa { start | stop}

Parameter

Parameter	Description	Value

Parameter	Description	Value
start	Enables NQA globally.	-
stop	Disables NQA globally.	-

Default

stop

View

Global configuration view

Usage Guidelines

NA

Example

Enable NQA globally.

```
Switch(config)#nqa start
```

```
Switch(config)#
```

11.7.2 nqa test-instance**Function**

The **nqa test-instance** command creates a test instance.

The **no nqa test-instance** command deletes a test instance.

Format

- **nqa test-instance** *admin-name operation-tag*
- **no nqa test-instance** *admin-name operation-tag*

Parameter

Parameter	Description	Value
admin-name	Name of the administrator for an NQA test instance	The value is a string of 1 to 31 characters.
operation-tag	Tag for specific test operations	The value is a string of 1 to 31 characters.

Default

NA

View

Global configuration view

Usage Guidelines

NA

Example

Create a test instance with the administrator named "admin" and operation tag of "admin".

```
Switch(config)#nqa test-instance admin admin
Switch(config-nqa-admin-admin)#
```

11.7.3 type

Function

The **type** command sets the test type of a test instance.

Format

type { icmp-echo | udp-echo | tcp | dhcp | dns | ftp | http | snmp | dlsr | icmp6-echo }

Parameter

Parameter	Description	Value
icmp-echo udp-echo tcp dhcp dns ftp http snmp dlsr icmp6-echo	Test type	-

Default

NA

View

NQA instance configuration view

Usage Guidelines

Currently, only **icmp-echo** is supported.

Example

Set the test type to icmp-echo for a test instance.

```
Switch(config-nqa-admin-admin)#type icmp-echo
Switch(nqa-admin-admin-icmp-echo)#
```

11.7.4 description

Function

The **description** command sets the description of a test instance.

Format

- **description** *text*
- **no description** *text*

Parameter

Parameter	Description	Value
text	Specifies the description.	The value is a string of 1 to 200 characters.

Default

NA

View

NQA instance test type configuration view

Usage Guidelines

This command describes the purpose of a test instance.

Example

Set the description of a test instance.

```
Switch(nqa-admin-admin-icmp-echo)#description test
Switch(nqa-admin-admin-icmp-echo)#
```

11.7.5 frequency

Function

The **frequency** command sets the interval at which a test is performed.

Format

frequency { *interval* | **default** }

Parameter

Parameter	Description	Value
interval	Specifies the interval at which a test is performed.	The value is an integer ranging from 1000 to 604800000, in milliseconds.

Default

NA

View

NQA instance test type configuration view

Usage Guidelines

NA

Example

Set the interval at which a test is performed to 1000 ms.

```
Switch(nqa-admin-admin-icmp-echo)#frequency 1000
Switch(nqa-admin-admin-icmp-echo)#
```

11.7.6 probe count**Function**

The **probe count** command sets the number of probes for a test.

Format

probe count { *times* | **default** }

Parameter

Parameter	Description	Value
times	Number of probes for a test	The value is an integer ranging from 1 to 15.

Default

1

View

NQA instance test type configuration view

Usage Guidelines

NA

Example

Set the number of probes to 2 for a test.

```
Switch(nqa-admin-admin-icmp-echo)#probe count 2
Switch(nqa-admin-admin-icmp-echo)#
```

11.7.7 probe timeout

Function

The **probe timeout** command sets the timeout period of a probe.

Format

probe timeout { *times* | **default** }

Parameter

Parameter	Description	Value
times	Specifies the timeout period of a probe.	The value is an integer ranging from 10 to 3600000, in milliseconds.

Default

3000 ms

View

NQA instance test type configuration view

Usage Guidelines

NA

Example

Set the timeout period of a probe to 3000 ms.

```
Switch(nqa-admin-admin-icmp-echo)#probe timeout 3000
Switch(nqa-admin-admin-icmp-echo)#
```

11.7.8 ttl

Function

The **ttl** command sets the maximum hop count of probe packets on the network.

Format

ttl { *value* | **default** }

Parameter

Parameter	Description	Value
value	Maximum hop count of probe packets on the network	The value is an integer ranging from 1 to 255.

Default

20

View

NQA instance test type configuration view

Usage Guidelines

NA

Example

Set the maximum hop count of probe packets on the network to 30.

```
Switch(nqa-admin-admin-icmp-echo)#ttl 30
Switch(nqa-admin-admin-icmp-echo)#
```

11.7.9 tos**Function**The **tos** command sets the ToS value of a probe packet.**Format****tos** { *value* | **default** }**Parameter**

Parameter	Description	Value
value	ToS value	The value is an integer ranging from 0 to 255.

Default

NA

View

NQA instance test type configuration view

Usage Guidelines

NA

Example

Set the ToS value of a probe packet to 10.

```
Switch(nqa-admin-admin-icmp-echo)#tos 10
Switch(nqa-admin-admin-icmp-echo)#
```


11.7.10 destination ip

Function

The **destination ip** command sets the destination IP address for a test.

Format

destination ip *ip-address*

Parameter

Parameter	Description	Value
ip-address	Destination IP address	The value is in dotted decimal notation.

Default

NA

View

NQA instance test type configuration view

Usage Guidelines

NA

Example

Set the destination IP address for the test to 10.0.0.2.

```
Switch(nqa-admin-admin-icmp-echo)#destination ip 10.0.0.2
Switch(nqa-admin-admin-icmp-echo)#
```

11.7.11 data-fill

Function

The **data-fill** command sets padding field of a probe packet.

The **no data fill** command deletes padding characters from a probe packet.

Format

- **data-fill** *string*
- **no data fill**

Parameter

Parameter	Description	Value

Parameter	Description	Value
string	Padding characters	The value is a string of 1 to 200 characters.

Default

NA

View

NQA instance test type configuration view

Usage Guidelines

NA

Example

Set the padding field of a probe packet to test.

```
Switch(nqa-admin-admin-icmp-echo)#data-fill test
Switch(nqa-admin-admin-icmp-echo)#
```

11.7.12 data-size**Function**The **data-size** command sets the size of a probe packet.**Format****data-size { size | default }****Parameter**

Parameter	Description	Value
size	Size of a probe packet	The value is an integer ranging from 20 to 1500.

Default

NA

View

NQA instance configuration view

Usage Guidelines

NA

Example

Set the size of a probe packet to 100.

```
Switch(nqa-admin-admin-icmp-echo)#data-size 100
Switch(nqa-admin-admin-icmp-echo)#
```

11.7.13 source ip

Function

The **source ip** command sets the source IP address of the test packet.

Format

- **source ip** *ip-address*
- **no source ip**

Parameter

Parameter	Description	Value
ip-address	Source IP address	The value is in dotted decimal notation.

Default

NA

View

NQA instance test type configuration view

Usage Guidelines

NA

Example

Set the source IP address of a test packet to 10.0.0.1.

```
Switch(nqa-admin-admin-icmp-echo)#source ip 10.0.0.1
Switch(nqa-admin-admin-icmp-echo)#
```

11.7.14 history-record {enable|disable}

Function

The **history-record enable** command enables NQA history recording.

The **history-record disable** command disables NQA history recording.

Format

history-record {enable|disable}**Parameter**

Parameter	Description	Value
enable	Enables NQA history recording.	-
disable	Disables NQA history recording.	-

Default

disable

View

NQA instance test type configuration view

Usage Guidelines

NA

Example

Enable NQA history recording.

```
Switch(nqa-admin-admin-icmp-echo)#history-record enable
Switch(nqa-admin-admin-icmp-echo)#
```

11.7.15 history-record keep-time**Function**

The **history-record keep-time** command sets the time for saving NQA history records.

Format

history-record keep-time *time*

Parameter

Parameter	Description	Value
time	Specifies the time for saving NQA history records.	The value is an integer ranging from 1 to 1440, in minutes.

Default

120min

View

NQA instance test type configuration view

Usage Guidelines

NA

Example

Set the time for saving NQA history records to 10 minutes.

```
Switch(nqa-admin-admin-icmp-echo)#history-record keep-time 10
Switch(nqa-admin-admin-icmp-echo)#
```

11.7.16 history-record number**Function**

The **history-record number** command sets the maximum number of NQA history entries.

Format

history-record number *number*

Parameter

Parameter	Description	Value
number	Specifies the maximum number of history entries.	The value is an integer ranging from 0 to 50.

Default

NA

View

NQA instance test type configuration view

Usage Guidelines

NA

Example

Set the maximum number of NQA history entries to 10.

```
Switch(nqa-admin-admin-icmp-echo)#history-record number 10
Switch(nqa-admin-admin-icmp-echo)#
```

11.7.17 nqa schedule**Function**

The **nqa schedule** command sets a scheduling mode for a test instance.

Format

- **nqa schedule** *admin-name operation-tag time-range list list-number*
- **nqa schedule** *admin-name operation-tag start-time now life-time forever*

Parameter

Parameter	Description	Value
admin-name	Name of the administrator for an NQA test instance	The value is a string of 1 to 31 characters.
operation-tag	Tag for specific test operations	The value is a string of 1 to 31 characters.
list-number	Name of the time-range module list	The value is an integer ranging from 1 to 128.

Default

NA

View

Global configuration view

Usage Guidelines

NA

Example

Set a scheduling mode for a test instance with the administrator named "admin" and operation tag of "admin".

```
Switch(config)#nqa schedule admin admin start-time now life-time forever
Switch(config)#
```

11.7.18 show nqa result**Function**

The **show nqa result** command displays the latest test result of a test instance.

The **show nqa statistics** command displays all test results of a test instance.

Format

- **show nqa result** *admin-name operation-tag*
- **show nqa statistics** *admin-name operation-tag*

Parameter

Parameter	Description	Value
admin-name	Name of the administrator for an NQA test instance	The value is a string of 1 to 31 characters.
operation-tag	Tag for specific test operations	The value is a string of 1 to 31 characters.

Default

NA

View

Global configuration view

Usage Guidelines

NA

Example

Display the latest test result of a test instance with the administrator named "admin" and operation tag of "admin".

```
Switch(config)#show nqa result admin admin
Group start time : 2023-01-28 02:30:47
Life Time(ms) : 0
Send operation times : 0
Receive response times : 0
Min round trip time(ms) : 0
Max round trip time(ms) : 0
Average round trip time(ms) : 0
Square-Sum of round trip time : 0
Failures due to timeout : 0
Failures due to no connection : 0
Failures due to disconnect : 0
Failures due to sequence error : 0
Failures due to internal error : 0
Failures due to other errors : 0
Packet(s) arrived late : 0
Switch(config)#
```

11.7.19 show nqa history**Function**

The **show nqa history** command displays history information of a test instance.

Format

- **show nqa history**
- **show nqa history** *admin-name operation-tag*

Parameter

Parameter	Description	Value
admin-name	Name of the administrator for an NQA test instance	The value is a string of 1 to 31 characters.
operation-tag	Tag for specific test operations	The value is a string of 1 to 31 characters.

Default

NA

View

Global configuration view

Usage Guidelines

NA

Example

Display history information of a test instance.

```
Switch(config)#show nqa history 2 2
Index Response Status Time
1 0 succeeded 2023-02-07 03:18:05
2 0 succeeded 2023-02-07 03:18:05
3 0 succeeded 2023-02-07 03:18:05
4 0 succeeded 2023-02-07 03:18:00
5 0 succeeded 2023-02-07 03:18:00
6 0 succeeded 2023-02-07 03:18:00
7 0 succeeded 2023-02-07 03:17:55
8 0 succeeded 2023-02-07 03:17:55
Switch(config)#
```

11.7.20 show nqa agent

Function

The **show nqa agent** command displays client information of a test instance.

Format

- **show nqa agent**

● **show nqa agent** *admin-name operation-tag*

Parameter

Parameter	Description	Value
admin-name	Name of the administrator for an NQA test instance	The value is a string of 1 to 31 characters.
operation-tag	Tag for specific test operations	The value is a string of 1 to 31 characters.

Default

NA

View

Global configuration view

Usage Guidelines

NA

Example

Display client information of a test instance.

```
Switch(config)#show nqa agent
Admin Tag Type Status In-test Entry
1 1 icmp-echo active enable valid
2 2 icmp-echo active disable valid
3 3 icmp-echo active enable valid
4 4 icmp-echo active enable valid
5 5 icmp-echo active enable valid
6 6 icmp-echo active enable valid
7 7 icmp-echo active enable valid
8 8 icmp-echo active enable valid
9 9 icmp-echo active enable valid
10 10 icmp-echo active enable valid
11 11 icmp-echo active enable valid
12 12 icmp-echo active disable valid
13 13 icmp-echo active disable valid
14 14 icmp-echo active disable valid
15 15 icmp-echo active disable valid
16 16 icmp-echo active disable valid
17 17 icmp-echo active enable valid
18 18 icmp-echo active enable valid
19 19 icmp-echo active enable valid
20 20 icmp-echo active enable valid
```

```
21 21 icmp-echo active enable valid
Switch(config)#
```

11.7.21 show nqa config

Function

The **show nqa config** command displays NQA configuration.

Format

show nqa config

Parameter

NA

Default

NA

View

Global configuration view

Usage Guidelines

NA

Example

Display NQA configuration.

```
Switch(config)#show nqa config
Switch(config)#
```

11.8 JSON-RPC Configuration Commands

11.8.1 batch-cmd jsonrpc { enable | disable }

Function

The **batch-cmd jsonrpc { enable | disable }** command enables or disables the JSON-RPC interface services.

Format

batch-cmd jsonrpc { enable | disable }

Parameter

Parameter	Description	Value
enable	Enables JSON-RPC interface services.	-
disable	Disables JSON-RPC interface services.	-

Default Value

disable

View

Global configuration view

Usage Guidelines

NA

Example

Enable JSON-RPC interface services.

```
Switch(config)#batch-cmd jsonrpc enable
Switch(config)#
```

11.8.2 batch-cmd jsonrpc auth-mode

Function

The **batch-cmd jsonrpc auth-mode** command sets authentication mode for JSON-RPC service interfaces.

Format

batch-cmd jsonrpc auth-mode { basic | strict | none | default }**Parameter**

Parameter	Description	Value
basic	Basic authentication mode, only verifying accounts and passwords.	-
strict	Strict authentication mode, verifying client IP addresses, accounts and passwords.	-
none	Disables authentication.	-
default	Default authentication mode.	strict

Default Value

strict

View

Global configuration view

Usage Guidelines

NA

Example# Set authentication mode to **basic** for JSON-RPC service interfaces.

```
Switch(config)#batch-cmd jsonrpc auth-mode basic
Switch(config)#
```

11.8.3 batch-cmd jsonrpc bind-ip**Function**

The **batch-cmd jsonrpc bind-ip** command binds an IP address with the JSON-RPC interface services.

Format

- **batch-cmd jsonrpc bind-ip** *ip-address*
- **batch-cmd jsonrpc bind-ip default**

Parameter

Parameter	Description	Value

Parameter	Description	Value
<i>ip-address</i>	Specifies an IPv4 address to be bound.	The value is in dotted decimal notation. For example, an IPv4 address is in the A.B.C.D format.
default	Binds the default IPv4 address.	0.0.0.0

Default Value

0.0.0.0

View

Global configuration view

Usage Guidelines

NA

Example

Bind an IPv4 address 10.1.1.1 with JASON-RPC interface services.

```
Switch(config)#batch-cmd jsonrpc bind-ip 10.1.1.1
Switch(config)#
```

11.8.4 batch-cmd jsonrpc bind-port**Function**The **batch-cmd jsonrpc bind-port** command binds a port with the JSON-RPC interface services.**Format****batch-cmd jsonrpc bind-port** { *port-value* | **default** }**Parameter**

Parameter	Description	Value
<i>port-value</i>	Port value	The value is an integer in the range from 1 to 65535.
default	Default port value	8080

Default Value

8080

View

Global configuration view

Usage Guidelines

NA

Example

Bind a port numbered 80 with JASON-RPC interface services.

```
Switch(config)#batch-cmd jsonrpc bind-port 80
Switch(config)#
```

11.8.5 batch-cmd jsonrpc whitelist**Function**

The **batch-cmd jsonrpc whitelist** command adds client IPv4 addresses to the whitelist of the JSON-RPC interface services.

The **no batch-cmd jsonrpc whitelist** command deletes client IPv4 addresses from the whitelist.

Format

- **batch-cmd jsonrpc whitelist** *ip-address*
- **batch-cmd jsonrpc whitelist default**
- **no batch-cmd jsonrpc whitelist** *ip-address*

Parameter

Parameter	Description	Value
<i>ip-address</i>	Adds an IPv4 address to the whitelist.	The value is in dotted decimal notation. For example, an IPv4 address is in the A.B.C.D format.
default	Allows all the IPv4 address requests.	-

Default Value

Allows all the IPv4 address requests.

View

Global configuration view

Usage Guidelines

NA

Example

Add a client IPv4 address 1.1.1.1 to the whitelist of the JASON-RPC interface services.

```
Switch(config)#batch-cmd jsonrpc whitelist 1.1.1.1
Switch(config)#
```

11.8.6 batch-cmd jsonrpc timeout

Function

The **batch-cmd jsonrpc timeout** command sets a request / response timeout period for JSON-RPC interface services.

Format

batch-cmd jsonrpc timeout { *time-value* | **default** }

Parameter

Parameter	Description	Value
<i>time -value</i>	Timeout period	The value is an integer in the range from 1 to 300, in seconds.
default	Default timeout period	60 seconds

Default Value

60

View

Global configuration view

Usage Guidelines

NA

Example

Set a request / response timeout period for JSON-RPC interface services.

```
Switch(config)#batch-cmd jsonrpc timeout 180
Switch(config)#
```

11.8.7 batch-cmd jsonrpc max-cmds

Function

The **batch-cmd jsonrpc max-cmds** command sets the maximum number of command lines allowed by a single batch request on JSON-RPC interface services.

Format

batch-cmd jsonrpc max-cmds { *value* | **default }**

Parameter

Parameter	Description	Value
<i>value</i>	Maximum number of command lines	The value is an integer in the range from 1 to 30.
default	Default maximum number of command lines	10

Default Value

10

View

Global configuration view

Usage Guidelines

NA

Example

Set the maximum number of command lines allowed by a single batch request on JSON-RPC interface services.

```
Switch(config)#batch-cmd jsonrpc max-cmds 30
Switch(config)#
```

11.8.8 show batch-cmd jsonrpc**Function**

The **show batch-cmd jsonrpc** command displays configuration parameters for the current JSON-RPC interface services.

Format

show batch-cmd jsonrpc

Parameter

NA

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

Show configurations of the current JSON-RPC interface services.

```
Switch#show batch-cmd jsonrpc
  Server State           :enable
  Server Host            :10.1.1.1
  Server Port            :80
  Authentication Mode    :basic
  Max Commands per Request :30
  Req/Rep timeout (s)    :180
  IP WhiteList           :1.1.1.1
```

Chapter 12 VPN Commands

This chapter mainly describes VPN-related configuration commands of Switch series switches.

12.1 L3VPN Configuration Commands

12.1.1 debug l3vpn

Function

The **debug l3vpn** command enables L3VPN debugging.

The **no debug l3vpn** command disables L3VPN debugging.

Format

- **debug l3vpn { io | event | error | nm | route | all }**
- **no debug l3vpn { io | event | error | nm | route | all }**

Parameter

NA

Default Value

By default, L3VPN debugging is disabled.

View

Privileged user view

Usage Guidelines

You can use this command to view the L3VPN process and packet sending and receiving situations. This command is used to maintain and debug the L3VPN function of the switch.

Example

Enable L3VPN debugging.

```
Switch#debug l3vpn all
Switch#
```

12.1.2 description

Function

The **description** command defines description of a VPN instance.

The **no description** command deletes description of a VPN instance.

Format

- **description** *description-information*
- **no description**

Parameter

Parameter	Description	Value
description-information	Specifies VPN instance description.	The value is a string of up to 64 characters.

Default Value

By default, the VPN instance description does not exist.

View

IP-VPN configuration view

Usage Guidelines

If you run the description command multiple times, the last configuration takes effect.

Example

Define the VPN instance description as fhn.

```
Switch(config-vpn-instance-111)#description fhn
Switch(config-vpn-instance-111)#
```

12.1.3 ip binding vpn-instance

Function

The **ip binding vpn-instance** command binds a VPN instance to a VPN-enabled Layer-3 interface (such as Layer-3 VLAN interface vlanif).

The **no ip binding vpn-instance** command deletes the bound VPN instance.

Format

- **ip binding vpn-instance** *vpn-instance-name*
- **no ip binding vpn-instance** *vpn-instance-name*

Parameter

Parameter	Description	Value
vpn-instance-name	Specifies a VPN instance name.	The value is a string of up to 64 characters.

Default Value

By default, an interface is not bound to any VPN instance.

View

VLANIF configuration view, Loopback interface configuration view, Tunnel interface configuration view, BD interface configuration view, Ethernet routing interface configuration view, Ethernet sub-interface configuration view, Trunk sub-interface configuration view, out-of-band configuration view, and GRP routing interface configuration view

Usage Guidelines

NA

Example

Bind the VLAN2 interface to the VPN instance named 111.

```
Switch(config-vlanif-2)#ip binding vpn-instance 111
Switch(config-vlanif-2)#
```

12.1.4 ip|ipv6 import-rib vpn-instance protocol static

Function

The **ip|ipv6 import-rib vpn-instance protocol static** command imports the static, ISIS or OSPF route of a VPN instance to the routing table of a public network.

The **no ip|ipv6 import-rib vpn-instance protocol static** command deletes the route of a VPN instance from the routing table of a public network.

Format

- **ip import-rib vpn-instance** *vpn-instance-name* **protocol static**
- **ip import-rib vpn-instance** *vpn-instance-name* **protocol static route-policy** *policy-name*
- **ipv6 import-rib vpn-instance** *vpn-instance-name* **protocol static**
- **ipv6 import-rib vpn-instance** *vpn-instance-name* **protocol static route-policy** *policy-name*
- **no ip import-rib vpn-instance** *vpn-instance-name* **protocol static**
- **no ipv6 import-rib vpn-instance** *vpn-instance-name* **protocol static**

Parameter

Parameter	Description	Value
vpn-instance-name	Specifies a VPN instance name.	The value is a character string containing a maximum of 64 characters.
policy-name	Specifies a route policy name.	The value is a character string containing a maximum of 20 characters.

Default Value

NA

View

Global configuration view

Usage Guidelines

Before running this command, create an instance.

Example

Import the static route of VPN instance 1 to the routing table of a public network.

```
Switch(config)#ip import-rib vpn-instance 1 protocol static
Switch(config)#
```

12.1.5 import-rib public protocol static**Function**

The **import-rib public protocol static** command imports the static, ISIS or OSPF route of a public network or a VPN instance to the routing table of a specified VPN instance.

The **no import-rib public protocol static** command deletes the route of a public network or a VPN instance from the routing table of a specified VPN instance.

Format

- **import-rib public protocol static**
- **import-rib public protocol static route-policy** *policy-name*
- **import-rib vpn-instance** *vpn-instance-name* **protocol static**
- **import-rib vpn-instance** *vpn-instance-name* **protocol static route-policy** *policy-name*
- **no import-rib public protocol static**
- **no import-rib vpn-instance** *vpn-instance-name* **protocol static**

Parameter

Parameter	Description	Value
vpn-instance-name	Specifies a VPN instance name.	The value is a character string containing a maximum of 64 characters.
policy-name	Specifies a routing policy name.	The value is a character string containing a maximum of 20 characters.

Default Value

NA

View

Ip-vpn-af-ipv4 configuration view and ip-vpn-af-ipv6 configuration view

Usage Guidelines

NA

Example

Import the static route of a public network or a VPN instance to the routing table of a specified VPN instance.

```
Switch(config-vpn-instance-af-ipv4)#import-rib public protocol static
Switch(config-vpn-instance-af-ipv4)#
```

12.1.6 ip vpn-instance snmp-trap**Function**

The **ip vpn-instance snmp-trap** command enables or disables the L3 alarm function.

Format

ip vpn-instance snmp-trap { enable | disable }

Parameter

Parameter	Description	Value
enable	Enables the L3VPN alarm function.	-
disable	Disables the L3VPN alarm function.	-

Default Value

Disable

View

Global configuration view

Usage Guidelines

NA

Example

Enable the L3VPN alarm function.

```
Switch(config)#ip vpn-instance snmp-trap enable
Switch(config)#
```

12.1.7 ipv4-family|ipv6-family

Function

The **ipv4-family|ipv6-family** command enables the IPv4 or IPv6 address family of a VPN instance and enters the IPv4 or IPv6 address family view of the VPN instance.

The **no ipv4-family|ipv6-family** command enables the IPv4 or IPv6 address family of a VPN instance.

Format

- **ipv4-family**
- **ipv6-family**
- **no ipv4-family**
- **no ipv6-family**

Description

NA

Default Value

NA

View

VPN configuration view

Usage Guidelines

NA

Example

Enter the IPv4 address family view of a VPN instance.

```
Switch(config-vpn-instance-111)#ipv4-family
Switch(config-vpn-instance-111-af-ipv4)#
```

12.1.8 vxlan vni

Function

The **vxlan vni** command configures a Layer-3 VNI and binds it to a VPN instance.

The **no vxlan vni** command deletes a Layer-3 VNI from a VPN instance.

Format

- **vxlan vni** *vni-id*
- **no vxlan vni**

Parameter

Parameter	Description	Value
vni-id	Specifies a VNI ID.	The value is an integer ranging from 1 to 16777215.

Default Value

By default, no VNI is bound to a VPN instance.

View

VPN configuration view

Usage Guidelines

NA

Example

Configure Layer-3 VNI 1 and bind it to a VPN instance.

```
Switch(config-vpn-instance-111)#vxlan vni 1
Switch(config-vpn-instance-111)#
```

12.1.9 vpn-target

Function

The **vpn-target** associates the current VPN instance with one or more VPN targets.

The **no vpn-target** deletes the VPN targets associated with the VPN instance.

Format

- **vpn-target target { both | export-extcommunity | import-extcommunity }**
- **no vpn-target**
- **no vpn-target target { both | export-extcommunity | import-extcommunity }**

Parameter

Parameter	Description	Value
target	Adds the VPN target extended community attribute to the inbound or outbound VPN target extended community attribute list of the VPN instance or the outbound or inbound VPN target extended community.	16-bit autonomous system number:32-bit user-defined number, for example, 1:3. The autonomous system number ranges from 0 to 65535. The user-defined number ranges from 0 to 4294967295. The autonomous system number and the user-defined number cannot be 0 simultaneously. That is, the VPN target value cannot be 0:0. 32-bit IP address:16-digit user-defined number, for example, 192.168.122.15:1. The IP address ranges from 0.0.0.0 to 255.255.255.255. The user-defined number ranges from 0 to 65535. 32-bit autonomous system number:16-bit user-defined number, for example, 100.5:1. Generally, the 32-bit automatic system number is in the x.y format, and the value range is 0–65535.0–65535. The user-defined number ranges from 0 to 65535. The autonomous system number and the user-defined number cannot be 0 simultaneously. That is, the VPN target value cannot be 0.0:0.
both	Adds the extended community attribute vpn-target to the extended community attribute list in the ingress and egress directions of VPN instances.	-
export-extcommunity	Specifies the extended community attribute value to the target VPN route information in the egress direction.	-
import-extcommunity	Defines that the route information containing a specified extended community attribute value can be received.	-

Default Value

NA

View

Ip-vpn-af-ipv4 configuration view and ip-vpn-af-ipv6 configuration view

Usage Guidelines

Before configuring the VPN target, run the route-distinguisher command to configure the Route Distinguisher (RD) value.

Example

Configure the VPN-target attribute for L2VPN named VPN1.

```
Switch(config-vpn-instance-111)#vpn-target 1:100 export-extcommunity
Switch(config-vpn-instance-111)#
```

12.1.10 route-distinguisher**Function**

The **route-distinguisher** command configures the route distinguisher (RD) of an VPN instance.

Format

route-distinguisher *rdstring*

Parameter

Parameter	Description	Value
rdstring	Specifies an RD value. Adds the VPN target extended community attribute to the inbound or outbound VPN target extended community attribute list of the VPN instance or the outbound or inbound VPN target extended community.	16-bit autonomous system number:32-bit user-defined number, for example, 1:3. The autonomous system number ranges from 0 to 65535. The user-defined number ranges from 0 to 4294967295. The autonomous system number and the user-defined number cannot be 0 simultaneously. That is, the VPN target value cannot be 0:0. 32-bit IP address:16-digit user-defined number, for example, 192.168.122.15:1. The IP address ranges from 0.0.0.0 to 255.255.255.255. The user-defined number ranges from 0 to 65535. 32-bit autonomous system number:16-bit user-defined number, for example, 100.5:1. Generally, the 32-bit automatic system number is

Parameter	Description	Value
		in the x.y format, and the value range is 0–65535.0–65535. The user-defined number ranges from 0 to 65535. The autonomous system number and the user-defined number cannot be 0 simultaneously. That is, the VPN target value cannot be 0.0:0.

Default Value

NA

View

Ip-vpn-af-ipv4 configuration view and ip-vpn-af-ipv6 configuration view

Usage Guidelines

A VPN instance takes effect only after the RD is configured. If you need to modify the RD, you must delete the corresponding VPN instance and create a VPN instance again.

Example

Set the RD of the VPN instance to 100:4.

```
Switch(config-vpn-instance-111)#route-distinguisher 100:4
Switch(config-vpn-instance-111)#
```

12.1.11 show ip vpn-instance**Function**

The **show ip vpn-instance** command displays all VPN instance information.

Format

show ip vpn-instance

Description

NA

Default Value

NA

View

Common user view

Usage Guidelines

The following table lists the fields in information about a VPN instance.

Item	Description	Value
VPN-Instance Name	Specifies a VPN instance name.	-
RD	Specifies an RD value.	-
Creation Time	Specifies the VPN instance creation time.	-

Example

Display all VPN instance information.

```
Switch>show ip vpn-instance
Total VPN-Instances configured : 2
VPN-Instance Name      Creation Time           Description
a                      2000-04-15 22:57:46    fh-a
b                      2000-04-15 23:27:07    fh-b
Switch>
```

12.1.12 show ip vpn-instance verbose

Function

The **show ip vpn-instance verbose** displays details of a VPN instance.

Format

- **show ip vpn-instance verbose**
- **show ip vpn-instance *name* verbose**

Parameter

Parameter	Description	Value
name	Specifies a VPN instance name.	The value is a string of up to 64 characters.

Default Value

NA

View

Common user view

Usage Guidelines

The following table lists the fields in detail of a VPN instance.

Item	Description
VPN-Instance Name	Displays a VPN instance name and VPN ID.
Creation Time	Specifies the VPN instance creation time.
Route Distinguisher	Specifies an RD.
Description	Specifies VPN instance description information.
Apply Label Per Instance	Specifies a label applied for each instance.
VPN Target	Specifies a VPN target.

Example

Display details of a VPN instance.

```
Switch> show ip vpn-instance verbose
VPN-Instance Name and ID: a, 1
  Creation Time: 2000-04-15 22:57:46
  Description: fh-a
  IPv4 Family:
    Route Distinguisher: 1:1
    Apply Label Per Instance: Disable
    Vpn Target : 11:11 import-extcommunity
                  11:11 export-extcommunity
                  1.1.1.1:1 import-extcommunity
                  1.1.1.1:1 export-extcommunity
    Multicast: Disable
  IPv6 Family:
    Route Distinguisher: 2:2
    Apply Label Per Instance: Disable
    Vpn Target : 22:22 import-extcommunity
                  22:22 export-extcommunity
VPN-Instance Name and ID: b, 2
  Creation Time: 2000-04-15 23:27:07
  Description: fh-b
  IPv4 Family:
    Route Distinguisher: 3:3
    Apply Label Per Instance: Disable
    Vpn Target : 33:33 import-extcommunity
                  33:33 export-extcommunity
    Multicast: Disable
  IPv6 Family:
    Route Distinguisher: 4:4
    Apply Label Per Instance: Disable
    Vpn Target : 44:44 import-extcommunity
                  44:44 export-extcommunity
VPN-Instance Name and ID: public, 0
```

```
Creation Time: 2000-04-14 00:50:01
```

```
Description: N/A
```

```
IPv4 Family:
```

```
Route Distinguisher:
```

```
Apply Label Per Instance: Disable
```

```
Multicast: Disable
```

```
IPv6 Family:
```

```
Route Distinguisher:
```

```
Apply Label Per Instance: Disable
```

```
Switch>
```

12.1.13 show ip vpn-instance config

Function

The **show ip vpn-instance config** command displays VPN instance configuration information.

Format

show ip vpn-instance config

Parameter

NA

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

Display VPN instance configuration information.

```
Switch> show ip vpn-instance config
```

```
ip vpn-instance 1
```

```
description testvpn1
```

```
ip vpn-instance 2
```

```
apply-label per-instance
```

```
Switch>
```

12.1.14 show ip vpn-instance import-vt

Function

The **show ip vpn-instance import-vt** command displays all VPN instances with the specified egress VPN-target attribute.

Format

show ip vpn-instance import-vt *target*

Parameter

Parameter	Description	Value
target	Specifies the egress VPN-target value.	16-bit autonomous system number:32-bit user-defined number, for example, 1:3. The autonomous system number ranges from 0 to 65535. The user-defined number ranges from 0 to 4294967295. The autonomous system number and the user-defined number cannot be 0 simultaneously. That is, the VPN target value cannot be 0:0. 32-bit IP address:16-digit user-defined number, for example, 192.168.122.15:1. The IP address ranges from 0.0.0.0 to 255.255.255.255. The user-defined number ranges from 0 to 65535. 32-bit autonomous system number:16-bit user-defined number, for example, 100.5:1. Generally, the 32-bit automatic system number is in the x.y format, and the value range is 0–65535.0–65535. The user-defined number ranges from 0 to 65535. The autonomous system number and the user-defined number cannot be 0 simultaneously. That is, the VPN target value cannot be 0.0:0.

Default Value

NA

View

Common user view

Usage Guidelines

The value of the target parameter in this command can be in one of the three formats:

IP<X.X.X.X>:NN<0-65535>

It indicates a 32-bit IP address:a 16-bit user-defined number, for example, 10.18.12.15:1. The IP address ranges from 0.0.0.0 to 255.255.255.255. The user-defined number ranges from 0 to 65535.

AS<0-65535>:NN<0-4294967295>

It indicates a 16-bit autonomous system number:a 32-bit user-defined number, for example, 1:5. The autonomous system number ranges from 0 to 65535. The user-defined number ranges from 0 to 4294967295. The autonomous system number and the user-defined number cannot be 0 simultaneously. That is, the VPN target value cannot be 0:0.

AS<0-65535>.<0-65535>:NN<0-65535>

It indicates a 32-bit autonomous system number:a 16-bit user-defined number, for example, 10.2:1. Generally, the 32-bit automatic system number is in the x.y format, and the value range is 0–65535.0–65535. The user-defined number ranges from 0 to 65535. The autonomous system number and the user-defined number cannot be 0 simultaneously. That is, the VPN target value cannot be 0.0:0.

Example

Display all VPN instances with the specified egress VPN-target attribute.

```
Switch>show ip vpn-instance import-vt 100:1
```

The vpn-instances are:

VPN-Instance Name and ID : a, 1

IP Address Family : ipv4

12.1.15 show import-route

Function

The **show import-route** command displays the introduced route information.

Format

- **show import-route { all | imported }**
- **show import-route vpn-instance name { all | imported }**

Parameter

Parameter	Description	Value
name	Specifies a VPN instance name.	The value is a string consisting of up to 64 characters.

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

Display information on all the introduced routes.

Switch>show import-route all

Switch>

12.1.16 route-distinguisher**Function**

The **route-distinguisher** command configures the RD for a VPN instance address family.

The **no route-distinguisher** command deletes the RD configuration of a VPN instance address family.

Format

- **route-distinguisher** *RDSTRING*
- **no route-distinguisher**

Parameter

Parameter	Description	Value
RDSTRING	Specifies a route identifier value (RD for short).	The RD formats are as follows: 2-byte autonomous system number:4-byte user-defined number, for example, 1:3. The autonomous system number ranges from 0 to 65535. The user-defined number ranges from 0 to 4294967295. The AS number and the user-defined number cannot both be 0, which means the value of RD cannot be 0:0. The value is an integer in the format of 4-byte autonomous system number:2-byte user-defined number. The autonomous

Parameter	Description	Value
		system number ranges from 65536 to 4294967295 and the user-defined number ranges from 0 to 65535, for example, 65537:3. The value is dotted in the format of 4-byte autonomous system number:2-byte user-defined number. The dotted automatic system number is in the x.y format, in which x and y range from 0 to 65535, and the user-defined number ranges from 0 to 65535, for example, 0.0:3 or 0.1:0. The AS number and the user-defined number cannot both be 0, which means the value of RD cannot be 0.0:0. 32-bit IP address:a 2-byte user-defined number, for example, 192.168.122.15:1. The IP address ranges from 0.0.0.0 to 255.255.255.255. The user-defined number ranges from 0 to 65535.

Default Value

By default, the RD is not configured for the VPN instance address family.

View

VPN IPv4 address family view and VPN IPv6 address family view

Usage Guidelines

NA

Example

Configure the RD for the VPN instance address family.

```
Switch(config-vpn-instance-af-ipv4)#route-distinguisher 22:1
Switch(config-vpn-instance-af-ipv4)#
```

12.1.17 routing-table limit

Function

The **routing-table limit** command configures the number of limits for a routing table.

Format

routing-table limit { *limit-value* | **default** }

Parameter

Parameter	Description	Value
limit-value	Specifies the number of limits for a routing table.	The value is an integer ranging from 1 to 49152.
default	Specifies the default number of limits.	49152

Default Value

By default, the value is 49152.

View

Ip-vpn-af-ipv4 configuration view and ip-vpn-af-ipv6 configuration view

Usage Guidelines

NA

Example

Configure the number of limits for a routing table.

```
Switch(config-vpn-instance-111)#ipv4-family
Switch(config-vpn-instance-111-af-ipv4)#routing-table limit 15000
S900(config-vpn-instance-111-af-ipv4)#
```

Chapter 13 Data Center Feature Commands

This chapter mainly describes scenarios such as using the VXLAN technology for virtualization and serving the data center.

13.1 VXLAN Configuration Commands

13.1.1 bridge-domain

Function

The **bridge-domain** command creates a bridge domain (BD) and displays its configuration view.

The **no bridge-domain** command deletes a BD.

Format

- **bridge-domain** *bd-id*
- **no bridge-domain** *bd-id*

Parameter

Parameter	Description	Value
bd-id	Specifies a BD ID.	The value is an integer ranging from 1 to 16777215.

Default Value

NA

View

Global configuration view

Usage Guidelines

NA

Example

Create BD 1 and enter its view.

```
Switch(config)#bridge-domain 1
Switch(config-bridge-domain-1)#
```

13.1.2 interface nve

Function

The **interface nve** command creates a network virtualization edge (NVE) interface and displays its configuration view.

The **no interface nve** command deletes an NVE interface.

Format

- **interface nve** *nve-id*
- **no interface nve** *nve-id*

Parameter

Parameter	Description	Value
nve-id	Specifies an NVE ID.	The value is an integer ranging from 1 to 32.

Default Value

NA

View

Global configuration view

Usage Guidelines

NA

Example

Create an NVE interface and enter its configuration view

```
Switch(config)#interface nve 1
Switch(config-nve-1)#
```

13.1.3 interface bridge-domain

Function

The **interface bridge-domain** command creates an L3 BD and displays its configuration view.

Format

interface bridge-domain *bd-id*

Parameter

Parameter	Description	Value

Parameter	Description	Value
bd-id	Specifies an L3 BD ID.	The value is an integer ranging from 1 to 16777215.

Default Value

NA

View

Global configuration view

Usage Guidelines

This command is similar to an L3 VLAN interface and can configure an IP address. Before creating an L3 BD interface, you need to create an L2 BD.

Example

Create L3 BD 1 and enter its view.

```
Switch(config)#bridge-domain 1
Switch(config-bridge-domain-1)#interface bridge-domain 1
```

13.1.4 vni ucast-peer**Function**

The **vni ucast-peer** command configures the VXLAN network identifier (VNI) and the peer IP address for a tunnel.

The **no vni ucast-peer** command deletes the tunnel with the specified VNI and peer IP address.

Format

- **vni** *vni-id* **ucast-peer** *peer-ip-address*
- **vni** *vni-id* **replication-protocol** **bgp**
- **no vni** *vni-id* **ucast-peer** *peer-ip-address*
- **no vni** *vni-id* **peer**
- **no vni** *vni-id* **replication-protocol** **bgp**

Parameter

Parameter	Description	Value
vni-id	Specifies a VNI ID.	The value is an integer ranging from 1 to 16777215.
peer-ip-address	Specifies a peer IP address.	The value is in dotted decimal notation.

peer-ipv6-address	Specifies a peer IPv6.	-
protocol bgp	Specifies that the protocol used to dynamically create a VXLAN tunnel is the BGP routing protocol.	-
out-vni-id	Specifies an out VNI ID.	The value is an integer ranging from 1 to 16777215.

Default Value

NA

View

NVE interface configuration view

Usage Guidelines

NA

Example

Configure and delete tunnel 2.2.2.2 with the specified VNI 1 and IP address on an NVE interface.

```
Switch(config)#interface nve 1
Switch(config-nve-1)#vni 1 ucast-peer 2.2.2.2
Switch(config-nve-1)#no vni 1 ucast-peer 2.2.2.2
Switch(config-nve-1)#
```

13.1.5 tunnel source

Function

The **tunnel source** command configures the source IP address and the IPv6 address of a tunnel.

The **no tunnel source** command deletes the source IP address and the IPv6 address of a tunnel.

Format

- **tunnel source** *ip-address*
- **tunnel source** **vlan** *vlan-id*
- **tunnel source** **loopback** *loopback-number*
- **no tunnel source**

Parameter

Parameter	Description	Value
ip-address	Specifies a source IPv4 address.	The value is in dotted decimal notation.

vlan-id	Specifies a VLAN ID.	The value is an integer ranging from 1 to 4094.
loopback-number	Specifies a loopback interface number.	The value is an integer ranging from 1 to 127.

Default Value

NA

View

NVE interface configuration view

Usage Guidelines

NA

Example

Set the source IP address of a tunnel to 1.1.1.1.

```
Switch(config)#interface nve 1
Switch(config-nve-1)#tunnel source 1.1.1.1
Switch(config-nve-1)#
```

13.1.6 debug vxlan**Function**The **debug vxlan** command enables or disables VXLAN debugging.**Format****debug vxlan { event | detect | did | hw | off | all }****Parameter**

Parameter	Description	Value
event	Debugs the VXLAN event function.	-
detect	Debugs the VXLAN detection function.	-
did	Debugs the DID function.	-
hw	Debugs the hardware function.	-
off	Disables the VXLAN debugging function.	-
all	Displays all VXLAN debugging information.	-

Default Value

NA

View

Privileged user view

Usage Guidelines

NA

Example

Enable debugging of VXLAN events.

```
Switch#debug vxlan event
Switch#
```

13.1.7 show bridge-domain**Function**

The **show bridge-domain** command displays all the configured L2 BD interface information, including a BD interface number, bound VNI, unknown unicast configuration, statistics collection on enabling or disabling, and bound sub-interface.

Format

- **show bridge-domain**
- **show bridge-domain** *bd-id*

Parameter

Parameter	Description	Value
bd-id	Specifies an L3 BD ID.	The value is an integer ranging from 1 to 16777215.

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

Display BD information.

```
Switch>show bridge-domain
```

Interface	Vni	Unknown-ucast	VAP Ports
bd-1	1	forward	xge-1/0/1.1
Switch>			

13.1.8 show vxlan resource

Function

The **show vxlan resource** command displays the VXLAN resource information.

Format

show vxlan resource

Parameter

NA

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

Display information about VXLAN resources.

```
Switch>show vxlan resource
Vxlan resource:
UDP port:4789
Peer detect interval:5
Max number of vni:5
Used number of vni:0
Max number of peer:5
Used number of peer:0
Switch>
```

13.1.9 show nve peer

Function

The **show nve peer** command displays information about all NVE peers or filtered information.

Format

- **show nve peer**
- **show nve peer *ip-address* verbose**
- **show nve peer *ip-address* vni *vni-id* verbose**
- **show nve peer verbose**

Description

Parameter	Description	Value
vni-id	Specifies a VNI ID.	The value is an integer ranging from 1 to 16777215.
ip-address	Specifies a peer IP address.	The value is in dotted decimal notation.

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

Display NVE peer information.

Switch>show nve peer					
Interface	Vni	Peer	Vpid	State	

nve1	1	4.4.4.4	214	up	
Switch>					

13.1.10 show interface nve**Function**The **show interface nve** command displays NVE information on interfaces.**Format****show interface nve****Parameter**

NA

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

Display NVE information on interfaces.

```
Switch>show interface nve
  Interface      SrcIP
  nve1           0.0.0.0
  nve5           0.0.0.0
Switch>
```

13.1.11 show ip arp vxlan**Function**The **show ip arp vxlan** command shows the VXLAN ARP information.**Format****show ip arp vxlan****Parameter**

NA

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

View the VXLAN ARP information.

```
Switch>show ip arp vxlan
```

```
-----
```

Total: 0	Dynamic: 0	Static: 0	Bgp: 0	Other: 0

```
Switch>
```

13.1.12 show vxlan vni

Function

The **show vxlan vni** command displays VNI information.

Format

- **show vxlan vni**
- **show vxlan vni vni-id verbose**

Parameter

Parameter	Description	Value
vni-id	Specifies a VNI ID.	The value is an integer ranging from 1 to 16777215.

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

Display VNI information.

```
Switch>show vxlan vni
```

Vni	BD	NVE	bgp
1	bd1	N/A	disable

```
Switch#
```

13.1.13 vxlan vni

Function

The **vxlan vni** command configures a VNI and binds it to a BD instance.

The **no vxlan vni** command deletes a VNI from a BD instance.

Format

- **vxlan vni** *vni-id*
- **no vxlan vni**

Parameter

Parameter	Description	Value
vni-id	Specifies a VNI ID.	The value is an integer ranging from 1 to 16777215.

Default Value

By default, no VNI is bound to a BD instance.

View

VPN configuration view, BD configuration view

Usage Guidelines

NA

Example

Configure VNI 1 and bind it to a BD instance.

```
Switch(config-bridge-domain-1)#vxlan vni 1
Switch(config-bridge-domain-1)#
```

13.1.14 unknown-ucast {forward|drop}**Function**

The **unknown-ucast { forward|drop }** command configures the switch to forward or drop the unknown unicast packets on a BD interface.

Format

unknown-ucast { forward | drop }

Parameter

Parameter	Description	Value
forward	Forwards unknown unicast packets.	-
drop	Drops unknown unicast packets.	-

Default Value

NA

View

BD configuration view

Usage Guidelines

NA

Example

Configure the switch to forward unknown unicast packets on a BD interface.

```
Switch(config-bridge-domain-1)#unknown-ucast forward
Switch(config-bridge-domain-1)#
```

13.1.15 vxlan anycast-gateway {enable|disable}**Function**

The **vxlan anycast-gateway {enable|disable}** command enables or disables the distributed gateway function.

Format

vxlan anycast-gateway { enable | disable }

Parameter

Parameter	Description	Value
enable	Enables the distributed gateway function.	-
disable	Disables the distributed gateway function.	-

Default Value

Disable

View

BD view

Usage Guidelines

NA

Example

Enable the distributed gateway function.

```
Switch(config)#bridge-domain 1
Switch(config-bridge-domain-1)#quit
Switch(config)#interface bridge-domain 1
```

```
Switch(config-bridge-domain1)#vxlan anycast-gateway enable
Switch(config-bridge-domain1)#
```

13.1.16 show ip bgp evpn route

Function

The **show ip bgp evpn route** command shows the BGP EVPN route information.

Format

- **show ip bgp evpn route**
- **show ip bgp evpn route { mac-ip| prefix | tunnel }**
- **show ip bgp evpn route arp ip-address**
- **show ip bgp evpn route count**
- **show ip bgp evpn route mac mac-address**
- **show ip bgp evpn route nd ipv6-address**
- **show ip bgp evpn route prefix ip-address**
- **show ip bgp evpn route prefix ipv6-address**
- **show ip bgp evpn route tunnel tunnel-source-ip-address tunnel-vni**
- **show ip bgp evpn route { arp | nd } peer peer-ipv4-address l2vni vni-id l3vni vni-id**
- **show ip bgp evpn route { arp | nd } peer peer-ipv6-address l2vni vni-id l3vni vni-id**
- **show ip bgp evpn route { arp | nd | prefix } peer peer-ipv4-address l3vni vni-id**
- **show ip bgp evpn route { arp | nd | prefix } peer peer-ipv6-address l3vni vni-id**
- **show ip bgp evpn route { mac | arp | nd } peer peer-ipv4-address l2vni vni-id**
- **show ip bgp evpn route { mac | arp | nd } peer peer-ipv6-address l2vni vni-id**
- **show ip bgp evpn route { mac | arp | nd | prefix | tunnel } peer peer-ipv4-address**
- **show ip bgp evpn route { mac | arp | nd | prefix | tunnel } peer peer-ipv6-address**

Parameter

Parameter	Description	Value
ip-address	Specifies an IP address in the static ARP entry.	The value is in dotted decimal notation.
mac-address	Specifies route information advertised	The value is in

Parameter	Description	Value
	by the MAC address.	AA:BB:CC:DD:EE:FF format.
ipv6-address	Specifies an IPv6 address.	-
tunnel-source-ip-address	Specifies the source IP address of a tunnel.	The value is in dotted decimal notation.
tunnel-source-ipv6-address	Specifies the source IPv6 address of a tunnel.	-
tunnel-vni	Specifies a tunnel VNI.	The value is an integer ranging from 1 to 16777215.
peer-ipv4-address	Specifies a peer IP address.	The value is in dotted decimal notation.
peer-ipv6-address	Specifies a peer IPv6 address.	-
vni-id	vni id	The value is an integer ranging from 1 to 16777215.

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

View the BGP EVPN route information.

```
Switch>show ip bgp evpn route
Switch#
```

13.1.17 debug ipv6 nd l2-proxy

Function

The **debug ipv6 nd l2-proxy** command enables the debugging function of ND proxy information in a BD.

The **no debug ipv6 nd l2-proxy** command disables the debugging function of ND proxy information in a BD.

Format

- **debug ipv6 nd l2-proxy**

- **no debug ipv6 nd l2-proxy**

Parameter

NA

Default Value

Disable

View

Privileged user view

Usage Guidelines

NA

Example

Enable the debugging function of ND proxy information in a BD.

```
Switch#debug ipv6 nd l2-proxy
Switch#
```

13.1.18 show ipv6 nd l2-proxy

Function

The **show ipv6 nd l2-proxy** command shows the ND proxy information in a BD.

Format

- **show ipv6 nd l2-proxy**
- **show ipv6 nd l2-proxy interface config**

Parameter

NA

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

Show the ND proxy information in a BD.

```
Switch>show ipv6 nd l2-proxy
Switch#
```

13.1.19 reset vxlan statistics peer-ip**Function**

The **reset vxlan statistics peer-ip** command clears the statistics information about VXLAN tunnel packets.

Format

- **reset vxlan statistics peer-ip** *ip-address*
- **reset vxlan statistics peer-ip** *ip-address vpn-instance name*

Parameter

Parameter	Description	Value
ip-address	Specifies the IP address of a remote VTEP.	The value is in dotted decimal notation.
name	Specifies a VPN instance name.	The value is a character string.

Default Value

NA

View

Global configuration view

Usage Guidelines

NA

Example

Clears statistics information about VXLAN tunnel packets.

```
Switch(config)#reset vxlan statistics peer-ip 10.1.1.1
Switch(config)#
```

13.1.20 debug trace vxlan**Function**

The **debug trace vxlan** command enables the debugging function of detecting the VXLAN tunnel connectivity.

The **no debug trace vxlan** command disables the debugging function of the VXLAN tunnel connectivity.

Format

- **debug trace vxlan**
- **no debug trace vxlan**

Parameter

NA

Default Value

Disable

View

Privileged user view

Usage Guidelines

NA

Example

Enable the debugging function of detecting the VXLAN tunnel connectivity.

```
Switch#debug trace vxlan
Switch#
```

13.1.21 ping vxlan vni source peer

Function

The **ping vxlan vni source peer** command detects the VXLAN tunnel connectivity and specifies the VXLAN source IP address.

Format

ping vxlan vni *vni-id* **source** *ip-address* **peer** *peer-ip-address* [*string*]

Parameter

Parameter	Description	Value
vni-id	Specifies a VNI ID.	The value is an integer ranging from 1 to 16777215.

Parameter	Description	Value
ip-address	Specifies a source IP address.	The value is in dotted decimal notation.
peer-ip-address	Specifies a peer IP address.	The value is in dotted decimal notation.
string	Specifies a character string.	-t -n <1-4294967295> -m <1-10000> -w <0-65535> -tos <0-255> -a A.B.C.D udp-port <1-65535> -vpn-instance VPNNAME NAMECR

Default Value

NA

View

Privileged user view

Usage Guidelines

NA

Example

Detect the VXLAN tunnel connectivity and specify the VXLAN source IP address and the peer IP address.

```
Switch#ping vxlan vni 1 source 3.3.3.3 peer 4.4.4.4
VXLAN PING: vni 1 source 3.3.3.3 peer 4.4.4.4 :
  Reply from 4.4.4.4: Sequence=1 time=2ms
  Reply from 4.4.4.4: Sequence=2 time=2ms
  Reply from 4.4.4.4: Sequence=3 time=2ms
  Reply from 4.4.4.4: Sequence=4 time=3ms
  Reply from 4.4.4.4: Sequence=5 time=2ms
VXLAN Ping statistics for 4.4.4.4 :
  5 packets transmitted, 5 packets received, 0% packet loss
  round-trip (ms)   min/avg/max = 0/2/3
```

13.1.22 trace vxlan vni source peer

Function

The **trace vxlan vni source peer** command detects the VXLAN tunnel connectivity and specifies the VXLAN source IP address and the peer IP address.

Format

trace vxlan vni *vni-id* **source** *ip-address* **peer** *peer-ip-address* { **-w** *wati-value* | **-h** *max-ttl* | **-a** *echo-ip-address* | **udp-port** *udpport-number* | *NAMECR* }

Parameter

Parameter	Description	Value
vni-id	Specifies a VNI ID.	The value is an integer ranging from 1 to 16777215.
ip-address	Specifies a source IP address.	The value is in dotted decimal notation.
-w	Specifies a timeout duration for each response.	The value is an integer ranging from 0 to 65535, in milliseconds. The default value is 2000 milliseconds.
-h	Specifies the maximum TTL value.	The value is an integer ranging from 1 to 255.
echo-ip-address	Specifies the source IP address of sending echo requests, which is the default egress interface IP address.	The value is in dotted decimal notation.
udpport-number	Specifies a destination UDP port number.	The value is an integer ranging from 1 to 65535.
NAMECR	Specifies a character string.	The value is a character string.

Default Value

NA

View

Privileged user view

Usage Guidelines

NA

Example

Detect the VXLAN tunnel connectivity and specify the VXLAN source IP address and the peer IP address.

```
Switch#trace vxlan vni 1 source 3.3.3.3 peer 4.4.4.4 -h 125
Tracing vxlan from 3.3.3.3 to 4.4.4.4 maximum : 125 hops.
  1      1 ms      2 ms      2 ms      2 ms      2 ms      13.0.0.1
  2      1 ms      3 ms      2 ms      1 ms      1 ms      4.4.4.4

Trace complete.
```

13.1.23 rewrite egress vid

Function

The **rewrite egress vid** command changes the VLAN tag added during packet decapsulation for the L2 sub-interface with the encapsulation type Dot1q.

The **no rewrite egress vid** command cancels change of the VLAN tag added during packet decapsulation for the L2 sub-interface with the encapsulation type Dot1q.

Format

- **rewrite egress vid** *vlan-id*
- **no rewrite egress vid**

Parameter

Parameter	Description	Value
vlan-id	Specifies the VLAN tag added during packet decapsulation for the L2 sub-interface with the encapsulation type Dot1q.	The value is an integer ranging from 1 to 4094.

Default Value

NA

View

Ethernet sub-interface configuration view and Trunk sub-interface configuration view

Usage Guidelines

NA

Example

Change the VLAN tag added during packet decapsulation for the L2 sub-interface 10GE1/0/1.1 to 20.

```
Switch(config-10ge1/0/1.1)#rewrite egress vid 20
Switch(config-10ge1/0/1.1)#
```

13.1.24 rewrite no-action

Function

The **rewrite no-action** command directly transparently transmits the packets received by the L2 interface with the encapsulation type Dot1q.

The **no rewrite no-action** command cancels direct transparent transmission of the packets received by the L2 interface with the encapsulation type Dot1q.

Format

- **rewrite no-action**

- **no rewrite no-action**

Parameter

NA

Default Value

NA

View

Ethernet sub-interface configuration view and Trunk sub-interface configuration view

Usage Guidelines

NA

Example

Configure the direct transparent transmission of packets received by the L2 interface 10GE1/0/1.1.

```
Switch(config-10ge1/0/1.1)#rewrite no-action
```

```
Switch(config-10ge1/0/1.1)#
```

13.1.25 rewrite pop double

Function

The **rewrite pop double** command directly transparently transmits the packets received by the L2 interface with the encapsulation type Dot1q.

The **no rewrite pop double** command cancels direct transparent transmission of the packets received by the L2 interface with the encapsulation type Dot1q.

Format

- **rewrite pop double**
- **no rewrite pop double**

Parameter

NA

Default Value

NA

View

Ethernet sub-interface configuration view and Trunk sub-interface configuration view

Usage Guidelines

NA

Example

Configure the L2 sub-interface 10GE1/0/1.1 to strip two-level VLAN tags from a received packet.

```
Switch(config-10ge1/0/1.1)#rewrite pop double
Switch(config-10ge1/0/1.1)#
```

13.1.26 debug hwvrf**Function**

The **debug hwvrf** command enables the Hwvrf debugging function.

The **no debug hwvrf** command disables the Hwvrf debugging function.

Format

- **debug hwvrf**
- **no debug hwvrf**

Parameter

NA

Default Value

NA

View

Privileged user view

Usage Guidelines

NA

Example

Enable the Hwvrf debugging function.

```
Switch#debug hwvrf
Switch#
```

13.1.27 debug grpc**Function**

The **debug grpc** command enables or disables the GRPC log.

Format

```
debug grpc { api | cares_address_sorting | cares_resolver | client_channel_call |
client_channel_routing | http | http_keepalive | chhttp2_refcount | channel | combiner | tcp |
polling | fd_trace | fd_refcount | polling_api | executor | timer | timer_check|op_failure |
pending_tags | cq_refcount | queue_pluck | connectivity_state | resource_quota | all } { on | off }
```

Parameter

Parameter	Description	Value
api	Debugs API call information.	-
cares_address_sorting	Debugs cares address parsing information.	-
cares_resolver	Debugs cares parsing information.	-
client_channel_call	Debugs client channel call information.	-
client_channel_routing	Debugs client channel routing information.	-
http	Debugs HTTP information.	-
http_keepalive	Debugs HTTP keepalive information.	-
chhttp2_refcount	Debugs HTTP reference count information.	-
channel	Debugs channel information.	-
combiner	Debugs adapter information.	-
tcp	Debugs TCP information.	-
polling	Debugs polling information.	-
fd_trace	Debugs socket information.	-
fd_refcount	Debugs socket reference count information.	-
polling_api	Debugs polling API call information.	-
executor	Debugs executor information.	-
timer	Debugs timer information.	-
timer_check	Debugs timer check information.	-
op_failure	Debugs operation failure information.	-
pending_tags	Debugs tag information.	-
cq_refcount	Debugs completed queue reference count information.	-
queue_pluck	Debugs queue pluck information.	-
connectivity_state	Debugs connection state information.	-
resource_quota	Debugs resource reference information.	-
all	Debugs all logs.	-
on	Indicates enabling.	-
off	Indicates disabling.	-

Default Value

NA

View

Privileged user view, global configuration view

Usage Guidelines

NA

Example

Enable the GRPC log.

```
Switch(config)# debug grpc all on

I1213 03:21:39.284012072    1372 timer_manager.cc:204]    wait ended: was_timed:1 kicked:0

I1213 03:21:39.284118529    1372 timer_generic.cc:717]    TIMER CHECK BEGIN: now=199894
next=9223372036854775807 tls_min=199210 glob_min=199894

I1213 03:21:39.284132982    1372 timer_generic.cc:612]    .. shard[0]->min_deadline = 199894

I1213 03:21:39.284141270    1372 timer_generic.cc:535]    .. shard[0]: heap_empty=true

I1213 03:21:39.284148692    1372 timer_generic.cc:510]    .. shard[0]->queue_deadline_cap -->
200703

I1213 03:21:39.284155926    1372 timer_generic.cc:575]    .. shard[0] popped 0

I1213 03:21:39.284163612    1372 timer_generic.cc:630]    .. result --> 1, shard[0]->min_deadline
199894 --> 200704, now=199894

I1213 03:21:39.284212300    1372 timer_generic.cc:740]    TIMER CHECK END: r=1; next=200037

I1213 03:21:39.284221002    1372 timer_manager.cc:188]    sleep for a 143 milliseconds

I1213 03:21:39.427068426    1372 timer_manager.cc:204]    wait ended: was_timed:1 kicked:0

I1213 03:21:39.427202096    1372 timer_generic.cc:717]    TIMER CHECK BEGIN: now=200037
next=9223372036854775807 tls_min=199894 glob_min=200037

I1213 03:21:39.427228026    1372 timer_generic.cc:612]    .. shard[3]->min_deadline = 200037

I1213 03:21:39.427247192    1372 timer_generic.cc:535]    .. shard[3]: heap_empty=true

I1213 03:21:39.427265776    1372 timer_generic.cc:510]    .. shard[3]->queue_deadline_cap -->
201036

I1213 03:21:39.427283672    1372 timer_generic.cc:575]    .. shard[3] popped 0
```

13.1.28 grpc debug-level**Function**

The **grpc debug-level { debug|info|error|none }** command sets the GRPC debugging level.

Format

grpc debug-level { debug | info | error | none }

Parameter

Parameter	Description	Value
debug	Debugs debugging information.	NA
info	Debugs prompt information.	NA
error	Debugs error information.	NA
none	Indicates no information.	NA

Default Value

NA

View

Global configuration view

Usage Guidelines

Set different debugging levels based on your needs.

Example

Set the GRPC debugging level.

```
Switch(config)#grpc debug-level debug
Switch(config)#
```

13.1.29 show mac-limit bridge-domain

Function

The **show mac-limit bridge-domain** command shows the configuration information on MAC address learning restrictions in all BDs or a specified BD.

Format

- **show mac-limit bridge-domain**
- **show mac-limit bridge-domain *bd-id***

Parameter

Parameter	Description	Value
bd-id	Specifies a BD ID.	The value is an integer ranging from 1 to

Parameter	Description	Value
		16777215.

Default Value

NA

View

Common user view

Usage Guidelines

After the dynamic MAC address learning rule is successfully configured, you can run this command to view the configuration result and check whether the configuration is correct, and troubleshoot carefully.

If a large number of BDs exist on the device, run this command to specify a BD to filter the display information.

Example

View the configuration information on MAC address learning restrictions in a specified BD.

```
Switch>show mac-limit bridge-domain 10
bridge-domain 10 MAC LIMIT:
Maximum MAC count: 300, used count: 0;
Action: drop, Alarm: disable.
Switch>
```

13.1.30 arp l2-proxy active-active gateway {enable|disable}

Function

The **arp l2-proxy active-active gateway {enable|disable}** command enables or disables the ARP learning function for active-active gateways.

Format

arp l2-proxy active-active gateway { enable | disable }

Parameter

Parameter	Description	Value
enable	Enables the ARP learning function for active-active gateways.	-
disable	Disables the ARP learning function for active-active gateways.	-

Default Value

Disable

View

BD configuration view

Usage Guidelines

To ensure the reliability in the VXLAN network, multiple gateways are deployed. However, in the traditional solution, multiple gateways work in active-standby mode. Only the active gateway can forward traffic, resulting in low gateway utilization. The VXLAN active-active gateway can solve the problem of low gateway utilization.

Example

Enable the ARP learning function for active-active gateways.

```
Switch(config-bridge-domain-10)#arp l2-proxy active-active gateway enable
Switch(config-bridge-domain-10)#
```

13.1.31 ipv6 nd l2-proxy active-active gateway {enable|disable}

Function

The **ipv6 nd l2-proxy active-active gateway {enable|disable}** command enables or disables the ND learning function for active-active gateways.

Format

ipv6 nd l2-proxy active-active gateway { enable | disable }

Parameter

Parameter	Description	Value
enable	Enables the ND learning function for active-active gateways.	-
disable	Disables the ND learning function for active-active gateways.	-

Default Value

Disable

View

BD configuration view

Usage Guidelines

To ensure the reliability in the VXLAN network, multiple gateways are deployed. However, in the traditional solution, multiple gateways work in active-standby mode. Only the active gateway can

forward traffic, resulting in low gateway utilization. The VXLAN active-active gateway can solve the problem of low gateway utilization.

Example

Enable the ND learning function for active-active gateways.

```
Switch(config-bridge-domain-10)#ipv6 nd l2-proxy active-active gateway enable
Switch(config-bridge-domain-10)#
```

13.2 EVPN Configuration Commands

13.2.1 debug evpn

Function

The **debug evpn** command enables or disables the EVPN debugging function.

Format

debug evpn { **error** | **nm** | **event** | **all** }

Parameter

Parameter	Description	Value
error	Specifies a debug switch for event processing.	-
nm	Specifies a debug switch for gateway configuration.	-
event	Specifies a debug switch for error prompt.	-
all	Enables all debug switches.	-

Default Value

NA

View

Privileged user view

Usage Guidelines

NA

Example

Enable the switch for debugging the EVPN event function.

```
Switch#debug evpn event
Switch#
```

13.2.2 evpn

Function

The **evpn** command creates a VXLAN-mode EVPN instance.

The **no evpn** command deletes a VXLAN-mode EVPN instance.

Format

evpn

no evpn

Default Value

NA

View

BD configuration view

Usage Guidelines

NA

Example

Create a VXLAN-mode EVPN instance.

```
Switch(config)#bridge-domain 2
Switch(config-bridge-domain-2)#evpn
Switch(config-bridge-domain-2)#
```

13.2.3 evpn-family

Function

The **evpn-family** command enters the BGP-EVPN address family view.

Format

evpn-family

Default Value

NA

View

BGP configuration view

Usage Guidelines

NA

Example

Enter the BGP-EVPN address family view.

```
Switch(config-bgp)#evpn-family
Switch(config-bgp-af-evpn)#
```

13.2.4 evpn route-distinguisher**Function**

The **evpn route-distinguisher** command configures an RD for the EVPN instance in a BD view.

Format

evpn route-distinguisher *RDSTRING*

Parameter

Parameter	Description	Value
RDSTRING	Specifies a route identifier value (RD for short).	The RD formats are as follows: 2-byte autonomous system number:4-byte user-defined number, for example, 1:3. The autonomous system number ranges from 0 to 65535. The user-defined number ranges from 0 to 4294967295. The AS number and the user-defined number cannot both be 0, which means the value of RD cannot be 0:0. The value is an integer in the format of 4-byte autonomous system number:2-byte user-defined number. The autonomous system number ranges from 65536 to 4294967295 and the user-defined number ranges from 0 to 65535, for example, 65537:3. The value is dotted in the format of 4-byte autonomous system number:2-byte user-defined number. The dotted automatic system number is in the x.y format, in which x and y range from 0 to 65535, and the user-defined number ranges from 0 to 65535, for example, 0.0:3 or 0.1:0. The AS number and the user-defined number cannot both be 0, which means the value of RD cannot be 0.0:0.

Parameter	Description	Value
		32-bit IP address:a 2-byte user-defined number, for example, 192.168.122.15:1. The IP address ranges from 0.0.0.0 to 255.255.255.255. The user-defined number ranges from 0 to 65535.

Default Value

By default, no RD is configured for the EVPN instance in the BD view.

View

BD configuration view

Usage Guidelines

NA

Example

Configure an RD for the EVPN instance in a BD view.

```
Switch(config)#bridge-domain 2
Switch(config-bridge-domain-2)#evpn route-distinguisher 1:1
Switch(config-bridge-domain-2)#
```

13.2.5 evpn vpn-target

Function

The **evpn vpn-target** command configures the vpn-target extended community attribute for the EVPN instance in a BD view.

The **no evpn vpn-target** command deletes the vpn-target extended community attribute of the EVPN instance in a BD view.

Format

- **evpn vpn-target** *TARGET* {**both**|**export-extcommunity**|**import-extcommunity**}
- **no evpn vpn-target** *TARGET* { **both**|**export-extcommunity**|**import-extcommunity**}
- **no evpn vpn-target**

Parameter

Parameter	Description	Value

Parameter	Description	Value
TARGET	Adds the specified vpn-target attribute to the vpn-target extended community attribute list of the EVPN instance address family in a BD view.	The vpn-target attribute can be in the following formats: 2-byte autonomous system number:4-byte user-defined number, for example, 1:3. The autonomous system number ranges from 0 to 65535. The user-defined number ranges from 0 to 4294967295. The autonomous system number and the user-defined number cannot be 0 at the same time, indicating that the value of the vpn-target attribute cannot be 0:0. The value is an integer in the format of 4-byte autonomous system number:2-byte user-defined number. The autonomous system number ranges from 65536 to 4294967295 and the user-defined number ranges from 0 to 65535, for example, 65537:3. The value is dotted in the format of 4-byte autonomous system number:2-byte user-defined number. The dotted automatic system number is in the x.y format, in which x and y range from 0 to 65535, and the user-defined number ranges from 0 to 65535, for example, 0.0:3 or 0.1:0. The autonomous system number and the user-defined number cannot be 0 simultaneously. That is, the VPN target value cannot be 0.0:0. 32-bit IP address:a 2-byte user-defined number, for example, 192.168.122.15:1. The IP address ranges from 0.0.0.0 to 255.255.255.255. The user-defined number ranges from 0 to 65535.
both	Adds the specified vpn-target attribute to the vpn-target extended community attribute list in the egress and ingress directions of the EVPN instance address family in a BD view.	-

Parameter	Description	Value
export-extcommunity	Adds the specified vpn-target attribute to the vpn-target extended community attribute list in the egress direction of the EVPN instance address family in a BD view.	-
import-extcommunity	Adds the specified vpn-target attribute to the vpn-target extended community attribute list in the ingress direction of the EVPN instance address family in a BD view.	-

Default Value

NA

View

BD configuration view

Usage Guidelines

NA

Example

Configure the vpn-target extended community attribute for the EVPN instance in a BD view.

```
Switch(config)#bridge-domain 2
Switch(config-bridge-domain-2)#evpn vpn-target 1:1 import-extcommunity
Switch(config-bridge-domain-2)#
```

13.2.6 neighbor enable**Function**

The **neighbor enable** command enables the EVPN address family function of the BGP neighbor.

Format

neighbor *ipv4 address* **enable**

Parameter

Parameter	Description	Value
ipv4 address	Specifies the IPv4 address of a BGP neighbor.	The value is in dotted decimal notation.

Default Value

EVPN is disabled.

View

BGP-EVPN address family configuration view

Usage Guidelines

NA

Example

Enable the EVPN address family function of the BGP neighbor.

```
Switch (config-bgp-af-evpn)#neighbor 2.2.2.2 enable
Switch (config-bgp-af-evpn)#
```

13.2.7 vni replication-protocol**Function**

The **vni replication-protocol** command configures the inbound replication protocol of the specified VNI on the NVE interface.

Format

vni *vni-id* **replication-protocol** **bgp**

Parameter

Parameter	Description	Value
vni-id	Specifies a VNI ID.	The value is an integer ranging from 1 to 16777215.
bgp	Specifies that the NVE interface tunnel is created by the BGP protocol.	-

Default Value

NA

View

NVE configuration view

Usage Guidelines

NA

Example

Configure the inbound replication protocol of the specified VNI on the NVE interface.

```
Switch(config-nve-1)#vni 10 replication-protocol bgp
Switch(config-nve-1)#
```

13.2.8 vxlan vni

Function

The **vxlan vni** command binds a VNI to a VPN instance.

Format

- **vxlan vni** *vni-id*

Parameter

Parameter	Description	Value
vni-id	Specifies a VNI ID.	The value is an integer ranging from 1 to 16777215.

Default Value

NA

View

VPN configuration view

Usage Guidelines

NA

Example

Bind a VNI to a VPN instance.

```
Switch(config)#ip vpn-instance 111
Switch(config-vpn-instance-111)#vxlan vni 1
```

13.2.9 show evpn

Function

The **show evpn** displays EVPN-related information.

Format

- **show evpn**
- **show evpn bridge-domain** *bd-id*

Parameter

Parameter	Description	Value
<i>bd-id</i>	Specifies the ID of a bridge domain.	The value is an integer ranging from 1 to 16777215.

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

Display EVPN-related information.

```
Switch(config)# show evpn
BD          IfUnit      RD
-----
1           bd1         3:1
```

13.2.10 show evpn vpn-target**Function**The **show evpn vpn-target** command displays information related to EVPN vpn-target.**Format****show evpn vpn-target****Parameter**

NA

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

Display information related to EVPN vpn-target.

Switch(config)# show evpn vpn-target			
BD	IfUnit	VPN-TARGET	Type
1	bd1	1:1	import-extcommunity
1	bd1	1:1	export-extcommunity

13.3 NETCONF Configuration Commands

13.3.1 netconf {enable|disable}

FunctionThe **netconf {enable|disable}** command enables or disables the NETCONF protocol.**Format****netconf { enable | disable }****Parameter**

Parameter	Description	Value
enable	Enables the NETCONF protocol.	-
disable	Disables the NETCONF protocol.	-

Default Value

Disable

View

Global configuration view

Usage Guidelines

Enable the NETCONF protocol before initiating a NETCONF connection.

Example

Enable the NETCONF protocol.

Switch(config)#netconf enable
Switch(config)#

13.3.2 netconf log {none|terminal|file}

Function

The **netconf log {none|terminal|file}** command configures the NETCONF log output terminal.

Format

netconf log { none | terminal | file }

Parameter

Parameter	Description	Value
none	NA	-
terminal	Specifies the log output to a serial port.	-
file	Specifies the log output to a file.	-

Default Value

NA

View

Global configuration view

Usage Guidelines

NA

Example

Configure the NETCONF log output to a serial port.

```
Switch(config)#netconf log terminal
Switch(config)#
```

13.3.3 netconf debug-level {none|off|error|warn|info|debug|debug2|debug3|debug4}

Function

The **netconf debug-level {none|off|error|warn|info|debug|debug2|debug3|debug4}** command configures the NETCONF log output level.

Format

netconf debug-level { none | off | error | warn | info | debug | debug2 | debug3 | debug4 }

Parameter

Parameter	Description	Value

Parameter	Description	Value
none	NA	-
off	Disable	-
error	Error	-
warn	Alarms	-
info	Information	-
debug	Debug	-
debug2	Debug 2	-
debug3	Debug 3	-
debug4	Debug 4	-

Default Value

NA

View

Global configuration view

Usage Guidelines

NA

Example

Configure the NETCONF log level to debug4.

```
Switch(config)#netconf debug-level debug4
Switch(config)#
```

13.3.4 netconf log-per-size**Function**The **netconf log-per-size** command configures the size of a single NETCONF log file.**Format****netconf log-per-size** *log-per-size***Parameter**

Parameter	Description	Value
log-per-size	Specifies the size of a single log file.	The value is an integer ranging from 1 to 100, in MBs.

Default Value

NA

View

Global configuration view

Usage Guidelines

NA

Example

Configure the size of a single NETCONF log file to 10 MB.

```
Switch(config)#netconf log-per-size 10
Switch(config)#
```

13.3.5 clear netconf candidate database

Function

The **clear netconf candidate database** command clears the NETCONF candidate database.

Format

clear netconf candidate database

Parameter

NA

Default Value

NA

View

Global configuration view

Usage Guidelines

When the candidate database is blocked by incorrect configurations, subsequent correct configurations cannot be delivered. Then, you need to clear incorrect configurations from the candidate database. You can run the discard-changes command to clear the candidate database by using a controller, or configure the command line to clear the database.

Example

Clear configurations from the candidate database.

```
Switch(config)#clear netconf candidate database
```

```
Switch(config)#
```

13.3.6 show netconf candidate database

Function

The **show netconf candidate database** command shows the NETCONF candidate database.

Format

show netconf candidate database

Parameter

NA

Default Value

NA

View

Common user view

Usage Guidelines

View the candidate database content, which gives some indication to the operator.

Example

View configurations in the candidate database.

```
Switch>show netconf candidate database

nc:config container container none {
  bdif:bdif container container merge {
    bdif:bdIfTable container container merge {
      bdif:bdIfEntry list list merge 8 {
        bdif:bdIfIndex leaf int32 merge 8
        bdif:bdIfVxlanVni leaf int32 merge 200
      }
    }
  }
}
```

13.3.7 show netconf

Function

The **show netconf** command shows NETCONF basic configurations.

Format

show netconf**Parameter**

NA

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

View NETCONF basic configurations.

```

Switch>show netconf
      debug-level           : 6
      log-per-size          : 10M
      log-out-put           : file
      timeout-thread-kill   : false
      inmsg-timeout         : 60
      max-support-sessions  : 4
      mem-threshold         : 0
      active-sessions       : 1
      closed-sessions       : 0
      failed-sessions       : 0
      in-bad-hellos         : 0
      in-sessions           : 1
      dropped-sessions      : 0

```

Switch>

13.3.8 show netconf sessions**Function**The **show netconf sessions** command shows NETCONF session information.**Format**

- **show netconf sessions**
- **show netconf session** *session-id*

Parameter

Parameter	Description	Value
session-id	Specifies a session ID.	The value is an integer ranging from 1 to 1024.

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

View the NETCONF session information.

```
Switch>show netconf sessions
  session-id  protocol    transport  state    fd    username  peeraddr
  1           netconf 1.1 ssh      idle     19     admin     172.18.1.80
Switch>
```

13.3.9 show netconf session statistics**Function**The **show netconf session statistics** command shows NETCONF session statistics information.**Format**

- **show netconf session statistics**
- **show netconf session *session-id* statistics**

Parameter

Parameter	Description	Value
session-id	Specifies a session ID.	The value is an integer ranging from 1 to 1024.

Default Value

NA

View

Common user view

Usage Guidelines

NA

Example

View the NETCONF session statistics information.

```
Switch>show netconf session statistics
```

session-id	in-bytes	out-bytes	in-rpcs	in-bad-rpcs	out-rpc-errors	out-notifications
1	1015	7275	1	0	0	0

```
Switch>
```

Chapter 14 Virtualization Configuration Commands

This chapter introduces how to configure stack commands.

14.1 Stack Command Configuration

14.1.1 iss mode

Function

The **iss mode** command sets the running mode of the switch.

Format

iss mode {independence | iss}

Parameter

Parameter	Description	Value
independence	Indicates the standalone running mode.	-
iss	Indicates the stack mode.	-

Default Value

independence

View

Global configuration view

Usage Guidelines

This configuration requires a reboot to take effect. The member number is 1 by default.

If the current mode is the same as the configured mode, this command will not be executed.

To switch to the stack mode, after that mode is successfully configured, the system will automatically save the stack and system configuration files and reboot.

To switch to the standalone mode, after that mode is successfully configured, the system will automatically clear the stack and system configurations and reboot.

Example

```
Switch(config) #iss mode iss
```



```

After configure the mode , the device will reboot auto and make sure the config
take effect!
Are you sure?(Y/N) [N] : y
beginning configure iss mode, please wait for a moment.....
Configure iss mode succeeded!
Now rebooting, please wait.....

```

14.1.2 iss domain

Function

The **iss domain** command sets a stack domain ID.

Format

iss domain<1-8>

Parameter

Parameter	Description	Value
Specifies a stack domain ID.	NA	The value is an integer ranging from 1 to 8.

Default Value

1

View

Global configuration view

Usage Guidelines

This command, if modified, takes effect immediately in stack mode. Only switches with the same stack domain ID can negotiate stacking.

Example

```
Switch(config)# iss domain 1
```

14.1.3 iss member

Function

The **iss member** command sets the stack member number of the switch.

Format

iss member <1-2>

Parameter

Parameter	Description	Value
Stack member ID	NA	The value is an integer ranging from 1 to 4.

Default Value

1

View

Global configuration view

Usage Guidelines

You must configure a stack member number for a switch before switching it from standalone mode to stack mode.

If the switch is in stack mode, the stack member number, after being configured, takes effect only after a reboot. If that switch is in standalone mode, you have to switch to the stack mode to make the setting effective.

Example

```
Switch(config)#iss member 1
Succesed to configure iss member, it will not be actived until the
configuration saved and rebooted!
```

14.1.4 iss priority**Function**

The **iss priority** command sets the stack priority of the switch.

Format**iss priority****Parameter**

Parameter	Description	Value
Stack member priority	NA	The value is an integer ranging from 1 to 8.

Default Value

1

View

Global configuration view

Usage Guidelines

A higher stack priority value increases the probability of the stack member being elected master switch.

If the switch is in stack mode, the stack priority, after being configured, takes effect immediately. If that switch is in standalone mode, you have to switch to the stack mode to make the setting effective.

During stack negotiation, stack master and member elections are compared based on the switch's current stack role, whether master is specified, stack priority, stack runtime, and stack MAC address. The rules for role election are as follows:

- The current master switch has higher probability of being elected than the non-master members.
- The specified master member takes precedence.
- The switch with the highest member priority takes precedence.
- The switch with longer system uptime takes precedence.
- The switch with a smaller MAC address takes precedence.

Example

```
Switch(config)#iss priority 2
Now, it is independence mode, it will not be activated until the mode convert to
iss!
```

14.1.5 iss master

Function

The **iss master** command specifies a stack master.

Format

[no] iss master

Parameter

NA

Default Value

Non-specified master

View

Global configuration view

Usage Guidelines

This command, if modified, takes effect immediately in stack mode.

Example

```
Switch(config) #iss master
Switch(config) #
```

14.1.6 iss hello-interval

Function

The **iss hello-interval** command sets the interval for sending hello messages.

Format

iss hello-interval <1-10|default>

Parameter

Parameter	Description	Value
1-10	NA	The value is an integer ranging from 1 to 10, in seconds.

Default Value

4

View

Global configuration view

Usage Guidelines

This command, if modified, takes effect immediately in stack mode. The two stacked switches should use the same interval for sending hello messages.

Example

```
Switch(config) #iss hello-interval 5
Switch(config) #
```

14.1.7 interface stack-port

Function

The **interface stack-port** command creates a stack port and enters the stack port view.

Format

Interface stack-port 1

Parameter

NA

Default Value

By default, no stack port is created.

View

Global configuration view

Usage Guidelines

This command is edited in standalone mode and takes effect in stack mode.

Example

```
Switch(config) #interface stack-port 1
```

14.1.8 join stack-port**Function**The **join stack-port** command enables the current port to join or exit from a stacked port.**Format****[no]join stack-port 1****Parameter**

NA

Default Value

A port does not join the stack port by default.

View

Ethernet interface configuration view

Usage Guidelines

This command is edited in standalone mode and takes effect in stack mode.

Example

```
Switch(config) #(config-10ge1/0/2)#join stack-port 1
%Join stack-port1 successfully.
```

14.1.9 erase iss-config

Function

The **erase iss-config** command erases the stack configurations.

Format

erase iss-config

Parameter

NA

Default Value

NA

View

Global configuration view

Usage Guidelines

After erasing the stack configuration files, you need to reboot the switch to restore it to standalone mode.

Example

```
Switch(config) #erase iss-config
This will erase the configuration in the flash memory.
Are you sure?(y/n) [y]y
Erasing configuration.....
[OK]
Switch(config) #
```

14.1.10 show iss-config

Function

The **show iss-config** command shows the stack configurations.

Format

show iss-config

Parameter

NA

Default Value

NA

View

Global configuration view

Usage Guidelines

This command shows the stack configurations of a switch.

Example

```
Switch(config) #show iss-config
!
interface stack-port 2/1
!
interface 10gigaethernet 2/1/0/2
join stack-port 2/1
no shutdown
```

14.1.11 show iss interface

Function

The **show iss interface** command displays table entries of stack-enabled interfaces.

Format

show iss interface

Parameter

NA

Default Value

NA

View

Global configuration view

Usage Guidelines

This command shows states of the stacked ports and statistics of their Tx/Rx packets.

Example

```
Switch(config)#show iss interface
stack-port 1/1 (remote):
Link State : up
```

```

Port-List : 10gigaethernet1/1/0/1
stack-port 2/1 (local):
Link State : up
Port-List : 10gigaethernet2/1/0/2
Port Statistics :
Last KA TX time ago(s): 1 Last KA RX time ago(s): 0
TX KA Packets: 827 TX KA ERR Packets: 14
RX KA Packets: 811 RX KA ERR Packets: 7
TX HELLO Packets: 636 TX HELLO ERR Packets: 0
RX HELLO Packets: 596 RX HELLO ERR Packets: 0
TX SYSINFO Packets: 59 TX SYSINFO ERR Packets: 0
RX SYSINFO Packets: 58 RX SYSINFO ERR Packets: 0

```

14.1.12 show iss topo

Function

The **show iss topo** command displays topology information of stacked switches.

Format

show iss topo

Parameter

NA

Default Value

NA

View

Global configuration view

Usage Guidelines

This command shows topology information of a stack, including hop count, member ID, state and MAC address.

Example

```

Switch(config)#show iss topo
Interface: stack-port2/1, State: up, MAC: 00:04:67:00:00:10
Hop MemberId Port0 State MAC Port1 State MAC
0 2 1 up 00:04:67:00:00:10 0 down 00:00:00:00:00:00 1 1 0 down 00:00:00:00:00:00 1 up 00:04:67:00:00:20

```


14.1.13 show iss topo stack-port

Function

The **show iss topo stack-port** command displays topology information of a specified interface.

Format

show iss topo interface stack-port 1

Parameter

NA

Default Value

NA

View

Global configuration view

Usage Guidelines

Global configuration view, privileged user view, interface configuration view

Four-dimensional physical interfaces apply to switches running in stack mode; otherwise, three-dimensional interfaces are used.

This command displays basic interface information (interface, link state, and MAC address) and then the topology information (member ID, status, and MAC address) learned by the interface.

This command shows stack topology information of a specified interface.

Example

```
Switch(config)#show iss topo interface stack-port 2/1
Interface: stack-port2/1, State: up, MAC: 00:04:67:00:00:10
Hop MemberId Port0 State MAC Port1 State MAC
0 2 1 up 00:04:67:00:00:10 0 down 00:00:00:00:00:00
1 1 0 down 00:00:00:00:00:00 1 up 00:04:67:00:00:20
```

14.1.14 show iss topo stack-port hops

Function

The **show iss topo stack-port hops** command displays topology information of a specified interface with certain hops.

Format

show iss topo interface stack-port 1 hops**Parameter**

NA

Default Value

NA

View

Global configuration view

Usage Guidelines

This command shows stack topology information for a specified interface with certain hops.

Example

```
Switch(config)#show iss topo interface stack-port 2/1 hops 0
Hop MemberId Port0 State MAC Port1 State MAC
0 2 1 up 00:04:67:00:00:10 0 down 00:00:00:00:00:00
```

14.1.15 show iss member**Function**

The **show iss member** command displays table entries of stack members.

Format**show iss member****Parameter**

NA

Default Value

NA

View

Global configuration view

Usage Guidelines

This command shows information of stack members, including member role, negotiation state, specified master role, priority, runtime, member MAC address, eastbound/westbound port protocol state, and eastbound/westbound port MAC address.

A member ID preceded by an asterisk (*) denotes the switch itself.

Example

```
Switch(config)#show iss member
MemId MemRole MemState ConfRole Priority RunTime(s) MemMac Port0
Port0Mac Port1 Port1Mac
1 master done no 2 8756544 00:04:67:00:00:20 down
00:00:00:00:00:00 up 00:04:67:00:00:20
(*)2 slave done no 1 8756544 00:04:67:00:00:10 up
00:04:67:00:00:10 down 00:00:00:00:00:00
```

14.1.16 show iss

Function

The **show iss** command displays stack information of the switch.

Format

show iss

Parameter

NA

Default Value

NA

View

Global configuration view

Usage Guidelines

This command shows stack information, including the stack enable state, stack domain ID, member role, member number, priority, member MAC address, stack system state and runtime.

Example

```
Switch(config)#show iss
Version : ISS_VB3.00.03.00
RunMode : iss
DomainId : 1
MemberCount : 8
Version : 1
TopoComplete : yes
IsRing : no
```

```

CurrentMasterId : 1
NextMemberId : 2
HelloInterval : 4 s
MacSwitchDelay : N/A
PrevMasterId : 0
PrevMasterMac : 00:00:00:00:00:00
SystemRunMac : 00:04:67:00:00:20
SystemState : up
UpTime(s) : 3059
LastSplitTimeAgo(s) : 0
MemberState : done
stackRole : Slave

```

14.1.17 debug iss/no debug iss

Function

The **debug iss/no debug iss** command enables or disables iss debugging.

Format

- **debug iss{in|out|timer|link-change|conflict|election|all}**
- **no debug iss {in|out|timer|link-change|conflict|election|all}**

Parameter

Parameter	Description	Value
in	Received packets	-
out	Transmitted packets	-
timer	Timer	-
link-change	Link state change	-
conflict	Conflict	-
election	Selector	-
all	All of the above	-

Default Value

NA

View

Global configuration view

Usage Guidelines

This command enables or disables diagnostics on stack protocols.

Example

```
Switch(config)#debug iss all
Switch(config)#
```

14.1.18 mad detect

Function

The **mad detect** command enables or disables multi-active detection (MAD) for out-of-band ports.

Format

mad detect { enable|disable }

Parameter

Parameter	Description	Value
enable	Enables MAD for out-of-band ports.	-
disable	Disables MAD for out-of-band ports.	-

Default Value

NA

View

Out-of-band interface configuration view

Usage Guidelines

NA

Example

Enable MAD for out-of-band ports.

```
Switch(config-eth0/0/0)#mad detect enable
Switch(config-eth0/0/0)#
```

14.1.19 mad restore

Function

The **mad restore** command recovers a port from disabled state.

Format

mad restore

Parameter

NA

Default Value

NA

View

Privileged user view, global configuration view, interface configuration view (Ethernet interface, Trunk interface), interface group configuration view

Usage Guidelines

NA

Example

Recover a port from disabled state due to multi-active conflict.

```
Switch(config-eth-trunk-1)#mad restore
WARNING: This command will restore the device from multi-active conflict
state. Continue?
[Y/N]y
```

14.1.20 mad detect mode direct**Function**

The **mad detect mode direct** command sets MAD in direct mode on a physical interface.

Format

mad detect mode direct

Parameter

NA

Default Value

NA

View

Interface configuration view (Ethernet interface)

Usage Guidelines

NA

Example

Set MAD in direct mode on a physical interface.

```
Switch(config-xge1/0/34)#mad detect mode direct
WARNING:The interface will block common data packets, except BPDU packets.
Continue?
[Y/N]y
```

14.1.21 no mad detect

Function

The **no mad detect** command disables MAD in relay mode and disables MAD in direct mode for an interface respectively.

Format

no mad detect

Parameter

NA

Default Value

NA

View

Interface configuration view (Ethernet interface, Trunk Interface)

Usage Guidelines

In Trunk interface configuration view, this command disables the MAD in relay mode.

In Ethernet interface configuration view, this command disables MAD in direct mode.

Example

Disable MAD in relay mode for a Trunk interface.

```
Switch(config-eth-trunk-2)#no mad detect
Switch(config-eth-trunk-2)#
```

14.1.22 mad exclude { enable | disable }

Function

The **mad exclude { enable | disable }** command enables or disables excluded ports for MAD.

Format

mad exclude { enable | disable}**Parameter**

Parameter	Description	Value
enable	Enables excluded ports for MAD.	-
disable	Disables excluded ports for MAD.	-

Default Value

Disable

View

Interface configuration view (Ethernet interface)

Usage Guidelines

NA

Example

Enable a specified interface to act as an excluded port for MAD.

```
Switch(config-xge1/0/34)#mad exclude enable
Switch(config-xge1/0/34)#
```

14.1.23 mad backup ip address**Function**

The **mad backup ip address** command sets a backup IP address of the out-of-band port on an MAD member switch.

The **no mad backup ip address** command deletes the backup IP address of the out-of-band port on an MAD member switch.

Format

- **mad backup ip address ip-address mask-address { member | all }**
- **no mad backup ip address ip-address mask-address { member | all }**

Parameter

Parameter	Description	Value
ip-address	Backup IP address of an out-of-band port	The value is in dotted decimal notation.
mask-address	Backup mask address of an out-of-band port	The value is in dotted decimal notation.
member	MAD member	The value is an integer ranging from 1

Parameter	Description	Value
		to 4.
all	All MAD members	-

Default Value

NA

View

Global configuration view

Usage Guidelines

NA

Example

Set the backup IP address of the out-of-band port to 10.18.53.200/24 for the MAD member 2 switch.

```
Switch(config)#mad backup ip address 10.18.53.200 24 2
Switch(config)#
```

14.1.24 debug mad

Function

The **debug mad** command enables MAD debugging.

The **no debug mad** command disables MAD debugging.

Format

- **debug mad { recv | send | timer | state | notify | error | packet | all }**
- **no debug mad { recv | send | timer | state | notify | error | packet | all }**

Parameter

Parameter	Description	Value
recv	Received packets	-
send	Transmitted packets	-
timer	Timer	-
state	State	-
notify	Notification	-
error	Error	-
packet	Packet details	-
all	All	-

Default Value

NA

View

Privileged user view

Usage Guidelines

NA

Example

Enable MAD debugging.

```
Switch#debug mad all
Switch#
```

14.1.25 show mad**Function**The **show mad** command shows information of MAD.**Format****show mad****Parameter**

NA

Default Value

NA

View

Privileged user view, global configuration view, interface configuration view (Ethernet interface, Trunk interface), interface group configuration view

Usage Guidelines

NA

Example

Show MAD information.

```
Switch(config-eth-trunk-1)#show mad
Mad status : normal
```

```

Mad direct detect interfaces state:
xge-1/0/35 down
Mad relay detect interfaces state:
eth-trunk-1
xge-1/0/18 down
Excluded ports(configurable):
xge-1/0/34
Switch(config-eth-trunk-1)#

```

14.1.26 show mad config

Function

The **show mad config** command shows configuration of MAD.

Format

show mad config

Parameter

No

Default Value

NA

View

Privileged user view, global configuration view, interface configuration view (Ethernet interface, Trunk interface), interface group configuration view

Usage Guidelines

NA

Example

Show MAD configuration.

```

Switch(config-eth-trunk 2)#show mad config
interface xgigaethernet 1/0/34
mad detect mode direct
interface eth-trunk 2
mad detect mode relay

```