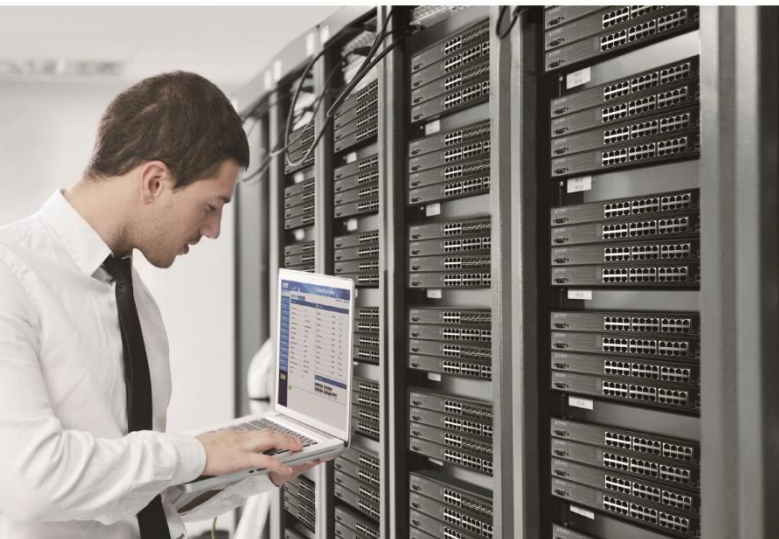




# User's Manual

## PLANET Layer 3 Gigabit/10 Gigabit Managed Ethernet Switch

- ▶ GS-6311 Series
- ▶ MGS-6311 Series
- ▶ XGS-6311 Series



## **Trademarks**

Copyright © PLANET Technology Corp. 2025.

Contents are subject to revision without prior notice.

PLANET is a registered trademark of PLANET Technology Corp. All other trademarks belong to their respective owners.

## **Disclaimer**

PLANET Technology does not warrant that the hardware will work properly in all environments and applications, and makes no warranty and representation, either implied or expressed, with respect to the quality, performance, merchantability, or fitness for a particular purpose. PLANET has made every effort to ensure that this User's Manual is accurate; PLANET disclaims liability for any inaccuracies or omissions that may have occurred.

Information in this User's Manual is subject to change without notice and does not represent a commitment on the part of PLANET. PLANET assumes no responsibility for any inaccuracies that may be contained in this User's Manual. PLANET makes no commitment to update or keep current the information in this User's Manual, and reserves the right to make improvements to this User's Manual and/or to the products described in this User's Manual, at any time without notice.

If you find information in this manual that is incorrect, misleading, or incomplete, we would appreciate your comments and suggestions.

## **FCC Warning**

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the Instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at whose own expense.

## **CE Mark Warning**

This device is compliant with Class A of CISPR 32. In a residential environment this equipment may cause radio interference.

## **WEEE Warning**



To avoid the potential effects on the environment and human health as a result of the presence of hazardous substances in electrical and electronic equipment, end users of electrical and electronic equipment should understand the meaning of the crossed-out wheeled bin symbol. Do not dispose of WEEE as unsorted municipal waste and have to collect such WEEE separately.

## **Energy Saving Note of the Device**

This power required device does not support Standby mode operation.

For energy saving, please remove the power cable to disconnect the device from the power circuit.

Without removing power cable, the device will still be consuming power from the power source. In the view of Saving the Energy and reduce the unnecessary power consuming, it is strongly suggested to remove the power connection for the device if this device is not intended to be active.

## **Revision**

User's Manual of PLANET Layer 3 Gigabit/10 Gigabit Managed Ethernet Switch

Models: GS-6311-24T4X, GS-6311-24HP4X, GS-6311-24P4XV, GS-6311-24PL4X, GS-6311-16S8C4XR, GS-6311-48T6X, GS-6311-48P6XR, MGS-6311-8P2X, MGS-6311-10T2X, XGS-6311-12X, XGS-6311-8X4TR.

Revision: 1.2

File Name: EM-GS-6311\_MGS-6311\_XGS-6311 Series\_v1.2

# Contents

<b>CHAPTER 1 INTRODUCTION .....</b>	<b>31</b>
1.1 PACKET CONTENTS .....	32
1.2 PRODUCT DESCRIPTION .....	33
1.3 PRODUCT FEATURES.....	38
1.4 PRODUCT SPECIFICATIONS.....	43
<b>CHAPTER 2 INSTALLATION .....</b>	<b>57</b>
2.1 HARDWARE DESCRIPTION .....	57
2.1.1 Switch Front Panel .....	57
2.1.2 LED Indications .....	59
2.2 SWITCH INSTALLATION .....	71
2.2.1 Desktop Installation .....	71
2.2.2 Rack Mounting .....	73
2.2.3 Installing the SFP/SFP+ Transceiver .....	75
2.2.4 AC Power Receptacle .....	77
<b>CHAPTER 3 SWITCH MANAGEMENT.....</b>	<b>78</b>
3.1 MANAGEMENT OPTIONS.....	78
3.2 OUT-OF-BAND MANAGEMENT .....	78
3.3 IN-BAND MANAGEMENT.....	78
3.4 REQUIREMENTS .....	79
3.5 TERMINAL SETUP.....	80
3.6 LOGGING ON TO THE CONSOLE.....	81
3.7 CONFIGURING IP ADDRESS .....	83
3.8 STARTING WEB MANAGEMENT .....	84
3.9 LOGGING IN TO THE MANAGED SWITCH.....	88
3.10 DISCOVERY THROUGH PLANET NMS CONTROLLER (NMS-500/NMS-1000V) .....	89
3.11 PLANET NMSVIEWERPRO APP .....	91
3.12 PLANET SMART DISCOVERY UTILITY .....	93
<b>CHAPTER 4 BASIC SWITCH CONFIGURATION.....</b>	<b>95</b>
4.1 BASIC CONFIGURATION .....	95
4.1.1 authentication line .....	95
4.1.2 banner .....	96



4.1.3 boot img.....	97
4.1.4 boot startup-config.....	98
4.1.5 clock set .....	99
4.1.6 config.....	100
4.1.7 disable .....	101
4.1.8 enable.....	102
4.1.9 enable password .....	103
4.1.10 end .....	104
4.1.11 exec-timeout.....	105
4.1.12 exit.....	106
4.1.13 help.....	107
4.1.14 hostname.....	108
4.1.15 ip host.....	109
4.1.16 ipv6 host .....	110
4.1.17 ip http server.....	111
4.1.18 login.....	112
4.1.19 password .....	113
4.1.20 privilege .....	114
4.1.21 reload .....	115
4.1.22 service password-encryption.....	116
4.1.23 service terminal-length .....	117
4.1.24 sysContact.....	118
4.1.25 sysLocation .....	119
4.1.26 set default.....	120
4.1.27 set boot password .....	121
4.1.28 setup.....	122
4.1.29 show clock.....	123
4.1.30 show cpu usage .....	124
4.1.31 show cpu utilization .....	125
4.1.32 show memory usage .....	126
4.1.33 show privilege.....	127
4.1.34 show privilege mode LINE .....	128
4.1.35 show tech-support.....	129
4.1.36 show version .....	130
4.1.37 username .....	131
4.1.38 web-auth privilege <1-15>.....	132
4.1.39 write.....	133
4.1.40 write running-config.....	134
<b>4.2 TELNET .....</b>	<b>135</b>
4.2.1 aaa authorization config-commands .....	135
4.2.2 accounting exec .....	136
4.2.3 accounting command .....	137
4.2.4 authentication enable .....	138
4.2.5 authentication ip access-class .....	139

4.2.6 authentication ipv6 access-class.....	140
4.2.7 authentication line login.....	141
4.2.8 authentication securityip.....	143
4.2.9 authentication securityipv6.....	144
4.2.10 authorization.....	145
4.2.11 authorization line vty command.....	146
4.2.12 clear line vty <0-31>.....	147
4.2.13 crypto key clear rsa.....	148
4.2.14 terminal length.....	149
4.2.15 telnet.....	150
4.2.16 telnet server enable.....	151
4.2.17 telnet-server max-connection.....	152
4.2.18 ssh-server authentication-retries.....	153
4.2.19 ssh-server enable.....	154
4.2.20 ssh-server host-key create rsa.....	155
4.2.21 ssh-server max-connection.....	156
4.2.22 ssh-server timeout.....	157
4.2.23 show crypto key.....	158
4.2.24 show ssh-server.....	159
4.2.25 show telnet login.....	160
4.2.26 show users.....	161
4.2.27 who.....	162
<b>4.3 CONFIGURING SWITCH IP.....</b>	<b>163</b>
4.3.1 interface vlan.....	163
4.3.2 ip address.....	164
4.3.3 ipv6 address.....	165
4.3.4 ip bootp-client enable.....	166
4.3.5 ip dhcp-client enable.....	167
<b>4.4 SNMP.....</b>	<b>168</b>
4.4.1 rmon enable.....	168
4.4.2 show private-mib oid.....	169
4.4.3 show snmp.....	170
4.4.4 show snmp engineid.....	171
4.4.5 show snmp group.....	172
4.4.6 show snmp mib.....	173
4.4.7 show snmp status.....	174
4.4.8 show snmp user.....	175
4.4.9 show snmp view.....	176
4.4.10 snmp-server community.....	177
4.4.11 snmp-server enable.....	178
4.4.12 snmp-server enable traps.....	179
4.4.13 snmp-server engineid.....	180
4.4.14 snmp-server group.....	181
4.4.15 snmp-server host.....	182

4.4.16 snmp-server securityip .....	183
4.4.17 snmp-server securityip enable .....	184
4.4.18 snmp-server trap-source .....	185
4.4.19 snmp-server user .....	186
4.4.20 snmp-server view .....	188
4.4.21 switchport updown notification enable .....	189
<b>4.5 SWITCH UPGRADE .....</b>	<b>190</b>
4.5.1 copy ( FTP ) .....	190
4.5.2 copy ( TFTP ) .....	192
4.5.3 ftp-dir .....	194
4.5.4 ftp-server enable .....	195
4.5.5 ftp-server timeout .....	196
4.5.6 ip ftp.....	197
4.5.7 show ftp .....	198
4.5.8 show tftp .....	199
4.5.9 tftp-server enable .....	200
4.5.10 tftp-server retransmission-number .....	201
4.5.11 tftp-server transmission-timeout .....	202
<b>4.6 FILE SYSTEM .....</b>	<b>203</b>
4.6.1 cd.....	203
4.6.2 copy.....	204
4.6.3 delete.....	205
4.6.4 dir.....	206
4.6.5 pwd .....	207
4.6.6 rename .....	208
<b>CHAPTER 5 PORT CONFIGURATION .....</b>	<b>209</b>
<b>5.1 ETHERNET PORT CONFIGURATION .....</b>	<b>209</b>
5.1.1 bandwidth .....	209
5.1.2 clear counters interface.....	210
5.1.3 description .....	211
5.1.4 flow control .....	212
5.1.5 interface ethernet .....	213
5.1.6 Loopback.....	214
5.1.7 Negotiation .....	215
5.1.8 Port-rate-statistics interval.....	216
5.1.9 rate-violation.....	217
5.1.10 rate-violation control .....	218
5.1.11 show interface .....	219
5.1.12 Shutdown .....	220
5.1.13 speed-duplex.....	221
5.1.14 storm-control .....	223
5.1.15 storm-control .....	224
5.1.16 storm-control bypass.....	225

5.1.17 virtual-cable-test .....	226
5.1.18 switchport discard packet.....	227
5.1.19 switchport flood-control .....	228
5.1.20 switchport flood-forwarding .....	229
<b>5.2 PORT ISOLATION FUNCTION.....</b>	<b>230</b>
5.2.1 isolate-port group .....	230
5.2.2 isolate-port group switchport interface .....	231
5.2.3 show isolate-port group.....	232
<b>5.3 PORT LOOPBACK DETECTION FUNCTION .....</b>	<b>233</b>
5.3.1 loopback-detection control .....	233
5.3.2 loopback-detection control-recovery timeout .....	234
5.3.3 loopback-detection interval-time .....	235
5.3.4 loopback-detection specified-vlan .....	236
5.3.5 show loopback-detection.....	237
<b>5.4 ULDP .....</b>	<b>238</b>
5.4.1 uldp aggressive-mode .....	238
5.4.2 uldp enable .....	239
5.4.3 uldp hello-interval .....	240
5.4.4 uldp manual-shutdown .....	241
5.4.5 uldp recovery-time .....	242
5.4.6 uldp reset.....	243
5.4.7 show uldp .....	244
<b>5.5 LLDP FUNCTION .....</b>	<b>245</b>
5.5.1 clear lldp remote-table.....	245
5.5.2 lldp enable .....	246
5.5.3 lldp enable ( port ) .....	247
5.5.4 lldp management-address tlv .....	248
5.5.5 lldp mode.....	249
5.5.6 lldp msgTxHold.....	250
5.5.7 lldp neighbors max-num .....	251
5.5.8 lldp notification interval .....	252
5.5.9 lldp tooManyNeighbors .....	253
5.5.10 lldp transmit delay .....	254
5.5.11 lldp transmit optional tlv .....	255
5.5.12 lldp trap.....	256
5.5.13 lldp tx-interval .....	257
5.5.14 show debugging lldp .....	258
5.5.15 show lldp .....	259
5.5.16 show lldp interface ethernet .....	260
5.5.17 show lldp neighbors interface ethernet .....	261
5.5.18 show lldp traffic.....	262
<b>5.6 PORT CHANNEL .....</b>	<b>263</b>
5.6.1 interface port-channel .....	263

5.6.2 lacp port-priority.....	264
5.6.3 lacp system-priority .....	265
5.6.4 lacp timeout .....	266
5.6.5 load-balance.....	267
5.6.6 port-group.....	268
5.6.7 port-group mode.....	269
5.6.8 show port-group .....	270
<b>5.7 MTU .....</b>	<b>271</b>
5.7.1 Mtu.....	271
<b>5.8 EFM OAM .....</b>	<b>272</b>
5.8.1 clear ethernet-oam .....	272
5.8.2 ethernet-oam .....	273
5.8.3 ethernet-oam errored-frame threshold high .....	274
5.8.4 ethernet-oam errored-frame threshold low .....	275
5.8.5 ethernet-oam errored-frame window.....	276
5.8.6 ethernet-oam errored-frame-seconds threshold high .....	277
5.8.7 ethernet-oam errored-frame-seconds threshold Low.....	278
5.8.8 ethernet-oam errored-frame-seconds window .....	279
5.8.9 ethernet-oam errored-symbol-period threshold High .....	280
5.8.10 ethernet-oam errored-symbol-period threshold Low.....	281
5.8.11 ethernet-oam errored-symbol-period window .....	282
5.8.12 ethernet-oam link-monitor .....	283
5.8.13 ethernet-oam mode .....	284
5.8.14 ethernet-oam period .....	285
5.8.15 ethernet-oam remote-failure.....	286
5.8.16 ethernet-oam remote-loopback .....	287
5.8.17 ethernet-oam remote-loopback supported.....	288
5.8.18 ethernet-oam timeout .....	289
5.8.19 show ethernet-oam.....	290
5.8.20 show ethernet-oam events.....	291
5.8.21 show ethernet-oam link-events-configuration .....	293
5.8.22 show ethernet-oam loopback status .....	294
<b>5.9 PORT SECURITY .....</b>	<b>295</b>
5.9.1 clear port-security.....	295
5.9.2 show port-security .....	296
5.9.3 switchport port-security .....	297
5.9.4 switchport port-security mac-address .....	298
5.9.5 switchport port-security maximum.....	299
5.9.6 switchport port-security violation .....	300
<b>5.10 DDM.....</b>	<b>301</b>
5.10.1 clear transceiver threshold-violation.....	301
5.10.2 show transceiver .....	302
5.10.3 show transceiver threshold-violation .....	303

5.10.4 transceiver-monitoring.....	304
5.10.5 transceiver-monitoring interval.....	305
5.10.6 transceiver threshold.....	306
<b>5.11 LLDP-MED .....</b>	<b>308</b>
5.11.1 civic location .....	308
5.11.2 description-language .....	309
5.11.3 ecs location.....	310
5.11.4 lldp med fast count .....	311
5.11.5 lldp med trap.....	312
5.11.6 lldp transmit med tlv all .....	313
5.11.7 lldp transmit med tlv capability .....	314
5.11.8 lldp transmit med tlv extendPoe .....	315
5.11.9 lldp transmit med tlv location .....	316
5.11.10 lldp transmit med tlv inventory.....	317
5.11.11 lldp transmit med tlv networkPolicy .....	318
5.11.12 network policy.....	319
5.11.13 show lldp.....	321
5.11.14 show lldp neighbors.....	322
5.11.15 show lldp traffic.....	323
<b>5.12 BPDU-TUNNEL.....</b>	<b>324</b>
5.12.1 bpdu-tunnel-protocol .....	324
5.12.2 bpdu-tunnel-protocol group-mac.....	325
5.12.3 bpdu-tunnel-protocol protocol-mac .....	326
5.12.4 bpdu-tunnel-protocol ethernetii .....	327
5.12.5 bpdu-tunnel-protocol snap .....	328
5.12.6 bpdu-tunnel-protocol llc.....	329
<b>5.13 EEE ENERGY-SAVING .....</b>	<b>330</b>
5.13.1 eee enable.....	330
<b>5.14 LED SHUT-OFF .....</b>	<b>331</b>
5.14.1 port-led shutoff time-range .....	331
<b>CHAPTER 6 MAC ADDRESS CONFIGURATION .....</b>	<b>332</b>
<b>6.1 MAC ADDRESS TABLE .....</b>	<b>332</b>
6.1.1 clear collision-mac-address-table.....	332
6.1.2 clear mac-address-table dynamic .....	333
6.1.3 mac-address-learning enable   disable .....	334
6.1.4 mac-address-table aging-time.....	335
6.1.5 mac-address-table static   blackhole.....	336
6.1.6 l2-address-table static-multicast address.....	337
6.1.7 show collision-mac-address-table .....	338
6.1.8 show mac-address-table .....	339
6.1.9 show l2-address-table multicast.....	340
6.1.10 clear mac-notification statistics .....	341

6.1.11 mac-address-table notification .....	342
6.1.12 mac-address-table notification history-size .....	343
6.1.13 mac-address-table notification interval .....	344
6.1.14 mac-notification .....	345
6.1.15 show mac-notification summary .....	346
6.1.16 snmp-server enable traps mac-notification .....	347

**CHAPTER 7 VLAN CONFIGURATION .....348**

<b>7.1 VLAN .....</b>	<b>348</b>
7.1.1 vlan .....	348
7.1.2 name (vlan) .....	349
7.1.3 switchport interface .....	350
7.1.4 switchport forbidden vlan .....	352
7.1.5 switchport mode .....	354
7.1.6 switchport hybrid native vlan .....	355
7.1.7 switchport hybrid allowed vlan .....	356
7.1.8 switchport access vlan .....	357
7.1.9 switchport trunk allowed vlan .....	358
7.1.10 switchport trunk native vlan .....	359
7.1.11 switchport mode trunk allow-null .....	360
7.1.12 vlan ingress enable .....	361
7.1.13 vlan-translation enable .....	362
7.1.14 vlan-translation .....	363
7.1.15 vlan-translation miss drop .....	364
7.1.16 dot1q-tunnel enable .....	365
7.1.17 dot1q-tunnel selective enable .....	366
7.1.18 dot1q-tunnel selective s-vlan .....	367
7.1.19 garp timer join .....	368
7.1.20 garp timer leave .....	369
7.1.21 garp timer leaveall .....	370
7.1.22 no garp timer .....	371
7.1.23 gvrp(Global) .....	372
7.1.24 gvrp(Port) .....	373
7.1.25 private-vlan .....	374
7.1.26 private-vlan association .....	375
7.1.27 show dot1q-tunnel .....	376
7.1.28 show garp timer .....	377
7.1.29 show gvrp fsm information .....	378
7.1.30 show gvrp leaveAll fsm information .....	379
7.1.31 show gvrp leavetimer running information .....	380
7.1.32 show gvrp port-member .....	381
7.1.33 show gvrp port registerd vlan .....	382
7.1.34 show gvrp timer running information .....	383
7.1.35 show gvrp vlan registerd port .....	384



7.1.36 show vlan .....	385
7.1.37 show vlan-translation.....	387
7.1.38 vlan-translation n-to-1 .....	388
7.1.39 show vlan-translation n-to-1 .....	389
7.1.40 dynamic-vlan mac-vlan prefer .....	390
7.1.41 dynamic-vlan subnet-vlan prefer .....	391
7.1.42 mac-vlan vlan .....	392
7.1.43 mac-vlan .....	393
7.1.44 protocol-vlan.....	394
7.1.45 show dynamic-vlan prefer .....	395
7.1.46 show mac-vlan interface .....	396
7.1.47 show protocol-vlan .....	397
7.1.48 show subnet-vlan .....	398
7.1.49 show subnet-vlan interface .....	399
7.1.50 subnet-vlan.....	400
7.1.51 switchport mac-vlan enable.....	401
7.1.52 switchport subnet-vlan enable.....	402
7.1.53 show voice-vlan.....	403
7.1.54 switchport voice-vlan enable .....	404
7.1.55 voice-vlan .....	405
7.1.56 voice-vlan vlan.....	407

**CHAPTER 8 ANTI-RING PROTOCOL .....408**

<b>8.1 MSTP .....</b>	<b>408</b>
8.1.1 abort .....	408
8.1.2 exit.....	409
8.1.3 instance vlan .....	410
8.1.4 Name.....	411
8.1.5 revision-level .....	412
8.1.6 spanning-tree .....	413
8.1.7 spanning-tree cost.....	414
8.1.8 spanning-tree digest-snooping.....	415
8.1.9 spanning-tree format .....	416
8.1.10 spanning-tree forward-time .....	417
8.1.11 spanning-tree hello-time .....	418
8.1.12 spanning-tree link-type p2p.....	419
8.1.13 spanning-tree maxage .....	420
8.1.14 spanning-tree max-hop .....	421
8.1.15 spanning-tree mcheck.....	422
8.1.16 spanning-tree mode .....	423
8.1.17 spanning-tree mst configuration.....	424
8.1.18 spanning-tree mst cost.....	425
8.1.19 spanning-tree cost-format .....	427
8.1.20 spanning-tree mst loopguard .....	428

8.1.21 spanning-tree mst port-priority .....	429
8.1.22 spanning-tree mst priority.....	430
8.1.23 spanning-tree mst rootguard .....	431
8.1.24 spanning-tree portfast .....	432
8.1.25 spanning-tree port-priority .....	433
8.1.26 spanning-tree priority .....	434
8.1.27 spanning-tree rootguard.....	435
8.1.28 spanning-tree tcflush (Global mode).....	436
8.1.29 spanning-tree tcflush (Port mode).....	437
8.1.30 spanning-tree transmit-hold-count .....	438
8.1.31 show mst-pending .....	439
8.1.32 show spanning-tree .....	440
8.1.33 show spanning-tree mst config .....	442
8.1.34 spanning-tree process.....	443
8.1.35 spanning-tree tc-notify process0 .....	444
8.1.36 spanning-tree binding-process.....	445
8.1.37 spanning-tree binding-process link-share .....	446
<b>8.2 ERPS CONFIGURATION.....</b>	<b>447</b>
8.2.1 ethernet tcn-propagation erps .....	447
8.2.2 erps-ring .....	448
8.2.3 version .....	449
8.2.4 open-ring .....	450
8.2.5 raps-virtual-channel.....	451
8.2.6 erps-ring .....	452
8.2.7 failure-detect.....	453
8.2.8 erps-instance .....	454
8.2.9 description .....	455
8.2.10 ring-id .....	456
8.2.11 rpl.....	457
8.2.12 non-revertive .....	458
8.2.13 guard-timer .....	459
8.2.14 holdoff-timer .....	460
8.2.15 wtr-timer .....	461
8.2.16 protected-instance.....	462
8.2.17 raps-mel .....	463
8.2.18 control-vlan.....	464
8.2.19 forced-switch .....	465
8.2.20 manual-switch .....	466
8.2.21 clear command.....	467
8.2.22 show erps ring.....	468
8.2.23 show erps instance.....	469
8.2.24 show erps status .....	471
8.2.25 show erps statistics .....	473
8.2.26 clear erps statistics.....	474

<b>CHAPTER 9 QOS AND FLOW-BASED REDIRECTION .....</b>	<b>475</b>
<b>9.1 QOS .....</b>	<b>475</b>
9.1.1 accounting .....	475
9.1.2 class .....	476
9.1.3 class-map .....	477
9.1.4 clear mls qos statistics .....	478
9.1.5 drop .....	479
9.1.6 match.....	480
9.1.7 mls qos aggregate-policy .....	481
9.1.8 mls qos cos .....	482
9.1.9 mls qos map .....	483
9.1.10 mls qos queue algorithm .....	485
9.1.11 mls qos queue wdr weight.....	486
9.1.12 mls qos queue wrr weight .....	487
9.1.13 mls qos queue bandwidth .....	488
9.1.14 mls qos trust.....	489
9.1.15 Policy burst.....	490
9.1.16 Policy.....	491
9.1.17 Policy aggregate.....	492
9.1.18 Policy-map.....	493
9.1.19 service-policy input.....	494
9.1.20 service-policy input vlan .....	495
9.1.21 set.....	496
9.1.22 show class-map.....	497
9.1.23 show policy-map.....	498
9.1.24 show mls qos interface.....	499
9.1.25 show mls qos.....	502
9.1.26 show mls qos maps.....	503
9.1.27 show mls qos vlan .....	505
9.1.28 show mls qos aggregate-policy.....	506
9.1.29 transmit.....	507
9.1.30 access-group redirect to interface ethernet .....	508
9.1.31 show flow-based-redirect .....	509
9.1.32 add .....	510
9.1.33 match.....	511
9.1.34 service-policy.....	512
9.1.35 set.....	513
 <b>CHAPTER 10 LAYER 3 INTERFACE AND ARP .....</b>	 <b>514</b>
<b>10.1 LAYER 3 INTERFACE .....</b>	<b>514</b>
10.1.1 description .....	514
10.1.2 interface vlan .....	515
10.1.3 no interface IFNAME .....	516
10.1.4 show ip route .....	517

<b>10.2 IPv4/v6 CONFIGURATION.....</b>	<b>518</b>
10.2.1 clear ip traffic .....	518
10.2.2 clear ipv6 neighbor .....	519
10.2.3 ip address .....	520
10.2.4 ip default-gateway .....	521
10.2.5 ipv6 address .....	522
10.2.6 ipv6 nd dad attempts .....	523
10.2.7 ipv6 nd ns-interval .....	524
10.2.8 ipv6 neighbor .....	525
10.2.9 show ip interface .....	526
10.2.10 show ip traffic .....	527
10.2.11 show ipv6 interface .....	529
10.2.12 show ipv6 route .....	531
10.2.13 show ipv6 neighbors .....	532
10.2.14 show ipv6 traffic.....	533
10.2.15 ip route .....	535
<b>10.3 ARP CONFIGURATION.....</b>	<b>536</b>
10.3.1 arp .....	536
10.3.2 clear arp-cache.....	537
10.3.3 clear arp traffic.....	538
10.3.4 show arp .....	539
10.3.5 show arp traffic .....	540
<b>10.4 ARP SCANNING PREVENTION .....</b>	<b>541</b>
10.4.1 anti-arpscan enable.....	541
10.4.2 anti-arpscan port-based threshold .....	542
10.4.3 anti-arpscan ip-based threshold .....	543
10.4.4 anti-arpscan trust.....	544
10.4.5 anti-arpscan trust ip.....	545
10.4.6 anti-arpscan recovery enable .....	546
10.4.7 anti-arpscan recovery time .....	547
10.4.8 anti-arpscan log enable .....	548
10.4.9 anti-arpscan trap enable .....	549
10.4.10 show anti-arpscan .....	550
<b>10.5 PREVENTING ARP SPOOFING.....</b>	<b>552</b>
10.5.1 ip arp-security updateprotect.....	552
10.5.2 ip arp-security learnprotect.....	553
10.5.3 ip arp-security convert .....	554
10.5.4 clear ip arp dynamic .....	555
10.5.5 clear ipv6 nd dynamic .....	556
<b>10.6 ARP GUARD .....</b>	<b>557</b>
10.6.1 arp-guard ip .....	557
<b>10.7 GRATUITOUS ARP CONFIGURATION .....</b>	<b>558</b>
10.7.1 ip gratuitous-arp .....	558

10.7.2 show ip gratuitous-arp .....	559
<b>10.8 DYNAMIC ARP INSPECTION .....</b>	<b>560</b>
10.8.1 ip arp inspection .....	560
10.8.2 ip arp inspection trust .....	561
10.8.3 ip arp inspection limit-rate .....	562
<b>CHAPTER 11 DHCP SERVER CONFIGURATION .....</b>	<b>563</b>
<b>11.1 DHCP .....</b>	<b>563</b>
11.1.1 bootfile .....	563
11.1.2 clear ip dhcp binding.....	564
11.1.3 clear ip dhcp conflict .....	565
11.1.4 clear ip dhcp server statistics .....	566
11.1.5 client-identifier .....	567
11.1.6 default-router .....	568
11.1.7 dns-server .....	569
11.1.8 domain-name.....	570
11.1.9 hardware-address.....	571
11.1.10 host.....	572
11.1.11 ip dhcp conflict logging .....	573
11.1.12 ip dhcp disable.....	574
11.1.13 ip dhcp excluded-address .....	575
11.1.14 ip dhcp pool .....	576
11.1.15 ip dhcp conflict ping-detection enable .....	577
11.1.16 ip dhcp ping packets.....	578
11.1.17 ip dhcp ping timeout .....	579
11.1.18 lease .....	580
11.1.19 max-lease-time .....	581
11.1.20 netbios-name-server.....	582
11.1.21 netbios-node-type.....	583
11.1.22 network-address .....	584
11.1.23 next-server.....	585
11.1.24 option.....	586
11.1.25 service dhcp .....	587
11.1.26 show ip dhcp binding .....	588
11.1.27 show ip dhcp conflict .....	589
11.1.28 show ip dhcp relay information option .....	590
11.1.29 show ip dhcp server statistics.....	591
11.1.30 ip dhcp broadcast suppress .....	593
11.1.31 ip dhcp relay share-vlan .....	594
11.1.32 ip forward-protocol udp bootps.....	595
11.1.33 ip helper-address.....	596
11.1.34 show ip forward-protocol .....	597
11.1.35 show ip helper-address .....	598
11.1.36 clear ipv6 dhcp binding.....	599

11.1.37 clear ipv6 dhcp conflict .....	600
11.1.38 clear ipv6 dhcp statistics.....	601
11.1.39 dns-server.....	602
11.1.40 domain-name.....	603
11.1.41 excluded-address .....	604
11.1.42 ipv6 address .....	605
11.1.43 ipv6 dhcp client pd.....	606
11.1.44 ipv6 dhcp client pd hint.....	607
11.1.45 ipv6 dhcp pool .....	608
11.1.46 ipv6 dhcp relay destination.....	609
11.1.47 ipv6 dhcp server .....	610
11.1.48 ipv6 general-prefix .....	611
11.1.49 ipv6 local pool.....	612
11.1.50 lifetime .....	613
11.1.51 network-address .....	614
11.1.52 prefix-delegation .....	615
11.1.53 prefix-delegation pool .....	616
11.1.54 service dhcpv6.....	617
11.1.55 show ipv6 dhcp.....	618
11.1.56 show ipv6 dhcp binding .....	619
11.1.57 show ipv6 dhcp conflict.....	620
11.1.58 show ipv6 dhcp interface.....	621
11.1.59 show ipv6 dhcp pool .....	622
11.1.60 show ipv6 dhcp statistics .....	623
11.1.61 show ipv6 general-prefix .....	625
11.1.62 show ipv6 local pool .....	626
11.1.63 ip dhcp relay information option .....	627
11.1.64 ip dhcp relay information option delimiter.....	628
11.1.65 ip dhcp relay information option remote-id .....	629
11.1.66 ip dhcp relay information option remote-id format.....	630
11.1.67 ip dhcp relay information option self-defined remote-id .....	631
11.1.68 ip dhcp relay information option self-defined remote-id format .....	632
11.1.69 ip dhcp relay information option self-defined subscriber-id.....	633
11.1.70 ip dhcp relay information option self-defined subscriber-id format.....	634
11.1.71 ip dhcp relay information option subscriber-id.....	635
11.1.72 ip dhcp relay information option subscriber-id format .....	636
11.1.73 ip dhcp relay information policy .....	637
11.1.74 ip dhcp server relay information enable .....	638
11.1.75 show ip dhcp relay information option .....	639
11.1.76 option 43 ascii LINE.....	640
11.1.77 option 43 hex WORD.....	641
11.1.78 option 43 ip A.B.C.D .....	642
11.1.79 option 60 ascii LINE.....	643
11.1.80 option 60 hex WORD.....	644
11.1.81 option 60 ip A.B.C.D .....	645

11.1.82 address range.....	646
11.1.83 class.....	647
11.1.84 ipv6 dhcp class .....	648
11.1.85 ipv6 dhcp relay remote-id .....	649
11.1.86 ipv6 dhcp relay remote-id option .....	650
11.1.87 ipv6 dhcp relay subscriber-id.....	651
11.1.88 ipv6 dhcp relay subscriber-id option.....	652
11.1.89 ipv6 dhcp relay subscriber-id select delimiter .....	653
11.1.90 ipv6 dhcp server remote-id option .....	654
11.1.91 ip dhcp server select relay-forw.....	655
11.1.92 ipv6 dhcp server subscriber-id option.....	656
11.1.93 ipv6 dhcp snooping information option remote-id format .....	657
11.1.94 ipv6 dhcp snooping information option subscriber-id format.....	658
11.1.95 ipv6 dhcp snooping remote-id .....	659
11.1.96 ipv6 dhcp snooping remote-id option .....	660
11.1.97 ipv6 dhcp snooping remote-id policy .....	661
11.1.98 ipv6 dhcp snooping subscriber-id.....	662
11.1.99 ipv6 dhcp snooping subscriber-id option .....	663
11.1.100 ipv6 dhcp snooping subscriber-id policy.....	664
11.1.101 ipv6 dhcp snooping subscriber-id select delimiter.....	665
11.1.102 ipv6 dhcp use class .....	666
11.1.103 remote-id subscriber-id.....	667
11.1.104 show ipv6 dhcp relay option .....	668
11.1.105 show ipv6 dhcp snooping option .....	669
11.1.106 enable trustview key .....	670
11.1.107 ip dhcp snooping .....	671
11.1.108 ip dhcp snooping action.....	672
11.1.109 ip dhcp snooping action MaxNum .....	673
11.1.110 ip dhcp snooping binding .....	674
11.1.111 ip dhcp snooping binding dot1x .....	675
11.1.112 ip dhcp snooping binding user.....	676
11.1.113 ip dhcp snooping binding user-control.....	677
11.1.114 ip dhcp snooping binding user-control max-user.....	678
11.1.115 ip dhcp snooping information enable.....	679
11.1.116 ip dhcp snooping information option allow-untrusted (replace).....	680
11.1.117 ip dhcp snooping information option delimiter .....	681
11.1.118 ip dhcp snooping information option remote-id.....	682
11.1.119 ip dhcp snooping information option self-defined remote-id.....	683
11.1.120 ip dhcp snooping information option self-defined remote-id format .....	684
11.1.121 ip dhcp snooping information option self-defined subscriber-id .....	685
11.1.122 ip dhcp snooping information option self-defined subscriber-id format.....	686
11.1.123 ip dhcp snooping information option subscriber-id.....	687
11.1.124 ipv6 dhcp snooping information option subscriber-id format.....	688
11.1.125 ip dhcp snooping limit-rate .....	689
11.1.126 ip dhcp snooping trust .....	690



11.1.127 ip dhcp snooping vlan.....	691
11.1.128 ip user helper-address.....	692
11.1.129 ip user private packet version two .....	693
11.1.130 show ip dhcp snooping .....	694
11.1.131 show ip dhcp snooping binding all.....	697
11.1.132 show trustview status .....	698
11.1.133 ip dhcp snooping information enable.....	699

**CHAPTER 12 MULTICAST PROTOCOL .....700**

<b>12.1 IPV4 MULTICAST.....</b>	<b>700</b>
12.1.1 access-list (Multicast Destination Control) .....	700
12.1.2 access-list (Multicast Source Control).....	701
12.1.3 ip multicast destination-control access-group .....	702
12.1.4 ip multicast destination-control access-group (sip).....	703
12.1.5 ip multicast destination-control access-group (vmac).....	704
12.1.6 ip multicast policy .....	705
12.1.7 ip multicast source-control .....	706
12.1.8 ip multicast source-control access-group.....	707
12.1.9 ip multicast destination-control.....	708
12.1.10 profile-id (Multicast Destination Control Rule List) .....	709
12.1.11 show ip multicast destination-control.....	710
12.1.12 show ip multicast destination-control access-list .....	711
12.1.13 show ip multicast destination-control filter-profile-list.....	712
12.1.14 show ip multicast policy.....	713
12.1.15 show ip multicast source-control .....	714
12.1.16 show ip multicast source-control access-list .....	715
12.1.17 clear ip igmp snooping vlan.....	716
12.1.18 clear ip igmp snooping vlan.....	717
12.1.19 ip igmp snooping .....	718
12.1.20 ip igmp snooping proxy .....	719
12.1.21 ip igmp snooping vlan .....	720
12.1.22 ip igmp snooping vlan immediate-leave .....	721
12.1.23 ip igmp snooping vlan .....	722
12.1.24 ip igmp snooping vlan l2-general-querier.....	723
12.1.25 ip igmp snooping vlan l2-general-querier-source.....	724
12.1.26 ip igmp snooping vlan l2-general-querier-version .....	725
12.1.27 ip igmp snooping vlan limit .....	726
12.1.28 ip igmp snooping vlan interface.....	727
12.1.29 ip igmp snooping vlan mrouter-port interface.....	728
12.1.30 ip igmp snooping vlan mrouter-port learnpim.....	729
12.1.31 ip igmp snooping vlan mrpt .....	730
12.1.32 ip igmp snooping vlan query-interval .....	731
12.1.33 ip igmp snooping vlan query-mrsp .....	732
12.1.34 ip igmp snooping vlan query-robustness .....	733

12.1.35 ip igmp snooping vlan report source-address .....	734
12.1.36 ip igmp snooping vlan specific-query-mrsp .....	735
12.1.37 ip igmp snooping vlan static-group.....	736
12.1.38 ip igmp snooping vlan suppression-query-time.....	737
12.1.39 show ip igmp snooping.....	738
12.1.40 clear ipv6 mld snooping vlan .....	740
12.1.41 clear ipv6 mld snooping vlan <1-4094> mrouter-port .....	741
12.1.42 ipv6 mld snooping .....	742
12.1.43 ipv6 mld snooping vlan.....	743
12.1.44 ipv6 mld snooping vlan immediate-leave .....	744
12.1.45 ipv6 mld snooping vlan l2-general-querier .....	745
12.1.46 ipv6 mld snooping vlan limit .....	746
12.1.47 ipv6 mld snooping vlan mrouter-port interface.....	747
12.1.48 ipv6 mld snooping vlan mrouter-port learnpim6.....	748
12.1.49 ipv6 mld snooping vlan mrpt .....	749
12.1.50 ipv6 mld snooping vlan query-interval.....	750
12.1.51 ipv6 mld snooping vlan query-mrsp .....	751
12.1.52 ipv6 mld snooping vlan query-robustness.....	752
12.1.53 ipv6 mld snooping vlan static-group.....	753
12.1.54 ipv6 mld snooping vlan suppression-query-time.....	754
12.1.55 show ipv6 mld snooping.....	755
12.1.56 multicast-vlan .....	757
12.1.57 multicast-vlan association .....	758
12.1.58 multicast-vlan association interface .....	759
12.1.59 multicast-vlan mode .....	760
12.1.60 switchport association multicast-vlan .....	761

**CHAPTER 13 SECURITY FUNCTION .....762**

<b>13.1 ACL.....</b>	<b>762</b>
13.1.1 absolute-periodic/periodic .....	762
13.1.2 absolute start.....	764
13.1.3 access-list (ip extended) .....	765
13.1.4 access-list (ip standard) .....	768
13.1.5 access-list(mac extended) .....	769
13.1.6 access-list(mac-ip extended) .....	770
13.1.7 access-list (mac standard) .....	773
13.1.8 clear access-group statistic.....	774
13.1.9 firewall .....	775
13.1.10 ip access extended .....	776
13.1.11 ip access standard.....	777
13.1.12 ipv6 access-list.....	778
13.1.13 ipv6 access standard .....	779
13.1.14 ipv6 access extended.....	780
13.1.15 access-group.....	781

13.1.16 mac access extended .....	782
13.1.17 mac-ip access extended .....	783
13.1.18 permit   deny (ip extended) .....	784
13.1.19 permit   deny (ip standard) .....	786
13.1.20 permit   deny (ipv6 extended).....	787
13.1.21 permit   deny (ipv6 standard) .....	789
13.1.22 permit   deny (mac extended) .....	790
13.1.23 permit   deny (mac-ip extended) .....	792
13.1.24 show access-lists .....	795
13.1.25 show access-group .....	796
13.1.26 show firewall.....	797
13.1.27 show ipv6 access-lists.....	798
13.1.28 show time-range.....	799
13.1.29 time-range .....	800
<b>13.2 SELF-DEFINED ACL.....</b>	<b>801</b>
13.2.1 userdefined-access-list standard offset.....	801
13.2.2 userdefined-access-list standard .....	803
13.2.3 userdefined access-group.....	804
13.2.4 vacl userdefined access-group .....	805
<b>13.3 802.1x.....</b>	<b>806</b>
13.3.1 dot1x accept-mac.....	806
13.3.2 dot1x eapor enable.....	807
13.3.3 dot1x enable.....	808
13.3.4 dot1x ipv6 passthrough .....	809
13.3.5 dot1x guest-vlan .....	810
13.3.6 dot1x macfilter enable .....	811
13.3.7 dot1x macbased guest-vlan .....	812
13.3.8 dot1x macbased port-down-flush .....	813
13.3.9 dot1x max-req .....	814
13.3.10 dot1x user allow-movement .....	815
13.3.11 dot1x user free-resource .....	816
13.3.12 dot1x max-user macbased.....	817
13.3.13 dot1x max-user userbased.....	818
13.3.14 dot1x portbased mode single-mode.....	819
13.3.15 dot1x port-control .....	820
13.3.16 dot1x port-method .....	821
13.3.17 dot1x privateclient enable .....	822
13.3.18 dot1x privateclient protect enable .....	823
13.3.19 dot1x re-authenticate .....	824
13.3.20 dot1x re-authentication.....	825
13.3.21 dot1x timeout quiet-period.....	826
13.3.22 dot1x timeout re-authperiod .....	827
13.3.23 dot1x timeout tx-period.....	828
13.3.24 dot1x unicast enable .....	829

13.3.25 show dot1x .....	830
<b>13.4 THE NUMBER LIMITATION FUNCTION OF MAC AND IP IN PORT, VLAN .....</b>	<b>832</b>
13.4.1 ip arp dynamic maximum .....	832
13.4.2 ipv6 nd dynamic maximum.....	833
13.4.3 show arp-dynamic count .....	834
13.4.4 show mac-address dynamic count.....	835
13.4.5 show nd-dynamic count .....	836
13.4.6 switchport arp dynamic maximum.....	837
13.4.7 switchport mac-address dynamic maximum .....	838
13.4.8 switchport mac-address violation .....	839
13.4.9 switchport nd dynamic maximum .....	840
13.4.10 vlan mac-address dynamic maximum.....	841
<b>13.5 AM CONFIGURATION.....</b>	<b>842</b>
13.5.1 am enable.....	842
13.5.2 am port .....	843
13.5.3 am ip-pool.....	844
13.5.4 am mac-ip-pool.....	845
13.5.5 no am all.....	846
13.5.6 show am .....	847
<b>13.6 SECURITY FEATURE .....</b>	<b>848</b>
13.6.1 dosattack-check srcip-equal-dstip enable .....	848
13.6.2 dosattack-check tcp-flags enable.....	849
13.6.3 dosattack-check srcport-equal-dstport enable .....	850
13.6.4 dosattack-check icmp-attacking enable .....	851
13.6.5 dosattack-check icmpV4-size.....	852
<b>13.7 ACACS+ .....</b>	<b>853</b>
13.7.1 tacacs-server authentication host .....	853
13.7.2 tacacs-server key .....	854
13.7.3 tacacs-server nas-ipv4 .....	855
13.7.4 tacacs-server timeout.....	856
<b>13.8 RADIUS .....</b>	<b>857</b>
13.8.1 aaa enable.....	857
13.8.2 aaa-accounting enable .....	858
13.8.3 aaa-accounting update.....	859
13.8.4 radius nas-ipv4 .....	860
13.8.5 radius nas-ipv6.....	861
13.8.6 radius-server accounting host .....	862
13.8.7 radius-server authentication host .....	863
13.8.8 radius-server dead-time .....	865
13.8.9 radius-server key.....	866
13.8.10 radius-server retransmit .....	867
13.8.11 radius-server timeout.....	868
13.8.12 radius-server accounting-interim-update timeout.....	869

13.8.13 show aaa authenticated-user .....	870
13.8.14 show aaa authenticating-user .....	871
13.8.15 show aaa config .....	872
13.8.16 show radius authenticated-user count .....	873
13.8.17 show radius authenticating-user count .....	874
13.8.18 show radius count .....	875
<b>13.9 IPV6 SECURITY RA.....</b>	<b>876</b>
13.9.1 ipv6 security-ra enable .....	876
13.9.2 ipv6 security-ra enable .....	877
13.9.3 show ipv6 security-ra.....	878
<b>13.10 MAB.....</b>	<b>879</b>
13.10.1 authentication mab .....	879
13.10.2 clear mac-authentication-bypass binding.....	880
13.10.3 mac-authentication-bypass binding-limit.....	881
13.10.4 mac-authentication-bypass enable .....	882
13.10.5 mac-authentication-bypass guest-vlan.....	883
13.10.6 mac-authentication-bypass spoofing-garp-check .....	884
13.10.7 mac-authentication-bypass timeout linkup-period.....	885
13.10.8 mac-authentication-bypass timeout offline-detect.....	886
13.10.9 mac-authentication-bypass timeout quiet-period .....	887
13.10.10 mac-authentication-bypass timeout reauth-period.....	888
13.10.11 mac-authentication-bypass timeout stale-period.....	889
13.10.12 mac-authentication-bypass username-format.....	890
13.10.13 show mac-authentication-bypass.....	891
<b>13.11 MAB PPPoE INTERMEDIATE AGENT .....</b>	<b>892</b>
13.11.1 pppoe intermediate-agent .....	892
13.11.2 pppoe intermediate-agent (Port) .....	893
13.11.3 pppoe intermediate-agent circuit-id .....	894
13.11.4 pppoe intermediate-agent delimiter .....	895
13.11.5 pppoe intermediate-agent format .....	896
13.11.6 pppoe intermediate-agent remote-id .....	897
13.11.7 pppoe intermediate-agent trust .....	898
13.11.8 pppoe intermediate-agent type self-defined circuit-id .....	899
13.11.9 pppoe intermediate-agent type self-defined remoteid.....	900
13.11.10 pppoe intermediate-agent type tr-101 circuit-id access-node-id .....	901
13.11.11 pppoe intermediate-agent type tr-101 circuit-id identifier-string option delimiter.....	902
13.11.12 pppoe intermediate-agent vendor-tag strip .....	903
13.11.13 show pppoe intermediate-agent identifier-string option delimiter.....	905
13.11.14 show pppoe intermediate-agent info .....	906
<b>13.12 VLAN-ACL .....</b>	<b>907</b>
13.12.1 clear vacl statistic vlan .....	907
13.12.2 show vacl vlan .....	908
13.12.3 vacl ip access-group .....	910

13.12.4	vacl ipv6 access-group .....	911
13.12.5	vacl mac access-group .....	912
13.12.6	vacl mac-ip access-group .....	913
<b>13.13</b>	<b>SAVI .....</b>	<b>914</b>
13.13.1	ipv6 cps prefix .....	914
13.13.2	ipv6 cps prefix check enable .....	915
13.13.3	ipv6 dhcp snooping trust .....	916
13.13.4	ipv6 nd snooping trust .....	917
13.13.5	savi enable .....	919
13.13.6	savi ipv6 binding num .....	920
13.13.7	savi ipv6 check source binding .....	921
13.13.8	savi ipv6 check source ip-address mac-address .....	922
13.13.9	savi ipv6 {dhcp-only   slaac-only   dhcp-slaac} enable .....	923
13.13.10	savi ipv6 mac-binding-limit .....	924
13.13.11	savi max-dad-dalay .....	925
13.13.12	savi max-dad-prepare-delay .....	926
13.13.13	savi max-slaac-life .....	927
13.13.14	savi timeout bind-protect .....	928
13.13.15	show savi ipv6 check source binding .....	929
<b>CHAPTER 14</b>	<b>RELIABILITY .....</b>	<b>930</b>
<b>14.1</b>	<b>MRPP .....</b>	<b>930</b>
14.1.1	control-vlan .....	930
14.1.2	clear mrpp statistics .....	931
14.1.3	enable .....	932
14.1.4	errp domain .....	933
14.1.5	fail-timer .....	934
14.1.6	hello-timer .....	935
14.1.7	mrpp eaps compatible .....	936
14.1.8	mrpp enable .....	937
14.1.9	mrpp errp compatible .....	938
14.1.10	mrpp poll-time .....	939
14.1.11	mrpp ring .....	940
14.1.12	mrpp ring primary-port .....	941
14.1.13	mrpp ring secondary-port .....	942
14.1.14	node-mode .....	943
14.1.15	show mrpp .....	944
14.1.16	show mrpp statistics .....	945
<b>14.2</b>	<b>ULPP .....</b>	<b>946</b>
14.2.1	clear ulpp flush counter interface .....	946
14.2.2	control vlan .....	947
14.2.3	description .....	948
14.2.4	flush {enable  disable} arp .....	949
14.2.5	flush {enable  disable} mac .....	950

14.2.6 flush {enable  disable} mac-vlan .....	951
14.2.7 preemption delay .....	952
14.2.8 preemption mode .....	953
14.2.9 protect vlan-reference-instance.....	954
14.2.10 show ulpp flush counter interface.....	955
14.2.11 show ulpp flush-receive-port .....	956
14.2.12 show ulpp group .....	957
14.2.13 ulpp control vlan .....	958
14.2.14 ulpp flush {enable disable} arp .....	959
14.2.15 ulpp flush {enable disable} mac .....	960
14.2.16 ulpp flush {enable disable} mac-vlan.....	961
14.2.17 ulpp group .....	962
14.2.18 ulpp group {master slave}.....	963
<b>14.3 ULPP GROUP &lt;INTEGER&gt; {MASTER SLAVE}.....</b>	<b>963</b>
<b>14.4 NO ULPP GROUP &lt;INTEGER&gt; {MASTER SLAVE} .....</b>	<b>963</b>
<b>14.5 ULSM.....</b>	<b>964</b>
14.5.1 show ulsm group .....	964
14.5.2 ulsm group.....	965
14.5.3 ulsm group {uplink   downlink}.....	966
<b>CHAPTER 15 MIRRORING CONFIGURATION.....</b>	<b>967</b>
<b>15.1 MIRRORING CONFIGURATION .....</b>	<b>967</b>
15.1.1 monitor session source interface .....	967
15.1.2 monitor session source interface access-list .....	968
15.1.3 monitor session destination interface.....	969
15.1.4 show monitor .....	970
15.1.5 mirror sample rate .....	971
<b>15.2 sFLOW .....</b>	<b>972</b>
15.2.1 sflow agent-address .....	972
15.2.2 sflow analyzer.....	973
15.2.3 sflow counter-interval .....	974
15.2.4 sflow data-len .....	975
15.2.5 sflow destination.....	976
15.2.6 sflow header-len .....	977
15.2.7 sflow priority .....	978
15.2.8 sflow rate .....	979
15.2.9 show sflow .....	980
<b>15.3 RSPAN CONFIGURATION .....</b>	<b>982</b>
15.3.1 remote-span .....	982
15.3.2 monitor session remote vlan .....	983
15.3.3 monitor session reflector-port.....	984
<b>CHAPTER 16 NETWORK TIME MANAGEMENT.....</b>	<b>985</b>



<b>16.1 SNTP .....</b>	<b>985</b>
16.1.1 clock timezone.....	985
16.1.2 sntp polltime .....	986
16.1.3 sntp server.....	987
16.1.4 show sntp .....	988
<b>16.2 NTP.....</b>	<b>989</b>
16.2.1 ntp access-group.....	989
16.2.2 ntp authenticate.....	990
16.2.3 ntp authentication-key .....	991
16.2.4 ntp broadcast server count.....	992
16.2.5 ntp disable .....	993
16.2.6 ntp enable.....	994
16.2.7 ntp ipv6 multicast client .....	995
16.2.8 ntp multicast client.....	996
16.2.9 ntp server .....	997
16.2.10 ntp syn-interval .....	998
16.2.11 ntp trusted-key.....	999
16.2.12 show ntp status .....	1000
16.2.13 show ntp session.....	1001
<b>16.3 SUMMER TIME .....</b>	<b>1002</b>
16.3.1 clock summer-time absolute .....	1002
16.3.2 clock summer-time recurring.....	1003
16.3.3 clock summer-time recurring.....	1004
 <b>CHAPTER 17 DEBUGGING AND DIAGNOSIS .....</b>	 <b>1006</b>
<b>17.1 SHOW.....</b>	<b>1006</b>
17.1.1 clear history all-users .....	1006
17.1.2 clear logging .....	1007
17.1.3 history all-users max-length .....	1008
17.1.4 logging.....	1009
17.1.5 logging executed-commands .....	1010
17.1.6 logging loghost sequence-number .....	1011
17.1.7 logging source-ip.....	1012
17.1.8 ping.....	1013
17.1.9 ping6.....	1015
17.1.10 show boot-files .....	1017
17.1.11 show flash.....	1018
17.1.12 show history .....	1019
17.1.13 show history all-users.....	1020
17.1.14 show logging buffered .....	1021
17.1.15 show logging executed-commands state.....	1022
17.1.16 show logging source .....	1023
17.1.17 show running-config .....	1024
17.1.18 show running-config current-mode.....	1025

17.1.19 show startup-config .....	1026
17.1.20 show switchport interface .....	1027
17.1.21 show tcp .....	1028
17.1.22 show tcp ipv6.....	1029
17.1.23 show telnet login.....	1030
17.1.24 show udp .....	1031
17.1.25 show udp ipv6 .....	1032
17.1.26 show version .....	1033
17.1.27 traceroute .....	1034
17.1.28 traceroute6 .....	1035
17.1.29 reload after .....	1036
17.1.30 reload cancel.....	1037
17.1.31 show reload .....	1038
17.1.32 clear cpu-rx-stat protocol.....	1039
17.1.33 cpu-rx-ratelimit protocol.....	1040
17.1.34 cpu-rx-ratelimit total.....	1041
17.1.35 show cpu-rx protocol .....	1042

**CHAPTER 18 POE ..... 1043**

**18.1 PoE CONFIGURATION ..... 1043**

18.1.1 power inline enable (Global) .....	1043
18.1.2 power inline enable (Port) .....	1044
18.1.3 power inline high-inrush .....	1045
18.1.4 power inline legacy.....	1046
18.1.5 power inline max (Global) .....	1047
18.1.6 power inline max (Port) .....	1048
18.1.7 power inline police.....	1049
18.1.8 power inline priority .....	1050
18.1.9 power inline monitor interval .....	1051
18.1.10 power inline monitor {on off }.....	1052

**18.2 POWER INLINE MONITOR {ON|OFF} ..... 1052**

18.1.11 power inline power-off .....	1053
18.1.12 power inline reset interval .....	1054

**18.1 ..... 1055**

**18.2 PoE MONITORING AND DEBUGGING..... 1055**

18.2.1 show power inline.....	1055
18.2.2 show power inline interface ethernet.....	1056

**CHAPTER 19 ROUTING PROTOCOL ..... 1057**

**19.1 RIP ..... 1057**

19.1.1 accept-lifetime .....	1057
19.1.2 clear ip rip route.....	1059
19.1.3 default-information originate.....	1060

19.1.4 default-metric.....	1061
19.1.5 distance .....	1062
19.1.6 distribute-list .....	1063
19.1.7 ip rip aggregate-address .....	1064
19.1.8 ip rip authentication key-chain.....	1065
19.1.9 ip rip authentication mode .....	1066
19.1.10 ip rip authentication string .....	1067
19.1.11 ip rip authentication cisco-compatible .....	1068
19.1.12 ip rip receive-packet .....	1069
19.1.13 ip rip receive version .....	1070
19.1.14 ip rip send-packet.....	1071
19.1.15 ip rip send version .....	1072
19.1.16 ip rip split-horizon .....	1073
19.1.17 key.....	1074
19.1.18 key chain .....	1075
19.1.19 key-string.....	1076
19.1.20 maximum-prefix.....	1077
19.1.21 neighbor .....	1078
19.1.22 network.....	1079
19.1.23 offset-list .....	1080
19.1.24 passive-interface .....	1081
19.1.25 recv-buffer-size.....	1082
19.1.26 redistribute.....	1083
19.1.27 route .....	1084
19.1.28 router rip .....	1085
19.1.29 send-lifetime .....	1086
19.1.30 timers basic .....	1087
19.1.31 version.....	1088
19.1.32 show ip protocols rip .....	1089
19.1.33 show ip rip .....	1091
19.1.34.....	1091
19.1.34 show ip rip database .....	1092
19.1.35 show ip rip interface .....	1093
19.1.36 show ip rip aggregate.....	1094
19.1.37 show ip rip redistribute .....	1095
<b>19.2 OSPF .....</b>	<b>1096</b>
19.2.1 area authentication.....	1096
19.2.2 area default-cost.....	1097
19.2.3 area filter-list.....	1098
19.2.4 area nssa.....	1099
19.2.5 area range .....	1100
19.2.6 area stub .....	1101
19.2.7 area virtual-link .....	1102
19.2.8 auto-cost reference-bandwidth.....	1103

19.2.9 compatible rfc1583 .....	1104
19.2.10 clear ip ospf process .....	1105
19.2.11 default-information originate .....	1106
19.2.12 default-metric.....	1107
19.2.13 distance .....	1108
19.2.14 distribute-list .....	1109
19.2.15 filter-policy .....	1110
19.2.16 host area .....	1111
19.2.17 ip ospf authentication .....	1112
19.2.18 ip ospf authentication-key .....	1113
19.2.19 ip ospf cost .....	1114
19.2.20 ip ospf database-filter .....	1115
19.2.21 ip ospf dead-interval .....	1116
19.2.22 ip ospf disable all.....	1117
19.2.23 ip ospf hello-interval .....	1118
19.2.24 ip ospf message-digest-key .....	1119
19.2.25 ip ospf mtu.....	1120
19.2.26 ip ospf mtu-ignore.....	1121
19.2.27 ip ospf network .....	1122
19.2.28 ip ospf priority .....	1123
19.2.29 ip ospf retransmit-interval.....	1124
19.2.30 ip ospf transmit-delay .....	1125
19.2.31 key.....	1126
19.2.32 key chain .....	1127
19.2.33 log-adjacency-changes detail.....	1128
19.2.34 max-concurrent-dd .....	1129
19.2.35 neighbor .....	1130
19.2.36 network area.....	1131
19.2.37 ospf abr-type .....	1132
19.2.38 ospf router-id .....	1133
19.2.39 overflow database .....	1134
19.2.40 overflow database external .....	1135
19.2.41 passive-interface .....	1136
19.2.42 redistribute.....	1137
19.2.43 redistribute ospf.....	1138
19.2.44 router ospf .....	1139
19.2.45 summary-address.....	1140
19.2.46 timers spf.....	1141
19.2.47 show ip ospf .....	1142
19.2.48 show ip ospf border-routers .....	1144
19.2.49 show ip ospf database .....	1145
19.2.50 show ip ospf interface .....	1147
19.2.51 show ip ospf neighbor .....	1148
19.2.52 show ip ospf redistribute .....	1149
19.2.53 show ip ospf route .....	1150

19.2.54 show ip ospf virtual-links .....	1151
19.2.55 show ip route process-detail .....	1152
19.2.56 show ip protocols.....	1153

# Chapter 1 INTRODUCTION

Thank you for purchasing Layer 3 Gigabit/10 Gigabit Managed Ethernet Switch.

The descriptions of these models are as follows:

Model	Description
<b>XGS-6311-12X</b>	Layer 3 12-Port 10GBASE-X SFP+ Managed Ethernet Switch
<b>XGS-6311-8T4XR</b>	L3 8-Port 10GBASE-T + 4-Port 10GBASE-X SFP+ Managed Ethernet Switch with Dual 100~240V AC Redundant Power
<b>GS-6311-24T4X</b>	L3 24-Port 10/100/1000T + 4-Port 10G SFP+ Managed Ethernet Switch
<b>GS-6311-16S8C4XR</b>	L3 16-Port 100/1000X SFP + 8-Port Gigabit TP/SFP + 4-Port 10G SFP+ Managed Ethernet Switch with 36-72V DC Redundant Power
<b>GS-6311-48T6X</b>	L3 48-Port 10/100/1000T + 6-Port 10G SFP+ Managed Ethernet Switch
<b>GS-6311-24HP4X</b>	L3 8-Port 2.5GBASE-T 802.3at PoE + 2-Port 10GBASE-T + 2-Port 10GBASE-X SFP+ Managed Ethernet Switch
<b>GS-6311-24P4XV</b>	L3 24-Port 802.3at PoE + 4-Port 10G SFP+ Managed Ethernet Switch with Smart LCD Screen
<b>GS-6311-24PL4X</b>	L3 24-Port 10/100/1000T 802.3at PoE + 4-Port 10G SFP+ Managed Ethernet Switch (720W)
<b>GS-6311-48P6X</b>	L3 48-Port 10/100/1000T 802.3at PoE + 6-Port 10G SFP+ Managed Ethernet Switch
<b>MGS-6311-10T2X</b>	L3 8-Port 2.5GBASE-T + 2-Port 10GBASE-T + 2-Port 10GBASE-X SFP+ Managed Ethernet Switch
<b>MGS-6311-8P2X</b>	L3 8-Port 2.5GBASE-T 802.3at PoE + 2-Port 10GBASE-X SFP+ Managed Ethernet Switch

## 1.1 Packet Contents

Unless specified, “**Managed Switch**” mentioned in this user’s manual refers to the GS-6311-24T4X, GS-6311-24HP4X, GS-6311-24P4XV, GS-6311-24PL4X, GS-6311-16S8C4XR, GS-6311-48T6X, GS-6311-48P6X, XGS-6311-12X, XGS-6311-8X4TR, MGS-6311-10T2X, and MGS-6311-8P2X.

Open the box of the Managed Switch and carefully unpack it. The box should contain the following items:

Model \ Item	Quick Installation Guide Sheet	DB9 to RJ45 Console Cable	Rack-mount Accessory Kit	SFP Dust Cap	AC Power Cord	Rubber Feet
<b>XGS-6311-12X</b>	■	■	■	12	1	4
<b>XGS-6311-8X4TR</b>	■	■	■	8	2	4
<b>GS-6311-24T4X</b>	■	■	■	4	1	4
<b>GS-6311-16S8C4XR</b>	■	■	■	28	1	4
<b>GS-6311-48T6X</b>	■	■	■	6	1	4
<b>GS-6311-24HP4X</b>	■	■	■	4	1	4
<b>GS-6311-24P4XV</b>	■	■	■	4	1	4
<b>GS-6311-24PL4X</b>	■	■	■	4	1	4
<b>GS-6311-48P6X</b>	■	■	■	6	1	4
<b>MGS-6311-10T2X</b>	■	■	■	2	1	4
<b>MGS-6311-8P2X</b>	■	■	■	2	1	4

If any item is found missing or damaged, please contact your local reseller for replacement.



## 1.2 Product Description

### Powerful 10Gbps and Layer 3 Routing Solution for Enterprise Backbone and Data Center Networking

PLANET M(X)GS-6311 series is a Layer 3 Managed Gigabit Switch that provides high-density performance, **Layer 3 IPv4/IPv6 static routing, RIP (Routing Information Protocol) and OSPF (Open Shortest Path First)**. With **10Gbps** interfaces, the M(X)GS-6311 series can handle extremely large amounts of data in a secure topology linking to an enterprise backbone or high-capacity servers. The powerful network security features make the M(X)GS-6311 series perform effective data traffic control for ISP and enterprise VoIP, video streaming, and multicast applications.

The hardware specifications of these models are shown below:

Models	Copper	Fiber	PoE Ports	Power Input
<b>XGS-6311-12X</b>	--	12 1G/10G SFP+	--	AC
<b>XGS-6311-8X4TR</b>	4 100/1G/2.5G/5G/10G RJ45	8 1G/2.5G/10G SFP+	--	AC+ AC
<b>GS-6311-24T4X</b>	24 10/100/1G RJ45	4 1G/10G SFP+	--	AC
<b>GS-6311-24HP4X</b>	24 10/100/1G RJ45	4 1G/10G SFP+	8bt + 16at	AC
<b>GS-6311-24P4XV</b>	24 10/100/1G RJ45	4 1G/10G SFP+	24at	AC
<b>GS-6311-24PL4X</b>	24 10/100/1G RJ45	4 1G/10G SFP+	24at	AC
<b>GS-6311-16S8C4XR</b>	8 (combo) 10/100/1G RJ45	24 100/1G SFP 4 1G/10G SFP+	--	AC + DC
<b>GS-6311-48T6X</b>	48 10/100/1G RJ45	6 1G/10G SFP+	--	AC
<b>GS-6311-48P6X</b>	48 10/100/1G RJ45	6 1G/10G SFP+	48at	AC
<b>MGS-6311-102X</b>	8 10/100/1G/2.5G RJ45 2 100/1G/2.5G/5G/10G RJ45	2 1G/10G SFP+	--	AC
<b>MGS-6311-8P2X</b>	8 10/100/1G/2.5G BASET	2 1G/10G SFP+	8at	AC

### High Performance 10Gbps Ethernet Capacity

The two to six SFP+ ports built in the M(X)GS-6311 series boasts a high-performance switch architecture that is capable of providing non-blocking switch fabric and wire-speed throughput as high as up to **120Gbps**, which greatly simplifies the tasks of upgrading the LAN for catering to increasing bandwidth demands. Each of the SFP+ ports supports **Dual-Speed, 10GBASE-SR/LR** or **1000BASE-SX/LX**, meaning the administrator now can flexibly choose the suitable SFP/SFP+ transceiver according to the transmission distance or the transmission speed required to extend the network efficiently.

### **UNI-NMS Remote Management Solution**

The M(X)GS-6311 series supports PLANET's Universal Network Management System (UNI-NMS) helping IT staff by remotely managing all network devices and monitoring PDs' operational statuses. Thus, they're designed for both the enterprises and industries where deployments of PDs can be as remote as possible, without having to go to the actual location once a bug or faulty condition is found. With the UNI-NMS, all kinds of businesses can now be speedily and efficiently managed from one platform.

### **Powerful NMSViewerPro Solution that Meets Evolving Network Management Challenges**

The M(X)GS-6311 series Managed Ethernet Switch, known for such features as QoS, Link aggregation, PoE, VLANs, IGMP, and so on, provides an eye-catching feature called NMS developed by PLANET to easily and remotely manage and monitor network devices in the local environment from mobile app. This feature not only improves operational convenience, but also ensures users have real-time control over their network infrastructure. It provides users with an unparalleled experience.

The intuitive interface of the local NMSViewerPro allows administrators to easily perform a variety of tasks, including monitoring traffic, setting configuration, troubleshooting, and more. At the same time, PLANET UNI-NMS application provides real-time alerts and notifications, allowing administrators to respond to any emergency situations anytime, anywhere to ensure the stable operation of the network.

NMSViewerPro meets users' requirements for managing a network more flexibly and efficiently. It helps users to know what the current statuses of the nodes are and to effectively manage the situations.

PLANET NMS and NMSViewerPro app, which with PLANET's free cloud service, allows users to quickly and easily detect, configure, deploy and manage devices remotely. You can just scan the NMS agent's (NMS-500/NMS-1000V) QR code using the mobile application to easily monitor and control the remote network devices via the private cloud.

### **Redundant Ring, Fast Recovery for Critical Network Applications**

The M(X)GS-6311 series supports redundant ring technology and features strong, rapid self-recovery capability to prevent interruptions and external intrusions. It incorporates advanced ITU-T **G.8032 ERPS** (Ethernet Ring Protection Switching) technology and Spanning Tree Protocol (802.1s MSTP) into customer's network to enhance system reliability and uptime in harsh environments. In a certain simple Ring network, the recovery time could be less than 15ms to quickly bring the network back to normal operation.

## Layer 3 Routing Support

The M(X)GS-6311 series enables the administrator to conveniently boost network efficiency by configuring Layer 3 static routing manually, the **RIP** (Routing Information Protocol) or **OSPF** (Open Shortest Path First) settings automatically.

- ▶ The RIP can employ the hop count as a routing metric and prevent routing loops by implementing a limit on the number of hops allowed in a path from the source to a destination.
- ▶ The OSPF is an interior dynamic routing protocol for autonomous system based on link state. The protocol creates a database for link state by exchanging link states among Layer 3 switches, and then uses the Shortest Path First algorithm to generate a route table based on that database.

## Strong Multicast

The M(X)GS-6311 series supports abundant multicast features. In Layer 2, it features IPv4 IGMPv1/v2/v3 snooping and IPv6 MLD v1/v2 snooping. With Multicast VLAN Register (MVR), multicast receiver/sender control and illegal multicast source detect functions which make the M(X)GS-6311 series great for any robust networking.

## Full IPv6 Support

The M(X)GS-6311 series provides **IPv6 management** and enterprise-level secure features such as **SSH, ACL, WRR** and **RADIUS** authentication. It thus helps the enterprises to step in the IPv6 era with the lowest investment. In addition, you don't need to replace the network facilities when the IPv6 FTTx edge network is built.

## Robust Layer 2 Features

The M(X)GS-6311 series can be programmed for basic switch management functions such as port speed configuration, port aggregation, VLAN, Multiple Spanning Tree Protocol, bandwidth control and IGMP snooping. This switch provides 802.1Q tagged VLAN, Q-in-Q, voice VLAN and GVRP Protocol functions. By supporting port aggregation, the M(X)GS-6311 series allows the operation of a high-speed trunk combined with multiple ports. It enables up to 64 groups for trunking with a maximum of 8 ports for each group.

## Excellent Layer 2 to Layer 4 Traffic Control

The M(X)GS-6311 series is loaded with powerful traffic management and WRR features to enhance services offered by telecoms. The WRR functionalities include wire-speed Layer 4 traffic classifiers and bandwidth limitation which are particularly useful for multi-tenant unit, multi-business unit, Telco, or network service applications. It also empowers the enterprises to take full advantage of the limited network resources and guarantees the best in VoIP and video conferencing transmission.

## Powerful Network Security

The M(X)GS-6311 series offers comprehensive Layer 2 to Layer 4 **Access Control List** (ACL) for enforcing security to the edge. It can be used to restrict network access by denying packets based on source and destination IP address, TCP/UDP ports or defined typical network applications. Its protection mechanism also comprises 802.1x Port-based, MAC-based and web-based user and device authentications, which can be deployed with RADIUS, to ensure the port level security and block illegal users.

## Advanced IP Network Protection

The M(X)GS-6311 series also provides DHCP Snooping, IP Source Guard and Dynamic ARP Inspection functions to prevent IP snooping from attack and discard ARP packets with invalid MAC address. The network administrators can now construct highly-secure corporate networks with considerably less time and effort than before.

## Efficient and Secure Management

For efficient management, the M(X)GS-6311 series is equipped with console, Web and SNMP management interfaces.

- With the built-in Web-based management interface, the M(X)GS-6311 series offers an easy-to-use, platform-independent management and configuration facility.
- For text-based management, it can be accessed via Telnet and the console port. For reducing product learning time, the M(X)GS-6311 series offers Cisco-like command and customer doesn't need to learn new command from these switches
- For standard-based monitor and management software, it offers SNMPv3 connection which encrypts the packet content at each session for secure remote management.

Moreover, the M(X)GS-6311 series offers secure remote management by supporting SSHv2 connection which encrypts the packet content at each session.

## Intelligent SFP Diagnosis Mechanism

The M(X)GS-6311 series supports **SFP-DDM (Digital Diagnostic Monitor)** function that greatly helps network administrator to easily monitor real-time parameters of the SFP and SFP+ transceivers, such as optical output power, optical input power, temperature, laser bias current, and transceiver supply voltage.

## Centralized Power Management for Gigabit Ethernet PoE Networking

To fulfill the needs of higher power required PoE network applications with Gigabit speed transmission. The GS-6311-24HP4X features 8 10/100/1000BASE-T high-performance Gigabit IEEE **802.3bt PoE++** up to 90 watts on port 1~port 8 and 16 IEEE 802.3at PoE+ up to 32 watts on port 9~port 24. The GS-6311-48P6X features 48 10/100/1000BASE-T high-performance Gigabit IEEE 802.3at PoE+ up to 32 watts on port 1~port 48. It perfectly meets the power requirements of PoE VoIP phone and all kinds of PoE IP cameras such as IR, PTZ, speed dome cameras or even box type IP cameras with built-in fan and heater.

The GS-6311-24P4X's PoE capabilities also help to reduce deployment costs for network devices as a result of freeing from the restrictions of power outlet locations. Power and data switching are integrated into one unit, delivered over a single cable and managed centrally. It thus eliminates the cost for additional AC wiring and reduces installation time.

## PoE Schedule for Energy Savings

Besides being used for IP surveillance, the MGS/GS-6311 PoE series is certainly applicable to build any PoE network including VoIP and wireless LAN. Under the trend of energy saving worldwide and contributing to the environmental protection on the Earth, the MGS/GS-6311 PoE Series can effectively control the power supply besides its capability of giving high watts power. The "PoE schedule" function helps you to enable or disable PoE power feeding for each PoE port during specified time intervals and it is a powerful function to help SMBs or enterprises save energy and budget.

## Smart and Intuitive LCD Control

The front panel of the GS-6311-24P4XV provides an intuitive color panel for easy Ethernet network management and PoE PD management. With the jog dial and LCD screen, users can quickly change the setting they want. Just select the setting you want by rotating the dial and then press the dial to enter the setting. This easy operation can enhance the management efficiency of large networks such as enterprises, hotels, shopping malls, government buildings and other public areas. The following special management and status functions are included:

- PoE management and status
- Port management and status
- Switch mode: Standard, VLAN or Extend
- IP setting and loop detection
- VLAN ownership setting
- Screen saver, factory default and save configuration

## 1.3 Product Features

### ➤ Physical Ports

#### GS-6311-24T4X

- 24 10/100/1000BASE-T RJ45 copper ports (Ports 1 to 24)
- 4 10GBASE-SR/LR SFP+ slots, compatible with 1000BASE-SX/LX/BX SFP (Ports 25 to 28)
- RJ45 to DB9 console interface for switch basic management and setup

#### GS-6311-24HP4X

- 8 10/100/1000BASE-T ports with **90W 802.3bt PoE++** injector function (Ports 1 to 8)
- 16 10/100/1000BASE-T ports with **32W 802.3at PoE+** injector function (Ports 9 to 24)
- 4 10GBASE-SR/LR SFP+ slots, compatible with 1000BASE-SX/LX/BX SFP (Ports 25 to 28)
- RJ45 to DB9 console interface for switch basic management and setup

#### GS-6311-24P4XV

- 24 10/100/1000BASE-T ports with **32W 802.3at PoE+** injector function
- 4 10GBASE-SR/LR SFP+ slots, compatible with 1000BASE-SX/LX/BX SFP
- RJ45 to DB9 console interface for switch basic management and setup

#### GS-6311-24PL4X

- 24 10/100/1000BASE-T ports with **32W 802.3at PoE+** injector function
- 4 10GBASE-SR/LR SFP+ slots, compatible with 1000BASE-SX/LX/BX SFP
- RJ45 to DB9 console interface for switch basic management and setup

#### GS-6311-16S8C4XR

- 24 100/1000BASE-X SFP ports (Ports 1 to 24)
- 8 10/100/1000BASE-T RJ45 copper ports
- 4 10GBASE-SR/LR SFP+ slots, compatible with 1000BASE-SX/LX/BX SFP
- RJ45 to DB9 console interface for switch basic management and setup

#### GS-6311-48T6X

- 48 10/100/1000BASE-T RJ45 copper ports (Ports 1 to 48)
- 6 10GBASE-SR/LR SFP+ slots, compatible with 1000BASE-SX/LX/BX SFP (Ports 49 to 54)
- RJ45 to DB9 console interface for switch basic management and setup

#### GS-6311-48P6X

- 48 10/100/1000BASE-T with **32W 802.3at PoE+** injector function
- 6 10GBASE-SR/LR SFP+ slots, compatible with 1000BASE-SX/LX/BX SFP
- RJ45 to DB9 console interface for switch basic management and setup

#### MGS-6311-8P2X

- 8 10/100/1000/2500BASE-T ports with 32W 802.3at PoE+ injector function
- 2 10GBASE-SR/LR SFP+ slots, compatible with 1000BASE-SX/LX/BX SFP
- RJ45 to DB9 console interface for switch basic management and setup

### MGS-6311-10T2X

- 8 10/100/1000/**2500BASE-T** RJ45 copper ports (Ports 1 to 8)
- 2 100/1G/2.5G/5G/**10GBASE-T** RJ45 auto-negotiation copper ports (Ports 9 to 10)
- 2 **10GBASE-SR/LR SFP+** slots, compatible with 1000BASE-SX/LX/BX SFP (Ports 11 to 12)
- RJ45 to DB9 console interface for switch basic management and setup

### XGS-6311-12X

- 12 **10GBASE-SR/LR SFP+** slots, backward compatible with 1000BASE-SX/LX/BX SFP
- RJ45 type RS232 console interface for switch basic management and setup

### XGS-6311-8T4XR

- 8 100/1G/2.5G/5G/**10GBASE-T** RJ45 auto-negotiation copper ports (Ports 1 to 8)
- 4 **10GBASE-X SFP+** slots, compatible with 1G/2.5GBASE-SX/LX/BX SFP (Ports 9 to 12)
- RJ45 type RS232 console interface for switch basic management and setup

#### ➤ **IP Routing Features**

- IPv4 routing protocol supports **RIPv1/v2** and **OSPFv2**
- IPv6 routing protocol supports **RIPng** and **OSPFv3**
- Routing interface provides per VLAN routing mode
- Supports route redistribution

#### ➤ **Layer 2 Features**

- Complies with the IEEE 802.3, IEEE 802.3u, IEEE 802.3ab, IEEE 802.3z Gigabit Ethernet standard
- Prevents packet loss flow control
  - IEEE 802.3x pause frame flow control in full-duplex mode
  - Back pressure flow control in half-duplex mode
- High performance Store-and-Forward architecture, broadcast storm control, port loopback detection
- 16K ~ 32K MAC address table, automatic source address learning and aging
- Supports VLAN
  - IEEE 802.1Q tag-based VLAN
  - GVRP for dynamic VLAN management
  - Provider Bridging (VLAN Q-in-Q, IEEE 802.1ad) supported
  - Private VLAN Edge (PVE) supported
  - GVRP protocol for Management VLAN
  - Protocol-based VLAN
  - MAC-based VLAN
  - IP subnet VLAN
- Supports Link Aggregation
  - Maximum 64 trunk groups, up to 8 ports per trunk group
  - IEEE 802.3ad LACP (Link Aggregation Control Protocol)
  - Cisco ether-channel (static trunk)

- Supports Spanning Tree Protocol
  - STP, IEEE 802.1D (Classic Spanning Tree Protocol)
  - RSTP, IEEE 802.1w (Rapid Spanning Tree Protocol)
  - MSTP, IEEE 802.1s (Multiple Spanning Tree Protocol, spanning tree by VLAN)
  - Supports BPDU & root guard
- Port mirroring to monitor the incoming or outgoing traffic on a particular port (many to many)
- Provides port mirror (many-to-1)
- Supports G.8032 ERPS (Ethernet Ring Protection Switching)
  
- **Quality of Service**
  - 8 priority queues on all switch ports
  - Support for strict priority and WRR (Weighted Round Robin) CoS policies
  - Traffic classification
    - IEEE 802.1p CoS/ToS
    - IPv4/IPv6 DSCP
    - Port-based WRR
  - Strict priority and WRR CoS policies
  
- **Multicast**
  - Supports IPv4 IGMP snooping v1, v2 and v3
  - Supports IPv6 MLD v1 and v2 snooping
  - Querier mode support
  - Supports Multicast VLAN Register (MVR)
  
- **Security**
  - IEEE 802.1x port-based network access authentication
  - MAC-based network access authentication
  - Built-in RADIUS client to cooperate with the RADIUS servers for IPv4 and IPv6
  - TACACS+ login users access authentication
  - IP-based Access Control List (ACL)
  - MAC-based Access Control List
  - Supports DHCP snooping
  - Supports ARP inspection
  - **IP Source Guard** prevents IP spoofing attacks
  - **Dynamic ARP Inspection** discards ARP packets with invalid MAC address to IP address binding
  
- **Management**
  - Management IP for IPv4 and IPv6
  - Switch Management Interface
    - Console/Telnet Command Line Interface
    - Web switch management
    - SNMP v1, v2c, and v3 switch management
    - SSH/TLS secure access



- BOOTP and DHCP for IP address assignment
- Firmware upload/download via TFTP or HTTP Protocol for IPv4 and IPv6
- SNTP (Simple Network Time Protocol) for IPv4 and IPv6
- User privilege levels control
- Syslog server for IPv4 and IPv6
- Supports DDM
- Four RMON groups 1, 2, 3, 9 (history, statistics, alarms and events)
- Supports sFlow
- Supports ULDP
- Supports ULPP (Uplink Protection Protocol)
- Supports ULSM (Uplink State Monitor protocol)
- Supports LLDP/LLDP MED
- Supports DHCP Option82/43/60/61/67
- Supports ping, trace route function for IPv4 and IPv6
- PLANET Smart Discovery Utility for deployment management
- PLANET NMS for deployment management
- PLANET NMSViewerPro for deployment management

➤ **Power over Ethernet**

**GS-6311-24HP4X**

- Complies with IEEE 802.3bt Power over Ethernet Plus Plus
- 8 IEEE 802.3bt PoE++ ports with up to 90 watts (Ports 1 to 8)
- 16 IEEE 802.3at PoE+ ports with up to 32 watts (Ports 9 to 24)
- Maximum 480-watt PoE budget

**GS-6311-24P4XV**

- Complies with IEEE 802.3at/af Power over Ethernet Plus
- Up to 24 ports of IEEE 802.3af/802.3at devices powered
- Supports PoE power up to 32 watts for each PoE port
- Maximum 370-watt PoE budget

**GS-6311-24P4XV**

- Complies with IEEE 802.3at/af Power over Ethernet Plus
- Up to 24 ports of IEEE 802.3af/802.3at devices powered
- Supports PoE power up to 32 watts for each PoE port
- Maximum 720-watt PoE budget

**GS-6311-48P6X**

- Complies with IEEE 802.3at/af Power over Ethernet Plus
- Up to 48 ports of IEEE 802.3af/802.3at devices powered
- Supports PoE power up to 32 watts for each PoE port
- 110VAC supports maximum 500-watt PoE budget
- 220VAC supports maximum 600-watt PoE budget

### **MGS-6311-8P2X**

- Complies with IEEE 802.3at/af Power over Ethernet Plus
- Up to 8 ports of IEEE 802.3af/802.3at devices powered
- Supports PoE power up to 32 watts for each PoE port
- Supports maximum 150-watt PoE budget
- Auto detects powered device (PD)
- Circuit protection prevents power interference between ports
- Remote power feeding up to 100 meters
- PoE management
  - Total PoE power budget control
  - Per port PoE function enable/disable
  - PoE port power feeding priority
  - Per PoE port power limitation
  - PD classification detection
- Intelligent PoE features
  - PD alive check
  - PoE schedule

#### ➤ **Redundant Power System**

### **GS-6311-16S8C4XR**

- 100~240V AC / 36 -72V DC dual power redundancy
- Active-active redundant power failure protection
- Backup of catastrophic power failure on one supply

### **XGS-6311-8T4XR**

- 100~240V AC dual power redundancy
- Active-active redundant power failure protection
- Backup of catastrophic power failure on one supply

#### ➤ **Smart LCD**

### **GS-6311-24P4XV**

- The LCD switch features Standard, VLAN modes; the Extend mode features 20-watt PoE transmission distance of 250m at speed of 10Mbps and VLAN isolation
- The LCD switch is able to isolate ports to prevent broadcast storm and defend DHCP spoofing
- Power low-voltage, power over-voltage and PSE over-temperature protection
- Screen saver, factory default and save configuration

## 1.4 Product Specifications

### GS-6311 Series: (without PoE)

Product	GS-6311-24T4X	GS-6311-16S8C4XR	GS-6311-48T6X
<b>Hardware Specifications</b>			
10/100/1000 RJ45 Ports	24	8 (combo)	48
100/1000BASE-X SFP Ports	--	24	--
10G SFP+ Ports	4	4	6
	10GBASE-SR/LR SFP+ interface Backward compatible with 1000BASE-SX/LX/BX SFP transceiver		
Console Port	1 x RJ45-to-RS232 serial port (9600, 8, N, 1)		
CPU	MIPS 800MHz		
RAM	512Mbytes		
Flash Memory	32Mbytes		
Dimensions (W x D x H)	440 x 207 x 44mm	440 x 260 x 44mm	440 x 260 x 44 mm
Weight	2742g	3495g	3676g
Power Consumption	23.2 watts/79.11 BTU	36.2 watts/ 102.9 BTU	53.7 watts/183BTU
Power Requirements- AC	AC 100~240V, 50/60Hz	AC 100~240V, 50/60Hz	AC: 100~240V, 50/60Hz
Power Requirements - DC	--	DC: 36~72V	--
Fan	--	2	1
LED	<b>System:</b> PWR (Green) SYS (Green)	<b>System:</b> PWR (Green) SYS (Green)	<b>System:</b> PWR (Green) SYS (Green)
	<b>Ports:</b> LNK/ACT (Green)	<b>Ports:</b> LNK/ACT (Green)	<b>Ports:</b> LNK/ACT (Green)
<b>Switching Specifications</b>			
Switch Architecture	Store-and-forward		
Switch Fabric	128Gbps/non-blocking		216Gbps/non-blocking
Switch Throughput	95.23Mpps		160.7Mpps
Address Table	16K MAC address table with auto learning function		32K MAC address table with auto learning function
ARP Table	8K	8K	8K
Routing Table	6K	6K	12K
IP Interface	1024	1024	1024
ACL Table	2K	2K	4K
Shared Data Buffer	12MB	12MB	16MB
Jumbo Frame	12KBytes		
Flow Control	Back pressure for half duplex IEEE 802.3x pause frame for full duplex		
<b>IPv4 Layer 3 Functions</b>			
IP Routing Protocol	Static route RIPv1/v2 OSPFv2		

	BGP4 Hardware-based Layer 3 routing
<b>Layer 3 Protocol</b>	ARP ARP Proxy IGMP Proxy
<b>IPv6 Layer 3 Functions</b>	
<b>IP Routing Protocol</b>	IPv6 Static Route RIPng OSPFv3 BGP6 (BGP4+) PIM6 IPv6 RA (Router Advertisement) IPv6 LPM Routing Hardware-based Layer 3 routing SNMP over IPv6 Support IPv6 IPsec Support IPv6 ACL
<b>Other</b>	ICMPv6,ND,DNSv6 DNS over IPv6 Support
<b>Layer 2 Functions</b>	
<b>Port Configuration</b>	Port disable/enable Flow control disable/enable Bandwidth control on each port Port loopback detect
<b>Port Status</b>	Display each port's speed duplex mode, link status, flow control status and auto negotiation status
<b>VLAN</b>	802.1Q tagged VLAN, up to 4K VLAN groups 802.1ad Q-in-Q (VLAN stacking) GVRP for VLAN management Private VLAN Edge (PVE) supported Protocol-based VLAN MAC-based VLAN IP subnet VLAN
<b>Bandwidth Control</b>	TX/RX/Both
<b>Link Aggregation</b>	IEEE 802.3ad LACP/static trunk Supports 64 groups with 8 ports per trunk group
<b>QoS</b>	8 priority queues on all switch ports Supports strict priority and Weighted Round Robin (WRR) CoS policies Traffic classification: <ul style="list-style-type: none"> <li>- IEEE 802.1p CoS/ToS</li> <li>- IPv4/IPv6 DSCP</li> <li>- Port-based WRR</li> </ul>
<b>Multicast</b>	IPv4 IGMP v1/v2/v3 snooping IPv4 Querier mode support IPv6 MLD v1/v2 snooping Multicast VLAN Register (MVR) Up to 1024
<b>Security Functions</b>	

<b>Access Control List</b>	<p>Supports Standard and Expanded ACL  IP-based ACL/MAC-based ACL  Time-based ACL  Up to 2K entries</p>
<b>Security</b>	<p>Port isolation  Supports IP + MAC + port binding  Identification and filtering of L2/L3/L4 based ACL  Defend against DOS or TCP attacks  Suppression of broadcast, multicast and unknown unicast packet  DHCP Snooping, DHCP Option 82/43/60/61/67  Command line authority control based on user levels</p>
<b>AAA</b>	TACACS+ and IPv4/IPv6 over RADIUS
<b>Authentication</b>	IEEE 802.1x port-based network access control
<b>Switch Management Functions</b>	
<b>System Configuration</b>	Console, Telnet, Web browser, SNMP v1, v2c
<b>Secure Management Interfaces</b>	SSHv2, TLSv1.2, SNMPv3
<b>Management</b>	<p>IPv4 and IPv6 dual stack management  SNMP over IPv6 Support  User IP security inspection for IPv4/IPv6 SNMP  SNMP v1, v2c and v3  SNMP MIB and TRAP  SNMP RMON 1, 2, 3, 9 four groups  HTTP over IPv6 Support  IPv4/IPv6 FTP/TFTP  IPv4/IPv6 SNTTP/NTP  Supports ping, trace route function for IPv4 and IPv6  RADIUS authentication for IPv4/IPv6 Telnet user name and password  IPv4/IPv6 SSH`  IPv4/IPv6 Telnet  IPv6 Radius+ Support  The right configuration for users to adopt RADIUS server's shell management  CLI, console, Telnet  Security IP safety net management function: avoid unlawful landing at nonrestrictive area  Syslog server for IPv4 and IPv6  IPv6 TACACS+ support  PLANET Smart Discovery Utility  PLANET NMS  PLANET NMSViewerPro</p>
<b>SNMP MIBs</b>	<p>RFC 1213 MIB-II  RFC 1215 Internet Engineering Task Force  RFC 1271 RMON  RFC 1354 IP-Forwarding MIB  RFC 1493 Bridge MIB  RFC 1643 Ether-like MIB  RFC 1907 SNMP v2  RFC 2011 IP/ICMP MIB  RFC 2012 TCP MIB</p>

	<p>RFC 2013 UDP MIB  RFC 2096 IP forward MIB  RFC 2233 if MIB  RFC 2452 TCP6 MIB  RFC 2454 UDP6 MIB  RFC 2465 IPv6 MIB  RFC 2466 ICMP6 MIB  RFC 2573 SNMP v3 notify  RFC 2574 SNMP v3 vacm  RFC 2674 Bridge MIB Extensions (IEEE 802.1Q MIB)  RFC 2674 Bridge MIB Extensions (IEEE 802.1P MIB)</p>
<b>Standard Conformance</b>	
<b>Regulatory Compliance</b>	FCC Part 15 Class A, CE
<b>Standards Compliance</b>	<p>IEEE 802.3 10BASE-T  IEEE 802.3u 100BASE-TX  IEEE 802.3z Gigabit 1000BASE-SX/LX  IEEE 802.3ab Gigabit 1000BASE-T  IEEE 802.3ae 10Gb/s Ethernet  IEEE 802.3x flow control and back pressure  IEEE 802.3ad port trunk with LACP  IEEE 802.1ag CFM  IEEE 802.1D Spanning Tree Protocol  IEEE 802.1w Rapid Spanning Tree Protocol  IEEE 802.1s Multiple Spanning Tree Protocol  IEEE 802.1p Class of Service  IEEE 802.1Q VLAN tagging  IEEE 802.1X port authentication network control  IEEE 802.1ab LLDP  IEEE 802.3af Power over Ethernet  IEEE 802.3at Power over Ethernet PLUS  IEEE 802.3bt 4-pair Power over Ethernet Plus Plus  RFC 768 UDP  RFC 783 TFTP  RFC 793 TCP  RFC 791 IP  RFC 792 ICMP  RFC 2068 HTTP  RFC 1112 IGMP v1  RFC 2236 IGMP v2  RFC 3376 IGMP v3  RFC 2710 MLD v1  RFC 3810 MLD v2  RFC 2328 OSPF v2  RFC 1058 RIP v1  RFC 2453 RIP v2  ITU-T G.8032 ERPS Ring</p>
<b>Environment</b>	
<b>Operating</b>	<p>Temperature: 0 ~ 50 degrees C  Relative Humidity: 5 ~ 90% (non-condensing)</p>
<b>Storage</b>	Temperature: -10 ~ 70 degrees C

	Relative Humidity: 5 ~ 90% (non-condensing)
--	---

**GS-6311 Series: (with PoE)**

Product	GS-6311-24HP4X	GS-6311-24P4XV	GS-6311-24PL4X	GS-6311-48P6X
<b>Hardware Specifications</b>				
<b>10/100/1000 RJ45 Ports</b>	24	24	24	48
<b>100/1000BASE-X SFP Ports</b>	--	--		--
<b>10G SFP+ Ports</b>	4	4	4	6
	10GBASE-SR/LR SFP+ interface Backward compatible with 1000BASE-SX/LX/BX SFP transceiver			
<b>Console Port</b>	1 x RJ45-to-RS232 serial port (9600, 8, N, 1)			
<b>CPU</b>	MIPS 800MHz	MIPS 800MHz	RTL9301-CG	MIPS 800MHz
<b>RAM</b>	512Mbytes	512Mbytes	4Gbytes	512Mbytes
<b>Flash Memory</b>	32Mbytes			
<b>Dimensions (W x D x H)</b>	440 x 207 x 44mm	440 x 207 x 44mm	440 x 330 x 44mm	440 x 330 x 44mm
<b>Weight</b>	3542g	3457g	4542g	5368g
<b>Power Consumption</b>	15 watts/ 51.1BTU (System)	14.5 watts/ 49.4BTU (System)	23.3 watts/ 79.5BTU (System)	39.9 watts/ 136BTU (System)
	540 watts/ 1841.4BTU (System+PoE)	425 watts/ 1449BTU (System+PoE)	745.5 watts/ 2544.8BTU (System+PoE)	698 watts/ 2380BTU (System+PoE)
<b>Power Requirements- AC</b>	AC 100~240V, 50/60Hz	AC 100~240V, 50/60Hz	AC 100~240V, 50/60Hz	AC 100~240V, 50/60Hz
<b>Fan</b>	2	2	4	5
<b>LED</b>	<b>System:</b> PWR (Green) SYS (Green)	<b>System:</b> PWR (Green) SYS (Green)	<b>System:</b> PWR (Green) SYS (Green)	<b>System:</b> PWR (Green) SYS (Green)
	<b>Ports:</b> LNK/ACT (Green) PoE-in-Use (Amber)	<b>Ports:</b> LNK/ACT (Green) PoE-in-Use (Amber)	<b>Ports:</b> LNK/ACT (Green) PoE-in-Use (Amber)	<b>Ports:</b> LNK/ACT (Green) PoE-in-Use (Amber)
<b>Switching Specifications</b>				
<b>Switch Architecture</b>	Store-and-forward			
<b>Switch Fabric</b>	128Gbps/non-blocking			216Gbps/non-blocking
<b>Switch Throughput</b>	95.23Mpps			160.7Mpps
<b>Address Table</b>	16K MAC address table with auto learning function			32K MAC address table with auto learning function
<b>ARP Table</b>	8K	8K	8K	8K
<b>Routing Table</b>	6K	6K	6K	12K
<b>IP Interface</b>	1024	1024	1024	1024

<b>ACL Table</b>	2K	2K	2K	4K
<b>Shared Data Buffer</b>	12MB	12MB	12MB	16MB
<b>Jumbo Frame</b>	12KBytes			
<b>Flow Control</b>	Back pressure for half duplex IEEE 802.3x pause frame for full duplex			
<b>Power over Ethernet Specifications</b>				
<b>PoE Standard</b>	IEEE 802.3bt PoE++ PSE (Ports 1 to 8) IEEE 802.3af/at PoE+ PSE (Ports 9 to 24)	IEEE 802.3at PoE+ PSE	IEEE 802.3at PoE+ PSE	IEEE 802.3at PoE+ PSE
<b>PoE Power Supply Type</b>	End-span/Mid-span/802.3bt (Ports 1 to 8) End-span (Ports 9 to 24)	End-span	End-span	End-span
<b>PoE Power Output</b>	Port 1-8 90W (max), Port 9-24 32W (max)	32W(MAX)	32W(MAX)	32W(MAX)
<b>Power Pin Assignment</b>	End-span: 1/2 (-), 3/6 (+) Mid-span: 4/5 (+), 7/8 (-) 802.3bt: 1/2 (-), 3/6 (+), 4/5 (+), 7/8 (-)	1/2(-), 3/6(+)	1/2(-), 3/6(+)	1/2(+), 3/6(-)
<b>PoE Power Budget</b>	480W (max.)	370W (max.)	720W (max.)	500W / 110V AC 600W / 220V AC
<b>IPv4 Layer 3 Functions</b>				
<b>IP Routing Protocol</b>	Static route RIPv1/v2 OSPFv2 BGP4 Hardware-based Layer 3 routing			
<b>Layer 3 Protocol</b>	ARP ARP Proxy IGMP Proxy			
<b>IPv6 Layer 3 Functions</b>				
<b>IP Routing Protocol</b>	IPv6 Static Route RIPng OSPFv3 BGP6 (BGP4+) PIM6 IPv6 RA (Router Advertisement) IPv6 LPM Routing Hardware-based Layer 3 routing SNMP over IPv6 Support IPv6 IPsec Support IPv6 ACL			



Other	ICMPv6,ND,DNSv6 DNS over IPv6 Support
<b>Layer 2 Functions</b>	
Port Configuration	Port disable/enable Flow control disable/enable Bandwidth control on each port Port loopback detect
Port Status	Display each port's speed duplex mode, link status, flow control status and auto negotiation status
VLAN	802.1Q tagged VLAN, up to 4K VLAN groups 802.1ad Q-in-Q (VLAN stacking) GVRP for VLAN management Private VLAN Edge (PVE) supported Protocol-based VLAN MAC-based VLAN IP subnet VLAN
<b>Bandwidth Control</b>	TX/RX/Both
<b>Link Aggregation</b>	IEEE 802.3ad LACP/static trunk Supports 64 groups with 8 ports per trunk group
<b>QoS</b>	8 priority queues on all switch ports Supports strict priority and Weighted Round Robin (WRR) CoS policies Traffic classification: <ul style="list-style-type: none"> <li>- IEEE 802.1p CoS/ToS</li> <li>- IPv4/IPv6 DSCP</li> <li>- Port-based WRR</li> </ul>
<b>Multicast</b>	IPv4 IGMP v1/v2/v3 snooping IPv4 Querier mode support IPv6 MLD v1/v2 snooping Multicast VLAN Register (MVR) Up to 1024
<b>Security Functions</b>	
<b>Access Control List</b>	Supports Standard and Expanded ACL IP-based ACL/MAC-based ACL Time-based ACL Up to 2K entries
<b>Security</b>	Port isolation Supports IP + MAC + port binding Identification and filtering of L2/L3/L4 based ACL Defend against DOS or TCP attacks Suppression of broadcast, multicast and unknown unicast packet DHCP Snooping, DHCP Option 82/43/60/61/67 Command line authority control based on user levels
<b>AAA</b>	TACACS+ and IPv4/IPv6 over RADIUS
<b>Authentication</b>	IEEE 802.1x port-based network access control
<b>Switch Management Functions</b>	
<b>System Configuration</b>	Console, Telnet, Web browser, SNMP v1, v2c
<b>Secure Management Interfaces</b>	SSHv2, TLSv1.2, SNMPv3

<p><b>Management</b></p>	<p>IPv4 and IPv6 dual stack management  SNMP over IPv6 Support  User IP security inspection for IPv4/IPv6 SNMP  SNMP v1, v2c and v3  SNMP MIB and TRAP  SNMP RMON 1, 2, 3, 9 four groups  HTTP over IPv6 Support  IPv4/IPv6 FTP/TFTP  IPv4/IPv6 SNTN/NTP  Supports ping, trace route function for IPv4 and IPv6  RADIUS authentication for IPv4/IPv6 Telnet user name and password  IPv4/IPv6 SSH`  IPv4/IPv6 Telnet  IPv6 Radius+ Support  The right configuration for users to adopt RADIUS server's shell management  CLI, console, Telnet  Security IP safety net management function: avoid unlawful landing at nonrestrictive area  Syslog server for IPv4 and IPv6  IPv6 TACACS+ support  PLANET Smart Discovery Utility  PLANET NMS  PLANET NMSViewerPro</p>
<p><b>SNMP MIBs</b></p>	<p>RFC 1213 MIB-II  RFC 1215 Internet Engineering Task Force  RFC 1271 RMON  RFC 1354 IP-Forwarding MIB  RFC 1493 Bridge MIB  RFC 1643 Ether-like MIB  RFC 1907 SNMP v2  RFC 2011 IP/ICMP MIB  RFC 2012 TCP MIB  RFC 2013 UDP MIB  RFC 2096 IP forward MIB  RFC 2233 if MIB  RFC 2452 TCP6 MIB  RFC 2454 UDP6 MIB  RFC 2465 IPv6 MIB  RFC 2466 ICMP6 MIB  RFC 2573 SNMP v3 notify  RFC 2574 SNMP v3 vacm  RFC 2674 Bridge MIB Extensions (IEEE 802.1Q MIB)  RFC 2674 Bridge MIB Extensions (IEEE 802.1P MIB)</p>
<p><b>Standard Conformance</b></p>	
<p><b>Regulatory Compliance</b></p>	<p>FCC Part 15 Class A, CE</p>
<p><b>Standards Compliance</b></p>	<p>IEEE 802.3 10BASE-T  IEEE 802.3u 100BASE-TX  IEEE 802.3z Gigabit 1000BASE-SX/LX  IEEE 802.3ab Gigabit 1000BASE-T  IEEE 802.3ae 10Gb/s Ethernet</p>

	<p>IEEE 802.3x flow control and back pressure  IEEE 802.3ad port trunk with LACP  IEEE 802.1ag CFM  IEEE 802.1D Spanning Tree Protocol  IEEE 802.1w Rapid Spanning Tree Protocol  IEEE 802.1s Multiple Spanning Tree Protocol  IEEE 802.1p Class of Service  IEEE 802.1Q VLAN tagging  IEEE 802.1X port authentication network control  IEEE 802.1ab LLDP  IEEE 802.3af Power over Ethernet  IEEE 802.3at Power over Ethernet PLUS  IEEE 802.3bt 4-pair Power over Ethernet Plus Plus  RFC 768 UDP  RFC 783 TFTP  RFC 793 TCP  RFC 791 IP  RFC 792 ICMP  RFC 2068 HTTP  RFC 1112 IGMP v1  RFC 2236 IGMP v2  RFC 3376 IGMP v3  RFC 2710 MLD v1  RFC 3810 MLD v2  RFC 2328 OSPF v2  RFC 1058 RIP v1  RFC 2453 RIP v2  ITU-T G.8032 ERPS Ring</p>
<b>Environment</b>	
<b>Operating</b>	<p>Temperature: 0 ~ 50 degrees C  Relative Humidity: 5 ~ 90% (non-condensing)</p>
<b>Storage</b>	<p>Temperature: -10 ~ 70 degrees C  Relative Humidity: 5 ~ 90% (non-condensing)</p>

MGS-6311/XGS-6311 Series:

Product	MGS-6311-8P2X	MGS-6311-10T2X	XGS-6311-12X	XGS-6311-8T4XR
<b>Hardware Specifications</b>				
<b>10/100/1000/2500 RJ45 Ports</b>	8	8	--	--
<b>100/1G/2.5G/5G/10G RJ45 Ports</b>	--	2	--	8
<b>10G SFP+ Ports</b>	2	2	12	4
	10GBASE-SR/LR SFP+ interface Backward compatible with 1G/2.5GBASE-SX/LX/BX SFP transceiver			
<b>Console Port</b>	1 x RJ45-to-RS232 serial port (9600, 8, N, 1)			
<b>CPU</b>	MIPS 800MHz			
<b>RAM</b>	512Mbytes			
<b>Flash Memory</b>	32Mbytes			
<b>Dimensions (W x D x H)</b>	330 x 230 x 43.6 mm, 1U height	330 x 230 x 43.6 mm, 1U height	330 x 230 x 43.6 mm, 1U height	441.5 x 207.5 x 44 mm, 1U height
<b>Weight</b>	2172g	1953g	1988g	2831g
<b>Power Consumption</b>	10.7 watts / 36.4BTU (System) 174 watts/ 593.3 BTU (System+PoE)	26.6 watts/ 90.7 BTU	30.2 watts/102.9 BTU	56 watts/190.96 BTU
<b>Power Requirements-AC</b>	AC 100~240V, 50/60Hz	AC 100~240V, 50/60Hz	AC 100~240V, 50/60Hz	Dual AC 100~240V, 50/60Hz
<b>Fan</b>	1	1	1	2
<b>LED</b>	<b>System:</b> PWR (Green), SYS (Green)	<b>System:</b> PWR (Green), SYS (Green)	<b>System:</b> PWR (Green), SYS (Green)	<b>System:</b> PWR (Green), SYS (Green)
	<b>Ports:</b> <b>Per 2.5GBASE-T RJ45 Port:</b> 2500Mbps LNK/ACT (Green) 10/100/1000Mbps LNK/ACT (Amber) 802.3at/af PoE-in-Use (Amber) <b>Per 10GBASE-X SFP Port:</b> 10G LNK/ACT (Green) 1G LNK/ACT (Amber)	<b>Ports:</b> <b>Per 2.5GBASE-T RJ45 Port:</b> 2500Mbps LNK/ACT (Green) 10/100/1000Mbps LNK/ACT (Amber) <b>Per 10GBASE-T RJ45 Port:</b> 10G LNK/ACT (Green) 100/1G/2.5G/5G LNK/ACT (Amber) <b>Per 10GBASE-X SFP Port:</b> 10G LNK/ACT (Green) 1G LNK/ACT (Amber)	<b>Ports:</b> <b>Per 10GBASE-X SFP+ Port:</b> 10G LNK/ACT (Green) 1G LNK/ACT (Amber)	<b>Ports:</b> <b>Per 10GBASE-T RJ45 Port:</b> 10G LNK/ACT (Green) 100/1G/2.5G/5GLN K/ACT (Amber) <b>Per 10GBASE-X SFP+ Port:</b> 10G LNK/ACT (Green) 1G/2.5G LNK/ACT (Amber)

Switching Specifications				
Switch Architecture	Store-and-forward	Store-and-forward	Store-and-forward	Store-and-forward
Switch Fabric	80Gbps/non-blocking	120Gbps/non-blocking	240Gbps/non-blocking	240Gbps/non-blocking
Switch Throughput	59.52Mpps	89.28Mpps	178.56Mpps	178.56Mpps
Address Table	16K MAC address table with auto learning function	16K MAC address table with auto learning function	32K MAC address table with auto learning function	32K MAC address table with auto learning function
ARP Table	8K	8K	8K	8K
Routing Table	6K	6K	12K	12K
IP Interface	1024	1024	1024	1024
ACL Table	4K	4K	4K	4K
Shared Data Buffer	12MB	12MB	16MB	16MB
Multicast Table	1K	1K	1K	1K
Jumbo Frame	12KBytes			
Flow Control	Back pressure for half duplex IEEE 802.3x pause frame for full duplex			
Power over Ethernet Specifications				
PoE Standard	IEEE 802.3at PoE+ PSE	--	--	--
PoE Power Supply Type	End-span	--	--	--
PoE Power Output	32W(max.)	--	--	--
Power Pin Assignment	1/2(-), 3/6(+)	--	--	--
PoE Power Budget	150 watts (max.)	--	--	--
IPv4 Layer 3 Functions				
IP Routing Protocol	Static route RIPv1/v2 OSPFv2 BGP4 Hardware-based Layer 3 routing			
Layer 3 Protocol	ARP ARP Proxy IGMP Proxy			
IPv6 Layer 3 Functions				
IP Routing Protocol	IPv6 Static Route RIPng OSPFv3 BGP6 (BGP4+) PIM6 IPv6 RA (Router Advertisement) IPv6 LPM Routing Hardware-based Layer 3 routing SNMP over IPv6 Support IPv6 IPsec Support IPv6 ACL			
Other	ICMPv6,ND,DNSv6			

	DNS over IPv6 Support
<b>Layer 2 Functions</b>	
Port Configuration	Port disable/enable Flow control disable/enable Bandwidth control on each port Port loopback detect
Port Status	Display each port's speed duplex mode, link status, flow control status and auto negotiation status
VLAN	802.1Q tagged VLAN, up to 4K VLAN groups 802.1ad Q-in-Q (VLAN stacking) GVRP for VLAN management Private VLAN Edge (PVE) supported Protocol-based VLAN MAC-based VLAN IP subnet VLAN
<b>Bandwidth Control</b>	TX/RX/Both
<b>Link Aggregation</b>	IEEE 802.3ad LACP/static trunk Supports 64 groups with 8 ports per trunk group
<b>QoS</b>	8 priority queues on all switch ports Supports strict priority and Weighted Round Robin (WRR) CoS policies Traffic classification: - IEEE 802.1p CoS/ToS - IPv4/IPv6 DSCP - Port-based WRR
<b>Multicast</b>	IPv4 IGMP v1/v2/v3 snooping IPv4 Querier mode support IPv6 MLD v1/v2 snooping Multicast VLAN Register (MVR) Up to 1024
<b>Security Functions</b>	
<b>Access Control List</b>	Supports Standard and Expanded ACL IP-based ACL/MAC-based ACL Time-based ACL Up to 2K entries
<b>Security</b>	Port isolation Supports IP + MAC + port binding Identification and filtering of L2/L3/L4 based ACL Defend against DOS or TCP attacks Suppression of broadcast, multicast and unknown unicast packet DHCP Snooping, DHCP Option 82/43/60/61/67 Command line authority control based on user levels
<b>AAA</b>	TACACS+ and IPv4/IPv6 over RADIUS
<b>Authentication</b>	IEEE 802.1x port-based network access control
<b>Switch Management Functions</b>	
<b>System Configuration</b>	Console, Telnet, Web browser, SNMP v1, v2c
<b>Secure Management Interfaces</b>	SSHv2, TLSv1.2, SNMPv3
<b>Management</b>	IPv4 and IPv6 dual stack management

	<p>SNMP over IPv6 Support          User IP security inspection for IPv4/IPv6 SNMP          SNMP v1, v2c and v3          SNMP MIB and TRAP          SNMP RMON 1, 2, 3, 9 four groups          HTTP over IPv6 Supports          IPv4/IPv6 FTP/TFTP          IPv4/IPv6 SNTTP/NTP          Supports ping, trace route function for IPv4 and IPv6          RADIUS authentication for IPv4/IPv6 Telnet user name and password          IPv4/IPv6 SSH          IPv4/IPv6 Telnet          IPv6 Radius+ Support          The right configuration for users to adopt RADIUS server's shell management          CLI, console, Telnet          Security IP safety net management function: avoid unlawful landing at nonrestrictive area          Syslog server for IPv4 and IPv6          IPv6 TACACS+ support          PLANET Smart Discovery Utility          PLANET NMS          PLANET NMSViewerPro</p>
<p><b>SNMP MIBs</b></p>	<p>RFC 1213 MIB-II          RFC 1215 Internet Engineering Task Force          RFC 1271 RMON          RFC 1354 IP-Forwarding MIB          RFC 1493 Bridge MIB          RFC 1643 Ether-like MIB          RFC 1907 SNMP v2          RFC 2011 IP/ICMP MIB          RFC 2012 TCP MIB          RFC 2013 UDP MIB          RFC 2096 IP forward MIB          RFC 2233 if MIB          RFC 2452 TCP6 MIB          RFC 2454 UDP6 MIB          RFC 2465 IPv6 MIB          RFC 2466 ICMP6 MIB          RFC 2573 SNMP v3 notify          RFC 2574 SNMP v3 vacm          RFC 2674 Bridge MIB Extensions (IEEE 802.1Q MIB)          RFC 2674 Bridge MIB Extensions (IEEE 802.1P MIB)</p>
<p><b>Standard Conformance</b></p>	
<p><b>Regulatory Compliance</b></p>	<p>FCC Part 15 Class A, CE</p>
<p><b>Standards Compliance</b></p>	<p>IEEE 802.3 10BASE-T          IEEE 802.3u 100BASE-TX          IEEE 802.3z Gigabit 1000BASE-SX/LX          IEEE 802.3ab Gigabit 1000BASE-T          IEEE 802.3ae 10Gb/s Ethernet          IEEE 802.3x flow control and back pressure</p>

	<p>IEEE 802.3ad port trunk with LACP</p> <p>IEEE 802.1ag CFM</p> <p>IEEE 802.1D Spanning Tree Protocol</p> <p>IEEE 802.1w Rapid Spanning Tree Protocol</p> <p>IEEE 802.1s Multiple Spanning Tree Protocol</p> <p>IEEE 802.1p Class of Service</p> <p>IEEE 802.1Q VLAN tagging</p> <p>IEEE 802.1X port authentication network control</p> <p>IEEE 802.1ab LLDP</p> <p>IEEE 802.3af Power over Ethernet</p> <p>IEEE 802.3at Power over Ethernet PLUS</p> <p>RFC 768 UDP</p> <p>RFC 783 TFTP</p> <p>RFC 793 TCP</p> <p>RFC 791 IP</p> <p>RFC 792 ICMP</p> <p>RFC 2068 HTTP</p> <p>RFC 1112 IGMP v1</p> <p>RFC 2236 IGMP v2</p> <p>RFC 3376 IGMP v3</p> <p>RFC 2710 MLD v1</p> <p>RFC 3810 MLD v2</p> <p>RFC 2328 OSPF v2</p> <p>RFC 1058 RIP v1</p> <p>RFC 2453 RIP v2</p> <p>ITU-T G.8032 ERPS Ring</p>
<b>Environment</b>	
<b>Operating</b>	<p>Temperature: 0 ~ 50 degrees C</p> <p>Relative Humidity: 5 ~ 90% (non-condensing)</p>
<b>Storage</b>	<p>Temperature: -10 ~ 70 degrees C</p> <p>Relative Humidity: 5 ~ 90% (non-condensing)</p>



# Chapter 2 Installation

This section describes the hardware features and installation of the Managed Switch on the desktop or rack mount. For easier management and control of the Managed Switch, familiarize yourself with its display indicators, and ports. Front panel illustrations in this chapter display the unit LED indicators. Before connecting any network device to the Managed Switch, please read this chapter completely.

## 2.1 Hardware Description

### 2.1.1 Switch Front Panel

The unit front panel provides a simple interface monitoring the switch. Are show the front panel of the Managed Switches as below.

#### GS-6311-16S8C4XR Front Panel



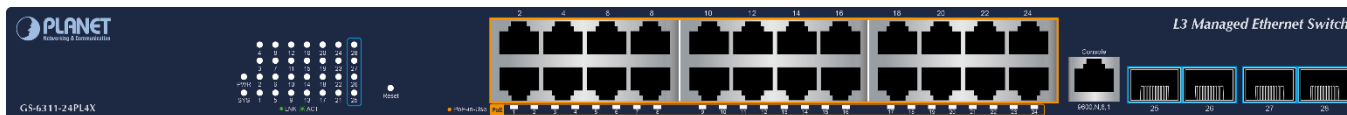
#### GS-6311-24HP4X Front Panel



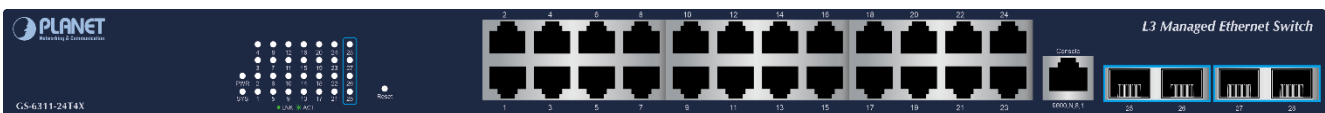
#### GS-6311-24P4XV Front Panel



#### GS-6311-24PL4X Front Panel



#### GS-6311-24T4X Front Panel



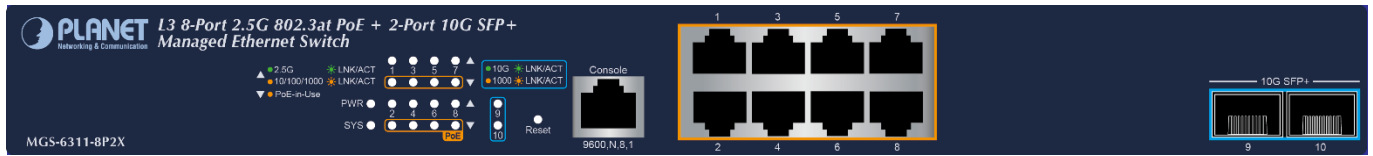
#### GS-6311-48P6X Front Panel



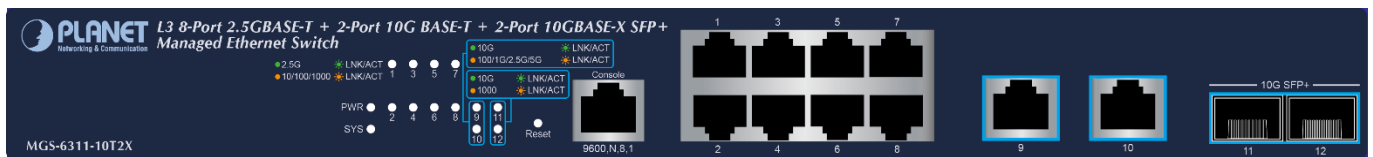
### GS-6311-48T6X Front Panel



### MGS-6311-8P2X Front Panel



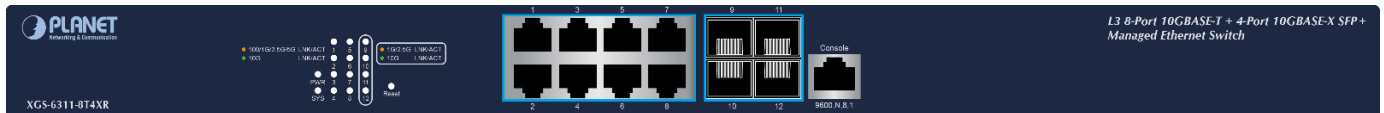
### MGS-6311-10T2X Front Panel



### XGS-6311-12X Front Panel



### XGS-6311-8T4XR Front Panel



#### ■ Gigabit TP interface

10/100/1000BASE-T copper, RJ45 twisted-pair: Up to 100 meters.

#### ■ SFP/SFP+ slots

SFP/SFP+ mini-GBIC slot, SFP (Small Factor Pluggable) transceiver module: From 550 meters (Multi-mode fiber) to 10/30/50/70/120 kilometers (Single-mode fiber).

#### ■ Console Port

The console port is an RJ45 type, RS232 male serial port connector. It is an interface for connecting a terminal directly. Through the console port, it provides rich diagnostic information including IP address setting, factory reset, port management, link status and system setting. Users can use the attached RS232 cable in the package and connect to the console port on the device. After the connection, users can run any terminal emulation program (Hyper Terminal, ProComm Plus, Telix, Winterm and so on) to enter the startup screen of the device.

## 2.1.2 LED Indications

The front panel LEDs indicate instant status of port links, data activity, system operation, stack status and system power, and helps monitor and troubleshoot when needed.

### GS-6311-24T4X



Figure GS-6311-24T4X front panel

#### ■ System

LED	Color	Function
PWR	Green	Lights to indicate that the Switch has power.
	Off	Power is off.
SYS	Green	Lights: to indicate the system is normally starting up.

#### ■ Interfaces

LED	Color	Function	
LNK/ACT	Green	<b>Lights</b>	Indicating the port is running and the connection is successfully established.
		<b>Blinks</b>	Indicating that the switch is actively sending or receiving data over that port.

GS-6311-24HP4X

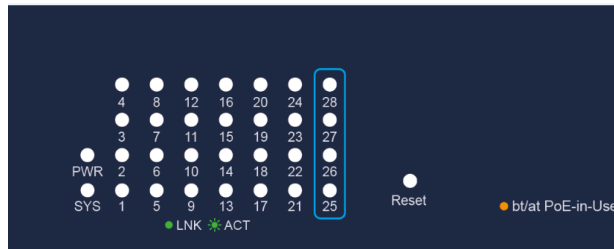


Figure GS-6311-24HP4X front panel

■ System

LED	Color	Function
PWR	Green	Lights to indicate that the Switch has power.
	Off	Power is off.
SYS	Green	Lights to indicate the system is normally starting up.

■ Interfaces

LED	Color	Function	
LNK/ACT	Green	Lights	Indicating the port is running and the connection is successfully established.
		Blinks	Indicating that the switch is actively sending or receiving data over that port.
PoE-in-Use	Amber	Lights	PD is connected and PoE power supply is normal.
		Off	PD is not connected or PoE power supply is not provided.

GS-6311-24P4XV



Figure GS-6311-24P4XV front panel

■ System

LED	Color	Function
PWR	Green	Lights to indicate that the Switch has power.
	Off	Power is off.
SYS	Green	Lights to indicate the system is normally starting up.

■ Interfaces

LED	Color	Function	
LNK/ACT	Green	Lights	Indicating the port is running and the connection is successfully established.
		Blinks	Indicating that the switch is actively sending or receiving data over that port.
PoE-in-Use	Amber	Lights	PD is connected and PoE power supply is normal.
		Off	PD is not connected or PoE power supply is not provided.

GS-6311-24PL4X

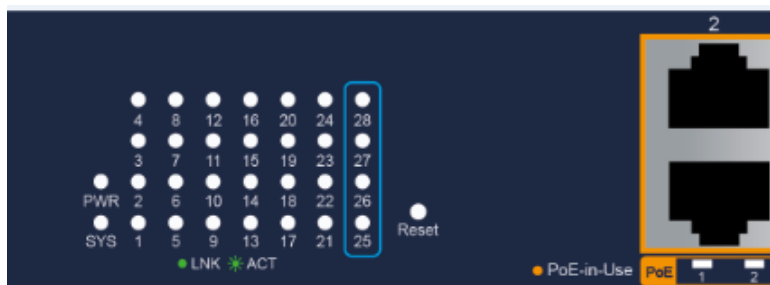


Figure GS-6311-24PL4X front panel

■ System

LED	Color	Function
PWR	Green	Lights to indicate that the Switch has power.
	Off	Power is off.
SYS	Green	Lights to indicate the system is normally starting up.

■ Interfaces

LED	Color	Function	
LNK/ACT	Green	Lights	Indicating the port is running and the connection is successfully established.
		Blinks	Indicating that the switch is actively sending or receiving data over that port.
PoE-in-Use	Amber	Lights	PD is connected and PoE power supply is normal.
		Off	PD is not connected or PoE power supply is not provided.

GS-6311-16S8C4XR

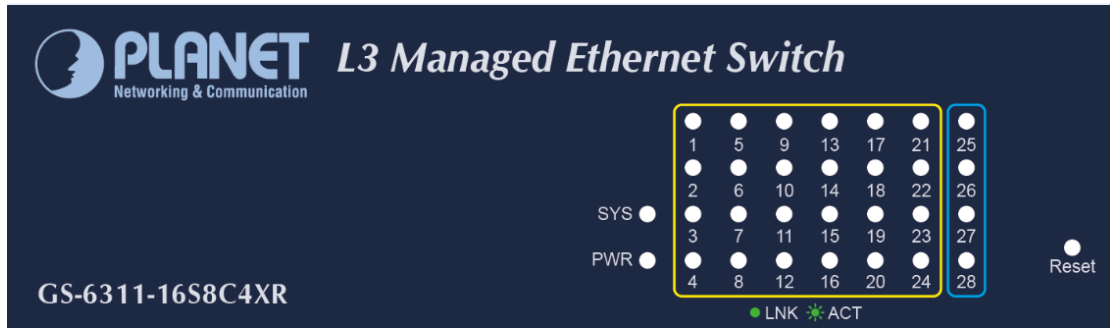


Figure GS-6311-16S8C4XR front panel

■ System

LED	Color	Function
PWR	Green	Lights to indicate that the Switch has power.
	Off	Power is off.
SYS	Green	Lights to indicate the system is normally starting up.

■ Interfaces

LED	Color	Function	
LNK/ACT	Green	<b>Lights</b>	Indicating the port is running and the connection is successfully established.
		<b>Blinks</b>	Indicating that the switch is actively sending or receiving data over that port.

GS-6311-48T6X

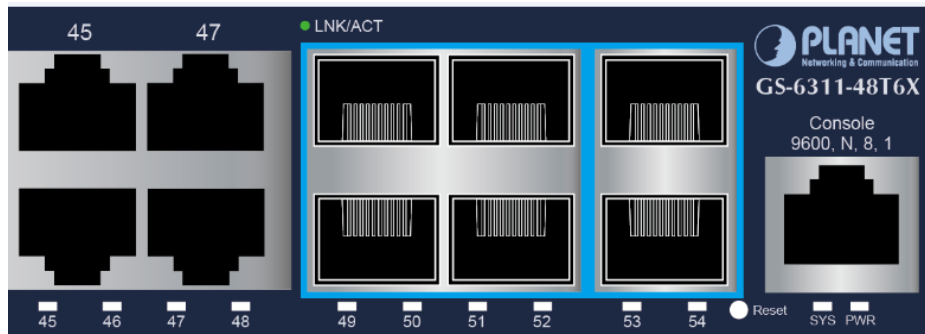


Figure GS-6311-48T6X front panel

■ System

LED	Color	Function
PWR	Green	Lights to indicate that the Switch has power.
	Off	Power is off.
SYS	Green	Lights to indicate the system is normally starting up.

■ Interfaces

LED	Color	Function	
LNK/ACT	Green	Lights	Indicating the port is running and the connection is successfully established.
		Blinks	Indicating that the switch is actively sending or receiving data over that port.



GS-6311-48P6X

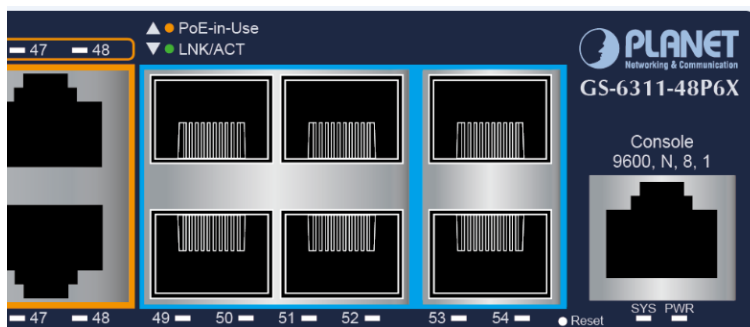


Figure GS-6311-48P6X front panel

■ System

LED	Color	Function
PWR	Green	Lights to indicate that the Switch has power.
	Off	Power is off.
SYS	Green	Lights to indicate the system is normally starting up.

■ Interfaces

LED	Color	Function	
LNK/ACT	Green	Lights	Indicating the port is running and the connection is successfully established.
		Blinks	Indicating that the switch is actively sending or receiving data over that port.
PoE-in-Use	Amber	Lights	PD is connected and PoE power supply is normal.
		Off	PD is not connected or PoE power supply is not provided.

MGS-6311-8P2X

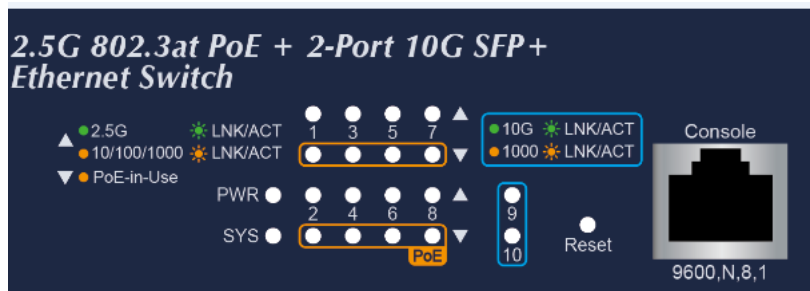


Figure MGS-6311-8P2X front panel

■ System

LED	Color	Function
PWR	Green	Lights to indicate that the Switch has power.
	Off	Power is off.
SYS	Green	Lights to indicate the system is normally starting up.

■ Per 10/100/1000/2500BASE-T RJ45 Port (Ports 1 to 8)

LED	Color	Function	
2.5G LNK/ACT	Green	Lights:	To indicate the port is running at <b>2500Mbps</b> and successfully established.
		Blinks:	To indicate that the switch is actively sending or receiving data over that port.
10/100/1000 LNK/ACT	Amber	Lights:	To indicate the port is running at <b>10/100/1000Mbps</b> and successfully established.
		Blinks:	To indicate that the switch is actively sending or receiving data over that port.
PoE In-Use	Amber	Lights	PD is connected and PoE power supply is normal.
		Off	PD is not connected or PoE power supply is not provided.

■ Per 1G/10G BASE-SR/LR SFP+ Port (Ports 9 to 10)

LED	Color	Function	
10G LNK/ACT	Green	Lights	To indicate the port is running at 10Gbps and successfully established
		Blinks	Indicating that the switch is actively sending or receiving data over that port.
1G LNK/ACT	Amber	Lights	To indicate the port is running at 1Gbps.
		Blinks	Indicating that the switch is actively sending or receiving data over that port.

MGS-6311-10T2X

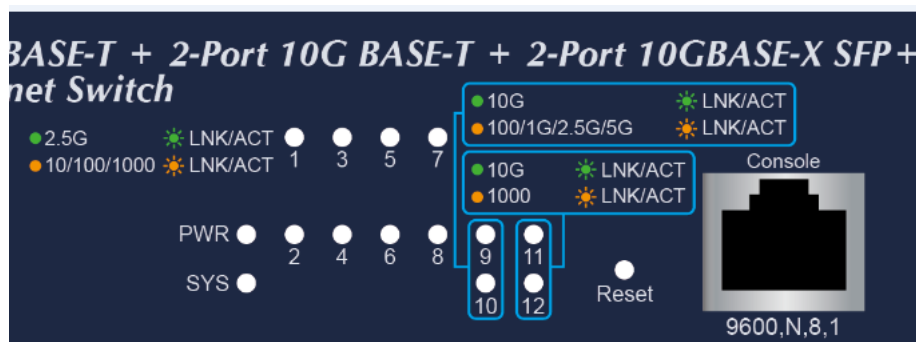


Figure MGS-6311-10T2X front panel

■ System

LED	Color	Function
PWR	Green	Lights to indicate that the Switch has power.
	Off	Power is off.
SYS	Green	Lights to indicate the system is normally starting up.

■ Per 10/100/1000/2500BASE-T RJ45 Port (Ports 1 to 8)

LED	Color	Function	
2.5G LNK/ACT	Green	Lights:	To indicate the port is running at <b>2500Mbps</b> and successfully established.
		Blinks:	To indicate that the switch is actively sending or receiving data over that port.
10/100/1000 LNK/ACT	Amber	Lights:	To indicate the port is running at <b>10/100/1000Mbps</b> and successfully established.
		Blinks:	To indicate that the switch is actively sending or receiving data over that port.

■ Per 100/1G/2.5G/5G/10GBASE-T RJ45 Port (Ports 9 to 10)

LED	Color	Function	
10G LNK/ACT	Green	Lights:	To indicate the port is running at <b>10Gbps</b> and successfully established.
		Blinks:	To indicate that the switch is actively sending or receiving data over that port.
100/1G/2.5G/5G LNK/ACT	Amber	Lights:	To indicate the port is running at <b>100/1G/2.5G/5Gbps</b> and successfully established.
		Blinks:	To indicate that the switch is actively sending or receiving data over that port.

■ Per 1G/10G BASE-SR/LR SFP+ Port (Ports 11 to 12)

LED	Color	Function	
10G LNK/ACT	Green	Lights	To indicate the port is running at 10Gbps and successfully established
		Blinks	Indicating that the switch is actively sending or receiving data over that port.
1G LNK/ACT	Amber	Lights	To indicate the port is running at 1Gbps.
		Blinks	Indicating that the switch is actively sending or receiving data over that port.

XGS-6311-12X



Figure XGS-6311-12X front panel

■ System

LED	Color	Function
PWR	Green	Lights to indicate that the Switch has power.
	Off	Power is off.
SYS	Green	Lights to indicate the system is normally starting up.

■ Per 1G/10G BASE-SR/LR SFP+ Port (Ports 1 to 12)

LED	Color	Function	
10G LNK/ACT	Green	Lights	To indicate the port is running at 10Gbps and successfully established
		Blinks	Indicating that the switch is actively sending or receiving data over that port.
1G LNK/ACT	Amber	Lights	To indicate the port is running at 1Gbps.
		Blinks	Indicating that the switch is actively sending or receiving data over that port.

XGS-6311-8T4XR

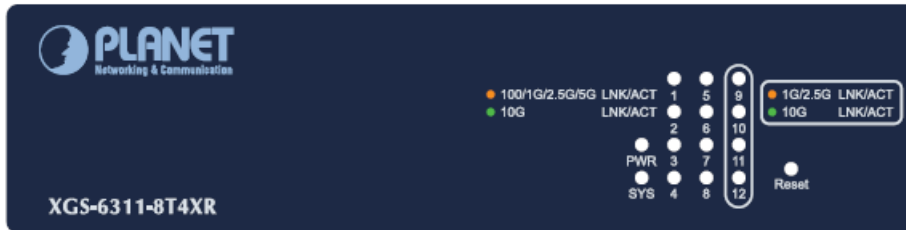


Figure XGS-6311-8T4XR front panel

■ System

LED	Color	Function
PWR	Green	Lights to indicate that the Switch has power.
	Off	Power is off.
SYS	Green	Lights to indicate the system is normally starting up.

■ 100/1G/2.5G/5G/10GBASE-T RJ45 (Ports 1 to 8)

LED	Color	Function	
10G LNK/ACT	Green	Lights:	To indicate the port is running at <b>10Gbps</b> and successfully established.
		Blinks:	To indicate that the switch is actively sending or receiving data over that port.
100/1G/2.5G/5G LNK/ACT	Amber	Lights:	To indicate the port is running at <b>100/1G/2.5G/5Gbps</b> and successfully established.
		Blinks:	To indicate that the switch is actively sending or receiving data over that port.

■ 1G/2.5G/10G BASE-SR/LR SFP+ (Ports 9 to 12)

LED	Color	Function	
10G LNK/ACT	Green	Lights	To indicate the port is running at 10Gbps and successfully established
		Blinks	To indicate that the switch is actively sending or receiving data over that port.
1G/2.5G LNK/ACT	Amber	Lights	To indicate the port is running at 1G/2.5Gbps.
		Blinks	To indicate that the switch is actively sending or receiving data over that port.

## 2.2 Switch Installation

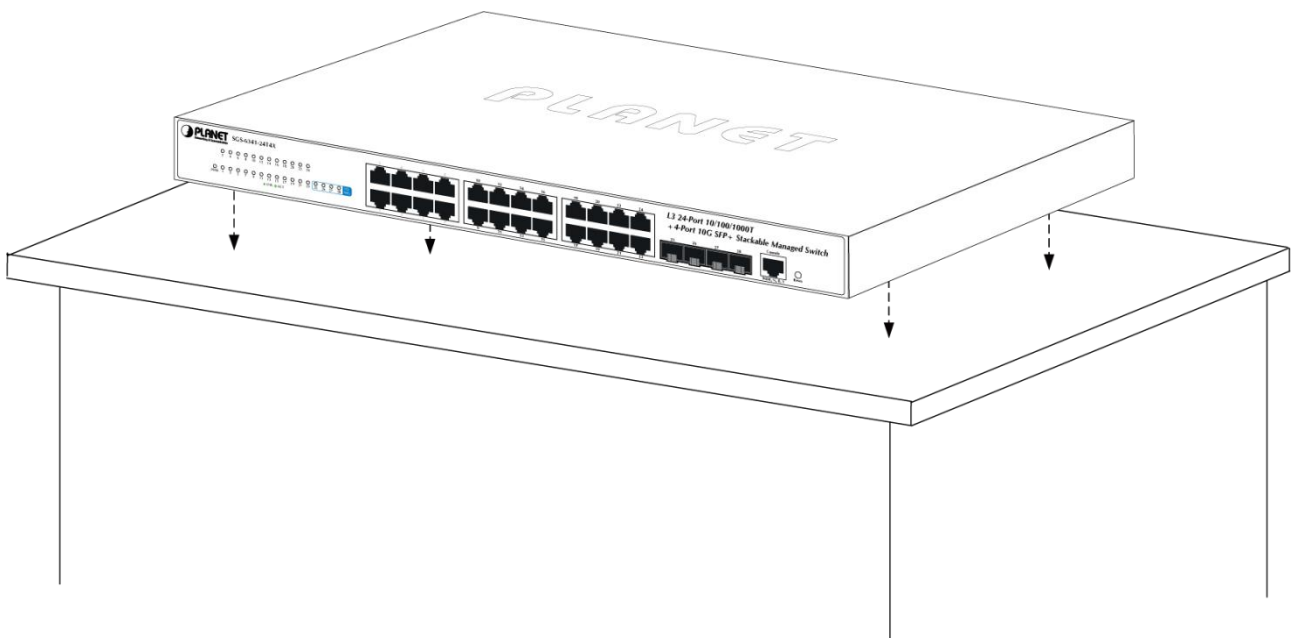
This section describes how to install your Managed Switch and make connections to the Managed Switch. Please read the following topics and perform the procedures in the order being presented. To install your Managed Switch on a desktop or shelf, simply complete the following steps.

### 2.2.1 Desktop Installation

To install the Managed Switch on desktop or shelf, please follow these steps:

**Step 1:** Attach the rubber feet to the recessed areas on the bottom of the Managed Switch.

**Step 2:** Place the Managed Switch on the desktop or the shelf near an AC power source, as shown in [Figure 2-2-1](#).



**Figure 2-2-1** Place the Managed Switch on the desktop

**Step 3:** Keep enough ventilation space between the Managed Switch and the surrounding objects.



---

When choosing a location, please keep in mind the environmental restrictions discussed in Chapter 1, Section 4 under **Specifications**.

---

**Step 4: Connect the Managed Switch to network devices.**

Connect one end of a standard network cable to the 10/100/1000 RJ45 ports on the front of the Managed Switch and connect the other end of the cable to the network devices such as printer servers, workstations or routers, etc.



---

Connection to the Managed Switch requires UTP Category 5 network cabling with RJ45 tips. For more information, please see the Cabling Specification in Appendix A.

---

**Step 5: Supply power to the Managed Switch.**

Connect one end of the power cable to the Managed Switch.

Connect the power plug of the power cable to a standard wall outlet.

When the Managed Switch receives power, the Power LED should remain solid Green.



## 2.2.2 Rack Mounting

To install the Managed Switch in a 19-inch standard rack, please follow the instructions described below:

**Step 1:** Place the Managed Switch on a hard flat surface, with the front panel positioned towards the front side.

**Step 2:** Attach the rack-mount bracket to each side of the Managed Switch with supplied screws attached to the package.

Figure 2-2-2 shows how to attach brackets to one side of the Managed Switch.

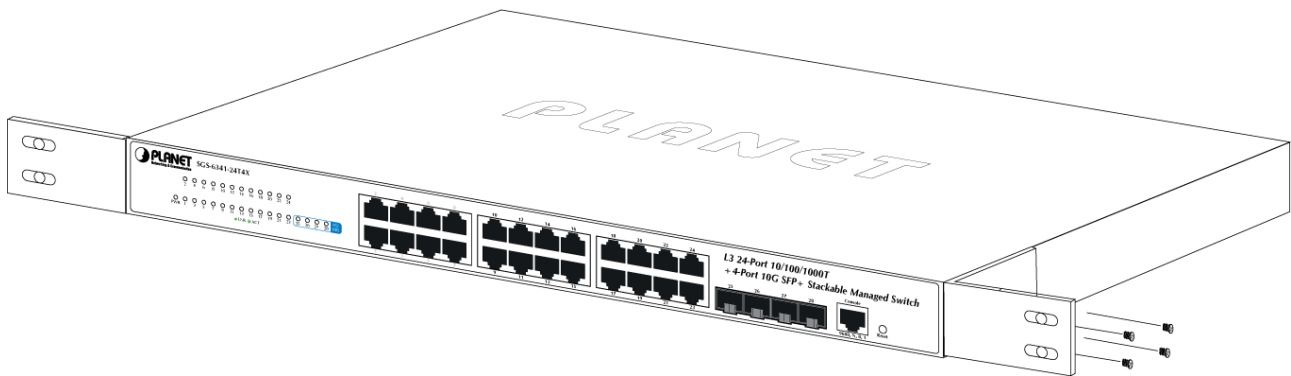


Figure 2-2-2 Attach brackets to the Managed Switch.



---

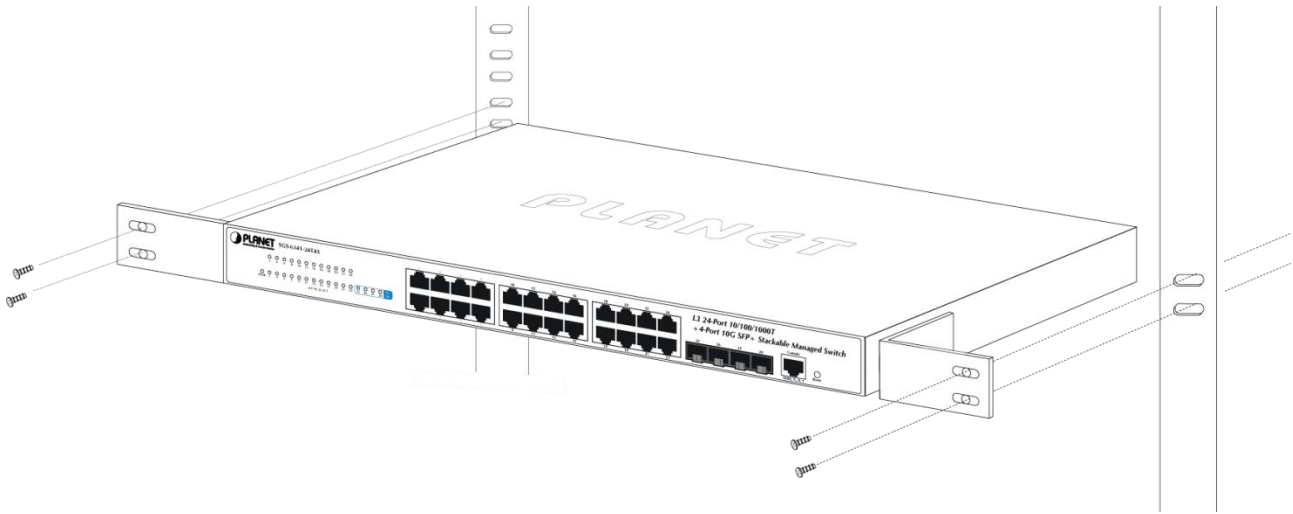
You must use the screws supplied with the mounting brackets. Damage caused to the parts by using incorrect screws would invalidate the warranty.

---

**Step 3:** Secure the brackets tightly.

**Step 4:** Follow the same steps to attach the second bracket to the opposite side.

**Step 5:** After the brackets are attached to the Managed Switch, use suitable screws to securely attach the brackets to the rack, as shown in [Figure 2-2-3](#).

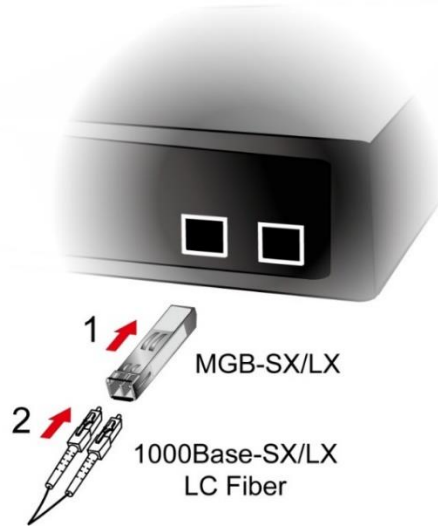


**Figure 2-2-3** Mounting X(M)GS-6311 Series in a Rack

**Step 6:** Proceed with Steps 4 and 5 of Session 2.2.1 Desktop Installation to connect the network cabling and supply power to the Managed Switch.

## 2.2.3 Installing the SFP/SFP+ Transceiver

The sections describe how to insert an SFP/SFP+ transceiver into an SFP/SFP+ slot. The SFP/SFP+ transceivers are hot-pluggable and hot-swappable. You can plug in and out the transceiver to/from any SFP/SFP+ port without having to power down the Managed Switch, as the [Figure 2-16](#) shows.



**Figure 2-16** Plug in the SFP transceiver

### ➤ Approved PLANET SFP/SFP+ Transceivers

PLANET Managed Switch supports both single mode and multi-mode SFP/SFP+ transceivers. The following list of approved PLANET SFP/SFP+ transceivers is correct at the time of publication:

#### 10Gigabit Ethernet Transceiver

MTB-LB40	1-Port 10GBASE-BX SFP+ Fiber Optic Module - 40km (TX:1330nm RX:1270nm)
MTB-LA40	1-Port 10GBASE-BX SFP+ Fiber Optic Module - 40km (TX:1270nm RX:1330nm)
MTB-LB20	1-Port 10GBASE-BX SFP+ Fiber Optic Module - 20km (TX:1330nm RX:1270nm)
MTB-LA20	1-Port 10GBASE-BX SFP+ Fiber Optic Module - 20km (TX:1270nm RX:1330nm)
MTB-SR	1-Port 10GBASE-SR SFP+ Fiber Optic Module - 300m
MTB-LR	1-Port 10GBASE-LR SFP+ Fiber Optic Module - 10km
MTB-LA60	1-Port 10GBASE-BX SFP+ Fiber Optic Module - 60km (TX:1270nm RX:1330nm)
MTB-LB60	1-Port 10GBASE-BX SFP+ Fiber Optic Module - 60km (TX:1330nm RX:1270nm)
MTB-RJ	1-Port 10GBASE-T SFP+ Copper Fiber Optic Module - 30m
MTB-LR40	1-Port 10GBASE-LR SFP+ Fiber Optic Module - 40km
MTB-SR2	1-Port 10GBASE-SR SFP+ Fiber Optic Module – 2km
MTB-LR20	1-Port 10GBASE-LR SFP+ Fiber Optic Module - 20km
MTB-LR60	1-Port 10GBASE-LR SFP+ Fiber Optic Module - 60km
MTB-LR80	1-Port 10GBASE-LR SFP+ Fiber Optic Module - 80km
MTB-LA10	1-Port 10GBASE-BX SFP+ Fiber Optic Module - 10km (TX:1270nm RX:1330nm)
MTB-LB10	1-Port 10GBASE-BX SFP+ Fiber Optic Module - 10km (TX:1330nm RX:1270nm)

### Gigabit Ethernet Transceiver (1000BASE-X SFP)

MGB-GT	SFP-Port 1000BASE-T Module
MGB-LX	SFP-Port 1000BASE-LX mini-GBIC module - 20km
MGB-SX	SFP-Port 1000BASE-SX mini-GBIC module - 550m
MGB-SX2	SFP-Port 1000BASE-SX mini-GBIC module - 2km
MGB-L40	SFP-Port 1000BASE-LX mini-GBIC module - 40km
MGB-L80	SFP-Port 1000BASE-LX mini-GBIC module - 80km
MGB-L120	SFP-Port 1000BASE-LX mini-GBIC module - 120km
MGB-LA10	SFP-Port 1000BASE-BX (WDM, TX:1310nm) mini-GBIC module - 10km
MGB-LB10	SFP-Port 1000BASE-BX (WDM, TX:1550nm) mini-GBIC module - 10km
MGB-LA20	SFP-Port 1000BASE-BX (WDM, TX:1310nm) mini-GBIC module - 20km
MGB-LB20	SFP-Port 1000BASE-BX (WDM, TX:1550nm) mini-GBIC module - 20km
MGB-LA40	SFP-Port 1000BASE-BX (WDM, TX:1310nm) mini-GBIC module - 40km
MGB-LB40	SFP-Port 1000BASE-BX (WDM, TX:1550nm) mini-GBIC module - 40km
MGB-LA80	SFP-Port 1000BASE-BX (WDM, TX:1490nm) mini-GBIC module - 80km
MGB-LB80	SFP-Port 1000BASE-BX (WDM, TX:1550nm) mini-GBIC module - 80km



It is recommended to use PLANET SFP/SFP+ on the Managed Switch. If you insert an SFP/SFP+ transceiver that is not supported, the Managed Switch will not recognize it.

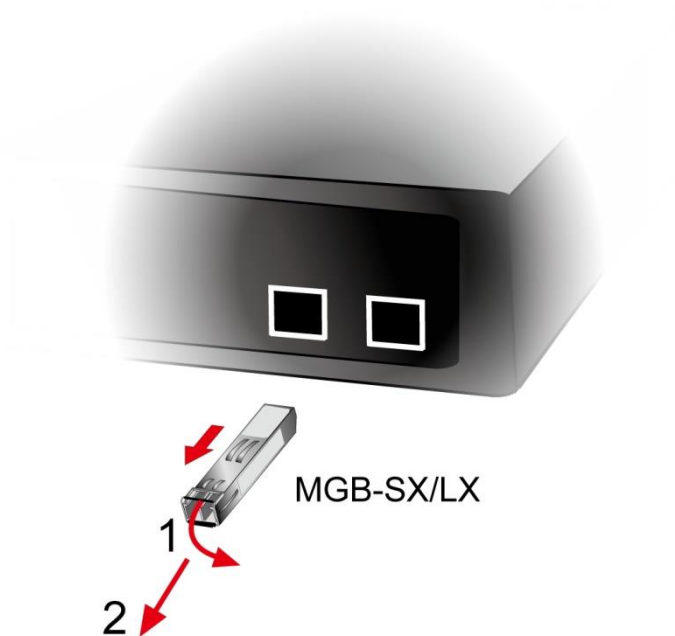
1. Before we connect the X(M)GS-6311 series to the other network device, we have to make sure both sides of the SFP transceivers are with the same media type, for example: 1000BASE-SX to 1000BASE-SX, 1000BASE-LX to 1000BASE-LX.
2. Check whether the fiber-optic cable type matches with the SFP transceiver requirement.
  - To connect to 1000BASE-SX SFP transceiver, please use the multi-mode fiber cable with one side being the male duplex LC connector type.
  - To connect to 1000BASE-LX SFP transceiver, please use the single-mode fiber cable with one side being the male duplex LC connector type.

#### ■ Connect the Fiber Cable

1. Insert the duplex LC connector into the SFP/SFP+ transceiver.
2. Connect the other end of the cable to a device with SFP/SFP+ transceiver installed.
3. Check the LNK/ACT LED of the SFP/SFP+ slot on the front of the Managed Switch. Ensure that the SFP/SFP+ transceiver is operating correctly.
4. Check the Link mode of the SFP/SFP+ port if the link fails. To function with some fiber-NICs or Media Converters, user has to set the port Link mode to **“10G Force”**, **“1000M Force”** or **“100M Force”**.

■ **Remove the Transceiver Module**

1. Make sure there is no network activity anymore.
2. Remove the Fiber-Optic Cable gently.
3. Lift up the lever of the MGB module and turn it to a horizontal position.
4. Pull out the module gently through the lever.



**Figure 2-17:** How to Pull Out the SFP/SFP+ Transceiver



Note

Never pull out the module without lifting up the lever of the module and turning it to a horizontal position. Directly pulling out the module could damage the module and the SFP/SFP+ module slot of the Managed Switch.

## 2.2.4 AC Power Receptacle

Compatible with electrical services in most areas of the world, the Managed Switch's power supply automatically adjusts to line power in the range of 100-240VAC and 50/60 Hz.

Plug the female end of the power cord firmly into the receptacle on the rear panel of the Managed Switch. Plug the other end of the power cord into an electrical outlet and then the power will be ready.

# Chapter 3 Switch Management

## 3.1 Management Options

To set up the Managed Switch, the user needs to configure the Managed Switch for network management. The Managed Switch provides two management options: Out-of-Band Management and In-Band Management.

## 3.2 Out-Of-Band Management

Out-of-band management is the management through Console interface. Generally, the user will use out-of-band management for the initial switch configuration, or when in-band management is not available. For instance, the X(M)GS-6311 series default IP address is 192.168.0.254 or the user can try to assign a new IP address to the switch via the Console interface to be able to access the switch through Telnet.

## 3.3 In-band Management

In-band management refers to the management by logging in to the Managed Switch using Telnet or HTTP, or using SNMP management software to configure the Managed Switch. In-band management enables the management of the Managed Switch to attach some devices to the Switch. The following procedures are required to enable in-band management:

1. Log on to console
2. Assign/Configure IP address
3. Create a remote login account
4. Enable HTTP or Telnet server on the Managed Switch

In case in-band management fails due to Managed Switch configuration changes, out-of-band management can be used for configuring and managing the Managed Switch.

---

The Managed Switch is shipped with **VLAN1 interface** IP address **192.168.0.254/24** assigned by **Important!** default. User can assign another IP address to the Managed Switch via the console interface to be able to remotely access the Managed Switch through Telnet or HTTP.

---

### 3.4 Requirements

Workstations running Windows 10/11, macOS 10.12 or later, Linux Kernel 2.6.18 or later, or other modern operating systems are compatible with TCP/IP Protocols.

Workstations are installed with Ethernet NIC (Network Interface Card)

Serial Port Connection (Terminal)

- 1) The above Workstations come with COM Port (DB9) or USB-to-RS232 converter.
- 2) The above Workstations have been installed with terminal emulator, such as Tera Term or PuTTY.
- 3) Serial cable -- one end is attached to the RS232 serial port, while the other end to the console port of the Managed Switch.

Ethernet Port Connection

- 4) Network cables -- Use standard network (UTP) cables with RJ45 connectors.
- 5) The above PC is installed with Web browser



It is recommended to use Google Chrome or above to access the Managed Switch. If the Web interface of the Managed Switch is not accessible, please turn off the anti-virus software or firewall and then try it again.

### 3.5 Terminal Setup

To configure the system, connect a serial cable to a **COM port** on a PC or notebook computer and to serial (console) port of the Managed Switch. The console port of the Managed Switch is DCE already, so that you can connect the console port directly through PC without the need of Null Modem.

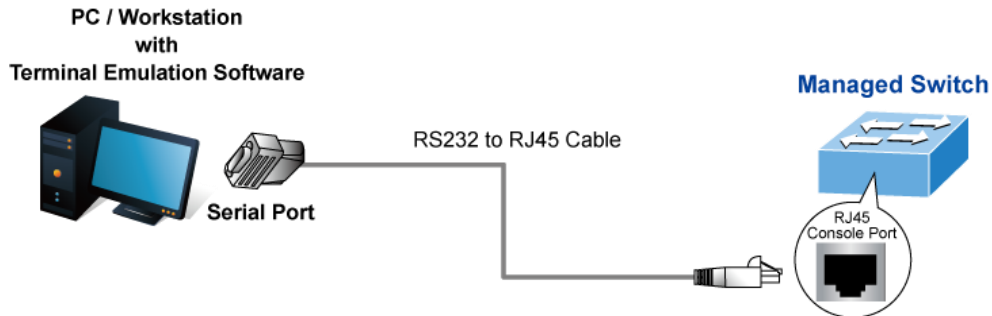


Figure 4-1 Managed Switch Console Connectivity

A terminal program is required to make the software connection to the Managed Switch. Tera Term program may be a good choice. The Tera Term can be accessed from the **Start** menu.

1. Click **START** menu, then **Programs**, and then **Tera Term**.
2. When the following screen appears, make sure that the COM port should be configured as:
  - **Baud: 9600**
  - **Parity: None**
  - **Data bits: 8**
  - **Stop bits: 1**
  - **Flow control: None**

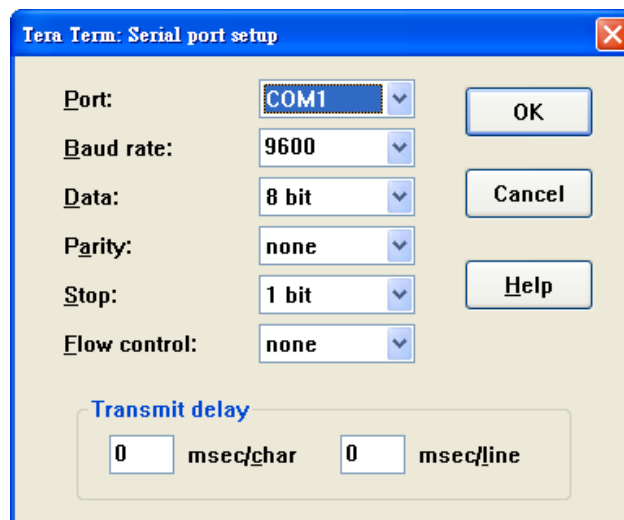


Figure 4-2 Tera Term COM Port Configuration



### 3.6 Logging on to the Console

Once the terminal is connected to the device, power on the Managed Switch, and the terminal will display “running testing procedures”.

Then, the following message asks for the login user name and password. The factory default user name and password are as follows as the login screen in Figure 4-3 appears.



The following console screen is based on the firmware version before **October of 2024**.

```
Username: admin
Password: admin
```

```
User Access Verification
Username: admin
Password:*****
Switch#
```

Figure 4-3 Managed Switch Console Login Screen

The user can now enter commands to manage the Switch. For a detailed description of the commands, please refer to the following chapters.



1. For security reason, please change and memorize the new password after this first setup.
2. Only accept command in lowercase letter under console interface.



The following console screen is based on the firmware version of **October of 2024 or after**.

Username: **admin**

Password: **sw + the last 6 characters of the MAC ID in lowercase**

Find the MAC ID on your device label. The default password is "sw" or "mc" followed by the last six lowercase characters of the MAC ID.

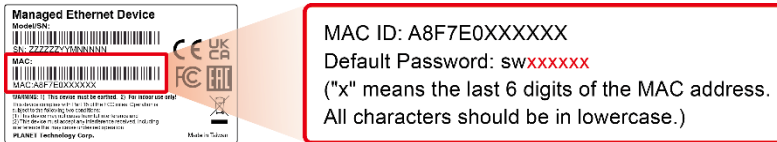


Figure 4-4: Industrial Managed Switch MAC ID Label

Enter the default username and password, then set a new password according to the rule-based prompt and confirm it.



Figure 4-5 Managed Switch Console Login Screen

The user can now enter commands to manage the Switch. For a detailed description of the commands, please refer to the following chapters.



1. For security reason, please change and memorize the new password after this first setup.
2. Accept command in lowercase or uppercase letter under console interface.

## 3.7 Configuring IP Address

The IP address configuration **VLAN1 interface** are listed below. Before using in-band management, the Managed Switch must be configured with an IP address by out-of-band management (i.e. console mode). The configuration commands are as follows:

```
Switch# config
Switch_config# interface vlan 1
Switch_config_v1# ip address 192.168.1.254 255.255.255.0
```

The previous command would apply the following settings for the Managed Switch.

**IPv4 Address: 192.168.1.254**  
**Subnet Mask: 255.255.255.0**

```
Switch#config
Switch_config#interface vlan 1
Switch_config_v1#ip address 192.168.1.254 255.255.255.0
Switch_config_v1#
```

Figure 4-6 Configuring IPv4 Address Screen

To check the current IP address or modify a new IP address for the Managed Switch, please use the procedures as follows:

### ■ Show the current IP address

1. On "**Switch#**" prompt, enter "**show ip interface brief**".
2. The screen displays the current IP address, subnet mask and gateway as shown in Figure 4-7.

```
Switch#config
Switch(config)#interface vlan 1
Switch(config-if-vlan1)#ip address 192.168.1.254 255.255.255.0
Switch(config-if-vlan1)#
Switch(config-if-vlan1)#exit
Switch(config)#show ip interface brief
Index      Interface      IP-Address      Protocol
11001     Vlan1          192.168.1.254   up
17500     Loopback       127.0.0.1       up
Switch(config)#
```

Figure 4-7 Showing IP Information Screen

If the IP is successfully configured, the Managed Switch will apply the new IP address setting immediately. You can access the Web interface of Managed Switch through the new IP address.



If you are not familiar with console command or the related parameter, enter "**help**" anytime in console to get the help description.

### 3.8 Starting Web Management

The Managed Switch provides a built-in browser interface. You can manage it remotely by having a remote host with Web browser, such as Google Chrome, Mozilla Firefox, Google Chrome or Apple Safari.



Figure IP Management Diagram

The following shows how to start up the Web Management of the Managed Switch. Please note the Managed Switch is configured through an Ethernet connection. Please make sure the manager PC must be set to the same IP subnet address.

For example, the IP address of the Managed Switch is configured with 192.168.0.254 on Interface VLAN 1, then the manager PC should be set to 192.168.0.x (where x is a number between 2 and 253, except 1 or 254), and the default subnet mask is 255.255.255.0.



The following console screen is based on the firmware version before **October of 2024**.

When the following dialog box appears, please enter the configured username “**admin**” and password “**admin**” (or the username/password you have changed via console). The login screen in Figure 5-2 appears.

The factory default user name and password are as follows:

Default IP of Interface VLAN 1: **192.168.0.254**  
Username: **admin**  
Password: **admin**

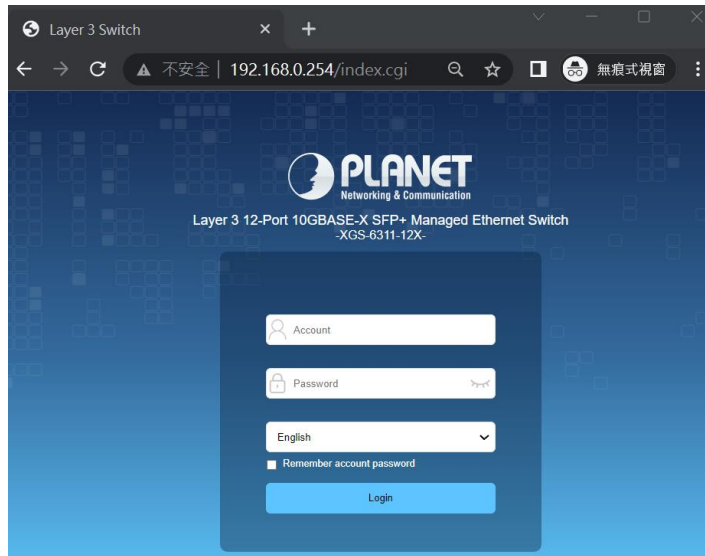


Figure 5-2 Login Screen



The following web screen is based on the firmware version of **October of 2024 or after**.

1. When the following dialog box appears, please enter the default user name “**admin**” and the password. Refer to **Section 4.1** to determine your initial login password.

Default IP Address: **192.168.0.254**

Default User Name: **admin**

Default Password: **sw + the last 6 characters of the MAC ID in lowercase**

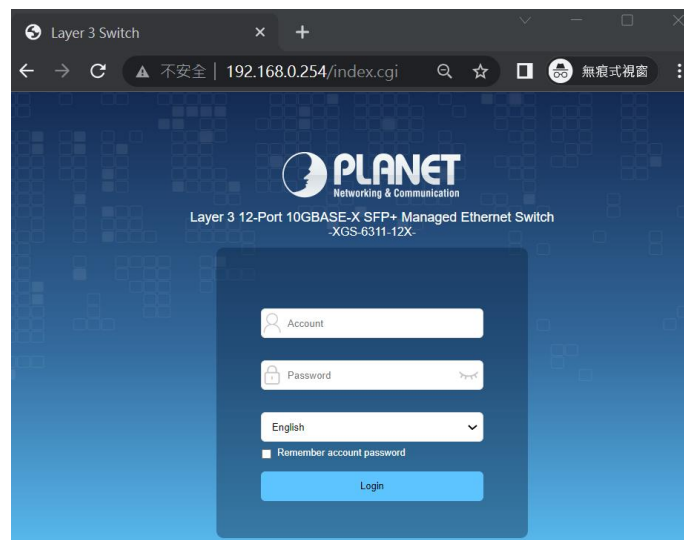


Figure 5-3: Create a New Password

- After logging in, you will be prompted to change the initial password to a permanent one.

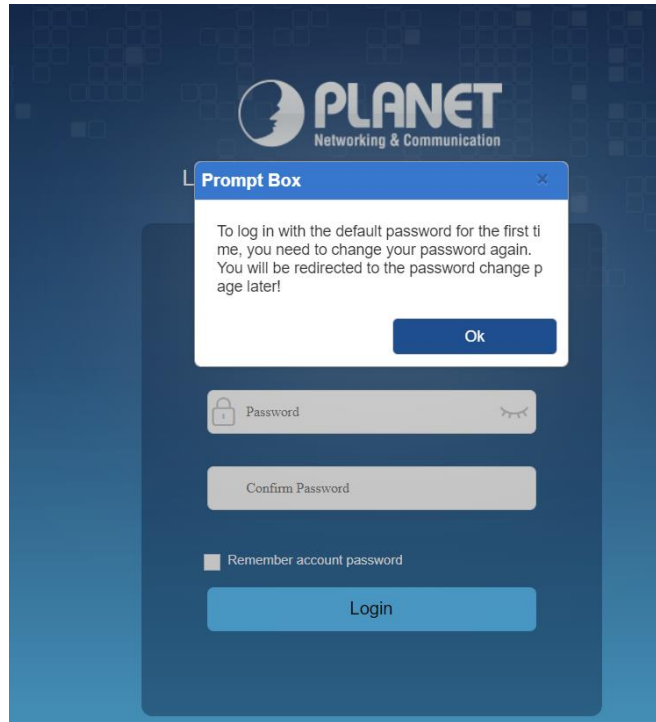


Figure 5-4: Create a New Password

Once the password change is complete, re-enter the web interface using your new password and the main screen appears as Figure 5-5 shows.

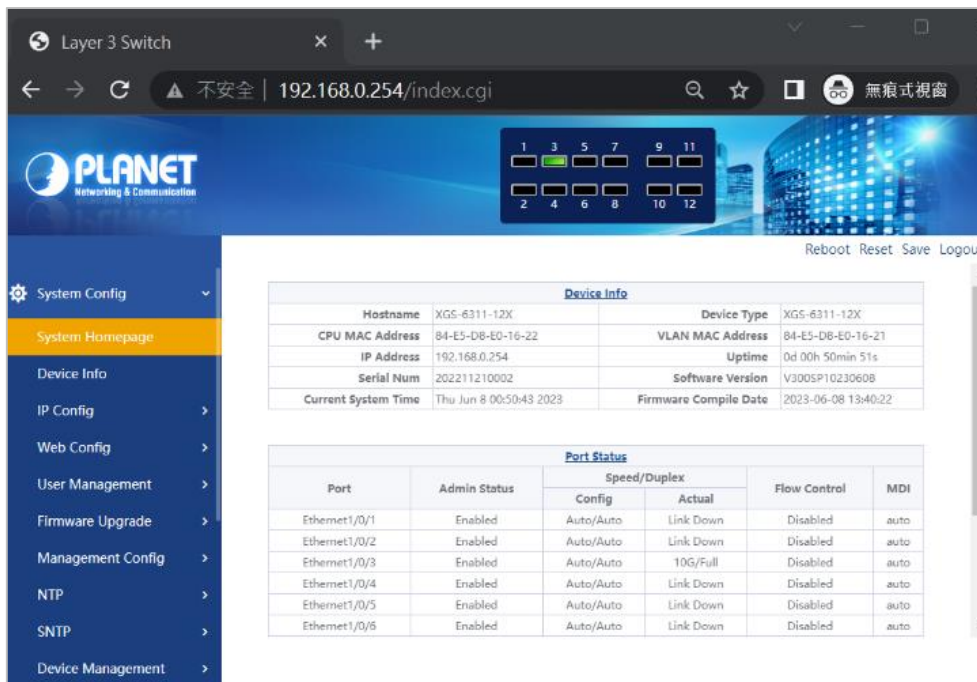


Figure 5-5 Web Main Screen of Managed Switch

3. The Switch Menu on the left of the Web page lets you access all the commands and statistics the Switch provides.

Now, you can use the Web management interface to continue the switch management or manage the Managed Switch by console interface. Please refer to the user manual for more.

### 3.9 Logging in to the Managed Switch

Use Google Chrome or above Web browser and enter IP address http://192.168.0.254 (that you have just set in console) to access the Web interface.

When the following dialog box appears, please enter the configured username “admin” and password “admin” (or the username/password you have changed via console). The login screen in below appears.

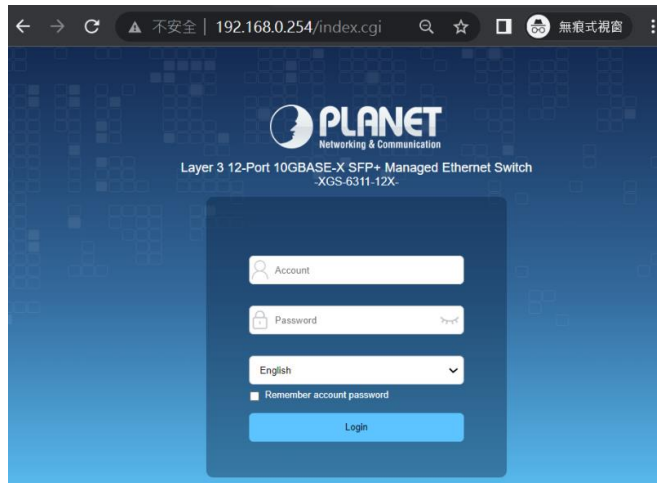


Figure Login Screen

After entering the password, the main screen appears as shown in below appears.

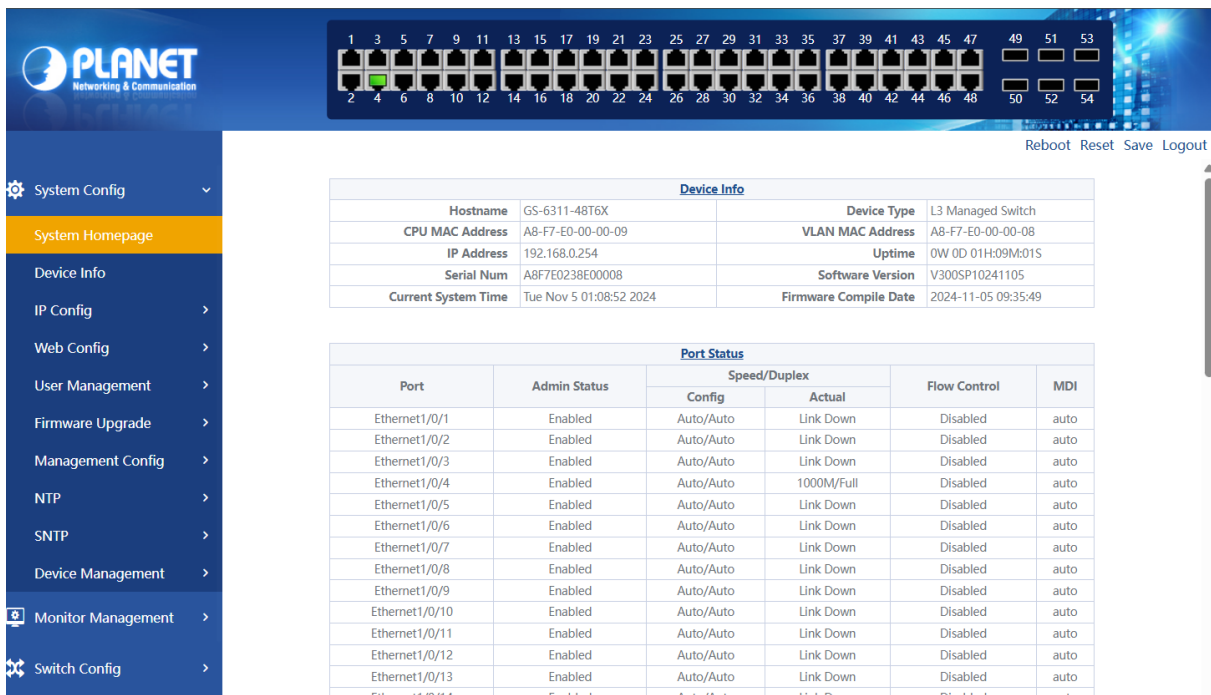


Figure Web Main Screen of Managed Switch

The Switch Menu on the left of the Web page lets you access all the commands and statistics the Switch provides. Now, you can use the Web management interface to continue the switch management or manage the Managed Switch by console interface. Please refer to the user manual for more.



### 3.10 Discovery through PLANET NMS Controller (NMS-500/NMS-1000V)

The X(M)GS-6311 Series is the Layer 3 Managed Ethernet Switch, which can be centrally monitored by PLANET NMS Controller.

Follow the steps below to discover the Layer 3 Managed Ethernet Switch through PLANET NMS controller (NMS-500/NMS-1000V). Please ensure each Layer 3 Managed Ethernet Switch uses a different static IP in the same subnet before physically connecting to the managed network.

It supports PLANET NMS system and NMSViewerPro app networking feature, which, with PLANET's free cloud service, allows users to quickly and easily detect, configure, deploy and manage devices remotely. Users can just scan the NMS agent's (NMS-500/NMS-1000V) QR code with their mobile devices in order to easily monitor and control the remote network via the private cloud.

- 
1. Please regularly check PLANET website for the latest compatible list of the Layer 3 Managed Ethernet Switch in each firmware version.
  2. Supports X(M)GS-6311 Series Layer 3 Managed Ethernet Switch. Please use the versions listed below:



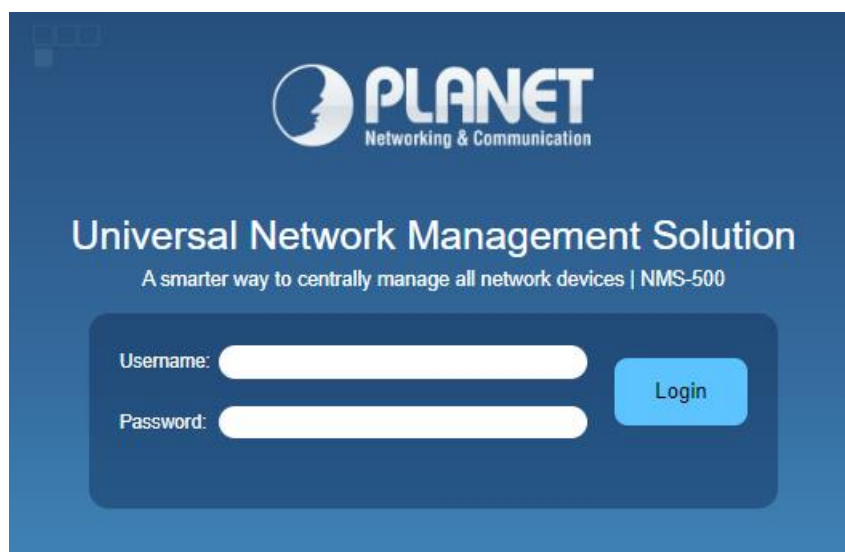
Note

X(M)GS-6311 Series: V300SP10241023  
NMS-500: v1.0b240812 (Newer than the last version)  
NMS-1000V-10/12: v1.0b240813 (Newer than the last version)

---

Step 1. Launch the Web browser (Google Chrome is recommended.) and enter the default IP address <https://192.168.1.100:8888> of the NMS controller. Then, enter the default username and password "admin" to log on to the system.

\*The secure login with SSL (HTTPS) prefix is required.



Step 2. Go to the “**Domain**” page to discover and add the Layer 3 Managed Ethernet Switch to the device list. Then, you can search and add them and go to the “**Device List**” and “**Topology View**” page to monitor the Layer 3 Managed Ethernet Switch.

Please refer to NMS-500/NMS-1000V [User's Manual](#) for the best experience.

### 3.11 PLANET NMSViewerPro App

To get PLANET NMSViewerPro app, you can follow the steps below. After it is done, you can now monitor and control your network devices, such as switches, routers, etc., from your iOS or Android based smartphone or tablet.

**How to begin:**

**Step 1. Setting the smart phone's Wi-Fi to connect with NMS and internet**

Turn on your smart phone's Wi-Fi setting to enable to be connected to the Wi-Fi within the NMS domain and to confirm that the Internet can be accessed normally.

**Step 2. Download PLANET NMSViewerPro App**

Get the **PLANET NMSViewerPro** App from the Apple App Store or Google play, or simply scan the QR code.



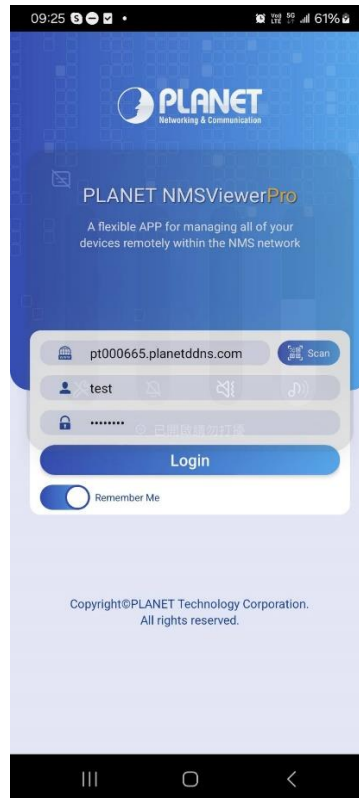
**Step 3. First use PLANET NMSViewerPro**

1. Open the PLANET NMSViewerPro app. You can log in by scanning the NMS-500/1000V QR code or entering the Domain Name/IP address of the NMS equipment provided in the NMS equipment.
2. Scan the NMS-500/1000V QR code only (No need to enter any Domain Name/IP address, and account and password), shown in the screen below:

Log in to the NMS and follow the steps below:

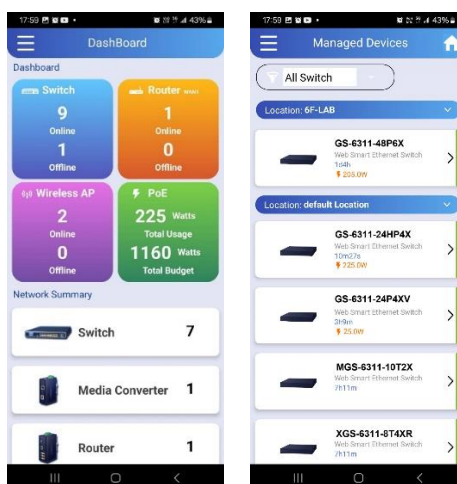


- Enter the NMS-500/1000V Domain Name/IP address, and account and password, shown in the screen below:



### Step 3. Find your device in Managed Devices list

After logging in the app, you can see the Dashboard and Managed Devices found in the NMS-500/1000V.



### 3.12 PLANET Smart Discovery Utility

For easily listing the Layer 3 Managed Ethernet Switch in your Ethernet environment, the Planet Smart Discovery Utility from user's manual CD-ROM is an ideal solution. The following installation instructions are to guide you to running the Planet Smart Discovery Utility.

1. Deposit the Planet Smart Discovery Utility in administrator PC.
2. Run this utility as the following screen appears.

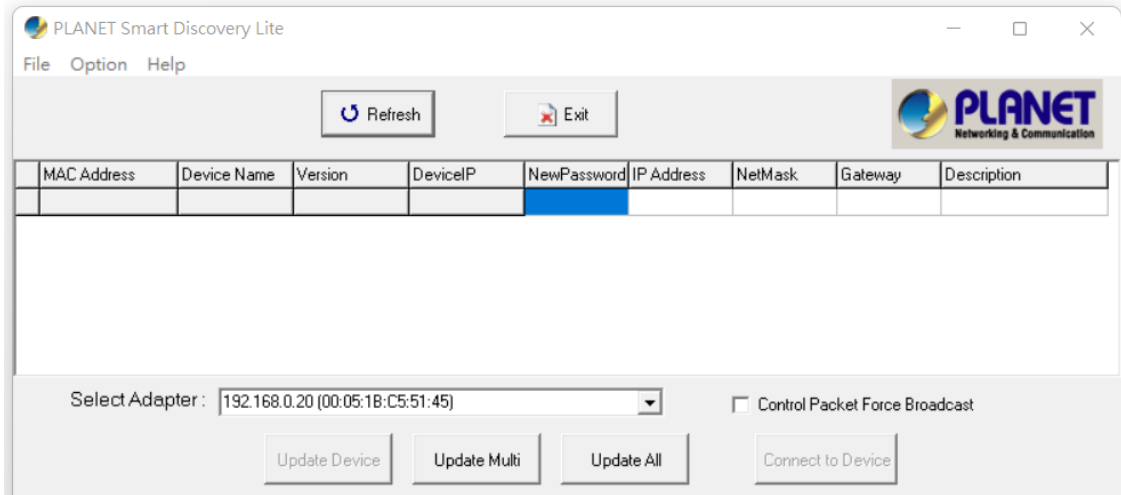


Figure 3-1-6: Planet Smart Discovery Utility Screen



If there are two LAN cards or above in the same administrator PC, choose a different LAN card by using the “**Select Adapter**” tool.

3. Press the “**Refresh**” button for the currently connected devices in the discovery list as the screen shows below:

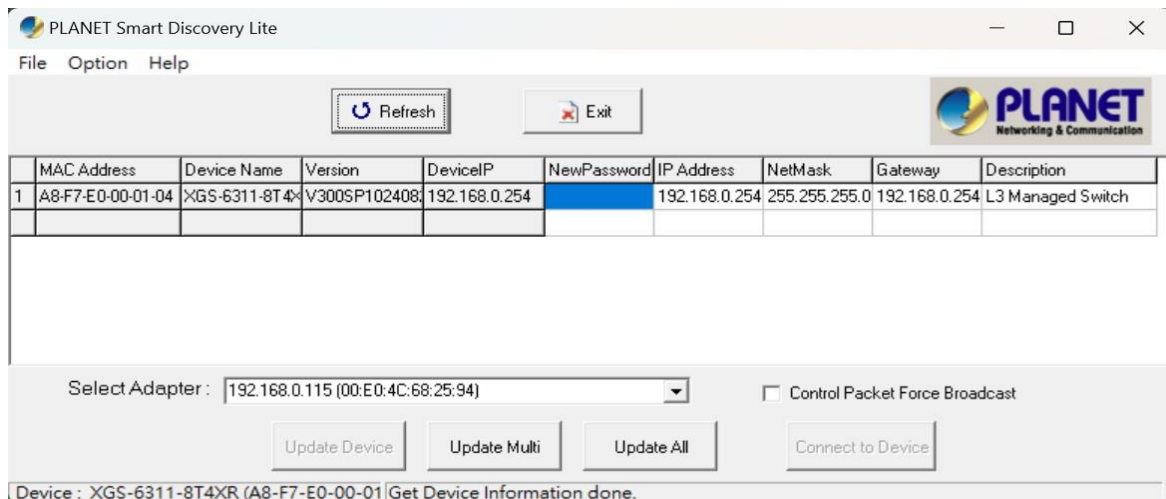


Figure 3-1-7: Planet Smart Discovery Utility Screen

1. This utility shows all necessary information from the devices, such as MAC address, device name, firmware version, and device IP subnet address. It can also assign new password, IP subnet address and description to the devices.
  
2. After setup is completed, press the **“Update Device”**, **“Update Multi”** or **“Update All”** button to take effect. The functions of the 3 buttons above are shown below:
  - **Update Device:** use current setting on one single device.
  - **Update Multi:** use current setting on choose multi-devices.
  - **Update All:** use current setting on whole devices in the list.

The same functions mentioned above also can be found in **“Option”** tools bar.

3. To click the **“Control Packet Force Broadcast”** function, it allows you to assign a new setting value to the Web Smart Switch under a different IP subnet address.
  
4. Press the **“Connect to Device”** button and the Web login screen appears.
  
5. Press the **“Exit”** button to shut down the Planet Smart Discovery Utility.

# Chapter 4 Basic Switch Configuration

## 4.1 Basic Configuration

### 4.1.1 authentication line

<b>Command</b>	<p><b>authentication line {console   vty   web} login {local   radius   tacacs}</b>  <b>no authentication line {console   vty   web} login</b></p>						
<b>Parameter</b>	<table border="1"> <tr> <td><b>console</b></td> <td>Log on the switch through the console serial port</td> </tr> <tr> <td><b>vty</b></td> <td>Log on the switch through the vty(SSH or Telnet)</td> </tr> <tr> <td><b>web</b></td> <td>Log on the switch through the web</td> </tr> </table>	<b>console</b>	Log on the switch through the console serial port	<b>vty</b>	Log on the switch through the vty(SSH or Telnet)	<b>web</b>	Log on the switch through the web
<b>console</b>	Log on the switch through the console serial port						
<b>vty</b>	Log on the switch through the vty(SSH or Telnet)						
<b>web</b>	Log on the switch through the web						
<b>Default</b>	No configuration is enabled for the console login method by default. Local authentication is enabled for the VTY and Web login method by default.						
<b>Mode</b>	Global Mode						
<b>Usage Guide</b>	<p>This command can configure the authentication methods for Console, VTY, and Web login separately.</p> <p>The authentication method can be any one or combination of Local. RADIUS and TACACS. Preferences from left to right when the login method is combined configuration.</p> <p>If the user has passed the authentication method, the authentication method of the lower preference is ignored.</p> <p>As long as pass an authentication method, the user can log in.</p> <p>AAA function and RADIUS server should be configured before the RADIUS authentication can be used.</p> <p>If local authentication is configured without configuring a local user, the user will be able to log on to the switch through the console method.</p> <p>They all support the following authentication methods.</p> <p>Local: Use the local user account database for authentication.</p> <p>Tacacs: Authentication using remote Tacas server.</p> <p>Radius: Authentication using remote Radius server.</p> <p>no command restores default authentication.</p>						
<b>Example</b>	<p>Configure Telnet and ssh login methods to Local and RADIUS authentication methods.</p> <p><b>Switch(config)# authentication line vty login local radius lists</b></p>						

## 4.1.2 banner

<b>Command</b>	<b>banner motd&lt;LINE&gt;</b> <b>no banner motd</b>
<b>Parameter</b>	<b>&lt;LINE&gt;</b> The information displayed when the authentication is successful, length limit from 1 to 100 characters
<b>Default</b>	Do not show the information when the authentication is successful.
<b>Mode</b>	Global Mode
<b>Usage Guide</b>	This command is used to configure the information displayed when the login authentication of a telnet or console user is successful, the no command configures that the information is not displayed when the authentication is successful.
<b>Example</b>	Display "Welcome" after authentication is successful.  <b>Switch(config)# banner motd Welcome</b>



### 4.1.3 boot img

<b>Command</b>	<b>boot img &lt;img-file-url&gt; {primary   backup}</b>
<b>Parameter</b>	<b>&lt;img-file-url&gt;</b> Full path to the img file
	<b>primary</b> First entry to the img document
	<b>backup</b> Second entry to the img document
<b>Default</b>	The factory original configuration only specifies the first booting IMG file, it is nos.img file in the FLASH, without the second booting IMG file.
<b>Mode</b>	admin Mode
<b>Usage Guide</b>	<p>This command is used to configure the first and second img files used by the switch next boot.</p> <p>The first and second img files can only use .img files stored in switch.</p> <ol style="list-style-type: none"> <li>1. The file path comprises of three parts: device prefix used as the root directory (flash:/), sub-directory, and the file name. No space is allowed in each part or between two parts.</li> <li>2. The suffix of all file names should be .img.</li> <li>3. The length of the full file path should not be longer than 128 characters, while the file name can not be longer than 80 characters.</li> </ol>
<b>Example</b>	<p>Set flash:/nos.img as the second booting IMG file used in the next booting of the switch.</p> <p><b>Switch#boot img flash:/nos.img backup</b></p>

## 4.1.4 boot startup-config

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

## 4.1.5 clock set

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

## 4.1.6 config

<b>Command</b>	<b>config [terminal]</b>
<b>Parameter</b>	<b>[terminal]</b> indicates terminal configuration
<b>Default</b>	None.
<b>Mode</b>	admin Mode.
<b>Usage Guide</b>	This command is used to switch from admin management mode to config global configuration mode.
<b>Example</b>	Enter config global configuration mode from admin management mode.  <b>Switch#config</b>

### 4.1.7 disable

<b>Command</b>	<b>disable</b>
<b>Parameter</b>	<b>none</b> none
<b>Default</b>	None.
<b>Mode</b>	admin Mode.
<b>Usage Guide</b>	This command is used for switch exit admin mode back to general user mode.
<b>Example</b>	Exit admin mode back to general user mode.  <b>Switch#disable</b> <b>Switch&gt;</b>

### 4.1.8 enable

<b>Command</b>	<b>enable [&lt;1-15&gt;]</b>
<b>Parameter</b>	<b>[&lt;1-15&gt;]</b> User Permission Level
<b>Default</b>	None.
<b>Mode</b>	User mode/ admin mode
<b>Usage Guide</b>	<p>Use enable command to enter Admin Mode from User Mode, or change the privilege level of the users.</p> <p>To prevent unauthorized access of non-admin user, user authentication is required (i.e. Admin user password is required) when entering Admin Mode from User Mode.</p> <p>If the correct Admin user password is entered, Admin Mode access is granted; if 3 consecutive entry of Admin user password are all wrong, it remains in the User Mode. When the user's privilege is changed from the low level to the high level, it needs to authenticate the password of the corresponding level, or else it will not authenticate the password.</p> <p>Set the Admin user password under Global Mode with "enable password" command.</p>
<b>Example</b>	<p>Enter management mode from user mode.</p> <pre>Switch&gt;enable Switch#</pre>

### 4.1.9 enable password

<b>Command</b>	<p><b>enable password [level &lt;1-15&gt;] [0   7] &lt;password&gt;</b>  <b>no enable password [level &lt;1-15&gt;]</b></p>						
<b>Parameter</b>	<table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="border-right: 1px solid black; padding: 2px;"><b>[level &lt;1-15&gt;]</b></td> <td style="padding: 2px;">used to specify the privilege level, the default level is 15</td> </tr> <tr> <td style="border-right: 1px solid black; padding: 2px;"><b>[0   7]</b></td> <td style="padding: 2px;">If enter option 0 on password settings,the password is not encrypted; If enter option 7 on password settings,the password is encrypted</td> </tr> <tr> <td style="border-right: 1px solid black; padding: 2px;"><b>&lt;password&gt;</b></td> <td style="padding: 2px;">the password for the user</td> </tr> </table>	<b>[level &lt;1-15&gt;]</b>	used to specify the privilege level, the default level is 15	<b>[0   7]</b>	If enter option 0 on password settings,the password is not encrypted; If enter option 7 on password settings,the password is encrypted	<b>&lt;password&gt;</b>	the password for the user
<b>[level &lt;1-15&gt;]</b>	used to specify the privilege level, the default level is 15						
<b>[0   7]</b>	If enter option 0 on password settings,the password is not encrypted; If enter option 7 on password settings,the password is encrypted						
<b>&lt;password&gt;</b>	the password for the user						
<b>Default</b>	This password is empty by system default.						
<b>Mode</b>	Global Mode						
<b>Usage Guide</b>	<p>Configure the password used for enter Admin Mode from the User Mode.  Configure this password to prevent unauthorized entering Admin Mode.  It is recommended to set the password at the initial switch configuration.  Also, it is recommended to exit Admin Mode with “exit” command when the administrator needs to leave the terminal for a long time.</p> <p>The “no enable password” command deletes this password.</p>						
<b>Example</b>	<p>Configure the command for general users to enter the admin mode by rule as test.</p> <p><b>Switch(config)#enable password 0 test</b></p>						

### 4.1.10 end

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



### 4.1.11 exec-timeout

<b>Command</b>	<code>exec-timeout &lt;minutes&gt; [&lt;seconds&gt;]</code> <code>no exec-timeout</code>				
<b>Parameter</b>	<table border="1"> <tr> <td><code>&lt;minutes&gt;</code></td> <td>the time value shown in minute and ranges between 0~35791</td> </tr> <tr> <td><code>[&lt;seconds&gt;]</code></td> <td>the time value shown in seconds and ranges between 0~59</td> </tr> </table>	<code>&lt;minutes&gt;</code>	the time value shown in minute and ranges between 0~35791	<code>[&lt;seconds&gt;]</code>	the time value shown in seconds and ranges between 0~59
<code>&lt;minutes&gt;</code>	the time value shown in minute and ranges between 0~35791				
<code>[&lt;seconds&gt;]</code>	the time value shown in seconds and ranges between 0~59				
<b>Default</b>	Default timeout is 10 minutes.				
<b>Mode</b>	Global mode				
<b>Usage Guide</b>	<p>This command is used Configure the timeout of exiting admin mode.</p> <p>Timeout exit admin management mode, need to enter management code and password to enter admin management mode again.</p> <p>When the timeout is set to 0, the timeout timer is disabled.</p> <p>“no exec-timeout”command to restore default values.</p>				
<b>Example</b>	<p>Set the admin mode timeout value to 5 minutes, 30 seconds.</p> <p><b>Switch(config)#exec-timeout 5 30</b></p>				

## 4.1.12 exit

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

### 4.1.13 help

<b>Command</b>	<b>help</b>
<b>Parameter</b>	<b>none</b> none
<b>Default</b>	None.
<b>Mode</b>	All Modes
<b>Usage Guide</b>	An instant online help provided by the switch. Help command displays information about the whole help system, including complete help and partial help. The user can type in '?' any time to get online help.
<b>Example</b>	Get help in global mode.  <b>Switch(config)#help</b> CLI provides advanced help feature. When you need help, anytime at the command line please press '?'.  If nothing matches, the help list will be empty and you must backup until entering a '?' shows the available options.

### 4.1.14 hostname

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

## 4.1.15 ip host

<b>Command</b>	<b>ip host &lt;hostname&gt; &lt;ip_addr&gt;</b> <b>no ip host {&lt;hostname&gt; all}</b>	
<b>Parameter</b>	<b>&lt;hostname&gt;</b>	the string for the prompt, up to 64 characters are allowed
	<b>&lt;ip_addr&gt;</b>	the corresponding IP address for the host name, takes a dot decimal format
	<b>all</b>	all of the host name
<b>Default</b>	None.	
<b>Mode</b>	Global Mode	
<b>Usage Guide</b>	<p>By using this command, you can set the mapping relationship between the host and the IP address.</p> <p>Set the association between host and IP address, which can be used in commands like “ping &lt;host&gt;”.</p> <p>The “no ip host” parameter of this command will delete the mapping.</p>	
<b>Example</b>	<p>Set IP address of a host with the hostname of “beijing” to 200.121.1.1.</p> <p><b>Switch(config)#ip host beijing 200.121.1.1</b></p>	

## 4.1.16 ipv6 host

<b>Command</b>	<pre>ipv6 host &lt;hostname&gt; &lt;ipv6_addr&gt; no ipv6 host { &lt;hostname&gt;   all}</pre>	
<b>Parameter</b>	<b>&lt;hostname&gt;</b>	the string for the prompt, up to 64 characters are allowed
	<b>&lt;ipv6_addr&gt;</b>	the corresponding IPv6 address for the host name, takes a dot decimal format
	<b>all</b>	all of the host name
<b>Default</b>	None.	
<b>Mode</b>	Global Mode	
<b>Usage Guide</b>	<p>By using this command, you can set the mapping relationship between the host and the IPv6 address.</p> <p>Set the association between host and IPv6 address, which can be used in commands like "traceroute6 &lt;host&gt;".</p> <p>The "no ip host" parameter of this command will delete the mapping.</p>	
<b>Example</b>	<p>Set the IPv6 address of the host named beijing to 2001:1:2:3::1.</p> <pre>Switch(config)#ipv6 host beijing 2001:1:2:3::1</pre>	

### 4.1.17 ip http server

<b>Command</b>	<b>ip http server</b> <b>no ip http server</b>
<b>Parameter</b>	<b>none</b> none
<b>Default</b>	Enable.
<b>Mode</b>	Global Mode
<b>Usage Guide</b>	Use this command to enable Web configuration.  The “no ip http server” command disables Web configuration.
<b>Example</b>	Enable Web Server function and enable Web configurations.  <b>Switch(config)#ip http server</b>

## 4.1.18 login

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



### 4.1.19 password

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

## 4.1.20 privilege

<b>Command</b>	<b>privilege mode level &lt;1-15&gt; LINE</b> <b>no privilege mode level &lt;1-15&gt; LINE</b>						
<b>Parameter</b>	<table border="1"> <tr> <td><b>mode</b></td> <td>register mode of the command, 'Tab' or '?' is able to show all register modes</td> </tr> <tr> <td><b>&lt;1-15&gt;</b></td> <td>level, its range between 1 and 15</td> </tr> <tr> <td><b>LINE</b></td> <td>the command needs to be configured, it supports the command abbreviation</td> </tr> </table>	<b>mode</b>	register mode of the command, 'Tab' or '?' is able to show all register modes	<b>&lt;1-15&gt;</b>	level, its range between 1 and 15	<b>LINE</b>	the command needs to be configured, it supports the command abbreviation
<b>mode</b>	register mode of the command, 'Tab' or '?' is able to show all register modes						
<b>&lt;1-15&gt;</b>	level, its range between 1 and 15						
<b>LINE</b>	the command needs to be configured, it supports the command abbreviation						
<b>Default</b>	None.						
<b>Mode</b>	Global Mode						
<b>Usage Guide</b>	<p>Use this command to configure the permission level for the specified command. This function cannot change the command itself. LINE must be the whole command format, the command with the abbreviation format must be analyzed successfully.</p> <p>Can choose to set the level of the NO command, but it does not affect the result. When using a no command, the LINE must be a configured command line. If the command line with the parameter, the parameter must be matched with the configured command.</p> <p>The no command restores the original level of the command.</p>						
<b>Example</b>	<p>Change the level of show ip route command to level 5. Restore the original level of the show ip route command.</p> <pre>Switch(config)#privilege exec level 5 show ip route Switch(config)#no privilege exec level 5 show ip route</pre>						

### 4.1.21 reload

<b>Command</b>	<b>reload</b>
<b>Parameter</b>	<b>none</b> none
<b>Default</b>	None.
<b>Mode</b>	Admin Mode
<b>Usage Guide</b>	The user can use this command to restart the switch continuously.
<b>Example</b>	Hot restart switch.  <b>Switch(config)#reload</b>

## 4.1.22 service password-encryption

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

### 4.1.23 service terminal-length

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

## 4.1.24 sysContact

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

## 4.1.25 sysLocation

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

### 4.1.26 set default

<b>Command</b>	<b>set default</b>
<b>Parameter</b>	<b>none</b> none
<b>Default</b>	None.
<b>Mode</b>	Admin Mode
<b>Usage Guide</b>	<p>Reset the switch to factory settings.</p> <p>That is to say, all configurations made by the user to the switch will disappear. When the switch is restarted, the prompt will be the same as when the switch was powered on for the first time.</p> <p><b>Note:</b> After the command, "write" command must be executed to save the operation. The switch will reset to factory settings after restart.</p>
<b>Example</b>	<p>Restore factory settings and restart.</p> <pre> <b>Switch#set default</b> Are you sure? [Y/N] = y <b>Switch#write</b> <b>Switch#reload</b> </pre>



## 4.1.27 set boot password

<b>Command</b>	<p>set boot password</p> <p>no set boot password</p>
<b>Parameter</b>	<p>none                      none</p>
<b>Default</b>	<p>None.</p>
<b>Mode</b>	<p>Global Mode</p>
<b>Usage Guide</b>	<p>Under the img mode, configure the password of entering the bootrom mode next time; under the global mode, input this command and the password according to the prompt and confirm it, then successfully to configure.</p> <p><b>Notice:</b> the characters length of the password is from 3 to 32.</p> <p>The no command cancels the password.</p>
<b>Example</b>	<p>Sets the password when entering boot mode.</p> <pre> Switch(config)#set boot password New password :***** Confirm password :***** Set password success! </pre>

## 4.1.28 setup

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

### 4.1.29 show clock

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

### 4.1.30 show cpu usage

<b>Command</b>	<b>show cpu usage [&lt;slotno&gt;]</b>
<b>Parameter</b>	<b>[&lt;slotno&gt;]</b> Specify slots
<b>Default</b>	None.
<b>Mode</b>	Admin and configuration mode
<b>Usage Guide</b>	<p>Display current, past 5 seconds, past 30 seconds, past 5 minutes CPU usage by this command.</p> <p>Only the chassis switch uses slotno parameter which is used to show the CPU usage rate of the card on specified slot, if there is no parameter, the default is current card.</p>
<b>Example</b>	<p>Show the current usage rate of CPU.</p> <p><b>Switch#show cpu usage</b>            Last 5 second CPU IDLE: 87%            Last 30 second CPU IDLE: 89%            Last 5 minute CPU IDLE: 89%            From running CPU IDLE: 89%</p>

### 4.1.31 show cpu utilization

<b>Command</b>	<b>show cpu utilization</b>
<b>Parameter</b>	<b>none</b> <b>none</b>
<b>Default</b>	None.
<b>Mode</b>	Admin Mode
<b>Usage Guide</b>	This command is used to show CPU utilization rate in the past 5 seconds, 30 seconds and 5 minutes.。
<b>Example</b>	Displays CPU utilization.  <b>Switch#show cpu utilization</b> Last 5 second CPU USAGE: 9% Last 30 second CPU USAGE: 11% Last 5 minute CPU USAGE: 11% From running CPU USAGE: 11%

### 4.1.32 show memory usage

<b>Command</b>	<b>show memory usage [&lt;slotno&gt;]</b>
<b>Parameter</b>	<b>[&lt;slotno&gt;]</b> Specify slots
<b>Default</b>	None.
<b>Mode</b>	Admin Mode
<b>Usage Guide</b>	<p>Show memory usage rate.</p> <p>Only the chassis switch uses slotno parameter which is used to show the memory usage rate of card on the specified slot, if there is no parameter, the default is current card.</p>
<b>Example</b>	<p>Show the current usage rate of the memory.</p> <p><b>Switch#show memory usage</b></p> <p>The memory total 128 MB, free 58914872 bytes, usage is 56.10%</p>

### 4.1.33 show privilege

<b>Command</b>	<b>show privilege</b>
<b>Parameter</b>	<b>none</b> none
<b>Default</b>	None.
<b>Mode</b>	Global Mode
<b>Usage Guide</b>	Show privilege of the current user.
<b>Example</b>	Show privilege of the current user.  <b>Switch(config)#show privilege</b> Current privilege level is 15

### 4.1.34 show privilege mode LINE

<b>Command</b>	<b>show privilege mode LINE</b>	
<b>Parameter</b>	<b>mode</b>	register mode of the command, 'Tab' or '?' is able to show all register modes
	<b>LINE</b>	the command needs to be configured, it supports the command abbreviation
<b>Default</b>	None.	
<b>Mode</b>	Admin mode/Global mode	
<b>Usage Guide</b>	<p>Show the level of the specified command.</p> <p>LINE must be the whole command format, the abbreviation format is used to the command which can be analyzed successfully.</p> <p>For half-baked command, false command about writing and command that abbreviation cannot be analyzed successfully, the level of them cannot be shown.</p>	
<b>Example</b>	<p>Show the level of privilege command.</p> <p><b>Switch(config)#show privilege exec show ip route</b></p> <p>The command : show ip route</p> <p>Privilege is : 15</p>	



### 4.1.35 show tech-support

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

### 4.1.36 show version

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

### 4.1.37 username

<b>Command</b>	<b>username &lt;username&gt; [privilege &lt;privilege&gt;] [password [0   7]&lt;password&gt;] no username &lt;username&gt;</b>								
<b>Parameter</b>	<table border="1"> <tr> <td><b>&lt;username&gt;</b></td> <td>the username, its range should not exceed 32 characters</td> </tr> <tr> <td><b>&lt;privilege&gt;</b></td> <td>the maximum privilege level of the commands that the user is able to execute, its value is limited between 1 and 15, and 1 by default</td> </tr> <tr> <td><b>[0   7]</b></td> <td>If input option 0 on password setting, the password is not encrypted; if input option 7, the password is encrypted (Use 32 bits password encrypted by MD5)</td> </tr> <tr> <td><b>&lt;password&gt;</b></td> <td>password for the user</td> </tr> </table>	<b>&lt;username&gt;</b>	the username, its range should not exceed 32 characters	<b>&lt;privilege&gt;</b>	the maximum privilege level of the commands that the user is able to execute, its value is limited between 1 and 15, and 1 by default	<b>[0   7]</b>	If input option 0 on password setting, the password is not encrypted; if input option 7, the password is encrypted (Use 32 bits password encrypted by MD5)	<b>&lt;password&gt;</b>	password for the user
<b>&lt;username&gt;</b>	the username, its range should not exceed 32 characters								
<b>&lt;privilege&gt;</b>	the maximum privilege level of the commands that the user is able to execute, its value is limited between 1 and 15, and 1 by default								
<b>[0   7]</b>	If input option 0 on password setting, the password is not encrypted; if input option 7, the password is encrypted (Use 32 bits password encrypted by MD5)								
<b>&lt;password&gt;</b>	password for the user								
<b>Default</b>	None.								
<b>Mode</b>	Global Mode								
<b>Usage Guide</b>	<p>Configure local login username and password along with its privilege level. 16 local users at most can be configured through this command, and the maximum length of the password should be no less than 32.</p> <p>The user can log in user and priority after the command configures, before issuing the command authentication line console login local, it should be made sure that at one user has be configured as preference level of 15, in order to login the switch and make configuration changes in privileged mode and global mode.</p> <p>If there are no configured local users with preference level of 15, while only Local authentication is configured for the Console login method, the switch can be login without any authentication. When using the HTTP method to login the switch, only users with preference level of 15 can login the switch, users with preference level other than 15 will be denied.</p> <p>The no command delete user.</p>								
<b>Example</b>	<p>Configure an administrator account named admin, with the preference level as 15. And configure two normal accounts with its preference level as 1. Then enable local authentication method.</p> <pre> Switch(config)#username admin privilege 15 password 0 admin Switch(config)# username user1 privilege 1 password 7 4a7d1ed414474e4033ac29ccb8653d9b Switch(config)# username user2 password 0 user2 Switch(config)# authentication line console login local </pre>								

### 4.1.38 web-auth privilege <1-15>

<b>Command</b>	<b>web-auth privilege &lt;1-15&gt;</b> <b>no web-auth privilege</b>
<b>Parameter</b>	<b>&lt;1-15&gt;</b> Appoint the level of logging in the switch by web and the range is from 1 to 15
<b>Default</b>	The default level is 15.
<b>Mode</b>	Global Mode
<b>Usage Guide</b>	<p>Configure the level of logging in the switch by web.</p> <p>After configured the level of logging in the switch by web, only the user with the level that is equal to or higher than it can login in the switch by web.</p>
<b>Example</b>	<p>Configure the level of logging in the switch by web as 10.</p> <p><b>Switch(config)# web-auth privilege 10</b></p>

### 4.1.39 write

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

### 4.1.40 write running-config

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

## 4.2 Telnet

### 4.2.1 aaa authorization config-commands

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

## 4.2.2 accounting exec

<b>Command</b>	<p>accounting line {console   vty} exec {start-stop   stop-only   none} method1 [method2...]</p> <p>no accounting line {console   vty} exec</p>												
<b>Parameter</b>	<table border="1"> <tr> <td><b>console</b></td> <td>log in through serial port</td> </tr> <tr> <td><b>vty</b></td> <td>log in through telnet or ssh</td> </tr> <tr> <td><b>start-stop</b></td> <td>sends the accounting start or the accounting stop when the user is logging or exit the login</td> </tr> <tr> <td><b>stop-only</b></td> <td>sends the accounting stop when the user exits the login only</td> </tr> <tr> <td><b>none</b></td> <td>does not send the accounting start or the accounting stop</td> </tr> <tr> <td><b>method</b></td> <td>the list of the accounting method, it only supports tacacs keyword; tacacs uses the remote TACACS+ server to count</td> </tr> </table>	<b>console</b>	log in through serial port	<b>vty</b>	log in through telnet or ssh	<b>start-stop</b>	sends the accounting start or the accounting stop when the user is logging or exit the login	<b>stop-only</b>	sends the accounting stop when the user exits the login only	<b>none</b>	does not send the accounting start or the accounting stop	<b>method</b>	the list of the accounting method, it only supports tacacs keyword; tacacs uses the remote TACACS+ server to count
<b>console</b>	log in through serial port												
<b>vty</b>	log in through telnet or ssh												
<b>start-stop</b>	sends the accounting start or the accounting stop when the user is logging or exit the login												
<b>stop-only</b>	sends the accounting stop when the user exits the login only												
<b>none</b>	does not send the accounting start or the accounting stop												
<b>method</b>	the list of the accounting method, it only supports tacacs keyword; tacacs uses the remote TACACS+ server to count												
<b>Default</b>	By default there is no accounting.												
<b>Mode</b>	Global Mode												
<b>Usage Guide</b>	<p>Configure the list of the accounting method for the login user with VTY (login with Telnet and SSH) and Console.</p> <p>console and vty login method are able to set the corresponding accounting method respectively, the accounting method only supports TACACS+ method currently.</p> <p>The no command restores the default accounting method.</p>												
<b>Example</b>	<p>Configure the login accounting with the telnet method.</p> <p><b>Switch(config)#accounting line vty exec start-stop tacacs</b></p>												



### 4.2.3 accounting command

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

## 4.2.4 authentication enable

<b>Command</b>	<p><b>authentication enable method1 [method2...]</b></p> <p><b>no authentication enable</b></p>
<b>Parameter</b>	<p><b>method</b>                    the list of the authentication method, it must be among local, tacacs and radius keywords;</p> <p>                                  local:uses the local database to authenticate;</p> <p>                                  tacacs:uses the remote TACACS+ authentication server to authenticate;</p> <p>                                  radius:uses the remote RADIUS authentication server to authenticate</p>
<b>Default</b>	The local authentication is enable command by default.
<b>Mode</b>	Global Mode
<b>Usage Guide</b>	<p>Configure the list of the enable authentication method.</p> <p>The enable authentication method can be any one or combination of Local,RADIUS and TACACS.</p> <p>When login method is configuration in combination, the preference goes from left to right. If the users have passed the authentication method, authentication method of lower preferences will be ignored.</p> <p>To be mentioned, if the user receives corresponding protocol's answer whether refuse or incept, it will not attempt the next authentication method (Exception: if the local authentication method failed, it will attempt the next authentication method); it will attempt the next authentication method if it receives nothing.</p> <p>And AAA function RADIUS server should be configured before the RADIUS configuration method can be used. And TACACS server should be configured before the TACACS configuration method can be used.</p> <p>The no command restores the default authentication method.</p>
<b>Example</b>	<p>Configure the enable authentication method to be tacacs and local.</p> <p><b>Switch(config)#authentication enable tacacs local</b></p>

## 4.2.5 authentication ip access-class

<b>Command</b>	<p><b>authentication ip access-class {&lt;num-std&gt; &lt;name&gt;}</b></p> <p><b>no authentication ip access-class</b></p>				
<b>Parameter</b>	<table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 20%;"><b>&lt;num-std&gt;</b></td> <td>the access-class number for standard numeric ACL, ranging between 1-99</td> </tr> <tr> <td><b>&lt;name&gt;</b></td> <td>the access-class name for standard ACL, the character string length is ranging between 1 and 32</td> </tr> </table>	<b>&lt;num-std&gt;</b>	the access-class number for standard numeric ACL, ranging between 1-99	<b>&lt;name&gt;</b>	the access-class name for standard ACL, the character string length is ranging between 1 and 32
<b>&lt;num-std&gt;</b>	the access-class number for standard numeric ACL, ranging between 1-99				
<b>&lt;name&gt;</b>	the access-class name for standard ACL, the character string length is ranging between 1 and 32				
<b>Default</b>	The binding ACL to Telnet/SSH/Web function is closed by default.				
<b>Mode</b>	Global Mode				
<b>Usage Guide</b>	<p>Binding standard IP ACL protocol to login with Telnet/SSH/Web.</p> <p>The no form command will cancel the binding ACL.</p>				
<b>Example</b>	<p>Binding standard IP ACL protocol to access-class 1.</p> <p><b>Switch(config)#authentication ip access-class 1 in</b></p>				

## 4.2.6 authentication ipv6 access-class

<b>Command</b>	<code>authentication ipv6 access-class {&lt;num-std&gt; &lt;name&gt;}</code> <code>no authentication ipv6 access-class</code>
<b>Parameter</b>	<b>&lt;num-std&gt;</b> the access-class number for standard numeric ACL, ranging between 500-599
	<b>&lt;name&gt;</b> the access-class name for standard ACL, the character string length is ranging between 1 and 32
<b>Default</b>	The binding ACL to Telnet/SSH/Web function is closed by default.
<b>Mode</b>	Global Mode
<b>Usage Guide</b>	Binding standard IPv6 ACL protocol to login with Telnet/SSH/Web.
	The no form command will cancel the binding ACL.
<b>Example</b>	Binding standard IP ACL protocol to access-class 500.
	<b>Switch(config)#authentication ipv6 access-class 500 in</b>

## 4.2.7 authentication line login

<b>Command</b>	<p><b>authentication line {console   vty   web} login method1 [method2...]</b></p> <p><b>no authentication line {console   vty   web} login</b></p>								
<b>Parameter</b>	<table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="border: none;"><b>console</b></td> <td>log in through serial port</td> </tr> <tr> <td style="border: none;"><b>vty</b></td> <td>log in through telnet or ssh</td> </tr> <tr> <td style="border: none;"><b>web</b></td> <td>log in through web</td> </tr> <tr> <td style="border: none;"><b>method</b></td> <td> <p>the list of the authentication method, it must be among local, tacacs and radius keywords;</p> <p>local:uses the local database to authenticate;</p> <p>tacacs:uses the remote TACACS+ authentication server to authenticate;</p> <p>radius:uses the remote RADIUS authentication server to authenticate</p> </td> </tr> </table>	<b>console</b>	log in through serial port	<b>vty</b>	log in through telnet or ssh	<b>web</b>	log in through web	<b>method</b>	<p>the list of the authentication method, it must be among local, tacacs and radius keywords;</p> <p>local:uses the local database to authenticate;</p> <p>tacacs:uses the remote TACACS+ authentication server to authenticate;</p> <p>radius:uses the remote RADIUS authentication server to authenticate</p>
<b>console</b>	log in through serial port								
<b>vty</b>	log in through telnet or ssh								
<b>web</b>	log in through web								
<b>method</b>	<p>the list of the authentication method, it must be among local, tacacs and radius keywords;</p> <p>local:uses the local database to authenticate;</p> <p>tacacs:uses the remote TACACS+ authentication server to authenticate;</p> <p>radius:uses the remote RADIUS authentication server to authenticate</p>								
<b>Default</b>	No configuration is enabled for the console login method by default. Local authentication is enabled for the VTY and Web login method by default.								
<b>Mode</b>	Global Mode								
<b>Usage Guide</b>	<p>Configure VTY (login with Telnet and SSH), Web and Console, so as to select the list of the authentication method for the login user.</p> <p>Authentication method can be any one or combination of Local, RADIUS and TACACS.</p> <p>When login method is configuration in combination, the preference goes from left to right.</p> <p>If the users have passed the authentication method, authentication method of lower preferences will be ignored.</p> <p>if the user receives corresponding protocol's answer whether refuse or incept, it will not attempt the next authentication method (Exception: if the local authentication method failed, it will attempt the next authentication method);</p> <p style="padding-left: 20px;">it will attempt the next authentication method if itreceives nothing.</p> <p>And AAA function RADIUS server should be configured before the RADIUS configuration method can be used. And TACACS server should be configured before the TACACS configuration method can be used.</p> <p>The authentication line console login command is exclusive with the "login"command. The authentication line console login command configures the switch to use the Console login method. And the login command makes the Console login to use the passwords configured by the password command for authentication.</p> <p><u>If local authentication is configured while no local users are configured, users will be able to</u></p>								

---

login the switch via the Console method.

The no form command restores the default authentication method.

---

**Example**

---

Configure the telnet and ssh login with the remote RADIUS authentication.

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

---

## 4.2.8 authentication securityip

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

## 4.2.9 authentication securityipv6

<b>Command</b>	<b>authentication securityipv6 &lt;ipv6-addr&gt;</b> <b>no authentication securityipv6 &lt;ipv6-addr&gt;</b>
<b>Parameter</b>	<b>&lt;ip-addr&gt;</b> the security IPv6 address which can login the switch
<b>Default</b>	No security IPv6 addresses are configured by default.
<b>Mode</b>	Global Mode
<b>Usage Guide</b>	<p>To configure the security IPv6 address for Telnet and HTTP login method. IPv6 address of the client which can login the switch is not restricted before the security IPv6 address is not configured.</p> <p>After the security IPv6 address is configured, only clients with security IPv6 addresses are able to login the switch.</p> <p>Up to 32 security IPv6 addresses can be configured in the switch.</p> <p>The no form of this command will remove the specified configuration.</p>
<b>Example</b>	<p>Configure the security IPv6 address is 2001:da8:123:1::1.</p> <p><b>Switch(config)#authentication securityipv6 2001:da8:123:1::1</b></p>



## 4.2.10 authorization

<b>Command</b>	<b>authorization line {console   vty   web} exec method [method...]</b> <b>no authorization line {console   vty   web} exec</b>								
<b>Parameter</b>	<table border="1"> <tr> <td><b>console</b></td> <td>log in through serial port</td> </tr> <tr> <td><b>vty</b></td> <td>log in through telnet or ssh</td> </tr> <tr> <td><b>web</b></td> <td>log in through web</td> </tr> <tr> <td><b>method</b></td> <td> <p>the list of the authentication method, it must be among local, tacacs and radius keywords;</p> <p>local:uses the local database to authenticate;</p> <p>tacacs:uses the remote TACACS+ authentication server to authenticate;</p> <p>radius:uses the remote RADIUS authentication server to authenticate</p> </td> </tr> </table>	<b>console</b>	log in through serial port	<b>vty</b>	log in through telnet or ssh	<b>web</b>	log in through web	<b>method</b>	<p>the list of the authentication method, it must be among local, tacacs and radius keywords;</p> <p>local:uses the local database to authenticate;</p> <p>tacacs:uses the remote TACACS+ authentication server to authenticate;</p> <p>radius:uses the remote RADIUS authentication server to authenticate</p>
<b>console</b>	log in through serial port								
<b>vty</b>	log in through telnet or ssh								
<b>web</b>	log in through web								
<b>method</b>	<p>the list of the authentication method, it must be among local, tacacs and radius keywords;</p> <p>local:uses the local database to authenticate;</p> <p>tacacs:uses the remote TACACS+ authentication server to authenticate;</p> <p>radius:uses the remote RADIUS authentication server to authenticate</p>								
<b>Default</b>	There is no authorization method by default.								
<b>Mode</b>	Global Mode								
<b>Usage Guide</b>	<p>Configure the list of the authorization method for the login user with VTY (login with Telnet and SSH), Web and Console.</p> <p>And authorization method can be any one or combination of Local,RADIUS or TACACS.</p> <p>When login method is configuration in combination, the preference goes from left to right.</p> <p>If the users have passed the authorization method, authorization method of lower preferences will be ignored.</p> <p>if the user receives corresponding protocol's answer whether refuse or incept, it will not attempt the next authorization method; it will attempt the next authorization method if it receives nothing.</p> <p>And AAA function RADIUS server should be configured before the RADIUS configuration method can be used. And TACACS server should be configured before the TACACS configuration method can be used.</p> <p>The local users adopt username command permission while authorization command is not configured, the users login the switch via RADIUS/TACACS method and works under common mode.</p> <p>The no command restores the default authorization method.</p>								
<b>Example</b>	<p>Configure the telnet authorization method to RADIUS.</p> <p><b>Switch(config)#authorization line vty exec radius</b></p>								

## 4.2.11 authorization line vty command

<b>Command</b>	<p>authorization line vty command &lt;1-15&gt; {local   radius   tacacs} (none)</p> <p>no authorization line vty command &lt;1-15&gt;</p>										
<b>Parameter</b>	<table border="1"> <tr> <td><b>command &lt;1-15&gt;</b></td> <td>Level scope of authorization orders 1~15</td> </tr> <tr> <td><b>local</b></td> <td>Authorization is granted locally</td> </tr> <tr> <td><b>radius</b></td> <td>Authorization for remote radius</td> </tr> <tr> <td><b>tacacs</b></td> <td>Authorization for remote tacacs</td> </tr> <tr> <td><b>none</b></td> <td>Authorization mode is empty</td> </tr> </table>	<b>command &lt;1-15&gt;</b>	Level scope of authorization orders 1~15	<b>local</b>	Authorization is granted locally	<b>radius</b>	Authorization for remote radius	<b>tacacs</b>	Authorization for remote tacacs	<b>none</b>	Authorization mode is empty
<b>command &lt;1-15&gt;</b>	Level scope of authorization orders 1~15										
<b>local</b>	Authorization is granted locally										
<b>radius</b>	Authorization for remote radius										
<b>tacacs</b>	Authorization for remote tacacs										
<b>none</b>	Authorization mode is empty										
<b>Default</b>	The authorization manner is not configured as default.										
<b>Mode</b>	Global Mode										
<b>Usage Guide</b>	<p>Configure command authorization manner and authorization selection priority of login user with VTY (login with Telnet and SSH).</p> <p>The enabling authorization method can be any one or combination of Local. RADIUS and TACACS.</p> <p>When using combination authorization manners, the priority of the front authorization manner is the highest and the others are in descending order.</p> <p>If the authorization with high priority passed, it is successful to configure command and the back authorization manner will be ignored.</p> <p>As long as one authorization manner receives a clear response of the corresponding agreement. Whether it is received or refused, the next authorization manner will not be attempted. If the clear response is not received, try the next manner.</p> <p>When using RADIUS authorization, AAA function must be enabled and configure RADIUS server. when using TACACS authorization, TACACS server must be configured.</p> <p>None is the manner of escaping and it only can be the last manner.</p> <p>This manner returns to passed authorization directly and it is successful to configure the command.</p> <p>The no command recovers to be default manner.</p>										
<b>Example</b>	<p>Configure level 1 command authorization manner of telnet login user as TACACS.</p> <p><b>Switch(config)#authorization line vty command 1 tacacs</b></p>										

## 4.2.12 clear line vty <0-31>

<b>Command</b>	<b>clear line vty &lt;0-31&gt;</b>
<b>Parameter</b>	<b>&lt;0-31&gt;</b> appointed line
<b>Default</b>	None.
<b>Mode</b>	Admin Mode
<b>Usage Guide</b>	After inputting this command, there is need to judge for this command, "Confirm[Y/N]: ", when inputting "Y" or "y", run to delete; when inputting "? ", do not run to delete, print the notice information only. When inputting other characters, do not run to delete.
<b>Example</b>	Admin users who are forced to log in through VTY (using Telnet or SSH login) are off line.  <b>Switch#clear line vty 0</b> Confirm[Y/N]:y [OK]

## 4.2.13 crypto key clear rsa

<b>Command</b>	crypto key clear rsa
<b>Parameter</b>	none                      none
<b>Default</b>	None.
<b>Mode</b>	Admin Mode
<b>Usage Guide</b>	This command is used to clear the secret key of the ssh and close the ssh service.
<b>Example</b>	<p>Clear the secret key of the ssh and close the ssh service.</p> <pre>Switch#crypto key clear rsa ssh host key is cleared successfully. ssh is closed successfully.</pre>

## 4.2.14 terminal length

<b>Command</b>	terminal length <0-512> terminal no length
<b>Parameter</b>	<0-512> Length of characters displayed in each screen, ranging between 0-512 (0 refers to non-stop display)
<b>Default</b>	Default Length is 25.
<b>Mode</b>	Admin Mode
<b>Usage Guide</b>	<p>Set length of characters displayed in each screen on terminal, so that the-More-message will be shown when displayed information exceeds the screen. Press any key to show information in next screen.</p> <p>The "terminal no length" cancels the screen switching operation and display content once in all.</p>
<b>Example</b>	<p>Configure length of characters in each display to 20.</p> <p><b>Switch#terminal length 20</b></p>

## 4.2.15 telnet

<b>Command</b>	<code>telnet [vrf &lt;vrf-name&gt;] [&lt;ip-addr&gt;   &lt;ipv6-addr&gt;   host &lt;hostname&gt;][&lt;port&gt;]</code>										
<b>Parameter</b>	<table border="1"> <tr> <td><code>&lt;vrf-name&gt;</code></td> <td>the specific VRF name</td> </tr> <tr> <td><code>&lt;ip-addr&gt;</code></td> <td>the IP address of the remote host, shown in dotted decimal notation</td> </tr> <tr> <td><code>&lt;ipv6-addr&gt;</code></td> <td>the IPv6 address of the remote host</td> </tr> <tr> <td><code>&lt;hostname&gt;</code></td> <td>the name of the remote host, containing max 64 characters</td> </tr> <tr> <td><code>&lt;port&gt;</code></td> <td>the port number, ranging between 0 and 65535</td> </tr> </table>	<code>&lt;vrf-name&gt;</code>	the specific VRF name	<code>&lt;ip-addr&gt;</code>	the IP address of the remote host, shown in dotted decimal notation	<code>&lt;ipv6-addr&gt;</code>	the IPv6 address of the remote host	<code>&lt;hostname&gt;</code>	the name of the remote host, containing max 64 characters	<code>&lt;port&gt;</code>	the port number, ranging between 0 and 65535
<code>&lt;vrf-name&gt;</code>	the specific VRF name										
<code>&lt;ip-addr&gt;</code>	the IP address of the remote host, shown in dotted decimal notation										
<code>&lt;ipv6-addr&gt;</code>	the IPv6 address of the remote host										
<code>&lt;hostname&gt;</code>	the name of the remote host, containing max 64 characters										
<code>&lt;port&gt;</code>	the port number, ranging between 0 and 65535										
<b>Default</b>	None.										
<b>Mode</b>	Admin Mode										
<b>Usage Guide</b>	<p>This command is used when the switch is applied as Telnet client, for logging on remote host to configure.</p> <p>When a switch is applied as a Telnet client, it can only establish one TCP connection with the remote host.</p> <p>To connect to another remote host, the current TCP connection must be disconnected with a hotkey "CTRL+ \".</p> <p>To telnet a host name, mapping relationship between the host name and the IP/IPv6 address should be previously configured.</p> <p>For required commands please refer to ip host and ipv6 host.</p> <p>In case a host corresponds to both an IPv4 and an IPv6 addresses, the IPv6 should be preferred when telnetting this host name.</p>										
<b>Example</b>	<p>The switch telnets to a remote host whose IP address is 20.1.1.1.</p> <pre> <b>Switch#telnet 20.1.1.1 23</b> Connecting Host 20.1.1.1 Port 23... Service port is 23 Connected to 20.1.1.1 login:123 password:*** router&gt; </pre>										

## 4.2.16 telnet server enable

<b>Command</b>	<b>telnet server enable</b> <b>no telnet server enable</b>
<b>Parameter</b>	<b>none</b> none
<b>Default</b>	Telnet server function is enabled by default.
<b>Mode</b>	Global Mode
<b>Usage Guide</b>	<p>Enable the Telnet server function in the switch</p> <p>This command is available in Console only.</p> <p>The administrator can use this command to enable or disable the Telnet client to login to the switch.</p> <p>The “no telnet server enable”command disables the Telnet function in the switch.</p>
<b>Example</b>	<p>Disable the Telnet server function in the switch.</p> <p><b>Switch(config)#no telnet server enable</b></p>

## 4.2.17 telnet-server max-connection

<b>Command</b>	<b>telnet-server max-connection {&lt;max-connection-number&gt;   default}</b>	
<b>Parameter</b>	<b>&lt;max-connection-number&gt;</b>	the max connection number supported by the Telnet service, ranging from 5 to 16
	<b>default</b>	restore the default configuration
	<b>Default</b>	The system default value of the max connection number is 5.
<b>Mode</b>	Global Mode	
<b>Usage Guide</b>	Configure the max connection number supported by the Telnet service of the switch.	
<b>Example</b>	Set the max connection number supported by the Telnet service as 10.	
	<b>Switch(config)#telnet-server max-connection 10</b>	



## 4.2.18 ssh-server authentication-retries

<b>Command</b>	<b>ssh-server authentication-retries &lt;authentication-retries&gt;</b> <b>no ssh-server authentication-retries</b>
<b>Parameter</b>	<b>&lt;authentication-retries&gt;</b> the number of times for retrying authentication, valid range is 1 to 10
<b>Default</b>	The number of times for retrying SSH authentication is 3 by default.
<b>Mode</b>	Global Mode
<b>Usage Guide</b>	Configure the number of times for retrying SSH authentication.  The “no ssh-server authentication-retries” command restores the default number of times for retrying SSH authentication.
<b>Example</b>	Set the time for retrying SSH authentication to 5.  <b>Switch(config)#ssh-server authentication-retries 5</b>

## 4.2.19 ssh-server enable

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

## 4.2.20 ssh-server host-key create rsa

<b>Command</b>	<b>ssh-server host-key create rsa [modulus &lt; modulus &gt;]</b>
<b>Parameter</b>	<b>&lt; modulus &gt;</b> the modulus which is used to compute the host key; valid range is 768 to 2048. The default value is 1024
<b>Default</b>	The system uses the key generated when the ssh-server is started at the first time.
<b>Mode</b>	Global Mode
<b>Usage Guide</b>	<p>This command is used to generate a new SSH service host rsa key.</p> <p>When SSH client logs on the server, the new host key is used for authentication. After the new host key is generated and "write" command is used to save the configuration, the system uses this key for authentication all the time. Because it takes quite a long time to compute the new key and some clients are not compatible with the key generated by the modulus 2048, it is recommended to use the key which is generated by the default modulus 1024.</p> <p>No command disables SSH service.</p>
<b>Example</b>	<p>Generate new host key.</p> <p><b>Switch(config)#ssh-server host-key create rsa</b></p>

## 4.2.21 ssh-server max-connection

<b>Command</b>	<b>ssh-server max-connection {&lt;max-connection-number&gt; default}</b>	
<b>Parameter</b>	<b>&lt;max-connection-number&gt;</b>	the max connection number supported by the SSH service, ranging from 5 to 16.
	<b>default</b>	restore default
	<b>Default</b>	
<b>Default</b>	The system default value of the max connection number is 5.	
<b>Mode</b>	Global Mode	
<b>Usage Guide</b>	Configure the max connection number supported by the SSH service of the switch.	
<b>Example</b>	Set the max connection number supported by the SSH service as 10.	
	<b>Switch(config)#ssh-server max-connection 10</b>	

## 4.2.22 ssh-server timeout

<b>Command</b>	<b>ssh-server timeout &lt;timeout&gt;</b> <b>no ssh-server timeout</b>
<b>Parameter</b>	<b>&lt;timeout&gt;</b> timeout value; valid range is 10 to 600 seconds
<b>Default</b>	SSH authentication timeout is 180 seconds by default.
<b>Mode</b>	Global Mode
<b>Usage Guide</b>	Configure timeout value for SSH authentication.  The “no ssh-server timeout”command restores the default timeout value for SSH authentication.
<b>Example</b>	Set SSH authentication timeout to 240 seconds.  <b>Switch(config)#ssh-server timeout 240</b>

### 4.2.23 show crypto key

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

## 4.2.24 show ssh-server

<b>Command</b>	<b>show ssh-server</b>
<b>Parameter</b>	<b>none</b> none
<b>Default</b>	None.
<b>Mode</b>	Admin Mode
<b>Usage Guide</b>	Display SSH state and users which log on currently.
<b>Example</b>	<p>Display SSH state and users which log on currently.</p> <pre> <b>Switch#show ssh-server</b> ssh server is enabled ssh-server timeout 180s ssh-server authentication-retries 3 ssh-server max-connection number 6 ssh-server login user number 2 </pre>

## 4.2.25 show telnet login

<b>Command</b>	<b>show telnet login</b>
<b>Parameter</b>	<b>none</b> none
<b>Default</b>	None.
<b>Mode</b>	Admin Mode
<b>Usage Guide</b>	Display the information of the Telnet client which currently establishes a Telnet connection with the switch.
<b>Example</b>	Display Telnet client information.  <b>Switch#show telnet login</b> Authenticate login by local Login user: aa



## 4.2.26 show users

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

## 4.2.27 who

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

## 4.3 Configuring Switch IP

### 4.3.1 interface vlan

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

### 4.3.2 ip address

<b>Command</b>	<p><b>ip address &lt;ip-address&gt; &lt;mask&gt; [secondary]</b></p> <p><b>no ip address [&lt;ip-address&gt; &lt;mask&gt;] [secondary]</b></p>						
<b>Parameter</b>	<table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="border: none;"><b>&lt;ip-address&gt;</b></td> <td style="border: none;">the IP address in dot decimal format</td> </tr> <tr> <td style="border: none;"><b>&lt;mask&gt;</b></td> <td style="border: none;">the subnet mask in dot decimal format</td> </tr> <tr> <td style="border: none;"><b>[secondary]</b></td> <td style="border: none;">indicates the IP configured is a secondary IP address</td> </tr> </table>	<b>&lt;ip-address&gt;</b>	the IP address in dot decimal format	<b>&lt;mask&gt;</b>	the subnet mask in dot decimal format	<b>[secondary]</b>	indicates the IP configured is a secondary IP address
<b>&lt;ip-address&gt;</b>	the IP address in dot decimal format						
<b>&lt;mask&gt;</b>	the subnet mask in dot decimal format						
<b>[secondary]</b>	indicates the IP configured is a secondary IP address						
<b>Default</b>	No IP address is configured upon switch shipment.						
<b>Mode</b>	VLAN Interface Mode						
<b>Usage Guide</b>	<p>Set the IP address and mask for the specified VLAN interface.</p> <p>A VLAN interface must be created first before the user can assign an IP address to the switch.</p> <p>The no command deletes the specified IP address setting.</p>						
<b>Example</b>	<p>Set 10.1.128.1/24 as the IP address of VLAN1 interface.</p> <pre> Switch(config)#interface vlan 1 Switch(Config-if-Vlan1)#ip address 10.1.128.1 255.255.255.0 Switch(Config-if-Vlan1)#exit Switch(config)# </pre>						

### 4.3.3 ipv6 address

<b>Command</b>	<p><b>ipv6 address &lt;ipv6address   prefix-length&gt; [eui-64]</b></p> <p><b>no ipv6 address &lt;ipv6address   prefix-length&gt; [eui-64]</b></p>						
<b>Parameter</b>	<table border="1"> <tr> <td><b>&lt;ipv6address &gt;</b></td> <td>the prefix of an IPV6 address</td> </tr> <tr> <td><b>&lt;prefix-length&gt;</b></td> <td>the length of the prefix of an IPV6 address, ranging from 3 to 128</td> </tr> <tr> <td><b>[eui-64]</b></td> <td>means that the eui64 interface id of the interface will automatically create an IPV6 address</td> </tr> </table>	<b>&lt;ipv6address &gt;</b>	the prefix of an IPV6 address	<b>&lt;prefix-length&gt;</b>	the length of the prefix of an IPV6 address, ranging from 3 to 128	<b>[eui-64]</b>	means that the eui64 interface id of the interface will automatically create an IPV6 address
<b>&lt;ipv6address &gt;</b>	the prefix of an IPV6 address						
<b>&lt;prefix-length&gt;</b>	the length of the prefix of an IPV6 address, ranging from 3 to 128						
<b>[eui-64]</b>	means that the eui64 interface id of the interface will automatically create an IPV6 address						
<b>Default</b>	No IPv6 address is configured upon switch shipment.						
<b>Mode</b>	VLAN Interface Mode						
<b>Usage Guide</b>	<p>Configure aggregatable global unicast address, site-local address and link-local address for the interface.</p> <p>The prefix of an IPV6 address should not be a multicast address, or other kinds of IPV6 addresses with specific usage.</p> <p>Different layer-three VLAN interfaces are forbidden to share a same address prefix. As for any global unicast address, the prefix should be limited in the range from 2001:: to 3fff ::, with a length no shorter than 3. And the prefix length of a site-local address or a link-local address should not be shorter than 10.</p> <p>The no command deletes the specified IPv6 address setting.</p>						
<b>Example</b>	<p>Configure an IPV6 address at the layer-three interface of VLAN1: set the prefix as 2001:3f:ed8::99, the length of which is 64.</p> <pre> Switch(config)#interface vlan 1 Switch(Config-if-Vlan1)#ipv6 address 2001:3f:ed8::99/64 Switch(Config-if-Vlan1)#exit Switch(config)# </pre>						

### 4.3.4 ip bootp-client enable

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

### 4.3.5 ip dhcp-client enable

<b>Command</b>	<p><b>ip dhcp-client enable</b></p> <p><b>no ip dhcp-client enable</b></p>
<b>Parameter</b>	<p><b>none</b>                      none</p>
<b>Default</b>	<p>By default, the dhcp service is disabled.</p>
<b>Mode</b>	<p>VLAN Interface Mode</p>
<b>Usage Guide</b>	<p>Enables the switch to be a DHCP client and obtain IP address and gateway address through DHCP negotiation.</p> <p>To obtain IP address via DHCP, a DHCP server is required in the network.</p> <p>Obtaining IP address by DHCP, Manual configuration and BootP are mutually exclusive, enabling any 2 methods for obtaining an IP address is not allowed.</p> <p>The no command disables the DHCP client function and releases the IP address obtained in DHCP.</p>
<b>Example</b>	<p>Getting an IP address through DHCP.</p> <pre> Switch(config)#interface vlan 1 Switch(Config-if-Vlan1)#ip dhcp-client enable Switch(Config-if-Vlan1)#exit Switch(config)# </pre>

## 4.4 SNMP

### 4.4.1 rmon enable

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



## 4.4.2 show private-mib oid

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

### 4.4.3 show snmp

<b>Command</b>	<b>show snmp</b>
<b>Parameter</b>	<b>none</b> none
<b>Default</b>	None.
<b>Mode</b>	Admin and configuration mode
<b>Usage Guide</b>	Display all SNMP counter information.
<b>Example</b>	<p>Display all SNMP counter information.</p> <pre> <b>Switch#show snmp</b> 0 SNMP packets input 0 Bad SNMP version errors 0 Unknown community name 0 Illegal operation for community name supplied 0 Encoding errors 0 Number of requested variables 0 Number of altered variables 0 Get-request PDUs 0 Get-next PDUs 0 Set-request PDUs 0 SNMP packets output 0 Too big errors (Max packet size 1500) 0 No such name errors 0 Bad values errors 0 General errors 0 Get-response PDUs 0 SNMP trap PDUs </pre>

### 4.4.4 show snmp engineid

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

### 4.4.5 show snmp group

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

## 4.4.6 show snmp mib

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

### 4.4.7 show snmp status

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

### 4.4.8 show snmp user

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

### 4.4.9 show snmp view

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



## 4.4.10 snmp-server community

<b>Command</b>	<pre>snmp-server community {ro   rw} {0   7} &lt;string&gt; [access {&lt;num-std&gt;   &lt;name&gt;}] [ipv6-access {&lt;ipv6-num-std&gt;   &lt;ipv6-name&gt;}] [read &lt;read-view-name&gt;] [write &lt;write-view-name&gt;] no snmp-server community {ro   rw} {0   7} &lt;string&gt; [access {&lt;num-std&gt;   &lt;name&gt;}] [ipv6-access {&lt;ipv6-num-std&gt;   &lt;ipv6-name&gt;}]</pre>																		
<b>Parameter</b>	<table border="1"> <tr> <td><b>{ro   rw}</b></td> <td>the specified access mode to MIB, ro for read-only and rw for read-write</td> </tr> <tr> <td><b>{0   7}</b></td> <td>if key option is set as 0, the specified community string is not encrypted, if key option is set as 7, the specified community string is encrypted</td> </tr> <tr> <td><b>&lt;string&gt;</b></td> <td>the configured community string</td> </tr> <tr> <td><b>&lt;num-std&gt;</b></td> <td>the access-class number for standard numeric ACL, ranging between 1-99</td> </tr> <tr> <td><b>&lt;name&gt;</b></td> <td>the access-class name for standard ACL, the character string length is ranging between 1-32</td> </tr> <tr> <td><b>&lt;ipv6-num-std&gt;</b></td> <td>the access-class number for standard numeric IPv6 ACL, ranging between 500-599</td> </tr> <tr> <td><b>&lt;ipv6-name&gt;</b></td> <td>the access-class name for standard IPv6 ACL, the character string length is ranging between 1-32</td> </tr> <tr> <td><b>&lt;read-view-name&gt;</b></td> <td>the name of readable view which includes 1-32 characters</td> </tr> <tr> <td><b>&lt;write-view-name&gt;</b></td> <td>the name of writable view which includes 1-32 characters</td> </tr> </table>	<b>{ro   rw}</b>	the specified access mode to MIB, ro for read-only and rw for read-write	<b>{0   7}</b>	if key option is set as 0, the specified community string is not encrypted, if key option is set as 7, the specified community string is encrypted	<b>&lt;string&gt;</b>	the configured community string	<b>&lt;num-std&gt;</b>	the access-class number for standard numeric ACL, ranging between 1-99	<b>&lt;name&gt;</b>	the access-class name for standard ACL, the character string length is ranging between 1-32	<b>&lt;ipv6-num-std&gt;</b>	the access-class number for standard numeric IPv6 ACL, ranging between 500-599	<b>&lt;ipv6-name&gt;</b>	the access-class name for standard IPv6 ACL, the character string length is ranging between 1-32	<b>&lt;read-view-name&gt;</b>	the name of readable view which includes 1-32 characters	<b>&lt;write-view-name&gt;</b>	the name of writable view which includes 1-32 characters
<b>{ro   rw}</b>	the specified access mode to MIB, ro for read-only and rw for read-write																		
<b>{0   7}</b>	if key option is set as 0, the specified community string is not encrypted, if key option is set as 7, the specified community string is encrypted																		
<b>&lt;string&gt;</b>	the configured community string																		
<b>&lt;num-std&gt;</b>	the access-class number for standard numeric ACL, ranging between 1-99																		
<b>&lt;name&gt;</b>	the access-class name for standard ACL, the character string length is ranging between 1-32																		
<b>&lt;ipv6-num-std&gt;</b>	the access-class number for standard numeric IPv6 ACL, ranging between 500-599																		
<b>&lt;ipv6-name&gt;</b>	the access-class name for standard IPv6 ACL, the character string length is ranging between 1-32																		
<b>&lt;read-view-name&gt;</b>	the name of readable view which includes 1-32 characters																		
<b>&lt;write-view-name&gt;</b>	the name of writable view which includes 1-32 characters																		
<b>Default</b>	None.																		
<b>Mode</b>	Global Mode																		
<b>Usage Guide</b>	<p>Configure the community string for the switch.</p> <p>The switch supports up to 4 community strings. It can realize the access-control for specifically community view by binding the community name to specifically readable view or writable view.</p> <p>The no command deletes the configured community string.</p>																		
<b>Example</b>	<p>Add a community string named "private" with read-write permission.</p> <pre>Switch(config)#snmp-server community rw 0 private</pre> <p>Delete the community string named "private".</p> <pre>Switch(config)#no snmp-server community 0 private</pre>																		

### 4.4.11 snmp-server enable

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

## 4.4.12 snmp-server enable traps

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

### 4.4.13 snmp-server engineid

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

## 4.4.14 snmp-server group

<b>Command</b>	<pre>snmp-server group &lt;group-string&gt; {NoauthNopriv   AuthNopriv   AuthPriv} [[read &lt;read-string&gt;] [write &lt;write-string&gt;] [notify &lt;notify-string&gt;]] [access {&lt;num-std&gt;   &lt;name&gt;}] [ipv6-access {&lt;ipv6-num-std&gt;   &lt;ipv6-name&gt;}] no snmp-server group &lt;group-string&gt; {NoauthNopriv   AuthNopriv   AuthPriv} [access {&lt;num-std&gt;   &lt;name&gt;}] [ipv6-access {&lt;ipv6-num-std&gt;   &lt;ipv6-name&gt;}]</pre>																						
<b>Parameter</b>	<table border="1"> <tr> <td><b>&lt;group-string&gt;</b></td> <td>group name which includes 1-32 characters</td> </tr> <tr> <td><b>NoauthNopriv</b></td> <td>Applies the non recognizing and non encrypting safety level</td> </tr> <tr> <td><b>AuthNopriv</b></td> <td>Applies the recognizing but non encrypting safety level</td> </tr> <tr> <td><b>AuthPriv</b></td> <td>Applies the recognizing and encrypting safety level</td> </tr> <tr> <td><b>&lt;read-string&gt;</b></td> <td>Name of readable view which includes 1-32 characters</td> </tr> <tr> <td><b>&lt;write-string&gt;</b></td> <td>Name of writable view which includes 1-32 characters</td> </tr> <tr> <td><b>&lt;notify-string&gt;</b></td> <td>Name of trappable view which includes 1-32 characters</td> </tr> <tr> <td><b>&lt;num-std&gt;</b></td> <td>the access-class number for standard numeric ACL, ranging between 1-99</td> </tr> <tr> <td><b>&lt;name&gt;</b></td> <td>the access-class name for standard ACL, the character string length is ranging between 1-32</td> </tr> <tr> <td><b>&lt;ipv6-num-std&gt;</b></td> <td>the access-class number for standard numeric IPv6 ACL, ranging between 500-599</td> </tr> <tr> <td><b>&lt;ipv6-name&gt;</b></td> <td>the access-class name for standard IPv6 ACL, the character string length is ranging between 1-32</td> </tr> </table>	<b>&lt;group-string&gt;</b>	group name which includes 1-32 characters	<b>NoauthNopriv</b>	Applies the non recognizing and non encrypting safety level	<b>AuthNopriv</b>	Applies the recognizing but non encrypting safety level	<b>AuthPriv</b>	Applies the recognizing and encrypting safety level	<b>&lt;read-string&gt;</b>	Name of readable view which includes 1-32 characters	<b>&lt;write-string&gt;</b>	Name of writable view which includes 1-32 characters	<b>&lt;notify-string&gt;</b>	Name of trappable view which includes 1-32 characters	<b>&lt;num-std&gt;</b>	the access-class number for standard numeric ACL, ranging between 1-99	<b>&lt;name&gt;</b>	the access-class name for standard ACL, the character string length is ranging between 1-32	<b>&lt;ipv6-num-std&gt;</b>	the access-class number for standard numeric IPv6 ACL, ranging between 500-599	<b>&lt;ipv6-name&gt;</b>	the access-class name for standard IPv6 ACL, the character string length is ranging between 1-32
<b>&lt;group-string&gt;</b>	group name which includes 1-32 characters																						
<b>NoauthNopriv</b>	Applies the non recognizing and non encrypting safety level																						
<b>AuthNopriv</b>	Applies the recognizing but non encrypting safety level																						
<b>AuthPriv</b>	Applies the recognizing and encrypting safety level																						
<b>&lt;read-string&gt;</b>	Name of readable view which includes 1-32 characters																						
<b>&lt;write-string&gt;</b>	Name of writable view which includes 1-32 characters																						
<b>&lt;notify-string&gt;</b>	Name of trappable view which includes 1-32 characters																						
<b>&lt;num-std&gt;</b>	the access-class number for standard numeric ACL, ranging between 1-99																						
<b>&lt;name&gt;</b>	the access-class name for standard ACL, the character string length is ranging between 1-32																						
<b>&lt;ipv6-num-std&gt;</b>	the access-class number for standard numeric IPv6 ACL, ranging between 500-599																						
<b>&lt;ipv6-name&gt;</b>	the access-class name for standard IPv6 ACL, the character string length is ranging between 1-32																						
<b>Default</b>	None.																						
<b>Mode</b>	Global Mode																						
<b>Usage Guide</b>	<p>This command is used to configure a new group.</p> <p>There is a default view "v1defaultviewname" in the system. It is recommended to use this view as the view name of the notification. If the read or write view name is empty, corresponding operation will be disabled.</p> <p>The "no" form of this command deletes this group.</p>																						
<b>Example</b>	<p>Create a group CompanyGroup, with the safety level of recognizing and encrypting, the read viewname is readview, and the writing is disabled.</p> <pre>Switch (config)#snmp-server group CompanyGroup AuthPriv read readview</pre>																						

## 4.4.15 snmp-server host

<b>Command</b>	<pre>snmp-server host { &lt;host-ipv4-address&gt;   &lt;host-ipv6-address&gt; } {v1   v2c   {v3 {NoauthNopriv   AuthNopriv   AuthPriv}}} &lt;user-string&gt; no snmp-server host { &lt;host-ipv4-address&gt;   &lt;host-ipv6-address&gt; } {v1   v2c   {v3 {NoauthNopriv   AuthNopriv   AuthPriv}}} &lt;user-string&gt;</pre>														
<b>Parameter</b>	<table border="1"> <tr> <td><b>&lt;host-ipv4-address&gt;</b></td> <td>IP address of NMS management station which receives Trap message</td> </tr> <tr> <td><b>&lt;host-ipv6-address&gt;</b></td> <td>IPv6 address of NMS management station which receives Trap message</td> </tr> <tr> <td><b>v1   v2c   v3</b></td> <td>the version number when sending the trap</td> </tr> <tr> <td><b>NoauthNopriv</b></td> <td>Applies the non recognizing and non encrypting safety level</td> </tr> <tr> <td><b>AuthNopriv</b></td> <td>Applies the recognizing but non encrypting safety level</td> </tr> <tr> <td><b>AuthPriv</b></td> <td>Applies the recognizing and encrypting safety level</td> </tr> <tr> <td><b>&lt;user-string&gt;</b></td> <td>the community character string applied when sending the Trap message at v1/v2, and will be the user name at v3</td> </tr> </table>	<b>&lt;host-ipv4-address&gt;</b>	IP address of NMS management station which receives Trap message	<b>&lt;host-ipv6-address&gt;</b>	IPv6 address of NMS management station which receives Trap message	<b>v1   v2c   v3</b>	the version number when sending the trap	<b>NoauthNopriv</b>	Applies the non recognizing and non encrypting safety level	<b>AuthNopriv</b>	Applies the recognizing but non encrypting safety level	<b>AuthPriv</b>	Applies the recognizing and encrypting safety level	<b>&lt;user-string&gt;</b>	the community character string applied when sending the Trap message at v1/v2, and will be the user name at v3
<b>&lt;host-ipv4-address&gt;</b>	IP address of NMS management station which receives Trap message														
<b>&lt;host-ipv6-address&gt;</b>	IPv6 address of NMS management station which receives Trap message														
<b>v1   v2c   v3</b>	the version number when sending the trap														
<b>NoauthNopriv</b>	Applies the non recognizing and non encrypting safety level														
<b>AuthNopriv</b>	Applies the recognizing but non encrypting safety level														
<b>AuthPriv</b>	Applies the recognizing and encrypting safety level														
<b>&lt;user-string&gt;</b>	the community character string applied when sending the Trap message at v1/v2, and will be the user name at v3														
<b>Default</b>	None.														
<b>Mode</b>	Global Mode														
<b>Usage Guide</b>	<p>As for the v1/v2c versions this command configures the IPv4 or IPv6 address and Trap community character string of the network manage station receiving the SNMP Trap message. And for v3 version, this command is used for receiving the network manage station IPv4 or IPv6 address and the Trap user name and safety level.</p> <p>The Community character string configured in this command is the default community string of the RMON event group. If the RMON event group has no community character string configured, the community character string configured in this command will be applied when sending the Trap of RMON, and if the community character string is configured, its configuration will be applied when sending the RMON trap. This command allows to configure IPv4 or IPv6 addresses of SNMP management station that receive Trap message at the same time, but IPv4 and IPv6 addresses of v1 and v2c version are less than 8 in all.</p> <p>The “no”form of this command cancels this IPv4 or IPv6 address.</p>														
<b>Example</b>	<p>Configure an IP address to receive Trap.</p> <pre>Switch(config)#snmp-server host 1.1.1.5 v1 usertrap</pre>														

## 4.4.16 snmp-server securityip

<b>Command</b>	<pre>snmp-server securityip {&lt;ipv4-address&gt;   &lt;ipv6-address&gt;} no snmp-server securityip {&lt;ipv4-address&gt;   &lt;ipv6-address&gt;}</pre>				
<b>Parameter</b>	<table border="1"> <tr> <td><b>&lt;ipv4-address&gt;</b></td> <td>NMS security IPv4 address, dotted decimal notation</td> </tr> <tr> <td><b>&lt;ipv6-address&gt;</b></td> <td>NMS security IPv6 address, colon hexadecimal</td> </tr> </table>	<b>&lt;ipv4-address&gt;</b>	NMS security IPv4 address, dotted decimal notation	<b>&lt;ipv6-address&gt;</b>	NMS security IPv6 address, colon hexadecimal
<b>&lt;ipv4-address&gt;</b>	NMS security IPv4 address, dotted decimal notation				
<b>&lt;ipv6-address&gt;</b>	NMS security IPv6 address, colon hexadecimal				
<b>Default</b>	None.				
<b>Mode</b>	Global Mode				
<b>Usage Guide</b>	<p>Configure security IPv4 or IPv6 address allowed to access NMS management station</p> <p>It is only the consistency between NMS administration station IPv4 or IPv6 address and security IPv4 or IPv6 address configured by the command, so it send SNMP packet could be processed by switch, the command only applies to SNMP. Allows configuration the IPv4 or IPv6 address of the network manage station receiving the SNMP Trap message, but the IP addresses are less than 20 in all.</p> <p>The no command deletes security IPv4 or IPv6 address configured.</p>				
<b>Example</b>	<p>Configure security IP address of NMS management station.</p> <pre><b>Switch(config)#snmp-server securityip 1.1.1.5</b></pre>				

## 4.4.17 snmp-server securityip enable

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



## 4.4.18 snmp-server trap-source

<b>Command</b>	<pre>snmp-server trap-source {&lt;ipv4-address&gt;   &lt;ipv6-address&gt;} no snmp-server trap-source {&lt;ipv4-address&gt;   &lt;ipv6-address&gt;}</pre>	
<b>Parameter</b>	<b>&lt;ipv4-address&gt;</b>	IPv4 address is used to send trap packet in dotted decimal notation
	<b>&lt;ipv6-address&gt;</b>	IPv6 address is used to send trap packet in colon hexadecimal
<b>Default</b>	None.	
<b>Mode</b>	Global Mode	
<b>Usage Guide</b>	<p>Set the source IPv4 or IPv6 address which is used to send trap packet.</p> <p>If there is no configuration, select the source address according to the interface address sent by actual trap packet, when configure the IP address, adopt the configured source address as the source address of trap packet.</p> <p>The no command deletes the configuration.</p>	
<b>Example</b>	<p>Set the IP address which is used to send trap packet.</p> <pre>Switch(config)#snmp-server trap-source 1.1.1.5</pre>	

## 4.4.19 snmp-server user

<b>Command</b>	<pre>snmp-server user &lt;use-string&gt; &lt;group-string&gt; [{authPriv [auth {md5   sha} &lt;word&gt;]}   {authNoPriv [{3des   aes   des} &lt;word&gt;]} [auth {md5   sha} &lt;word&gt;]] [access {&lt;num-std&gt; &lt;name&gt;}] [ipv6-access {&lt;ipv6-num-std&gt; &lt;ipv6-name&gt;}]  no snmp-server user &lt;user-string&gt; [access {&lt;num-std&gt; &lt;name&gt;}] [ipv6-access {&lt;ipv6-num-std&gt; &lt;ipv6-name&gt;}]</pre>																														
<b>Parameter</b>	<table border="1"> <tr> <td><b>&lt;use-string&gt;</b></td> <td>the user name containing 1-32 characters</td> </tr> <tr> <td><b>&lt;group-string&gt;</b></td> <td>the name of the group the user belongs to, containing 1-32 characters</td> </tr> <tr> <td><b>authPriv</b></td> <td>use DES for the packet encryption</td> </tr> <tr> <td><b>authNoPriv</b></td> <td>not use DES for the packet encryption</td> </tr> <tr> <td><b>auth</b></td> <td>perform packet authentication</td> </tr> <tr> <td><b>md5</b></td> <td>packet authentication using HMAC MD5 algorithm</td> </tr> <tr> <td><b>sha</b></td> <td>packet authentication using HMAC SHA algorithm</td> </tr> <tr> <td><b>3des</b></td> <td>packet authentication using 3DES to encrypt</td> </tr> <tr> <td><b>aes</b></td> <td>packet authentication using AES to encrypt</td> </tr> <tr> <td><b>des</b></td> <td>packet authentication using DES to encrypt</td> </tr> <tr> <td><b>&lt;word&gt;</b></td> <td>user password, containing 8-32 character</td> </tr> <tr> <td><b>&lt;num-std&gt;</b></td> <td>the access-class number for standard numeric ACL, ranging between 1-99</td> </tr> <tr> <td><b>&lt;name&gt;</b></td> <td>the access-class name for standard ACL, the character string length is ranging between 1-32</td> </tr> <tr> <td><b>&lt;ipv6-num-std&gt;</b></td> <td>the access-class number for standard numeric IPv6 ACL, ranging between 500-599</td> </tr> <tr> <td><b>&lt;ipv6-name&gt;</b></td> <td>the access-class name for standard IPv6 ACL, the character string length is ranging between 1-32</td> </tr> </table>	<b>&lt;use-string&gt;</b>	the user name containing 1-32 characters	<b>&lt;group-string&gt;</b>	the name of the group the user belongs to, containing 1-32 characters	<b>authPriv</b>	use DES for the packet encryption	<b>authNoPriv</b>	not use DES for the packet encryption	<b>auth</b>	perform packet authentication	<b>md5</b>	packet authentication using HMAC MD5 algorithm	<b>sha</b>	packet authentication using HMAC SHA algorithm	<b>3des</b>	packet authentication using 3DES to encrypt	<b>aes</b>	packet authentication using AES to encrypt	<b>des</b>	packet authentication using DES to encrypt	<b>&lt;word&gt;</b>	user password, containing 8-32 character	<b>&lt;num-std&gt;</b>	the access-class number for standard numeric ACL, ranging between 1-99	<b>&lt;name&gt;</b>	the access-class name for standard ACL, the character string length is ranging between 1-32	<b>&lt;ipv6-num-std&gt;</b>	the access-class number for standard numeric IPv6 ACL, ranging between 500-599	<b>&lt;ipv6-name&gt;</b>	the access-class name for standard IPv6 ACL, the character string length is ranging between 1-32
<b>&lt;use-string&gt;</b>	the user name containing 1-32 characters																														
<b>&lt;group-string&gt;</b>	the name of the group the user belongs to, containing 1-32 characters																														
<b>authPriv</b>	use DES for the packet encryption																														
<b>authNoPriv</b>	not use DES for the packet encryption																														
<b>auth</b>	perform packet authentication																														
<b>md5</b>	packet authentication using HMAC MD5 algorithm																														
<b>sha</b>	packet authentication using HMAC SHA algorithm																														
<b>3des</b>	packet authentication using 3DES to encrypt																														
<b>aes</b>	packet authentication using AES to encrypt																														
<b>des</b>	packet authentication using DES to encrypt																														
<b>&lt;word&gt;</b>	user password, containing 8-32 character																														
<b>&lt;num-std&gt;</b>	the access-class number for standard numeric ACL, ranging between 1-99																														
<b>&lt;name&gt;</b>	the access-class name for standard ACL, the character string length is ranging between 1-32																														
<b>&lt;ipv6-num-std&gt;</b>	the access-class number for standard numeric IPv6 ACL, ranging between 500-599																														
<b>&lt;ipv6-name&gt;</b>	the access-class name for standard IPv6 ACL, the character string length is ranging between 1-32																														
<b>Default</b>	None.																														
<b>Mode</b>	Global Mode																														
<b>Usage Guide</b>	<p>Add a new user to an SNMP group.</p> <p>If the encryption and authentication is not selected, the default settings will be no encryption and no authentication. If the encryption is selected, the authentication must be done. When deleting a user, if correct username and incorrect group name is inputted, the user can still be deleted.</p>																														

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

---

**Example**

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

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

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

---

## 4.4.20 snmp-server view

<b>Command</b>	<pre>snmp-server view &lt;view-string&gt; &lt;oid-string&gt; {include   exclude} no snmp-server view &lt;view-string&gt; [ &lt;oid-string&gt; ]</pre>						
<b>Parameter</b>	<table border="1"> <tr> <td><b>&lt;view-string&gt;</b></td> <td>view name, containing 1-32 characters</td> </tr> <tr> <td><b>&lt;oid-string&gt;</b></td> <td>OID number or corresponding node name, containing 1-255 characters</td> </tr> <tr> <td><b>include   exclude</b></td> <td>include/exclude this OID</td> </tr> </table>	<b>&lt;view-string&gt;</b>	view name, containing 1-32 characters	<b>&lt;oid-string&gt;</b>	OID number or corresponding node name, containing 1-255 characters	<b>include   exclude</b>	include/exclude this OID
<b>&lt;view-string&gt;</b>	view name, containing 1-32 characters						
<b>&lt;oid-string&gt;</b>	OID number or corresponding node name, containing 1-255 characters						
<b>include   exclude</b>	include/exclude this OID						
<b>Default</b>	None.						
<b>Mode</b>	Global Mode						
<b>Usage Guide</b>	<p>This command is used to create or renew the view information.</p> <p>The command supports not only the input using the character string of the variable OID as parameter. But also supports the input using the node name of the parameter.</p> <p>the "no" form of this command deletes the view information.</p>						
<b>Example</b>	<p>Create a view named readview, include iso nodes but not iso.3 nodes, and then delete them.</p> <pre>Switch(config)#snmp-server view readview iso include Switch(config)#snmp-server view readview iso.3 exclude  Switch(config)#no snmp-server view readview</pre>						

## 4.4.21 switchport updown notification enable

<b>Command</b>	<b>switchport updown notification enable</b> <b>no switchport updown notification enable</b>
<b>Parameter</b>	<b>none</b> none
<b>Default</b>	Send the trap message to the port of IP/DOWN event as default.
<b>Mode</b>	Port Mode
<b>Usage Guide</b>	<p>Enable/disable the function of sending the trap message to the port of UP/DOWN event. This command can control to send the trap message when the port happens the UP/DOWN event or not. As default, send the trap message to all the ports of UP/DOWN event after enabled snmp trap.</p> <p>The no command deletes the configuration.</p>
<b>Example</b>	<p>Disable the function of sending the trap message to the port 1/0/1 of the UP/DOWN event.</p> <pre> Switch(config)#in e 1/0/1 Switch(config-if-ethernet1/0/1)#no switchport updown notification enable Switch(config-if-ethernet1/0/1)#show running-config current-mode ! Interface Ethernet1/0/1 no switchport updown notification enable           </pre>

## 4.5 Switch Upgrade

### 4.5.1 copy (FTP)

<b>Command</b>	<b>copy &lt;source-url&gt; &lt;destination-url&gt; [ascii   binary]</b>								
<b>Parameter</b>	<table border="1"> <tr> <td><b>&lt;source-url&gt;</b></td> <td>the location of the source files or directories to be copied</td> </tr> <tr> <td><b>&lt;destination-url&gt;</b></td> <td>the destination address to which the files or directories to be copied</td> </tr> <tr> <td><b>ascii</b></td> <td>ASCII standards will be adopted</td> </tr> <tr> <td><b>binary</b></td> <td>File transfer will be in binary mode (default transfer method)</td> </tr> </table>	<b>&lt;source-url&gt;</b>	the location of the source files or directories to be copied	<b>&lt;destination-url&gt;</b>	the destination address to which the files or directories to be copied	<b>ascii</b>	ASCII standards will be adopted	<b>binary</b>	File transfer will be in binary mode (default transfer method)
<b>&lt;source-url&gt;</b>	the location of the source files or directories to be copied								
<b>&lt;destination-url&gt;</b>	the destination address to which the files or directories to be copied								
<b>ascii</b>	ASCII standards will be adopted								
<b>binary</b>	File transfer will be in binary mode (default transfer method)								
<b>Default</b>	None.								
<b>Mode</b>	Admin Mode								

#### Usage Guide

This command is used to transfer files by TFP.

When URL represents an FTP address, its form should be:

ftp://<username>:<password>@{<ipaddress>|<ipv6address>|<hostname> }/<filename>, amongst <username> is the FTP user name, <password> is the FTP user password, <ipaddress>|<ipv6address> is the IPv4 or IPv6 address of the FTP server/client, <hostname> is the name of the host mapping with the IPv6 address, it does not support the file download and upload with hosts mapping with IPv4 addresses, <filename> is the name of the FTP upload/download file.

#### Special keywords of the filename

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

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

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

---

ftp username>

ftp password>

ftp filename>

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

---

**Example**

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

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

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

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

Save the running configuration files.

**Switch#copy running-config startup-config**

---

## 4.5.2 copy ( TFTP )

<b>Command</b>	<b>copy &lt;source-url&gt; &lt;destination-url&gt; [ascii   binary]</b>										
<b>Parameter</b>	<table border="1"> <tr> <td><b>&lt;source-url&gt;</b></td> <td>the location of the source files or directories to be copied</td> </tr> <tr> <td><b>&lt;destination-url&gt;</b></td> <td>the destination address to which the files or directories to be copied</td> </tr> <tr> <td><b>ascii</b></td> <td>ASCII standards will be adopted</td> </tr> <tr> <td><b>binary</b></td> <td>File transfer will be in binary mode (default transfer method)</td> </tr> </table>	<b>&lt;source-url&gt;</b>	the location of the source files or directories to be copied	<b>&lt;destination-url&gt;</b>	the destination address to which the files or directories to be copied	<b>ascii</b>	ASCII standards will be adopted	<b>binary</b>	File transfer will be in binary mode (default transfer method)		
<b>&lt;source-url&gt;</b>	the location of the source files or directories to be copied										
<b>&lt;destination-url&gt;</b>	the destination address to which the files or directories to be copied										
<b>ascii</b>	ASCII standards will be adopted										
<b>binary</b>	File transfer will be in binary mode (default transfer method)										
<b>Default</b>	None.										
<b>Mode</b>	Admin Mode										
<b>Usage Guide</b>	<p>This command is used to transfer files by TFTP.</p> <p>When URL represents a TFTP address, its form should be:  tftp://{&lt;ipaddress&gt; &lt;ipv6address&gt; &lt;hostname&gt;}/&lt;filename&gt;, amongst &lt;ipaddress&gt; &lt;ipv6address&gt; is the IPv4 or IPv6 address of the TFTP server/client, &lt;hostname&gt; is the name of the host mapping with the IPv6 address, it does not support the file download and upload with hosts mapping with IPv4 addresses, &lt;filename&gt; is the name of the TFTP upload/download file.</p> <p>Special keyword of the filename</p> <table border="1"> <thead> <tr> <th>keywords</th> <th>explain</th> </tr> </thead> <tbody> <tr> <td>running-config</td> <td>Running configuration files</td> </tr> <tr> <td>startup-config</td> <td>It means the reboot configuration files when using copy running-config startup-config command</td> </tr> <tr> <td>nos.img</td> <td>System files</td> </tr> <tr> <td>boot.rom</td> <td>System startup files</td> </tr> </tbody> </table> <p>This command supports command line hints, namely if the user can enter commands in following forms: copy &lt;filename&gt; tftp:// or copy tftp:// &lt;filename&gt; and press Enter, following hints will be provided by the system:tftp server ip/ipv6 address[x.x.x.x]/[x::x:x]&gt;tftp filename&gt; Requesting for TFTP server address, file name</p>	keywords	explain	running-config	Running configuration files	startup-config	It means the reboot configuration files when using copy running-config startup-config command	nos.img	System files	boot.rom	System startup files
keywords	explain										
running-config	Running configuration files										
startup-config	It means the reboot configuration files when using copy running-config startup-config command										
nos.img	System files										
boot.rom	System startup files										
<b>Example</b>	<p>Save images in the FLASH to the TFTP server of 10.1.1.1</p> <p><b>Switch#copy nos.img tftp://10.1.1.1/nos.img</b></p> <p>Obtain system file nos.img from the TFTP server 10.1.1.1</p>										



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

Save the running configuration files

**Switch#copy running-config startup-config**

---

### 4.5.3 ftp-dir

<b>Command</b>	<b>ftp-dir &lt;ftp-server-url&gt;</b>
<b>Parameter</b>	<b>&lt;ftp-server-url&gt;</b> ftp server address
<b>Default</b>	None.
<b>Mode</b>	Admin Mode
<b>Usage Guide</b>	<p>Browse the file list on the FTP server.</p> <p>The form of &lt;ftp-server-url&gt; is :</p> <p>ftp://&lt;username&gt;:&lt;password&gt;@{ &lt;ipv4address&gt;   &lt;ipv6address&gt; }, amongst &lt;username&gt; is the FTP user name, &lt;password&gt; is the FTP user password, { &lt;ipv4address&gt;   &lt;ipv6address&gt; } is the IPv4 or IPv6 address of the FTP server.</p>
<b>Example</b>	<p>Browse the list of the files on the server with the FTP client, the username is "Switch", the password is "superuser".</p> <pre>Switch#ftp-dir ftp://Switch:superuser @10.1.1.1</pre>

### 4.5.4 ftp-server enable

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

### 4.5.5 ftp-server timeout

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

## 4.5.6 ip ftp

<b>Command</b>	<b>ip ftp username &lt;username&gt; password [0   7] &lt;password&gt;</b> <b>no ip ftp username &lt;username&gt;</b>	
<b>Parameter</b>	<b>&lt;username&gt;</b>	the username of the FTP link, its range should not exceed 32 characters
	<b>[0   7]</b>	0 means password is not encrypted ,7 means password is encrypted
	<b>&lt;password&gt;</b>	FTP link password
<b>Default</b>	The system uses anonymous FTP links by default.	
<b>Mode</b>	Global Mode	
<b>Usage Guide</b>	<p>Configure the username and password for logging in to the FTP.</p> <p>The no operation of this command will delete the configured username and password simultaneously.</p>	
<b>Example</b>	<p>Configure the username as Switch and the password as superuser.</p> <p><b>Switch(config)#ip ftp username Switch password 0 superuser</b></p>	

## 4.5.7 show ftp

<b>Command</b>	<b>show ftp</b>
<b>Parameter</b>	<b>none</b> none
<b>Default</b>	None.
<b>Mode</b>	Admin and Global Mode
<b>Usage Guide</b>	Display the parameter settings for the FTP server.
<b>Example</b>	Display the parameter settings for the FTP server.  <b>Switch#show ftp</b> Timeout : 600

## 4.5.8 show tftp

<b>Command</b>	<b>show tftp</b>
<b>Parameter</b>	<b>none</b> none
<b>Default</b>	None.
<b>Mode</b>	Admin and Global Mode
<b>Usage Guide</b>	Display the parameter settings for the TFTP server.
<b>Example</b>	Display the parameter settings for the TFTP server.  <b>Switch#show tftp</b> timeout : 60 Retry Times : 10

### 4.5.9 tftp-server enable

<b>Command</b>	<b>tftp-server enable</b> <b>no tftp-server enable</b>
<b>Parameter</b>	<b>none</b> none
<b>Default</b>	Disable TFTP Server.
<b>Mode</b>	Global Mode
<b>Usage Guide</b>	<p>This command is used to start the TFTP server.</p> <p>The “no ftp-server enable” command shuts down TFTP server and prevents TFTP user from logging in.</p>
<b>Example</b>	<p>Start the TFTP server.</p> <p><b>Switch(config)#tftp-server enable</b></p>



## 4.5.10 tftp-server retransmission-number

<b>Command</b>	<b>tftp-server retransmission-number &lt;number&gt;</b>
<b>Parameter</b>	<b>&lt;number&gt;</b> the time to re-transfer, the valid range is 1 to 20
<b>Default</b>	Retransmit 5 times.
<b>Mode</b>	Global Mode
<b>Usage Guide</b>	Set the retransmission time for TFTP server.
<b>Example</b>	Modify the retransmission to 10 times.  <b>Switch(config)#tftp-server retransmission-number 10</b>

## 4.5.11 tftp-server transmission-timeout

<b>Command</b>	<b>tftp-server transmission-timeout &lt;seconds&gt;</b>
<b>Parameter</b>	<b>&lt;seconds&gt;</b> the timeout value, the valid range is 5 to 3600s
<b>Default</b>	The system default timeout setting is 600 seconds.
<b>Mode</b>	Global Mode
<b>Usage Guide</b>	Set the transmission timeout value for TFTP server.
<b>Example</b>	Modify the timeout value to 60 seconds.  <b>Switch(config)#tftp-server transmission-timeout 60</b>

## 4.6 File System

### 4.6.1 cd

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

## 4.6.2 copy

<b>Command</b>	<b>copy &lt;source-file-url &gt; &lt;dest-file-url&gt;</b>				
<b>Parameter</b>	<table border="1"> <tr> <td><b>&lt;source-file-url&gt;</b></td> <td>The source address of the file or directory to be copied</td> </tr> <tr> <td><b>&lt;dest-file-url&gt;</b></td> <td>The destination address of the file or directory to be copied</td> </tr> </table>	<b>&lt;source-file-url&gt;</b>	The source address of the file or directory to be copied	<b>&lt;dest-file-url&gt;</b>	The destination address of the file or directory to be copied
<b>&lt;source-file-url&gt;</b>	The source address of the file or directory to be copied				
<b>&lt;dest-file-url&gt;</b>	The destination address of the file or directory to be copied				
<b>Default</b>	None.				
<b>Mode</b>	Admin Mode				
<b>Usage Guide</b>	<p>Copy a designated file on the switch and store it as a new file.</p> <p>When users operate on files stored in backup master board and line cards under IMG mode, URLs of the source file and the destination file should take such a form as described in the following requirements.</p> <ol style="list-style-type: none"> <li>The prefix of the source file URL should be in one of the following forms: <ul style="list-style-type: none"> <li>□ starting with "flash:/"</li> <li>□ "ftp://username:pass@server-ip/file-name"</li> <li>□ "tftp://server-ip/file-name"</li> </ul> </li> <li>The prefix of the destination file URL should be in one of the following forms: <ul style="list-style-type: none"> <li>□ starting with "flash:/"</li> <li>□ "ftp://username:pass@server-ip/file-name"</li> <li>□ "tftp://server-ip/file-name"</li> </ul> </li> </ol> <p>when the prefix of the source file URL is ftp:// or tftp://, that of the destination file URL should not be either of them.</p> <p>To use this command, the designated source file should exist, and the destination file should not be named the same as any existing directory or file, otherwise, there might be a prompt warning about a failed copy operation or an attempt to overwrite an existing file.</p> <p>If the source and destination files are in different directories, with this command implemented, users can copy files from other directories into the current one.</p>				
<b>Example</b>	<p>Copy the file "flash:/nos.img" and store it as "flash/ 6.1.11.0.img".</p> <pre> Switch#copy flash:/nos.img flash:/nos-6.1.11.0.img Copy flash:/nos.img to flash:/nos-6.1.11.0.img? [Y:N] y Copied file flash:/nos.img to flash:/nos-6.1.11.0.img </pre>				

### 4.6.3 delete

<b>Command</b>	<b>delete &lt;file-url&gt;</b>
<b>Parameter</b>	<b>&lt;file-url&gt;</b> the full path of the file to be deleted
<b>Default</b>	None.
<b>Mode</b>	Admin Mode
<b>Usage Guide</b>	Delete the designate file on the storage device.
<b>Example</b>	Delete file flash:/nos.img.  <b>Switch#delete flash:/nos5.img</b> Delete file flash:/nos5.img?[Y:N]y Deleted file flash:/nos.img

## 4.6.4 dir

<b>Command</b>	<b>dir [WORD]</b>
<b>Parameter</b>	<b>[WORD]</b> the name of the shown directory. There may be the following formats: directory name, slot-xx#directory name, flash:/directory name, cf:/directory name.
<b>Default</b>	No <WORD> means to display information of the current working directory.
<b>Mode</b>	Admin Mode
<b>Usage Guide</b>	Display the information of the designated directory on the storage device. This command does not support a recursive display of all sub-directories.
<b>Example</b>	<p>Display information of the directory "flash:/".</p> <pre> <b>Switch#dir flash:/</b> nos.img          2,449,496    1980-01-01 00:01:06 ---- startup-config   2,064        1980-01-01 00:30:12 ----  Total 7, 932, 928 byte(s) in 4 file(s) · free 4, 966, 400 byte(s)  <b>Switch#</b> </pre>

## 4.6.5 pwd

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

## 4.6.6 rename

<b>Command</b>	<b>rename &lt;source-file-url&gt; &lt;new-filename &gt;</b>				
<b>Parameter</b>	<table border="1"> <tr> <td><b>&lt;source-file-url&gt;</b></td> <td>the source file, in which whether specifying or not its path are both acceptable</td> </tr> <tr> <td><b>&lt;new-filename &gt;</b></td> <td>filename without specifying its path</td> </tr> </table>	<b>&lt;source-file-url&gt;</b>	the source file, in which whether specifying or not its path are both acceptable	<b>&lt;new-filename &gt;</b>	filename without specifying its path
<b>&lt;source-file-url&gt;</b>	the source file, in which whether specifying or not its path are both acceptable				
<b>&lt;new-filename &gt;</b>	filename without specifying its path				
<b>Default</b>	None.				
<b>Mode</b>	Admin Mode				
<b>Usage Guide</b>	<p>Rename a designated file on the switch.</p> <p>When using this command, if the new file name is not used as that of any existing directory or file, the rename operation can be done, or a prompt will indicate its failure.</p>				
<b>Example</b>	<p>Change the name of file "nos.img" in the current working directory to "nos-6.1.11.0.img".</p> <p><b>Switch# rename nos5.img nos-6.1.11.0.img</b></p> <p>Rename flash:/nos5.img to flash:/nos-6.1.11.0.img ok !</p>				



# Chapter 5 Port Configuration

## 5.1 Ethernet Port Configuration

### 5.1.1 bandwidth

<b>Command</b>	<code>bandwidth control &lt;bandwidth&gt; {transmit   receive   both}</code> <code>no bandwidth control</code>
<b>parameter</b>	<i>bandwidth</i> is the bandwidth limit, which is shown in kbps ranging between 1-1000000K
<b>default</b>	Disable bandwidth restrictions by default
<b>Mode</b>	Port Configuration Mode
<b>Usage Guide</b>	Use the <b>bandwidth control &lt;bandwidth&gt;[both   receive   transmit]</b> command to set the bandwidth rate.  Use the <b>no bandwidth control</b> restore default configuration
<b>Example</b>	Set the bandwidth limit of 1/0/1-8 port is 40000K. Switch(config)#interface ethernet 1/0/1-8 Switch(Config-If-Port-Range)#bandwidth control 40000 both

## 5.1.2 clear counters interface

<b>Command</b>	<b>clear counters [interface {ethernet &lt;interface-list&gt;   vlan &lt;vlan-id&gt;   port-channel &lt;port-channel-number&gt;   &lt;interface-name&gt;}]</b>								
<b>parameter</b>	<table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="padding: 5px;"><i>interface-list</i></td> <td style="padding: 5px;">stands for the Ethernet port number;</td> </tr> <tr> <td style="padding: 5px;"><i>vlan-id</i></td> <td style="padding: 5px;">stands for the VLAN interface number;</td> </tr> <tr> <td style="padding: 5px;"><i>port-channel-number</i></td> <td style="padding: 5px;">for trunk interface number;</td> </tr> <tr> <td style="padding: 5px;"><i>interface-name</i></td> <td style="padding: 5px;">for interface name, such as port-channel 1.</td> </tr> </table>	<i>interface-list</i>	stands for the Ethernet port number;	<i>vlan-id</i>	stands for the VLAN interface number;	<i>port-channel-number</i>	for trunk interface number;	<i>interface-name</i>	for interface name, such as port-channel 1.
<i>interface-list</i>	stands for the Ethernet port number;								
<i>vlan-id</i>	stands for the VLAN interface number;								
<i>port-channel-number</i>	for trunk interface number;								
<i>interface-name</i>	for interface name, such as port-channel 1.								
<b>default</b>	Port statistics default not cleared								
<b>Mode</b>	Admin Mode								
<b>Usage Guide</b>	If no port is specified, statistics for all ports are cleared.								
<b>Example</b>	<p>Clearing the statistics for Ethernet port1/0/1.</p> <pre>Switch#clear counters interface ethernet 1/0/1</pre>								

### 5.1.3 description

<b>Command</b>	<b>description &lt;string&gt;</b> <b>no description</b>
<b>parameter</b>	<div style="border: 1px solid black; padding: 5px;"> <i>string</i> is a character string, which should not exceeds 200 characters         </div>
<b>default</b>	No port name by default
<b>Mode</b>	Port Mode
<b>Usage Guide</b>	<p>This command is for helping the user manage switches, such as the user assign names according to the port application, e.g. financial as the name of 1/0/1-2 ports which is used by financial department, engineering as the name of 1/0/9 ports which belongs to the engineering department, while the name of 1/0/12 ports is assigned with Server, which is because they connected to the server. In this way the port distribution state will be brought to the table.</p>
<b>Example</b>	<p>Specify the description of 1/0/1-2 port as financial.</p> <pre>Switch(config)#interface ethernet 1/0/1-2 Switch(Config-If-Port-Range)#description financial</pre>

### 5.1.4 flow control

<b>Command</b>	<b>flow control</b> no flow control
<b>parameter</b>	-
<b>default</b>	Disable port traffic control by default
<b>Mode</b>	Port Mode
<b>Usage Guide</b>	<p>After the flow control function is enabled, the port will notify the sending device to slow down the sending speed to prevent packet loss when traffic received exceeds the capacity of port cache. Ports support IEEE802.3X flow control; the ports work in half-duplex mode, supporting back-pressure flow control. If flow control results in serious HOL, the switch will automatically start HOL control (discarding some packets in the COS queue that may result in HOL) to prevent drastic degradation of network performance.</p>
<b>Example</b>	<p>Enabling the flow control function in ports 1/0/1-8.</p> <pre>Switch(config)#interface ethernet 1/0/1-8 Switch(Config-If-Port-Range)#flow control</pre>

## 5.1.5 interface ethernet

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

## 5.1.6 Loopback

---

<b>Command</b>	<b>loopback</b> <b>no loopback</b>
----------------	---------------------------------------

---

<b>parameter</b>	-
<b>default</b>	By default, disable loop testing in the Ethernet port

---

<b>Mode</b>	Port Mode
-------------	-----------

---

<b>Usage Guide</b>	Loopback test can be used to verify the Ethernet ports are working normally. After loopback has been enabled, the port will assume a connection established to itself, and all traffic sent from the port will be received at the very same port.
--------------------	---

---

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

## 5.1.7 Negotiation

<b>Command</b>	<code>negotiation {on   off}</code>
<b>parameter</b>	-
<b>default</b>	Auto-negotiation is enabled by default.
<b>Mode</b>	Port configuration Mode
<b>Usage Guide</b>	This command applies to 1000Base-FX interface only. The negotiation command is not available for 1000Base-TX or 100Base-TX interface. To change the negotiation mode, speed and duplex mode of 1000Base-TX port, use speed-duplex command instead.
<b>Example</b>	Port 21 of Switch1 is connected to port 21 of Switch2, the following will disable the negotiation for both ports. Switch1(config)#interface ethernet1/0/21 Switch1(Config-If-Ethernet1/0/21)#negotiation off Switch2(config)#interface ethernet1/0/21 Switch2(Config-If-Ethernet1/0/21)#negotiation off

## 5.1.8 Port-rate-statistics interval

<b>Command</b>	<code>port-rate-statistics interval &lt;interval-value&gt;</code>
<b>parameter</b>	<i>interval-value</i> The interval of port-rate-statistics, unit is second, ranging from 5 to 600 with the configuration step of 5.
<b>default</b>	Only port-rate-statistics of 5 seconds and 5 minutes are displayed.
<b>Mode</b>	Global Mode
<b>Usage Guide</b>	This command can be used to set the port rate statistics interval time.
<b>Example</b>	Count the interval of port-rate-statistics as 20 seconds. Switch(config)#port-rate-statistics interval 20



### 5.1.9 rate-violation

<b>Command</b>	<b>rate-violation [broadcast   multicast   unicast   all] &lt;200-2000000&gt;</b> <b>no rate-violation</b>	
<b>parameter</b>	<b>broadcast</b>	broadcast packet
	<b>multicast</b>	multicast packet
	<b>unicast</b>	unicast packet
	<b>all</b>	all packets
	<b>&lt;200-2000000&gt;</b>	the number of packets allowed to pass per second.

**default** There is no limit for the packet reception rate.

**Mode** Port Mode

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

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

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

### 5.1.10 rate-violation control

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

## 5.1.11 show interface

<b>Command</b>	<b>show interface [ethernet &lt;interface-number&gt;   port-channel &lt;port-channel-number&gt;   vlan &lt;vlan-id&gt;   &lt;interface-name&gt;] [detail]</b> <b>show interface ethernet status</b> <b>show interface ethernet counter {packet   rate}</b>
<b>parameter</b>	<i>interface-number</i> is the port number of the Ethernet, <i>port-channel-number</i> is the number of the aggregation interface <i>vlan-id</i> is the VLAN interface number, the value range from 1 to 4094 <i>interface-name</i> is the name of the interface such as port-channel1 <b>detail</b> show the detail of the port
<b>default</b>	Information not displayed by default
<b>Mode</b>	Admin and Configuration Mode.
<b>Usage Guide</b>	Use this command to view interface-related configuration information
<b>Example</b>	<p>Show the information of VLAN 1 .</p> <pre> Vlan1 is up, line protocol is up, dev index is 11001   Device flag 0x1003(UP BROADCAST MULTICAST)   Time since last status change:0w-0d-1h-14m-57s (4497 seconds)   IPv4 address is:     192.168.2.1      255.255.255.0    (Primary)   VRF Bind: Not Bind   Hardware is EtherSVI, address is 00-1f-ce-10-b0-1a   MTU is 1500 bytes , BW is 0 Kbit   Encapsulation ARPA, loopback not set   5 minute input rate 244 bits/sec, 0 packets/sec   5 minute output rate 0 bits/sec, 0 packets/sec   The last 5 second input rate 0 bits/sec, 0 packets/sec   The last 5 second output rate 0 bits/sec, 0 packets/sec   Input packets statistics:     Input queue 0/600, 0 drops     1012 packets input, 193127 bytes, 0 no buffer     0 input errors, 0 CRC, 0 oversize, 0 undersize     0 jabber, 0 fragments   Output packets statistics:     448 packets output, 108316 bytes, 0 underruns     0 output errors, 0 collisions           </pre>

## 5.1.12 Shutdown

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

### 5.1.13 speed-duplex

<b>Command</b>	<pre>speed-duplex {auto [10 [100 [1000]] [auto   full   half ]]   force10-half   force10-full   force100-half   force100-full   force100-fx [module-type {auto-detected   no-phy-integrated   phy-integrated}}   {{force1g-half   force1g-full} [nonegotiate [master   slave]]}} no speed-duplex</pre>																																		
<b>parameter</b>	<table border="1"> <tr> <td><b>auto</b></td> <td>is the auto speed and duplex negotiation</td> </tr> <tr> <td>10</td> <td>10kbps</td> </tr> <tr> <td>100</td> <td>100kbps</td> </tr> <tr> <td>1000</td> <td>1000kbps</td> </tr> <tr> <td><b>force10-half</b></td> <td>is the forced 10Mbps at half-duplex mode</td> </tr> <tr> <td><b>force10-full</b></td> <td>is the forced 10Mbps at full-duplex mode</td> </tr> <tr> <td><b>force100-half</b></td> <td>is the forced 100Mbps at half-duplex mode</td> </tr> <tr> <td><b>force100-full</b></td> <td>is the forced 100Mbps at full-duplex mode</td> </tr> <tr> <td><b>force1g-half</b></td> <td>is the forced 1000Mbps at half-duplex mode</td> </tr> <tr> <td><b>force1g-full</b></td> <td>is the forced 1000Mbps at full-duplex mode</td> </tr> <tr> <td><b>force100-fx</b></td> <td>is the forced 100Mbps at full-duplex mode</td> </tr> <tr> <td><b>auto-detected</b></td> <td>automatic detection</td> </tr> <tr> <td><b>no-phy-integrated</b></td> <td>there is no phy-integratd 100Base-FX module</td> </tr> <tr> <td><b>phy-integrated</b></td> <td>phy-integratd 100Base-FX module</td> </tr> <tr> <td><b>nonegotiate</b></td> <td>disables auto-negotiation forcibly for 1000Mb port</td> </tr> <tr> <td><b>master</b></td> <td>forces the 1000Mb port to be master mode</td> </tr> <tr> <td><b>slave</b></td> <td>Forces the 1000Mb port to be slave mode</td> </tr> </table>	<b>auto</b>	is the auto speed and duplex negotiation	10	10kbps	100	100kbps	1000	1000kbps	<b>force10-half</b>	is the forced 10Mbps at half-duplex mode	<b>force10-full</b>	is the forced 10Mbps at full-duplex mode	<b>force100-half</b>	is the forced 100Mbps at half-duplex mode	<b>force100-full</b>	is the forced 100Mbps at full-duplex mode	<b>force1g-half</b>	is the forced 1000Mbps at half-duplex mode	<b>force1g-full</b>	is the forced 1000Mbps at full-duplex mode	<b>force100-fx</b>	is the forced 100Mbps at full-duplex mode	<b>auto-detected</b>	automatic detection	<b>no-phy-integrated</b>	there is no phy-integratd 100Base-FX module	<b>phy-integrated</b>	phy-integratd 100Base-FX module	<b>nonegotiate</b>	disables auto-negotiation forcibly for 1000Mb port	<b>master</b>	forces the 1000Mb port to be master mode	<b>slave</b>	Forces the 1000Mb port to be slave mode
<b>auto</b>	is the auto speed and duplex negotiation																																		
10	10kbps																																		
100	100kbps																																		
1000	1000kbps																																		
<b>force10-half</b>	is the forced 10Mbps at half-duplex mode																																		
<b>force10-full</b>	is the forced 10Mbps at full-duplex mode																																		
<b>force100-half</b>	is the forced 100Mbps at half-duplex mode																																		
<b>force100-full</b>	is the forced 100Mbps at full-duplex mode																																		
<b>force1g-half</b>	is the forced 1000Mbps at half-duplex mode																																		
<b>force1g-full</b>	is the forced 1000Mbps at full-duplex mode																																		
<b>force100-fx</b>	is the forced 100Mbps at full-duplex mode																																		
<b>auto-detected</b>	automatic detection																																		
<b>no-phy-integrated</b>	there is no phy-integratd 100Base-FX module																																		
<b>phy-integrated</b>	phy-integratd 100Base-FX module																																		
<b>nonegotiate</b>	disables auto-negotiation forcibly for 1000Mb port																																		
<b>master</b>	forces the 1000Mb port to be master mode																																		
<b>slave</b>	Forces the 1000Mb port to be slave mode																																		
<b>default</b>	Auto-negotiation for speed and duplex mode is set by default																																		
<b>Mode</b>	Port Mode																																		
<b>Usage Guide</b>	<p>This command is configures the port speed and duplex mode. When configuring port speed and duplex mode, the speed and duplex mode must be the same as the setting of the remote end, i.e., if the remote device is set to auto-negotiation, then auto-negotiation should be set at the local port. If the remote end is in forced mode, the same should be set in the local end.</p> <p>1000Gb ports are by default <b>master</b> when configuring <b>nonegotiate</b> mode. If one end is set to <b>master</b> mode, the other end must be set to <b>slave</b> mode.</p> <p><b>force1g-half</b> is not supported yet.</p>																																		

---

---

**Example**

Port 1 of Switch1 is connected to port 1 of Switch2, the following will set both ports in forced 100Mbps at half-duplex mode.

```
Switch1(config)#interface ethernet1/0/1
```

```
Switch1(Config-If-Ethernet1/0/1)#speed-duplex force100-half
```

```
Switch2(config)#interface ethernet1/0/1
```

```
Switch2(Config-If-Ethernet1/0/1)#speed-duplex force100-half
```

## 5.1.14 storm-control

<b>Command</b>	<code>storm-control { kbps   pps }</code> <code>no storm-control pps</code>				
<b>parameter</b>	<table border="1"><tr><td><b>kbps</b></td><td>means the unit of limit is kbits/s</td></tr><tr><td><b>pps</b></td><td>means the limit unit is packets/s.</td></tr></table>	<b>kbps</b>	means the unit of limit is kbits/s	<b>pps</b>	means the limit unit is packets/s.
<b>kbps</b>	means the unit of limit is kbits/s				
<b>pps</b>	means the limit unit is packets/s.				
<b>default</b>	The default is kbps.				
<b>Mode</b>	Global Mode				
<b>Usage Guide</b>	Configure the kbps or pps as the limit mode in global mode, then set broadcast, multicast or unknown unicast limit value in port mode.				
<b>Example</b>	Setting ports 1-8 allow 1000kbit broadcast packets per second. Switch(config)#storm-control kbps Switch(config-if-port-range)#storm-control broadcast 1000				

## 5.1.15 storm-control

<b>Command</b>	<b>storm-control {unicast   broadcast   multicast} &lt;value&gt;</b> <b>no storm-control {unicast   broadcast   multicast}</b>								
<b>parameter</b>	<table border="1"> <tr> <td><b>unicast</b></td> <td>to limit unicast traffic for unknown destination</td> </tr> <tr> <td><b>broadcast</b></td> <td>to limit broadcast traffic.</td> </tr> <tr> <td><b>multicast</b></td> <td>to limit multicast traffic</td> </tr> <tr> <td><b>value</b></td> <td>Limit the flow rate per second, PPS range from 1 to 1488095; kbps range from 1 to 1000000.</td> </tr> </table>	<b>unicast</b>	to limit unicast traffic for unknown destination	<b>broadcast</b>	to limit broadcast traffic.	<b>multicast</b>	to limit multicast traffic	<b>value</b>	Limit the flow rate per second, PPS range from 1 to 1488095; kbps range from 1 to 1000000.
<b>unicast</b>	to limit unicast traffic for unknown destination								
<b>broadcast</b>	to limit broadcast traffic.								
<b>multicast</b>	to limit multicast traffic								
<b>value</b>	Limit the flow rate per second, PPS range from 1 to 1488095; kbps range from 1 to 1000000.								
<b>default</b>	No limit is set by default. So, broadcasts, multicasts and unknown destination unicasts are allowed to pass at line speed.								
<b>Mode</b>	Port Mode								
<b>Usage Guide</b>	<p>All ports in the switch belong to a same broadcast domain if no VLAN has been set. The switch will send the above mentioned three traffics to all ports in the broadcast domain, which may result in broadcast storm and so may greatly degrade the switch performance. Enabling Broadcast Storm Control can better protect the switch from broadcast storm. If the allowed traffic is set to 1000kbps, this means allow 1000 kbit per second and suppress the rest. The switch supports two kind of speed limit, it includes kbps which is limit by bandwidth and pps which is limit by the numbers of packets. It only can select one from the two ways and cannot set the two way in the same time (by global mode)</p> <p>Broadcast suppression is similar to bandwidth control. There is granularity limitation for the chip; the switch support 16Kbps granularities. If the &lt;Kbits&gt; that user input is not the integer times of 16, the system will adjust to the integer times of 16 automatically and print the true limit value to user.</p>								
<b>Example</b>	<p>Setting ports 1-8 allow 1000kbit broadcast packets per second.</p> <pre>Switch(config-if-port-range)#storm-control broadcast 1000</pre>								



### 5.1.16 storm-control bypass

<b>Command</b>	<code>storm-control bypass {arp   bpdu   igmp   rma   rek } &lt;enable   disable &gt;</code>														
<b>parameter</b>	<table border="1"> <tr> <td><b>arp</b></td> <td>means the protocol packets of arp-request</td> </tr> <tr> <td><b>bpdu</b></td> <td>means bpdu protocol packets</td> </tr> <tr> <td><b>igmp</b></td> <td>means igmp protocol packets</td> </tr> <tr> <td><b>rma</b></td> <td>means multicast address is the saved multicast packets</td> </tr> <tr> <td><b>rek</b></td> <td>means the special private packets that realtak used</td> </tr> <tr> <td><b>enable</b></td> <td>enable some protocol to limit filter function</td> </tr> <tr> <td><b>disable</b></td> <td>disable some protocol to broadcast limit filter function.</td> </tr> </table>	<b>arp</b>	means the protocol packets of arp-request	<b>bpdu</b>	means bpdu protocol packets	<b>igmp</b>	means igmp protocol packets	<b>rma</b>	means multicast address is the saved multicast packets	<b>rek</b>	means the special private packets that realtak used	<b>enable</b>	enable some protocol to limit filter function	<b>disable</b>	disable some protocol to broadcast limit filter function.
<b>arp</b>	means the protocol packets of arp-request														
<b>bpdu</b>	means bpdu protocol packets														
<b>igmp</b>	means igmp protocol packets														
<b>rma</b>	means multicast address is the saved multicast packets														
<b>rek</b>	means the special private packets that realtak used														
<b>enable</b>	enable some protocol to limit filter function														
<b>disable</b>	disable some protocol to broadcast limit filter function.														
<b>default</b>	Disable														
<b>Mode</b>	Global Mode.														
<b>Usage Guide</b>	Configure broadcast limit filter function of some protocol in global mode, then configure broadcast limit in port mode. At this moment, the protocol packets flow from the port cannot be limited.														
<b>Example</b>	<p>Configure arp protocol filter function to make the arp-request data packets that from 1 port in cannot be limited.</p> <pre>Switch (config)#storm-control bypass arp enable Switch(config-if-ethernet1/0/1)#storm-control broadcast 1000</pre>														

### 5.1.17 virtual-cable-test

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

<b>Example</b>	<p>Test the link status of the twisted pair connected to the 1000M port 1/0/1.</p> <pre>Switch#virtual-cable-test interface ethernet 1/0/1</pre> <p>Interface Ethernet1/0/1:</p> <pre>-----</pre> <table border="1"> <thead> <tr> <th>Cable pairs</th> <th>Cable status</th> <th>Length (meters)</th> </tr> <tr> <th>-----</th> <th>-----</th> <th>-----</th> </tr> </thead> <tbody> <tr> <td>(1, 2)</td> <td>well</td> <td>1</td> </tr> <tr> <td>(3, 6)</td> <td>well</td> <td>1</td> </tr> <tr> <td>(4, 5)</td> <td>well</td> <td>1</td> </tr> <tr> <td>(7, 8)</td> <td>well</td> <td>1</td> </tr> </tbody> </table>		Cable pairs	Cable status	Length (meters)	-----	-----	-----	(1, 2)	well	1	(3, 6)	well	1	(4, 5)	well	1	(7, 8)	well	1
Cable pairs	Cable status	Length (meters)																		
-----	-----	-----																		
(1, 2)	well	1																		
(3, 6)	well	1																		
(4, 5)	well	1																		
(7, 8)	well	1																		

## 5.1.18 switchport discard packet

<b>Command</b>	<code>switchport discard packet { all   untag }</code> <code>no switchport discard packet { all   untag }</code>
<b>parameter</b>	<b>all</b> means it does not receive any packet including untag, tag and the deal packet <b>untag</b> means it does not receive untag
<b>default</b>	The default does not have the restriction.
<b>Mode</b>	Port Mode
<b>Usage Guide</b>	This command is not suggested to be configured only if there is the special requirement.
<b>Example</b>	Configure the port of 1/0/8 not to receive all packets. Switch(config)#interface ethernet 1/0/8 Switch(config-if-ethernet1/0/8)#switchport discard packet all

## 5.1.19 switchport flood-control

<b>Command</b>	<b>switchport flood-control { bcast mcast ucast }</b> <b>no switchport flood-control { bcast mcast ucast }</b>	
<b>parameter</b>	<b>bcast</b>	prevents that broadcast packets cannot be transmitted to the specified port
	<b>mcast</b>	prevents that unknown multicast packets cannot be transmitted to the specified port
	<b>ucast</b>	prevents that unknown unicast packets cannot be transmitted to the specified port
<b>default</b>	Switch transmits broadcast, unknown multicast and unknown unicast packets to other port in broadcast domain.	
<b>Mode</b>	Port configuration mode.	
<b>Usage Guide</b>	<p>This command takes effect for 100M and 1000M ports; it is also takes effect for Access, Trunk and Hybrid ports. When this command is valid, the port will allow unicast or multicast flow to pass after port learned the corresponding unicast mac or multicast mac. This command only control that broadcast, multicast and unknown unicast packets sent by other ports cannot be transmitted to the specified port, but it cannot control these packets from the specified port. For example, set switchport flood-control bcast command in port 1/0/1, broadcast packets cannot be transmitted from other ports to port 1/0/1, but port 1/0/1 can receive and transmit broadcast packets.</p>	
<b>Example</b>	<p>Configure flood-control of bcast and mcast for port 1/0/1 or port 1/0/8-10 respectively.</p> <pre>Switch(config)#interface ethernet 1/0/1 Switch(config-if-ethernet1/0/1)#switchport flood-control bcast Switch(config)#interface ethernet 1/0/8-10 Switch(config-if-port-range)#switchport flood-control mcast</pre>	

## 5.1.20 switchport flood-forwarding

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

## 5.2 Port Isolation Function

### 5.2.1 isolate-port group

<b>Command</b>	<code>isolate-port group &lt;WORD&gt;</code> <code>no isolate-port group &lt;WORD&gt;</code>
<b>parameter</b>	<i>WORD</i> is the name identification of the group, no longer than 32 characters
<b>default</b>	-
<b>Mode</b>	Global Mode
<b>Usage Guide</b>	Users can create different port isolation groups based on their requirements. For example, if a user wants to isolate all downlink ports in a vlan of a switch, he can implement that by creating a port isolation group and adding all downlink ports of the vlan into it. No more than 16 port isolation groups can a switch have. When the users need to change or redo the configuration of the port isolation group, he can delete the existing group with the no operation of this command.
<b>Example</b>	Create a port isolation group and name it as "test". Switch>enable Switch#config Switch(config)#isolate-port group test

## 5.2.2 isolate-port group switchport interface

<b>Command</b>	<code>isolate-port group &lt;WORD&gt; switchport interface [ethernet] &lt;IFNAME&gt;</code> <code>no isolate-port group &lt;WORD&gt; switchport interface [ethernet] &lt;IFNAME&gt;</code>	
<b>parameter</b>	<i>WORD</i>	is the name identification of the group, no longer than 32 characters
	<i>IFNAME</i>	is the name of the interface
<b>default</b>	-	
<b>Mode</b>	Global Mode or Vlan Configuration Mode	
<b>Usage Guide</b>	<p>Users can add Ethernet ports into a port isolation group according to their requirements, the isolation group can isolation it from each other (Global mode) in all vlan, it also can isolate it from each other (vlan mode) in some vlan or remove them from a port isolation group according to their requirements. When an Ethernet port is a member of more than one port isolate group, it will be isolated from every port of all groups it belongs to.</p>	
<b>Example</b>	<p>Add Ethernet ports 1/0/1-2 and 1/0/5 into a port isolation group named as "test", add Ethernet ports 1/0/3-4 into a port isolation group named as "1" in vlan10.</p> <pre>Switch(config)#isolate-port group test switchport interface ethernet 1/0/1-2; 1/0/5 Switch(config-vlan10)#isolate-port group 1 switchport interface ethernet 1/0/3-4</pre>	

### 5.2.3 show isolate-port group

<b>Command</b>	<code>show isolate-port group [&lt;WORD&gt;]</code>
<b>parameter</b>	<i>WORD</i> the name identification of the group, no longer than 32 characters
<b>default</b>	Display the configuration of all port isolation groups.
<b>Mode</b>	Admin Mode and Global Mode
<b>Usage Guide</b>	Users can view the configuration of port isolation with this command.
<b>Example</b>	Display the port isolation configuration of the port isolation group named as "test". Switch(config)#show isolate-port group test  Isolate-port group test The isolate-port Ethernet1/0/5 The isolate-port Ethernet1/0/2



## 5.3 Port Loopback Detection Function

### 5.3.1 loopback-detection control

<b>Command</b>	<b>loopback-detection control {shutdown  block }</b> <b>no loopback-detection control</b>	
<b>parameter</b>	<b>shutdown</b>	set the control method as shutdown, which means to close down the port if a port loopback is found.
	<b>block</b>	set the control method as block, which means to block a port by allowing bpd and loopback detection messages only if a port loopback is found.
<b>default</b>	Disable the function of loopback diction control.	
<b>Mode</b>	Port Mode.	
<b>Usage Guide</b>	Enable loopback detection control on the port, which is disabled by the NO operation of this command.	
<b>Example</b>	Enable the function of loopback detection control under port1/2 mode. Switch(config)#interface ethernet 1/0/2 Switch(Config-If-Ethernet1/0/2)#loopback-detection control shutdown Switch(Config-If-Ethernet1/0/2)#no loopback-detection control	

### 5.3.2 loopback-detection control-recovery timeout

<b>Command</b>	<b>loopback-detection control-recovery timeout &lt;0-3600&gt;</b>	
<b>parameter</b>	<b>0-3600</b>	second is recovery time for be controlled state, 0 is not recovery state.
<b>default</b>	The recovery is not automatic by default.	
<b>Mode</b>	Global Configuration Mode.	
<b>Usage Guide</b>	<p>When a port detects a loopback and works in control mode, the ports always work in control mode and not recover. The port will not sent packet to detection in shutdown mode, however, the port will sent loopback-detection packet to detection whether have loopback in block or learning mode. If the recovery time is configured, the ports will recovery normal state when the overtime is time-out. The recovery time is a useful time for shutdown control mode, because the port can keep on detection loopback in the other modes, so suggest not to use this command.</p>	
<b>Example</b>	<p>Enable automatic recovery of the loopback-detection control mode after 30s. Switch(config)#loopback-detection control-recovery timeout 30</p>	

### 5.3.3 loopback-detection interval-time

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

### 5.3.4 loopback-detection specified-vlan

<b>Command</b>	<p>loopback-detection specified-vlan &lt;vlan-list&gt;  no loopback-detection specified-vlan [&lt;vlan-list&gt;]</p>
<b>parameter</b>	<p>vlan-list                      VLAN ID</p>
<b>default</b>	<p>Disable the function of detecting the loopbacks through the port.</p>
<b>Mode</b>	<p>Port Mode</p>
<b>Usage Guide</b>	<p>If a port can be a TRUNK port of multiple Vlans, the detection of loopbacks can be implemented on the basis of port+Vlan, which means the objects of the detection can be the specified Vlans on a port. If the port is an ACCESS port, only one Vlan on the port is allowed to be checked despite the fact that multiple Vlans can be configured. This function is not supported under Port-channel.</p>
<b>Example</b>	<p>Enable the function of loopback detection under port 1/2 mode.  Switch(config)#interface ethernet 1/0/2  Switch(Config-If-Ethernet1/0/2)#switchport mode trunk  Switch(Config-If-Ethernet1/0/2)#switchport trunk allowed vlan all  Switch(Config-If-Ethernet1/0/2)#loopback-detection specified-vlan 1;3;5-20  Switch(Config-If-Ethernet1/0/2)#no loopback-detection specified-vlan 1;3;5-20</p>

### 5.3.5 show loopback-detection

<b>Command</b>	<code>show loopback-detection [interface &lt;interface-list&gt;]</code>
<b>parameter</b>	<i>interface-list</i> the list of ports to be displayed, for example: ethernet 1/0/1.
<b>default</b>	-
<b>Mode</b>	Admin and Configuration Mode.
<b>Usage Guide</b>	Display the state and result of loopback detection on ports with this command.
<b>Example</b>	<p>Display the state of loopback detection on port 4.</p> <pre>Switch(config)#show loopback-detection interface Ethernet 1/0/4</pre> <p>loopback detection config and state information in the switch!</p> <pre>PortName Loopback Detection Control Mode Is Controlled Ethernet1/4 Enable Shutdown No</pre>

## 5.4 ULDP

### 5.4.1 uldp aggressive-mode

<b>Command</b>	<b>uldp aggressive-mode</b> <b>no uldp aggressive-mode</b>
<b>parameter</b>	-
<b>default</b>	Global Configuration Mode and Port Configuration Mode.
<b>Mode</b>	Normal mode.
<b>Usage Guide</b>	The ULDP working mode can be configured only if it is enabled globally. When ULDP aggressive mode is enabled globally, all the existing fiber ports will work in aggressive mode. For the copper ports and fiber ports which are available after the configuration is available, aggressive mode should be enabled in port configuration mode.
<b>Example</b>	To enable ULDP aggressive mode globally. Switch(config)#uldp aggressive-mode

## 5.4.2 uldp enable

<b>Command</b>	<code>uldp {enable disable}</code>
<b>parameter</b>	-
<b>default</b>	By default ULDP is not configured.
<b>Mode</b>	Global Configuration Mode and Port Configuration Mode.
<b>Usage Guide</b>	ULDP can be configured for the ports only if ULDP is enabled globally. If ULDP is enabled globally, it will be effect for all the existing fiber ports. For copper ports and fiber ports which are available after ULDP is enabled, this command should be issued in the port configuration mode to make ULDP be effect.
<b>Example</b>	Enable ULDP in global configuration mode. Switch(config)#uldp enable

### 5.4.3 uldp hello-interval

<b>Command</b>	<code>uldp hello-interval &lt;integer&gt;</code> <code>no uldp hello-interval</code>
<b>parameter</b>	<i>integer</i> The interval for the Hello messages, with its value limited between 5 and 100 seconds, 10 seconds by default.
<b>default</b>	10 seconds by default.
<b>Mode</b>	Global Configuration Mode.
<b>Usage Guide</b>	Interval for hello messages can be configured only if ULDP is enabled globally, its value limited between 5 and 100 seconds.
<b>Example</b>	To configure the interval of Hello messages to be 12 seconds. Switch(config)#uldp hello-interval 12



## 5.4.4 uldp manual-shutdown

---

<b>Command</b>	<code>uldp manual-shutdown</code> <code>no uldp manual-shutdown</code>
<b>parameter</b>	-
<b>default</b>	Auto mode.
<b>Mode</b>	Global Configuration Mode
<b>Usage Guide</b>	This command can be issued only if ULDP has been enabled globally
<b>Example</b>	To enable manual shutdown globally. Switch(config)#uldp manual-shutdown

### 5.4.5 uldp recovery-time

<b>Command</b>	<code>uldp recovery-time&lt;integer&gt;</code> <code>no uldp recovery-time</code>
<b>parameter</b>	<i>integer</i> the time out value for the ULDP recovery timer. Its value is limited between 30 and 86400 seconds.
<b>default</b>	0 is set by default which means the recovery is disabled.
<b>Mode</b>	Global Configuration Mode.
<b>Usage Guide</b>	If an interface is shutdown by ULDP, and the recovery timer times out, the interface will be reset automatically. If the recovery timer is set to 0, the interface will not be reset.
<b>Example</b>	To set the recovery timer to be 600 seconds. Switch(config)#uldp recovery-time 600

## 5.4.6 uldp reset

<b>Command</b>	<b>uldp reset</b>
<b>parameter</b>	-
<b>default</b>	-
<b>Mode</b>	Globally Configuration Mode and Port Configuration Mode.
<b>Usage Guide</b>	This command can only be effect only if the specified interface is disabled by ULDP.
<b>Example</b>	To reset all the port which are disabled by ULDP. Switch(config)#uldp reset

## 5.4.7 show uldp

<b>Command</b>	<code>show uldp [interface ethernet&lt;interface-name&gt;]</code>
<b>parameter</b>	<code>interface-name</code> is the interface name.
<b>default</b>	-
<b>Mode</b>	Admin and Configuration Mode.
<b>Usage Guide</b>	If no parameters are appended, the global ULDP information will be displayed. If the interface name is specified, information about the interface and its neighbors will be displayed along with the global information.

<b>Example</b>	<p>To display the global ULDP information.</p> <pre>Switch(config)#show uldp</pre> <pre> uldp enable uldp hello interval is          10 uldp shut down mode is         AUTO uldp global work mode is       NORMAL the total number of the port is 4 </pre> <table border="1"> <thead> <tr> <th>PortName</th> <th>PhyLink</th> <th>LineProto</th> <th>WorkMode</th> <th>PortState</th> <th>NeighborNum</th> </tr> </thead> <tbody> <tr> <td>Ethernet1/0/25</td> <td>UP</td> <td>DOWN</td> <td>NORMAL</td> <td>INACTIVE</td> <td>0</td> </tr> <tr> <td>Ethernet1/0/26</td> <td>UP</td> <td>DOWN</td> <td>NORMAL</td> <td>INACTIVE</td> <td>0</td> </tr> <tr> <td>Ethernet1/0/27</td> <td>UP</td> <td>DOWN</td> <td>NORMAL</td> <td>INACTIVE</td> <td>0</td> </tr> <tr> <td>Ethernet1/0/28</td> <td>UP</td> <td>DOWN</td> <td>NORMAL</td> <td>INACTIVE</td> <td>0</td> </tr> </tbody> </table>	PortName	PhyLink	LineProto	WorkMode	PortState	NeighborNum	Ethernet1/0/25	UP	DOWN	NORMAL	INACTIVE	0	Ethernet1/0/26	UP	DOWN	NORMAL	INACTIVE	0	Ethernet1/0/27	UP	DOWN	NORMAL	INACTIVE	0	Ethernet1/0/28	UP	DOWN	NORMAL	INACTIVE	0
PortName	PhyLink	LineProto	WorkMode	PortState	NeighborNum																										
Ethernet1/0/25	UP	DOWN	NORMAL	INACTIVE	0																										
Ethernet1/0/26	UP	DOWN	NORMAL	INACTIVE	0																										
Ethernet1/0/27	UP	DOWN	NORMAL	INACTIVE	0																										
Ethernet1/0/28	UP	DOWN	NORMAL	INACTIVE	0																										

## 5.5 LLDP Function

### 5.5.1 clear lldp remote-table

<b>Command</b>	clear lldp remote-table
<b>parameter</b>	-
<b>default</b>	Do not clear the entries.
<b>Mode</b>	Port Configuration Mode
<b>Usage Guide</b>	Clear the Remote table entries on this port.
<b>Example</b>	Clear the Remote table entries on this port. Switch(Config-If-Ethernet 1/0/1)# clear lldp remote-table

## 5.5.2 lldp enable

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

### 5.5.3 Ildp enable ( port )

---

<b>Command</b>	Ildp {enable disable}
<b>parameter</b>	-
<b>default</b>	Default Open
<b>Mode</b>	Port Configuration Mode.

---

**Usage Guide** When LLDP is globally enabled, it will be enabled on every port, the switch on a port is used to disable this function when it is unnecessary on the port.

---

**Example** Disable LLDP function of port on the port ethernet 1/0/5 of the switch.  
Switch(config)#in ethernet 1/0/5  
Switch(Config-If-Ethernet1/0/5)#Ildp disable

### 5.5.4 Ildp management-address tlv

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



### 5.5.5 Ildp mode

Command	Ildp mode <send   receive   both   disable>	
parameter	<b>send</b>	Configure the LLDP function as only being able to send messages.
	<b>receive</b>	Configure the LLDP function as only being able to receive messages.
	<b>both</b>	Configure the LLDP function as being able to both send and receive messages.
	<b>disable</b>	Configure the LLDP function as not being able to send or receive messages.
<b>default</b>	The operating state of the port is "both".	
<b>Mode</b>	Port Configuration Mode.	
<b>Usage Guide</b>	Choose the operating state of the Ildp Agent on the port.	
<b>Example</b>	Configure the state of port ethernet 1/0/5 of the switch as "receive". Switch(config)#in ethernet 1/0/5 Switch(Config-If-Ethernet1/0/5)#Ildp mode receive	

## 5.5.6 Ildp msgTxHold

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

## 5.5.7 Ildp neighbors max-num

<b>Command</b>	<code>lldp neighbors max-num &lt;value&gt;</code> <code>no lldp neighbors max-num</code>
<b>parameter</b>	<i>value</i> is the configured number of entries, ranging from 5 to 500.
<b>default</b>	The maximum number of entries can be stored in Remote MIB is 100.
<b>Mode</b>	Port Configuration Mode.
<b>Usage Guide</b>	The maximum number of entries can be stored in Remote MIB.
<b>Example</b>	Set the Remote as 200 on port ethernet 1/0/5 of the switch. Switch(config)#in ethernet 1/0/5 Switch(Config-If-Ethernet1/0/5)# lldp neighbors max-num 200

## 5.5.8 Ildp notification interval

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

## 5.5.9 Ildp tooManyNeighbors

<b>Command</b>	Ildp tooManyNeighbors {discard   delete}	
<b>parameter</b>	<b>discard</b>	discard the current message.
	<b>delete</b>	Delete the message with the least TTL in the Remoter Table
<b>default</b>	Discard	
<b>Mode</b>	Port Configuration Mode	
<b>Usage Guide</b>	When the Remote MIB is full, Discard means to discard the received message; Delete means to the message with the least TTL in the Remoter Table.	
<b>Example</b>	<p>Set port ethernet 1/0/5 of the switch as delete.</p> <pre>Switch(config)#in ethernet 1/0/5 Switch(Config-If-Ethernet1/0/5)#Ildp tooManyNeighbors delete</pre>	

### 5.5.10 Ildp transmit delay

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

### 5.5.11 Ildp transmit optional tlv

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

## 5.5.12 Ildp trap

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



### 5.5.13 lldp tx-interval

<b>Command</b>	lldp tx-interval <integer> no lldp tx-interval	
<b>parameter</b>	<i>integer</i>	is the interval of sending updating messages, ranging from 5 to 32768 seconds.
<b>default</b>	30s	
<b>Mode</b>	Global Mode	
<b>Usage Guide</b>	<p>After configuring the interval of sending messages, LLDP messages can only be received after a period as long as configured. The interval should be less than or equal with half of aging time, for a too long interval will cause the state of being aged and reconstruction happen too often; while a too short interval will increase the flow of the network and decrease the bandwidth of the port. The value of the aging time of messages is the product of the multiplier and the interval of sending messages. The maximum aging time is 65535 seconds.</p> <p>When tx-interval is the default value and transmit delay is configured via some commands, tx-interval will become four times of the latter, instead of the default 40.</p>	
<b>Example</b>	<p>Set the interval of sending messages as 40 seconds.</p> <pre>Switch(config)#lldp tx-interval 40</pre>	

## 5.5.14 show debugging lldp

<b>Command</b>	show debugging lldp
<b>parameter</b>	-
<b>default</b>	-
<b>Mode</b>	Admin and Configuration Mode
<b>Usage Guide</b>	With show debugging lldp, all ports with lldp debug enabled will be displayed.
<b>Example</b>	Display all ports with lldp debug enabled. Switch(config)#show debugging lldp  ====BEGINNING OF LLDP DEBUG SETTINGS====  debug lldp packets interface Ethernet1/0/1 =====END OF DEBUG SETTINGS=====

### 5.5.15 show lldp

<b>Command</b>	<b>show lldp</b>
<b>parameter</b>	-
<b>default</b>	Do not display the configuration information of global LLDP.
<b>Mode</b>	Admin Mode, Global Mode.
<b>Usage Guide</b>	Users can check all the configuration information of global LLDP by using "show lldp".
<b>Example</b>	<p>Check the configuration information of global LLDP after it is enabled on the switch.</p> <pre>Switch(config)#show lldp</pre> <pre> -----LLDP GLOBAL INFORMATIONS----- LLDP has been enabled globally. LLDP enabled port : Ethernet1/0/1 Ethernet1/0/7 LLDP interval :30 LLDP txTTL :120 LLDP NotificationInterval :5 LLDP txDelay :2 LLDP-MED FastStart Repeat Count :4 -----END----- </pre>

### 5.5.16 show lldp interface ethernet

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

### 5.5.17 show lldp neighbors interface ethernet

<b>Command</b>	show lldp neighbors interface ethernet < IFNAME >
<b>parameter</b>	<i>IFNAME</i> Interface name
<b>default</b>	Do not display the LLDP neighbor information of the port.
<b>Mode</b>	Admin Mode, Global Mode.
<b>Usage Guide</b>	Users can check the configuration information of LLDP on the port by using "show lldp interface ethernet XXX".
<b>Example</b>	<p>Check the LLDP neighbor information of the port after LLDP is enabled on the port.</p> <p>Switch (config-if-ethernet1/0/1)#show lld nei int e 1/0/1</p> <p>Port name : Ethernet1/0/1  Port Remote Counter : 1  TimeMark :92  ChassisIdSubtype :4  ChassisId :00-e0-4c-00-00-00  PortIdSubtype :Local  PortId :gi1</p> <p>Lldp Port Pvid TLV :  Lldp port Pvid : 1</p> <p>*****</p>

### 5.5.18 show lldp traffic

<b>Command</b>	show lldp traffic																								
<b>parameter</b>	-																								
<b>default</b>	Do not display the statistics of LLDP data packets.																								
<b>Mode</b>	Admin Mode, Global Mode.																								
<b>Usage Guide</b>	Users can check the statistics of LLDP data packets by using "show lldp traffic".																								
<b>Example</b>	<p>Check the statistics of LLDP data packets after LLDP is enabled on the switch.</p> <pre>Switch(config)#show lldp traffic</pre> <table border="1"> <thead> <tr> <th>PortName</th> <th>Ageouts</th> <th>FramesDiscarded</th> <th>FramesInErrors</th> </tr> <tr> <th>FramesIn</th> <th>FramesOut</th> <th>TLVsDiscarded</th> <th>TLVsUnrecognized</th> </tr> </thead> <tbody> <tr> <td>Ethernet1/0/1</td> <td>0</td> <td>0</td> <td>0</td> </tr> <tr> <td>42</td> <td>0</td> <td>0</td> <td>43</td> </tr> <tr> <td>Ethernet1/0/7</td> <td>0</td> <td>0</td> <td>0</td> </tr> <tr> <td>42</td> <td>0</td> <td>0</td> <td>0</td> </tr> </tbody> </table>	PortName	Ageouts	FramesDiscarded	FramesInErrors	FramesIn	FramesOut	TLVsDiscarded	TLVsUnrecognized	Ethernet1/0/1	0	0	0	42	0	0	43	Ethernet1/0/7	0	0	0	42	0	0	0
PortName	Ageouts	FramesDiscarded	FramesInErrors																						
FramesIn	FramesOut	TLVsDiscarded	TLVsUnrecognized																						
Ethernet1/0/1	0	0	0																						
42	0	0	43																						
Ethernet1/0/7	0	0	0																						
42	0	0	0																						

## 5.6 Port Channel

### 5.6.1 interface port-channel

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

## 5.6.2 lacp port-priority

<b>Command</b>	<b>lacp port-priority</b> <port-priority> <b>no lacp port-priority</b>
<b>parameter</b>	<i>port-priority</i> the port priority of LACP protocol, the range from 0 to 65535.
<b>default</b>	The default priority is 32768 by system.
<b>Mode</b>	Port Mode.
<b>Usage Guide</b>	Use this command to modify the port priority of LACP protocol, the no command restores the default value.
<b>Example</b>	Set the port priority of LACP protocol. Switch(Config-If-Ethernet1/0/1)# lacp port-priority 30000



### 5.6.3 lacp system-priority

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

## 5.6.4 lacp timeout

---

<b>Command</b>	lacp timeout {short   long} no lacp timeout
<b>parameter</b>	-
<b>default</b>	Long
<b>Mode</b>	Port Mode
<b>Usage Guide</b>	Set the timeout mode of LACP protocol.
<b>Example</b>	Set the timeout mode as short in LACP protocol. Switch(Config-If-Ethernet1/0/1)#lacp timeout short

### 5.6.5 load-balance

<b>Command</b>	<b>load-balance {src-mac   dst-mac   dst-src-mac   src-ip   dst-ip   dst-src-ip    ingress-port   dst-src-mac-ip}</b> <b>no load-balance</b>	
<b>parameter</b>	<b>src-mac</b>	performs load-balance according to the source MAC
	<b>dst-mac</b>	performs load-balance according to the destination MAC
	<b>dst-src-mac</b>	performs load-balance according to the source and destination MAC
	<b>src-ip</b>	performs load-balance according to the source IP
	<b>dst-ip</b>	performs load-balance according to the destination IP
	<b>dst-src-ip</b>	performs load-balance according to the destination and source IP
	<b>ingress-port</b>	performs load-balance according to the destination and source mac and destination, source IP
	<b>dst-src-mac-ip</b>	performs load-balance according to the port of receive flow.
<b>default</b>	Perform load-balance according to the source MAC.	
<b>Mode</b>	Global mode.	
<b>Usage Guide</b>	Use port-channel to implement load-balance, user can configure the load-balance mode according to the requirements. If the specific load-balance mode of the command line is different with the current load-balance mode of port-group, then modify the load-balance of port-group as the specific load-balance of command line; otherwise return a message to notice that the current mode is already configured.	
<b>Example</b>	Set load-balance mode of port-group. Switch(config)# load-balance src-mac	

## 5.6.6 port-group

<b>Command</b>	<b>port-group</b> <port-group-number> <b>no port-group</b> <port-group-number>
<b>parameter</b>	<i>port-group-number</i> is the group number of a port channel from 1 ~ 128.
<b>default</b>	There is no port-group
<b>Mode</b>	Global Mode
<b>Usage Guide</b>	it can create 16 port group at most
<b>Example</b>	Creating a port group. Switch(config)# port-group 1 Delete a port group. Switch(config)#no port-group 1

## 5.6.7 port-group mode

<b>Command</b>	<b>port-group &lt;port-group-number&gt; mode {active   passive   on}</b> <b>no port-group</b>								
<b>parameter</b>	<table border="1"> <tr> <td><i>port-group-number</i></td> <td>is the group number of port channel, from 1~128</td> </tr> <tr> <td><b>active</b></td> <td>enables LACP on the port and sets it in Active mode</td> </tr> <tr> <td><b>passive</b></td> <td>enables LACP on the port and sets it in Passive mode</td> </tr> <tr> <td><b>on</b></td> <td>forces the port to join a port channel without enabling LACP.</td> </tr> </table>	<i>port-group-number</i>	is the group number of port channel, from 1~128	<b>active</b>	enables LACP on the port and sets it in Active mode	<b>passive</b>	enables LACP on the port and sets it in Passive mode	<b>on</b>	forces the port to join a port channel without enabling LACP.
<i>port-group-number</i>	is the group number of port channel, from 1~128								
<b>active</b>	enables LACP on the port and sets it in Active mode								
<b>passive</b>	enables LACP on the port and sets it in Passive mode								
<b>on</b>	forces the port to join a port channel without enabling LACP.								
<b>default</b>	Switch ports do not belong to a port channel by default; LACP not enabled by default.								
<b>Mode</b>	Port Mode								
<b>Usage Guide</b>	Add a physical port to the port channel NO remove the specified port from the port channel								
<b>Example</b>	<p>Under the Port Mode of Ethernet1/0/1, add current port to “port-group 1” in “active” mode.</p> <pre>Switch(Config-If-Ethernet1/0/1)#port-group 1 mode active</pre>								

## 5.6.8 show port-group

<b>Command</b>	<b>show port-group [&lt;port-group-number&gt;] {brief   detail }</b>													
<b>parameter</b>	<i>port-group-number</i>	is the group number of port channel to be displayed, from 1 ~ 128												
<b>default</b>	-													
<b>Mode</b>	All Configuration Mode													
<b>Usage Guide</b>	If the user does not input port-group-number, that means the information of all the existent port-group are showed; if the port channel corresponds to port-group-number parameter and is not exist, then print a error message, otherwise display the current port-channel information of the specified group number.													
<b>Example</b>	<p>Display summary information for port-group 1</p> <pre>Switch#show port-group brief</pre> <p>ID: port group number; Mode: port group mode such as on active or passive;  Ports: different types of port number of a port group,  the first is selected ports number, the second is standby ports number, and  the third is unselected ports number.</p> <table border="1"> <thead> <tr> <th>ID</th> <th>Mode</th> <th>Partner ID</th> <th>Ports</th> <th>Load-balance</th> </tr> </thead> <tbody> <tr> <td>1</td> <td>active</td> <td>0x0000,00-00-00-00-00-00</td> <td>0,0,1</td> <td>src-mac</td> </tr> </tbody> </table>				ID	Mode	Partner ID	Ports	Load-balance	1	active	0x0000,00-00-00-00-00-00	0,0,1	src-mac
ID	Mode	Partner ID	Ports	Load-balance										
1	active	0x0000,00-00-00-00-00-00	0,0,1	src-mac										

## 5.7 MTU

### 5.7.1 Mtu

<b>Command</b>	<b>mtu [&lt;mtu-value&gt;]</b> <b>no mtu</b>
<b>parameter</b>	<i>mtu-value</i> the MTU value of frames that can be received, in byte, ranging from <1500-12270>. The corresponding frame size is <1518/1522-12288/12292>. Without setting is parameter, the allowed max frame size is 12288/12292.
<b>default</b>	MTU function not enabled by default
<b>Mode</b>	Global Mode
<b>Usage Guide</b>	Set switch of both ends mtu necessarily, or mtu frame will be dropped at the switch has not be set
<b>Example</b>	Enable the mtu function of the switch. Switch(config)#mtu

## 5.8 EFM OAM

### 5.8.1 clear ethernet-oam

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



## 5.8.2 ethernet-oam

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

### 5.8.3 ethernet-oam errored-frame threshold high

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

### 5.8.4 ethernet-oam errored-frame threshold low

<b>Command</b>	<b>ethernet-oam errored-frame threshold low &lt;low-frames&gt;</b> <b>no ethernet-oam errored-frame threshold low</b>	
<b>parameter</b>	<i>low-frames</i>	the low detection threshold of errored frame event, ranging from 1 to 4294967295
<b>default</b>	1	
<b>Mode</b>	Port mode	
<b>Usage Guide</b>	<p>During the specific detection period, errored frame event is induced if the number of errored frame is larger than or equal to the low threshold and the device notifies the peer by sending event notification OAMPDU. Note that the low threshold can not be larger than the high threshold.</p>	
<b>Example</b>	<p>Configure the low threshold of errored frame event on Ethernet 1/0/4 to 100.</p> <pre>Switch(Config-If-Ethernet1/0/4)#ethernet-oam errored-frame threshold low 100</pre>	

### 5.8.5 ethernet-oam errored-frame window

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

## 5.8.6 ethernet-oam errored-frame-seconds threshold high

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

## 5.8.7 ethernet-oam errored-frame-seconds threshold Low

<b>Command</b>	<b>ethernet-oam errored-frame-seconds threshold low</b> <low-seconds> no ethernet-oam errored-frame-seconds threshold low	
<b>parameter</b>	<i>low-seconds</i>	the low detection threshold of errored frame seconds event, ranging from 1 to 65535 seconds.
<b>default</b>	1	
<b>Mode</b>	Port mode	
<b>Usage Guide</b>	During the specific detection period, errored frame period event is induced if the number of errored frame is larger than or equal to the low threshold and the device notifies the peer by event notification OAMPDU. Note that the low threshold should not be larger than the high threshold.	
<b>Example</b>	Configure the low threshold of errored frame period event on port 1/0/4 to be 100. Switch(Config-If-Ethernet1/0/4)#ethernet-oam errored-frame-seconds threshold low 100	

### 5.8.8 ethernet-oam errored-frame-seconds window

<b>Command</b>	<b>ethernet-oam errored-frame-seconds window &lt;seconds&gt;</b> <b>no ethernet-oam errored-frame-seconds window</b>	
<b>parameter</b>	<i>seconds</i>	is the time for counting the specified frame number, its range from 50 to 450, unit is 200ms.
<b>default</b>	300	
<b>Mode</b>	Port mode	
<b>Usage Guide</b>	Detect errored frame seconds of the port after the time of specific detection period. If the number of errored frame seconds is larger than or equal to the threshold, corresponding event is induced and the device notified the peer through OAMPDU.	
<b>Example</b>	Configure the detection period of errored frame seconds event on port 1/0/4 to be 120s. Switch(Config-If-Ethernet1/0/4)#ethernet-oam errored-frame-seconds window 600	

## 5.8.9 ethernet-oam errored-symbol-period threshold High

<b>Command</b>	<pre>ethernet-oam errored-symbol-period threshold high {&lt;high-symbols&gt;   none} no ethernet-oam errored-symbol-period threshold high</pre>	
<b>parameter</b>	<i>high-symbols</i>	the high detection threshold of errored symbol event, ranging from 2 to 18446744073709551615 symbols.
	<b>none</b>	cancel the high threshold configuration.
<b>default</b>	<b>none</b>	
<b>Mode</b>	Port mode	
<b>Usage Guide</b>	<p>During the specific detection period, serious link event is induced if the number of errored symbols is larger than or equal to the high threshold and the device notifies the peer by sending Information OAMPDU of which the value of Link Fault flag in Flags field is 1. Note that the high threshold should not be less than the low threshold.</p>	
<b>Example</b>	<p>Set the high threshold of errored symbol event on port 1/0/4 to none.</p> <pre>Switch(Config-If-Ethernet1/0/4)#ethernet-oam errored-symbol-period threshold high none</pre>	



### 5.8.10 ethernet-oam errored-symbol-period threshold Low

<b>Command</b>	<b>ethernet-oam errored-symbol-period threshold low &lt;low-symbols&gt;</b> <b>no ethernet-oam errored-symbol-period threshold low</b>	
<b>parameter</b>	<i>low-symbols</i>	the low threshold of errored symbol event, ranging from 1 to 18446744073709551615 symbols.
<b>default</b>	1	
<b>Mode</b>	Port mode	
<b>Usage Guide</b>	<p>During the specific detection period, errored symbol event is induced if the number of errored symbols is larger than or equal to the low threshold and the device notifies the peer by sending event notification OAMPDU. Note that the low threshold should not be larger than the high threshold.</p>	
<b>Example</b>	<p>Set the low threshold of errored symbol event on port 1/0/4 to be 5.</p> <pre>Switch(Config-If-Ethernet1/0/4)#ethernet-oam errored-symbol-period threshold low 5</pre>	

### 5.8.11 ethernet-oam errored-symbol-period window

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

## 5.8.12 ethernet-oam link-monitor

---

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

### 5.8.13 ethernet-oam mode

<b>Command</b>	ethernet-oam mode {active   passive} no ethernet-oam mode	
<b>parameter</b>	<b>active</b>	active mode
	<b>passive</b>	passive mode
<b>default</b>	active mode	
<b>Mode</b>	Port mode	
<b>Usage Guide</b>	<p>At least one of the two connected OAM entities should be configured to active mode. Once OAM is enabled, the working mode of OAM cannot be changed and you need to disable OAM function if you have to change the working mode.</p>	
<b>Example</b>	<p>Set the mode of OAM function on ethernet 1/0/4 to passive mode. Switch(Config-If-Ethernet1/0/4)#ethernet-oam mode passive</p>	

### 5.8.14 ethernet-oam period

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

## 5.8.15 ethernet-oam remote-failure

<b>Command</b>	<b>ethernet-oam remote-failure</b> <b>no ethernet-oam remote-failure</b>
<b>parameter</b>	-
<b>default</b>	Enable
<b>Mode</b>	Port mode
<b>Usage Guide</b>	With remote failure indication is enabled, if critical-event or link fault event is occurred locally, it will notify the peer by sending Information OAMPDU, log the fault information and send SNMP trap warning. When the remote failure indication is disabled, although local critical-event or link fault event is not monitored, failure indication information from the peer is still normally received and processed.
<b>Example</b>	Enable remote failure indication of ethernet 1/0/4. Switch(Config-If-Ethernet1/0/4)#ethernet-oam remote-failure

## 5.8.16 ethernet-oam remote-loopback

---

<b>Command</b>	<code>ethernet-oam remote-loopback</code> <code>no ethernet-oam remote-loopback</code>
<b>parameter</b>	-
<b>default</b>	Disable
<b>Mode</b>	port mode
<b>Usage Guide</b>	<p>Only OAM can send remote loopback reques in auto mode, the OAM work in passive mode can not send remote loopback; when remote OAM working in loopback mode, all packets except OAM PDU packets will back local port according to the same route (Notice: during OAM loopback, it can not communicate), administrator can check the link delay of loopback, shake and throughput capacity. It can do loopback configuration after create OAM link, if OAM link is broken during loopback, the loopback will be cancel automatically. The command mutex with ethernet-oam remote-loopback supported.</p>
<b>Example</b>	<p>Enable the remote OAM of port 1/0/4 to remote loopback mode.</p> <pre>Switch(Config-If-Ethernet1/0/4)#ethernet-oam remote-loopback</pre> <p>Normal forwarding will be suspended during the remote-loopback, are you sure to start remote-loopback? [Y/N]</p>

## 5.8.17 ethernet-oam remote-loopback supported

<b>Command</b>	<b>ethernet-oam remote-loopback supported</b> <b>no ethernet-oam remote-loopback supported</b>
<b>parameter</b>	-
<b>default</b>	Disable
<b>Mode</b>	Port mode.
<b>Usage Guide</b>	The port that only enable loopback support function can receive OAM loopback request and in loopback mode. So when enable remote and in OAM loopback, please ensure remote configured loopback support. The command mutex with ethernet-oam remote-loopback.
<b>Example</b>	Enable OAM loopback support function of ethernet 1/0/4 Switch(Config-If-Ethernet1/0/4)#ethernet-oam remote-loopback supported



## 5.8.18 ethernet-oam timeout

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

### 5.8.19 show ethernet-oam

<b>Command</b>	<code>show ethernet-oam [{local   remote} interface {ethernet  }] &lt;IFNAME&gt;</code>
<b>parameter</b>	<i>IFNAME</i> the port that OAM connection information will be shown
<b>default</b>	N/A.
<b>Mode</b>	Admin mode
<b>Usage Guide</b>	N/A.
<b>Example</b>	<p>Show overview information of Ethernet OAM connection.</p> <pre>Switch#show ethernet-oam</pre> <p>Switch#show ethernet-oam</p> <p>Capability codes: L - Link Monitor, R - Remote Loopback  U - Unidirection, V - Variable Retrieval</p> <p>-----</p> <pre>Interface Local-Mode Local-Capability Remote-MAC-Addr Remote-Mode Remote- Capability 1/0/1 active L</pre>

## 5.8.20 show ethernet-oam events

<b>Command</b>	<b>show ethernet-oam events {local   remote} [interface {ethernet {} &lt;IFNAME&gt;}]</b>	
<b>parameter</b>	<i>IFNAME</i>	the port that the statistic information of OAM link events needs to be shown
<b>default</b>	N/A.	
<b>Mode</b>	Admin mode	
<b>Usage Guide</b>	N/A.	
<b>Example</b>	<p>Show the statistic information of link events on Ethernet 1/0/1.</p> <pre>Switch#show ethernet-oam events local interface 1/0/1</pre> <p>ethernet1/0/1 link-events:</p> <pre>OAM_local_errored-symbol-period-events: ----- event time stamp: 3539 errored symbol window(200ms): 5 errored symbol low threshold: 1 errored symbol high threshold: none errored symbol: 1200120 errored running total: 2302512542 event running total: 232 OAM_local_errored-frame-period-events: ----- event time stamp: 3539 errored frame window(200ms): 50 errored frame low threshold: 1 errored frame high threshold: none errored frame: 1200120 errored running total: 2302512542 event running total: 52 OAM_local_errored-frame-events: ----- event time stamp: 3539 errored frame window(200ms): 5 errored frame low threshold: 1 errored frame high threshold: none errored frame: 1200120 errored running total: 2302512542 event running total: 75 OAM_local_errored-frame-seconds-summary-events: ----- event time stamp: 3520 errored frame seconds summary window(200ms): 300</pre>	

---

errored frame low threshold: 1 errored frame high threshold: none  
errored frame: 1200120 errored running total: 2302512542  
event running total: 232  
OAM\_local\_link-fault: 0  
OAM\_local\_dying gasp: 0  
OAM\_local\_critical event: 0

## 5.8.21 show ethernet-oam link-events-configuration

<b>Command</b>	<b>show ethernet-oam link-events-configuration [interface {ethernet   } &lt;IFNAME&gt;]</b>	
<b>parameter</b>	<i>IFNAME</i>	the port that the statistic information of OAM link events needs to be shown
<b>default</b>	N/A.	
<b>Mode</b>	Admin mode	
<b>Usage Guide</b>	N/A.	
<b>Example</b>	<p>Show configuration of link events on ethernet 1/0/1.</p> <pre>Switch#show ethernet-oam link-events-configuration interface ethernet 1/0/1 Ethernet1/0/1 link-monitor configuration: event high-threshold low-threshold window(200ms) ----- Err-symbol-Period none 1 2 Err-frame-Period none 1 10 Err-frame none 2 5 Err-frame-second-summary none 2 600 -----</pre>	

## 5.8.22 show ethernet-oam loopback status

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

## 5.9 PORT SECURITY

### 5.9.1 clear port-security

---

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

---

<b>parameter</b>	<b>all</b>	All secure MAC entries on the interfaces
	<b>configured</b>	The configured secure MAC
	<b>dynamic</b>	The dynamic secure MAC learnt by the interface
	<b>sticky</b>	The secure MAC of sticky
	<b>mac-addr</b>	The specified secure MAC address
	<b>interface-id</b>	The secure MAC entries of the specified interface
	<b>vlan-id</b>	The specified VLAN

---

**default**

---

-

**Mode**

---

Admin mode

**Usage Guide**

---

Clear secure MACs on the interface

**Example**

---

Clear all secure MACs on the interface  
Switch#clear port-security all

## 5.9.2 show port-security

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



### 5.9.3 switchport port-security

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

### 5.9.4 switchport port-security mac-address

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

## 5.9.5 switchport port-security maximum

<b>Command</b>	<pre>switchport port-security maximum &lt;value&gt; [vlan &lt;vlan-list&gt;] no switchport port-security maximum &lt;value&gt; [vlan &lt;vlan-list&gt;]</pre>	
<b>parameter</b>	<i>value</i>	Configure the maximum number of the secure MAC allowed by the interface, its range between 1 and 128. It is determined by the maximum MAC number of the device
	<i>vlan-list</i>	Configure the maximum value for the specified VLAN, it only takes effect on trunk and hybrid interfaces.
<b>default</b>	After enabling port-security, if there is no other configuration, the maximum number of the secure MAC is 1 on the interface. The interface number in VLAN is no limit by default	
<b>Mode</b>	Port mode	
<b>Usage Guide</b>	Pay attention to the coupling relation about the number between the interface and VLAN, set the maximum number configured by the interface as the standard firstly.	
<b>Example</b>	<p>Configure the maximum number of the secure MAC on the interface.</p> <pre>Switch(config-if- ethernet1/0/1)# switchport port-security maximum 100</pre>	

## 5.9.6 switchport port-security violation

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

## 5.10 DDM

### 5.10.1 clear transceiver threshold-violation

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

## 5.10.2 show transceiver

<b>Command</b>	<b>show transceiver [interface ethernet &lt;interface-list&gt;] [detail]</b>																						
<b>parameter</b>	<b>interface-list</b>	The interface list that the monitoring of the transceiver needs to be shown.																					
	<b>detail</b>	Show the detailed monitoring of the transceiver.																					
<b>default</b>	-																						
<b>Mode</b>	User mode, admin mode and global mode																						
<b>Usage Guide</b>	Displays the transceiver's detailed monitoring information.																						
<b>Example</b>	<p>Show the brief DDM information of all ports.</p> <pre>Switch#show transceiver</pre> <table border="1"> <thead> <tr> <th>Interface</th> <th>Temp (°C)</th> <th>Voltage (V)</th> <th>Bias (mA)</th> <th>RX Power (dBm)</th> <th>TX Power (dBm)</th> </tr> </thead> <tbody> <tr> <td>1/0/25</td> <td>33</td> <td>3.31</td> <td>6.11</td> <td>-30.54(A-)</td> <td>-6.01</td> </tr> <tr> <td>1/0/26</td> <td>33</td> <td>5.00 (W+)</td> <td>6.11</td> <td>-20.54(W-)</td> <td>-6.02</td> </tr> </tbody> </table>					Interface	Temp (°C)	Voltage (V)	Bias (mA)	RX Power (dBm)	TX Power (dBm)	1/0/25	33	3.31	6.11	-30.54(A-)	-6.01	1/0/26	33	5.00 (W+)	6.11	-20.54(W-)	-6.02
Interface	Temp (°C)	Voltage (V)	Bias (mA)	RX Power (dBm)	TX Power (dBm)																		
1/0/25	33	3.31	6.11	-30.54(A-)	-6.01																		
1/0/26	33	5.00 (W+)	6.11	-20.54(W-)	-6.02																		

### 5.10.3 show transceiver threshold-violation

<b>Command</b>	<b>show transceiver threshold-violation [interface ethernet &lt;interface-list&gt;]</b>																																																	
<b>parameter</b>	<b>interface-list</b>	The interface list that the transceiver monitoring needs to be shown.																																																
<b>default</b>	-																																																	
<b>Mode</b>	Admin mode and global mode																																																	
<b>Usage Guide</b>	Show the transceiver monitoring																																																	
<b>Example</b>	<p>Show the transceiver monitoring</p> <pre>Switch(config)#show transceiver threshold-violation interface ethernet 1/0/25-26</pre> <p>Ethernet 1/0/25 transceiver threshold-violation information:          Transceiver monitor is enabled. Monitor interval is set to 30 minutes.          The current time is Jan 02 12:30:50 2010.          The last threshold-violation time is Jan 01 1:30:50 2010.          Brief alarm information:          RX loss of signal          RX power low          Detail diagnostic and threshold information:</p> <table border="1"> <thead> <tr> <th></th> <th>Diagnostic</th> <th>Threshold</th> <th></th> <th></th> <th></th> </tr> <tr> <th></th> <th>Realtime Value</th> <th>High Alarm</th> <th>Low Alarm</th> <th>High Warn</th> <th>Low Warn</th> </tr> <tr> <th></th> <th>-----</th> <th>-----</th> <th>-----</th> <th>-----</th> <th>-----</th> </tr> </thead> <tbody> <tr> <td>Temperature (°C)</td> <td>33</td> <td>70</td> <td>0</td> <td>70</td> <td>0</td> </tr> <tr> <td>Voltage (V)</td> <td>7.31</td> <td>10.00</td> <td>0.00</td> <td>5.00</td> <td>0.00</td> </tr> <tr> <td>Bias current (mA)</td> <td>3.11</td> <td>10.30</td> <td>0.00</td> <td>5.00</td> <td>0.00</td> </tr> <tr> <td>RX Power (dBm)</td> <td>-30.54(A-)</td> <td>9.00</td> <td>-25.00 (-34)</td> <td>9.00</td> <td>-25.00</td> </tr> <tr> <td>TX Power (dBm)</td> <td>-1.01</td> <td>9.00</td> <td>-12.05</td> <td>9.00</td> <td>-10.00</td> </tr> </tbody> </table> <p>Ethernet 1/0/26 transceiver threshold-violation information:          Transceiver monitor is disabled. Monitor interval is set to 30 minutes.          The last threshold-violation doesn't exist.</p>			Diagnostic	Threshold					Realtime Value	High Alarm	Low Alarm	High Warn	Low Warn		-----	-----	-----	-----	-----	Temperature (°C)	33	70	0	70	0	Voltage (V)	7.31	10.00	0.00	5.00	0.00	Bias current (mA)	3.11	10.30	0.00	5.00	0.00	RX Power (dBm)	-30.54(A-)	9.00	-25.00 (-34)	9.00	-25.00	TX Power (dBm)	-1.01	9.00	-12.05	9.00	-10.00
	Diagnostic	Threshold																																																
	Realtime Value	High Alarm	Low Alarm	High Warn	Low Warn																																													
	-----	-----	-----	-----	-----																																													
Temperature (°C)	33	70	0	70	0																																													
Voltage (V)	7.31	10.00	0.00	5.00	0.00																																													
Bias current (mA)	3.11	10.30	0.00	5.00	0.00																																													
RX Power (dBm)	-30.54(A-)	9.00	-25.00 (-34)	9.00	-25.00																																													
TX Power (dBm)	-1.01	9.00	-12.05	9.00	-10.00																																													

## 5.10.4 transceiver-monitoring

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



### 5.10.5 transceiver-monitoring interval

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

### 5.10.6 transceiver threshold

<b>Command</b>	transceiver threshold {default   {temperature   voltage   bias   rx-power   tx-power} {high-alarm   low-alarm   high-warn   low-warn} {<value>   default}}	
<b>parameter</b>	<b>default</b>	Restore the threshold as the default threshold set by the manufacturer. If the monitoring index is not specified, restore all thresholds, if the monitoring index is specified, restore the corresponding threshold only.
	<b>temperature</b>	The monitoring index—temperature
	<b>voltage</b>	The monitoring index—voltage
	<b>bias</b>	The monitoring index—bias current
	<b>rx-power</b>	The monitoring index—receiving power
	<b>tx-power</b>	The monitoring index—sending power
	<b>high-alarm</b>	High-alarm of the monitoring index, namely there is alarm with A+ if exceeding the threshold.
	<b>low-alarm</b>	Low-alarm of the monitoring index, namely there is alarm with Aif exceeding the threshold.
	<b>high-warn</b>	High-warn of the monitoring index, namely there is warning with W+ if exceeding the threshold.
	<b>low-warn</b>	Low-warn of the monitoring index, namely there is warning with W- if exceeding the threshold.
<b>default</b>	The threshold is set by the manufacturer	
<b>Mode</b>	Port mode	
<b>Usage Guide</b>	<p>The range of the threshold parameters is shown for each monitoring index in the following :</p> <p>Temperature: -128.00~128.00 °C</p> <p>Voltage: 0.00~7.00 V</p> <p>Bias current: 0.00~140.00 mA</p> <p>x-power: -50.00~9.00 dBM</p> <p>tx-power: -50.00~9.00 dBM</p> <p>The maximum length of the threshold parameter configured by the user is 20 bits.</p>	

---

After the user configured a parameter threshold, the threshold set by the manufacturer will be labeled with the bracket when showing the threshold, and decide whether give an alarm according to the user's configuration.

---

**Example**

Configure tx-power threshold of the fiber module, the low-warn threshold is configured as -12 on ethernet1/0/1.

```
Switch(config-if-ethernet1/0/1)#transceiver threshold tx-power low-warn -12
```

## 5.11 LLDP-MED

### 5.11.1 civic location

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

## 5.11.2 description-language

<b>Command</b>	<p>{description-language   province-state   city   county   street   locationNum   location   floor   room   postal   otherInfo} &lt;address&gt;</p> <p>no {description-language   province-state   city   county   street   locationNum   location   floor   room   postal   otherInfo}</p>	
<b>parameter</b>	<b>description-language</b>	language for describing location, such as 'English'
	<b>province-state</b>	state, canton, region, province prefecture, and so on, such as 'clara'
	<b>city</b>	city, such as 'New York'
	<b>county</b>	county, parish, such as 'santa clara'
	<b>street</b>	street, such as '1301 Shoreway Road'
	<b>locationNum</b>	house number, such as '9'
	<b>location</b>	name and occupant of a location, such as 'Carrillo's Holiday Market'
	<b>floor</b>	floor number, such as '13'
	<b>room</b>	room number, such as '1308'
	<b>postal</b>	postal/zip code, such as '10027-1234'
	<b>otherInfo</b>	Additional location information, such as 'South Wing'
	<i>address</i>	detailed address information, it cannot exceed 250 characters
<b>default</b>	No detailed information of the location with Civic Address LCI is configured on the port.	
<b>Mode</b>	Civic Address LCI address mode	
<b>Usage Guide</b>	With this command, configure the detailed information of the location with Civic Address LCI on the port, it is able to configure 10 kinds of address types at most.	
<b>Example</b>	<p>Configure the detailed location information in Civic Address LCI address mode.</p> <pre>Switch(Med-Civic)# city Beijing Switch(Med-Civic)# street shangdi</pre>	

### 5.11.3 ecs location

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

### 5.11.4 Ildp med fast count

<b>Command</b>	Ildp med fast count <value> no Ildp med fast count	
<b>parameter</b>	<i>value</i>	The number of sending the packets fast, its range from 1 to 10, unit is entries.
<b>default</b>	4	
<b>Mode</b>	Global mode	
<b>Usage Guide</b>	With this command, set the number for sending the packets fast.	
<b>Example</b>	Set the number of quick packages to 5 Switch(config)#Ildp med fast count 5	

### 5.11.5 Ildp med trap

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



### 5.11.6 Ildp transmit med tlv all

<b>Command</b>	Ildp transmit med tlv all no Ildp transmit med tlv all
<b>parameter</b>	-
<b>default</b>	Port does not enable the function for Sending LLDP-MED TLV.
<b>Mode</b>	Port mode
<b>Usage Guide</b>	After configuring this command, if the port is able to send LLDP-MED TLV, the sent LLDP packets with LLDP-MED TLV supported by all switches. However, LLDP packets sent by the port without any LLDP-MED TLV after the switch configured the corresponding no command.
<b>Example</b>	Port 19 enables the function for sending LLDP-MED TLV. Switch(Config-If-Ethernet1/0/19)# Ildp transmit med tlv all

### 5.11.7 Ildp transmit med tlv capability

<b>Command</b>	<b>Ildp transmit med tlv capability</b> <b>no Ildp transmit med tlv capability</b>
<b>parameter</b>	-
<b>default</b>	The function is disabled for sending LLDP-MED Capability TLV.
<b>Mode</b>	Port mode
<b>Usage Guide</b>	After configuring this command, if the port is able to send LLDP-MED TLV, the sent LLDP packets with LLDP-MED Capability TLV. However, LLDP packets sent by the port without LLDP-MED Capability TLV after the switch configured the corresponding no command. Note: LLDP-MED Capability TLV is the important LLDP-MED TLV, if do not configure the port to send LLDP-MED Capability TLV firstly, other LLDP-MED TLV will not be sent.
<b>Example</b>	Port 19 enables the function for sending LLDP-MED Capability TLV. Switch(Config-If-Ethernet1/0/19)# Ildp transmit med tlv capability

### 5.11.8 Ildp transmit med tlv extendPoe

<b>Command</b>	<code>lldp transmit med tlv extendPoe</code> <code>no lldp transmit med tlv extendPoe</code>
<b>parameter</b>	-
<b>default</b>	The function is disabled for sending LLDP-MED Extended Power-Via-MDI TLV.
<b>Mode</b>	Port mode
<b>Usage Guide</b>	Configure specified port to send LLDP-MED extended power supply - Via-MDITLV. No command disables the function.
<b>Example</b>	Port 19 enables the function for sending LLDP-MED Extended Power-Via-MDI TLV. Switch(Config-If-Ethernet1/0/19)# <code>lldp transmit med tlv extendPoe</code>

### 5.11.9 Ildp transmit med tlv location

<b>Command</b>	Ildp transmit med tlv location no Ildp transmit med tlv location
<b>parameter</b>	-
<b>default</b>	Disable
<b>Mode</b>	Port Mode
<b>Usage Guide</b>	<p>Configure the specified port to send LLDP-MED Location Identification TLV. After configured this command, if the port has the capability of sending LLDP-MED TLV, the LLDP packets sent from the port will include LLDP-MED Location Identification TLV. Otherwise, the LLDP packets sent from the port will not include LLDP-MED Location Identification TLV by the no command even if the port has the capability of sending LLDP-MED TLV. Notice: Before configuring this function, the capability of sending LLDP-MED Capability TLV must be configured. If the device does not support POE or the POE function of the port is disabled by the command, this TLV will not be sent.</p>
<b>Example</b>	<p>Enable the port 19 to send LLDP-MED Location Identification TLV. Switch(Config-If-Ethernet1/0/19)#Ildp transmit med tlv location</p>

### 5.11.10 Ildp transmit med tlv inventory

<b>Command</b>	<b>Ildp transmit med tlv inventory</b> <b>no Ildp transmit med tlv inventory</b>
<b>parameter</b>	-
<b>default</b>	The function is disabled for sending LLDP-MED Inventory Management TLVs
<b>Mode</b>	Port mode
<b>Usage Guide</b>	<p>After configuring this command, if the port is able to send LLDP-MED TLV, LLDP packets with LLDP-MED Inventory Management TLVs sent by the port. However, LLDP packets without LLDP-MED Inventory Management TLVs sent by the port after the switch configured the corresponding no command. Note: LLDP-MED Capability TLV sent by the port must be configured before sending LLDP-MED Inventory Management TLVs, or else the configuration cannot be successful.</p>
<b>Example</b>	<p>Port 19 enables the function for sending LLDP-MED Inventory Management TLVs.</p> <pre>Switch(Config-If-Ethernet1/0/19)# Ildp transmit med tlv inventory</pre>

### 5.11.11 Ildp transmit med tlv networkPolicy

<b>Command</b>	<b>Ildp transmit med tlv networkPolicy</b> <b>no Ildp transmit med tlv networkPolicy</b>
<b>parameter</b>	-
<b>default</b>	The function is disabled for sending LLDP-MED Network Policy TLV.
<b>Mode</b>	Port mode
<b>Usage Guide</b>	After configuring this command, if the port is able to send LLDP-MED TLV, LLDP packets with LLDP-MED Network Policy TLV sent by the port. However, LLDP packets without LLDP-MED Network Policy TLV sent by the port after the switch configured the corresponding no command. Note: LLDP-MED Capability TLV sent by the port must be configured before sending LLDP-MED Network Policy TLV, or else the configuration cannot be successful.
<b>Example</b>	Port 19 enables the function for sending LLDP-MED Network Policy TLV. Switch(Config-If-Ethernet1/0/19)# Ildp transmit med tlv networkPolicy

### 5.11.12 network policy

<b>Command</b>	<p>network policy {voice   voice-signaling   guest-voice   guest-voice-signaling   softphone-voice   video-conferencing   streaming-video   video-signaling} [status {enable   disable}] [tag {tagged   untagged}] [vid {&lt;vlan-id&gt;   dot1p}] [cos &lt;cos-value&gt;] [dscp &lt;dscp-value&gt; ]</p> <p>no network policy {voice   voice-signaling   guest-voice   guest-voice-signaling   softphone-voice   video-conferencing   streaming-video   video-signaling}</p>	
<b>parameter</b>	<b>status</b>	Whether the network policy is usable.
	<b>enable</b>	Network Policy of the specified application type has been defined, enable is the default value of the network policy.
	<b>disable</b>	Network Policy of the specified application type has been defined, disable is the default value of the network policy
	<b>tag</b>	Configure the specified application to uses tagged or untagged VLAN method
	<b>tagged</b>	Configure the flow of the specified application to use the tagged vlan method, here, the fields (such as VLAN ID, Layer2 priority and DSCP value) are take effect
	<b>untagged</b>	Configure the flow without tag for the specified application, the fields (such as VLAN ID, Layer2 priority) are ignored, only DSCP value field takes effect. Untagged is the default value of VLAN method.
	<b>vid</b>	Configure VLAN ID that the specified application belongs to
	<i>vlan-id</i>	Configure the value of VLAN ID, its range from 1 to 4094
	<b>dot1p</b>	Configure the specified application to tag the flow by using 802.1p priority, at the same time, use vlan 0 to load the flow.
	<b>cos</b>	Configure the priority of Ethernet frame for VLAN
	<b>cos-value</b>	Configure the value of Ethernet frame priority for VLAN, its range from 0 to 7, the default value is 5.
	<b>dscp</b>	Configure DSCP of VLAN.
	<i>dscp-value</i>	DSCP value input by the user, its range from 0 to 63, the default value is 46
<b>default</b>	No network policy is configured on the port.	
<b>Mode</b>	Port mode	

---

**Usage Guide**

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

---

**Example**

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



### 5.11.13 show lldp

<b>Command</b>	<b>show lldp [interface ethernet &lt;IFNAME&gt;]</b>	
<b>parameter</b>	<b>IFNAME</b>	Port name
<b>default</b>	-	
<b>Mode</b>	Admin mode	
<b>Usage Guide</b>	Show LLDP and LLDP-MED configurations on the current port.	
<b>Example</b>	<p>Show LLDP and LLDP-MED configuration of the port 19.</p> <pre>Switch#show lldp interface ethernet 1/0/19</pre> <p>Port name :Ethernet1/0/19  LLDP Agent Adminstatus : Both  LLDP Operation TLV : default  LLDP Trap Status : disable  LLDP maxRemote :100  LLDP Overflow handle : discard  LLDP interface remote status : Free  MED Optional TLV : capabilities networkPolicy location power inventory  MED Trap Status:Enable  MED TLV Transmit Status:Disable  MED Fast Transmit Status:Disable</p>	

## 5.11.14 show lldp neighbors

<b>Command</b>	<b>show lldp neighbors [interface ethernet &lt;IFNAME&gt;]</b>
<b>parameter</b>	<b>IFNAME</b> Port number; for example :1/0/1
<b>default</b>	-
<b>Mode</b>	Admin mode
<b>Usage Guide</b>	With this command, checking LLDP and LLDP-MED information of the neighbors after the port received LLDP packets sent by the neighbors.
<b>Example</b>	<p>Show the neighbor information on port 1.</p> <pre>Switch #show lldp neighbors interface ethernet 1/0/1</pre> <p>Port name : Ethernet1/0/1  Port Remote Counter : 1  TimeMark :20  ChassisIdSubtype :4  ChassisId :00-03-0f-00-00-02  PortIdSubtype :Local  PortId :3  PortDesc :Ethernet1/0/1  SysName :switch  SysDesc :switch Device, Compiled Feb 12 17:39:53 2011  SoftWare Version 6.2.30.0  BootRom Version 4.0.1  HardWare Version  Device serial number  Copyright (C) 2001-2011 by Vendor.  All rights reserved</p>

### 5.11.15 show lldp traffic

<b>Command</b>	show lldp traffic
<b>parameter</b>	-
<b>default</b>	-
<b>Mode</b>	Admin Mode.
<b>Usage Guide</b>	After the port received the LLDP packets from the neighbor, this command can be used to view the statistics of the sent and received packets of LLDP and LLDP-MED.
<b>Example</b>	<p>View the statistics of the sent and received packets after the LLDP function is enabled.</p> <pre>Switch(config)#show lldp traffic</pre> <pre>PortName Ageouts FramesDiscarded FramesInErrors FramesIn FramesOut TLVsDiscarded TLVsUnrecognized ----- Ethernet1/0/1 0 0 0 0 7 0</pre>

## 5.12 bpdu-tunnel

### 5.12.1 bpdu-tunnel-protocol

**Command**                    bpdu-tunnel-protocol{stp| gvrp| dot1x| user-defined-protocol <name>}

**no bpdu-tunnel-protocol {stp| gvrp| dot1x| user-defined-protocol <name>}**

parameter	stp	enable bpdu-tunnel-protocol of stp function in port.
	<b>gvrp</b>	enable bpdu-tunnel-protocol of avrp function in port.
	<b>dot1x</b>	enable bpdu-tunnel-protocol of dot1x function in port.
	<b>name</b>	enable bpdu-tunnel-protocol of neme function in port, the protocol name range from 1 to 32 bytes, and it made up with character, data, underline and the head and tail character can not be underline

**default**                    -

**Mode**                      Port Mode.

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

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

## 5.12.2 bpdu-tunnel-protocol group-mac

<b>Command</b>	bpdu-tunnel-protocol {stp  gvrp  dot1x} {group-mac <mac>   default-group-mac}	
	<b>no bpdu-tunnel-protocol {stp  gvrp  dot1x}</b>	
<b>parameter</b>	<b>stp</b>	configure bpdu-tunnel-protocol mac of stp protocol;
	<b>gvrp</b>	configure bpdu-tunnel-protocol mac of gvrp protocol;
	<b>dot1x</b>	configure bpdu-tunnel-protocol mac of dot1x protocol;
	<b>mac</b>	bpdu-tunnel-protocol mac address must be multicast address and it can not be protocol saved address, namely address between 01-80-c2-00-00-00 and 01-80-c2-00-00-30;
	<b>default-group-mac</b>	the default mac address is 01-00-0c-cd-00-02.
<b>default</b>	-	
<b>Mode</b>	Global Mode.	
<b>Usage Guide</b>	This command must be configured before configure bpdu-tunnel-protocol in port.	
<b>Example</b>	Configure 01-01-00-0c -00-02 bpdu-tunnel-protocol of stp protocol. Switch(Config)# bpdu-tunnel-protocol stp group-mac 01-01-00-0c -00-02	

### 5.12.3 bpdu-tunnel-protocol protocol-mac

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

## 5.12.4 bpdu-tunnel-protocol ethernetii

<b>Command</b>	<pre>bpdu-tunnel-protocol user-defined-protocol &lt;name&gt; protocol-mac &lt;mac&gt; encape-type ethernetii protocol-type &lt;type&gt; {group-mac &lt;mac&gt;   default-group-mac} no bpdu-tunnel-protocol user-defined-protocol &lt;name&gt;</pre>	
<b>parameter</b>	<b>name</b>	it is the protocol name and the protocol name includes 1 to 32 characters, and it makes up with character, data and underline, the head and tail character can not be underline;
	<b>protocol-mac &lt;mac&gt;</b>	it is the mac address of protocol;
	<b>type</b>	the value of protocol and the format is xx-xx
	<b>group-mac &lt;mac&gt;</b>	it is the address of bpdu-tunnel-protocol mac and it must be multicast address, and it is not protocol saved address, namely the address between 01-80-c2-00-00-00 and 01-80-c2-00-00-30;
	<b>default-group-mac</b>	The default mac address is 01-00-0c-cd-00-02.
<b>default</b>	-	
<b>Mode</b>	Global Mode	
<b>Usage Guide</b>	The command must be configured before bpdu-tunnel-protocol in port.	
<b>Example</b>	<pre>Configure 01-01-00-0c-00-04 to be the bpdu-tunnel-protocol of lldp protocol. Switch(Config)# bpdu-tunnel-protocol user-defined-protocol lldp protocol-mac 01-80-c2-00-00-0e encape-type ethernetii protocol-type 88-cc group-mac 01-01-00-0c -00-04</pre>	

## 5.12.5 bpdu-tunnel-protocol snap

<b>Command</b>	<pre>bpdu-tunnel-protocol user-defined-protocol &lt;name&gt; protocol-mac &lt;mac&gt; escape-type snap {oui &lt;oui&gt;  } protocol-type &lt;type&gt; {group-mac &lt;mac&gt;   default-group-mac} no bpdu-tunnel-protocol user-defined-protocol &lt;name&gt;</pre>	
<b>parameter</b>	<b>name</b>	it is the protocol name and the protocol name includes 1 to 32 characters, and it makes up with character, data and underline, the head and tail character can not be underline
	<b>protocol-mac &lt;mac&gt;</b>	it is the mac address of protocol
	<b>oui</b>	the value of oui and the format is xx-xx-xx
	<b>type</b>	the value of protocol and the format is xx-xx
	<b>group-mac &lt;mac&gt;</b>	it is the address of bpdu-tunnel-protocol mac and it must be multicast address, and it is not protocol saved address, namely the address between 01-80-c2-00-00-00 and 01-80-c2-00-00-30
	<b>default-group-mac</b>	The default mac address is 01-00-0c-cd-00-02
<b>default</b>	-	
<b>Mode</b>	Global Mode	
<b>Usage Guide</b>	The command must be configured before bpdu-tunnel-protocol in port.	
<b>Example</b>	<pre>Configure 01-01-00-0c-00-05 to be the bpdu-tunnel-protocol of Apple Talk protocol. Switch(Config)# bpdu-tunnel-protocol user-defined-protocol lldp protocol-mac 00-03-c2-00-00-05 escape-type snap oui 08-00-07 protocol-type 80-9b group-mac 01-01-00-0c -00-05</pre>	



## 5.12.6 bpdu-tunnel-protocol llc

<b>Command</b>	<pre>bpdu-tunnel-protocol user-defined-protocol &lt;name&gt; protocol-mac &lt;mac&gt; escape-type llc dsap &lt;dsap&gt; ssap &lt;ssap&gt; {group-mac &lt;mac&gt;   default-group-mac} no bpdu-tunnel-protocol user-defined-protocol &lt;name&gt;</pre>	
<b>parameter</b>	<b>name</b>	it is the protocol name and the protocol name includes 1 to 32 characters, and it makes up with character, data and underline, the head and tail character can not be underline
	<b>protocol-mac &lt;mac&gt;</b>	it is the mac address of protocol
	<b>dsap</b>	The dsap value of protocol and it ranges from 0 to 255
	<b>ssap</b>	The ssap value of protocol and it ranges from 0 to 255;
	<b>group-mac &lt;mac&gt;</b>	it is the address of bpdu-tunnel-protocol mac and it must be multicast address, and it is not protocol saved address, namely the address between 01-80-c2-00-00-00 and 01-80-c2-00-00-30
	<b>default-group-mac</b>	The default mac address is 01-00-0c-cd-00-02
<b>default</b>	-	
<b>Mode</b>	Global Mode	
<b>Usage Guide</b>	The command must be configured before bpdu-tunnel-protocol in port.	
<b>Example</b>	<p>Configure 01-01-00-0c-00-06 to be the bpdu-tunnel-protocol of NetBIOS protocol.</p> <pre>Switch(Config)# bpdu-tunnel-protocol user-defined-protocol lldp protocol-mac 00-03-c2-00-00-06 escape-type llc dsap 240 ssap 224 group-mac 01-01-00-0c -00-06</pre>	

## 5.13 EEE Energy-saving

### 5.13.1 eee enable

---

<b>Command</b>	<b>eee enable</b> <b>no eee enable</b>
<b>parameter</b>	-
<b>default</b>	-
<b>Mode</b>	Port Mode

---

<b>Usage Guide</b>	It supports that configure EEE energy-saving function for the appointed port. There is not the EEE energy-saving function on port as default. After configuring the port to enable EEE energy-saving function, the port will enter the energy-saving state if stop to send packets to the port, the state of port is down. When sending packets to the port, the mode will changed from power saving mode to normal mode.
--------------------	---

---

<b>Example</b>	Enable EEE energy-saving function: Switch(config-if-ethernet1/0/1)#eee enable
----------------	--

## 5.14 LED shut-off

### 5.14.1 port-led shutoff time-range

<b>Command</b>	<b>port-led shutoff time-range</b> <i>&lt;time-range-name&gt;</i> <b>no port-led shutoff</b>	
<b>parameter</b>	<i>time-range-name</i>	it is the name of the time-range defined by user, it is made up by 1 to 64 characters including letters, numbers, underlines. The first and last characters cannot be the underlines
<b>default</b>	-	
<b>Mode</b>	Global Configuration Mode	
<b>Usage Guide</b>	<p>The LED shut-off function of the port can make all the LEDs off according to the configured time-range by user no matter what the link-act status is. It can save power. When there is no configured time-range, the default is all the times; when the range is exceeded, the port LED can be on according to the link-act status</p>	
<b>Example</b>	<p>Configure all the LEDs to be off in t1.</p> <pre>switch(config)#: port-led shutoff time-range t1</pre>	

# Chapter 6 MAC Address Configuration

## 6.1 MAC Address Table

### 6.1.1 clear collision-mac-address-table

<b>Syntax</b>	clear collision-mac-address-table
<b>Parameter</b>	none
<b>Default</b>	none
<b>Mode</b>	Admin Mode
<b>Usage</b>	If enable the function of the hash collision mac table that issued ffp (mac-address-table avoid-collision), the mac cannot be cleared.
<b>Example</b>	Clear the hash collision mac table. Switch#clear collision-mac-address-table

## 6.1.2 clear mac-address-table dynamic

<b>Syntax</b>	clear mac-address-table dynamic [address <mac-addr>] [vlan <vlan-id>] [interface [ethernet   portchannel] <interface-name>]						
<b>Parameter</b>	<table border="1"> <tr> <td>&lt;mac-addr&gt;</td> <td>MAC address will be deleted</td> </tr> <tr> <td>&lt;vlan-id&gt;</td> <td>Vlan id</td> </tr> <tr> <td>&lt;interface-name&gt;</td> <td>port name for forwarding the MAC packets</td> </tr> </table>	<mac-addr>	MAC address will be deleted	<vlan-id>	Vlan id	<interface-name>	port name for forwarding the MAC packets
<mac-addr>	MAC address will be deleted						
<vlan-id>	Vlan id						
<interface-name>	port name for forwarding the MAC packets						
<b>Default</b>	None						
<b>Mode</b>	Admin mode.						
<b>Usage</b>	Delete all dynamic address entries which exist in MAC address table, except application, system entries. MAC address entries can be classified according to different sources, the types are as follows: DYNAMIC, STATIC, APPLICATION, SYSTEM. DYNAMIC is the dynamic MAC address entries learned by switch, it can be aged by switch automatically.						
<b>Example</b>	<p>Delete all dynamic MAC</p> <pre>Switch#clear mac-address-table dynamic</pre>						

### 6.1.3 mac-address-learning enable | disable

<b>Syntax</b>	mac-address-learning (enable   disable) (vlan <vlan-id>   interface ethernet <interface-name>)
<b>Parameter</b>	enable Enable MAC learning through port
	disable Disable MAC learning through port
	<vlan-id> VLAN ID,range:1-4094
	<interface-name> Port name
<b>Default</b>	all port auto learning mac address
<b>Mode</b>	Global mode
<b>Usage</b>	After disabling the MAC address learning function of the port, the port will not be able to automatically learn the MAC address, and the user can manage it by statically adding the MAC address.
<b>Example</b>	Disable the MAC learning function of port 8 Switch#config Switch(config)#mac-address-learning disable interface ethernet 1/0/8

### 6.1.4 mac-address-table aging-time

---

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

---

## 6.1.5 mac-address-table static | blackhole

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



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

### 6.1.6 I2-address-table static-multicast address

<b>Syntax</b>	<p>I2-address-table static-multicast address {&lt;ip-addr&gt;  &lt;mac-addr&gt;} vlan &lt;vlan-id&gt; interface [ethernet &lt;interface-name&gt;]   port-channel &lt;port-channel-id&gt;</p> <p>no I2-address-table static-multicast (address {&lt;ip-addr&gt;  &lt;mac-addr&gt;}   vlan &lt;vlan-id&gt;) [interface (ethernet &lt;interface-name&gt;]   port-channel &lt;port-channel-id&gt;)]</p>										
<b>Parameter</b>	<table border="1"> <tr> <td>&lt;ip-addr&gt;</td> <td>IP address add or delete IP address</td> </tr> <tr> <td>&lt;mac-addr&gt;</td> <td>add or delete MAC address</td> </tr> <tr> <td>&lt;interface-name&gt;</td> <td>port that transfer MAC data packets</td> </tr> <tr> <td>&lt;port-channel-id&gt;</td> <td>aggregate port name of transfer MAC data packets</td> </tr> <tr> <td>&lt;vlan-id&gt;</td> <td>VLAN number</td> </tr> </table>	<ip-addr>	IP address add or delete IP address	<mac-addr>	add or delete MAC address	<interface-name>	port that transfer MAC data packets	<port-channel-id>	aggregate port name of transfer MAC data packets	<vlan-id>	VLAN number
<ip-addr>	IP address add or delete IP address										
<mac-addr>	add or delete MAC address										
<interface-name>	port that transfer MAC data packets										
<port-channel-id>	aggregate port name of transfer MAC data packets										
<vlan-id>	VLAN number										
<b>Default</b>	When VLAN interface is configured and is up, the system will generate a static address mapping entry of which the inherent MAC address corresponds to the VLAN number										
<b>Mode</b>	Global Mode										
<b>Usage</b>	<p>In certain special applications or when the switch is unable to dynamically learn the MAC address, users can use this command to manually establish mapping relation between the MAC address and port and VLAN.</p> <p>After configure the static multicast MAC by this command, the multicast MAC traffic will be forwarded to the specified port of the specified VLAN.</p>										
<b>Example</b>	<p>Configure a static multicast ip 232.0.0.1, the egress is ethernet 1/0/1.</p> <pre>Switch#config Switch(config)# I2-address-table static-multicast address 232.0.0.1 vlan 200 interface ethernet 1/0/1</pre>										

## 6.1.7 show collision-mac-address-table

<b>Syntax</b>	show collision-mac-address-table			
<b>Parameter</b>	None			
<b>Default</b>	None			
<b>Mode</b>	Global Mode.			
<b>Usage</b>	If enable the function of the hash collision mac table that issued ffp ( mac-address-table avoid-collision), the collision mac which issued ffp use * to sign.			
<b>Example</b>	<p>Show the hash collision mac table.</p> <pre>Switch#config Switch(config)#show collision-mac-address-table</pre> <p>The max number can be recorded is 200  The max number of collision is 0  The current number recorded is 0</p>			
	<table border="1"> <thead> <tr> <th>MAC Address</th> <th>VLAN</th> <th>Collision-count</th> </tr> </thead> </table>	MAC Address	VLAN	Collision-count
MAC Address	VLAN	Collision-count		

## 6.1.8 show mac-address-table

<b>Syntax</b>	show mac-address-table [static   blackhole   aging-time <aging-time>   count] [address <mac-addr>] [vlan <vlan-id>] [count] [interface <interface-name>]														
<b>Parameter</b>	<table border="1"> <tr> <td>static</td> <td>static entries</td> </tr> <tr> <td>blackhole</td> <td>filter entries</td> </tr> <tr> <td>&lt;aging-time&gt;</td> <td>address aging time</td> </tr> <tr> <td>count</td> <td>entry's number</td> </tr> <tr> <td>&lt;mac-addr&gt;</td> <td>entry's MAC address</td> </tr> <tr> <td>&lt;vlan-id&gt;</td> <td>entry's VLAN number</td> </tr> <tr> <td>&lt;interface-name&gt;</td> <td>entry's interface name</td> </tr> </table>	static	static entries	blackhole	filter entries	<aging-time>	address aging time	count	entry's number	<mac-addr>	entry's MAC address	<vlan-id>	entry's VLAN number	<interface-name>	entry's interface name
static	static entries														
blackhole	filter entries														
<aging-time>	address aging time														
count	entry's number														
<mac-addr>	entry's MAC address														
<vlan-id>	entry's VLAN number														
<interface-name>	entry's interface name														
<b>Default</b>	MAC address table is not displayed by default														
<b>Mode</b>	Admin and Configuration Mode.														
<b>Usage</b>	This command can display various classes of MAC address entries. Users can also use show mac-address-table to display all the MAC address entries.														
<b>Example</b>	<p>Display all the filter MAC address entries.</p> <p>Switch#show mac-address-table blackhole</p>														

## 6.1.9 show I2-address-table multicast

<b>Syntax</b>	show I2-address-table multicast ([count]   [ vlan <vlan-id>] )										
<b>Parameter</b>	<vlan-id> entry's VLAN number,range:1-4094										
<b>Default</b>	MAC address table is not displayed by default										
<b>Mode</b>	Admin and Configuration Mode.										
<b>Usage</b>	This command can display various classes of multicast address entries.										
<b>Example</b>	<p>Display all the vlan1 multicast address entries.</p> <pre>Switch#show I2-address-table multicast vlan 1</pre> <table border="1"> <thead> <tr> <th>Vlan Address</th> <th>Insert</th> <th>Type</th> <th>Creator</th> <th>Ports</th> </tr> </thead> <tbody> <tr> <td>-----</td> <td>-----</td> <td>-----</td> <td>-----</td> <td>-----</td> </tr> </tbody> </table>	Vlan Address	Insert	Type	Creator	Ports	-----	-----	-----	-----	-----
Vlan Address	Insert	Type	Creator	Ports							
-----	-----	-----	-----	-----							

## 6.1.10 clear mac-notification statistics

---

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

## 6.1.11 mac-address-table notification

<b>Syntax</b>	mac-address-table notification no mac-address-table notification
<b>Parameter</b>	none
<b>Default</b>	Disable
<b>Mode</b>	Global Mode
<b>Usage</b>	This command is used with trap switch of snmp. When disabling the MAC address notification, other configuration can be shown, but the function is invalid °
<b>Example</b>	Enable the MAC address notification. Switch#config Switch(config)#mac-address-table notification Switch(config)#

## 6.1.12 mac-address-table notification history-size

---

<b>Syntax</b>	mac-address-table notification history-size <0-500> no mac-address-table notification history-size
<b>Parameter</b>	history-size                      data length of sending the notification, its range from 1 to 500
<b>Default</b>	10
<b>Mode</b>	Global Mode
<b>Usage</b>	After the global switch is disabled, this command is also able to be configured sequentially.
<b>Example</b>	Change the maximum history-size to be 256. Switch#config Switch(config)#mac-address-table notification history-size 256

---

### 6.1.13 mac-address-table notification interval

<b>Syntax</b>	mac-address-table notification interval <1-30> no mac-address-table notification interval
<b>Parameter</b>	interval interval for sending the notification, unit is second, its range from 0 to 30 °
<b>Default</b>	30s
<b>Mode</b>	Global Mode
<b>Usage</b>	After the global switch is disabled, this command is also able to be configured sequentially.
<b>Example</b>	Configure the interval as 30s for sending the MAC address notification Switch#config Switch(config)#mac-address-table notification interval 30



## 6.1.14 mac-notification

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

## 6.1.15 show mac-notification summary

---

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

---

## 6.1.16 snmp-server enable traps mac-notification

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

# Chapter 7 VLAN Configuration

## 7.1 VLAN

### 7.1.1 vlan

<b>Syntax</b>	vlan WORD				
	no vlan				
<b>Parameter</b>	WORD	WORD is the VLAN ID to be created/deleted, valid range is 1 to 4094, connect with ',' and '-'.			
<b>Default</b>	Only VLAN1 is set by default.				
<b>Mode</b>	Global Mode				
<b>Usage</b>	VLAN1 is the default VLAN and cannot be configured or deleted by the user. The maximal VLAN number is 4094. It should be noted that dynamic VLANs learnt by GVRP cannot be deleted by this command.				
<b>Example</b>	<pre> Create VLAN100 and enter the configuration mode for VLAN 100.Display the status for the current VLAN; Switch#config Switch(config)#vlan 100 Switch#show vlan VLAN Name          Type            Media           Ports ----- 1    default          Static          ENET            Ethernet1/0/2    Ethernet1/0/3                                      Ethernet1/0/4    Ethernet1/0/5                                      Ethernet1/0/6    Ethernet1/0/7                                      Ethernet1/0/8    Ethernet1/0/9                                      Ethernet1/0/10   Ethernet1/0/11                                      Ethernet1/0/12   Ethernet1/0/13                                      Ethernet1/0/14   Ethernet1/0/15                                      Ethernet1/0/16   Ethernet1/0/17                                      Ethernet1/0/18   Ethernet1/0/19                                      Ethernet1/0/20   Ethernet1/0/21                                      Ethernet1/0/22   Ethernet1/0/23                                      Ethernet1/0/24   Ethernet1/0/25                                      Ethernet1/0/26   Ethernet1/0/27                                      Ethernet1/0/28 100  VLAN0100          Static          ENET Switch# </pre>				

## 7.1.2 name (vlan)

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

### 7.1.3 switchport interface

<b>Syntax</b>	switchport interface [ethernet   portchannel] [<interface-name   interface-list> no switchport interface [ethernet   portchannel] [<interface-name   interface-list>]																																																																						
<b>Parameter</b>	<table border="1"> <tr> <td>ethernet</td> <td>Ethernet port to be added</td> </tr> <tr> <td>portchannel</td> <td>link-aggregation port to be added</td> </tr> <tr> <td>interface-name</td> <td>port name, such as e1/0/1. If this option is selected, ethernet or portchannel should not be.</td> </tr> <tr> <td>interface-list</td> <td>port list to be added or deleted, “,” and “-” are supported, for example: ethernet1/0/1;3;4-7;8.</td> </tr> </table>	ethernet	Ethernet port to be added	portchannel	link-aggregation port to be added	interface-name	port name, such as e1/0/1. If this option is selected, ethernet or portchannel should not be.	interface-list	port list to be added or deleted, “,” and “-” are supported, for example: ethernet1/0/1;3;4-7;8.																																																														
ethernet	Ethernet port to be added																																																																						
portchannel	link-aggregation port to be added																																																																						
interface-name	port name, such as e1/0/1. If this option is selected, ethernet or portchannel should not be.																																																																						
interface-list	port list to be added or deleted, “,” and “-” are supported, for example: ethernet1/0/1;3;4-7;8.																																																																						
<b>Default</b>	A newly created VLAN contains no port by default.																																																																						
<b>Mode</b>	VLAN Mode																																																																						
<b>Usage</b>	Access ports are normal ports and can join a VLAN, but a port can only join one VLAN for a time.																																																																						
<b>Example</b>	<p>Assign Ethernet port 1 , 3 , 4-7 of VLAN100.</p> <pre>Switch#config Switch(config)#vlan 100 Switch(config-vlan100)#switchport interface ethernet 1/0/1;3;4-7</pre> <p>Set the port Ethernet1/0/1 access vlan 100 successfully  Set the port Ethernet1/0/3 access vlan 100 successfully  Set the port Ethernet1/0/4 access vlan 100 successfully  Set the port Ethernet1/0/5 access vlan 100 successfully  Set the port Ethernet1/0/6 access vlan 100 successfully  Set the port Ethernet1/0/7 access vlan 100 successfully</p> <pre>Switch#show vlan</pre> <table border="1"> <thead> <tr> <th>VLAN Name</th> <th>Type</th> <th>Media</th> <th>Ports</th> </tr> </thead> <tbody> <tr> <td>1</td> <td>default</td> <td>Static</td> <td>ENET</td> <td>Ethernet1/0/2</td> <td>Ethernet1/0/8</td> </tr> <tr> <td></td> <td></td> <td></td> <td></td> <td>Ethernet1/0/9</td> <td>Ethernet1/0/10</td> </tr> <tr> <td></td> <td></td> <td></td> <td></td> <td>Ethernet1/0/11</td> <td>Ethernet1/0/12</td> </tr> <tr> <td></td> <td></td> <td></td> <td></td> <td>Ethernet1/0/13</td> <td>Ethernet1/0/14</td> </tr> <tr> <td></td> <td></td> <td></td> <td></td> <td>Ethernet1/0/15</td> <td>Ethernet1/0/16</td> </tr> <tr> <td></td> <td></td> <td></td> <td></td> <td>Ethernet1/0/17</td> <td>Ethernet1/0/18</td> </tr> <tr> <td></td> <td></td> <td></td> <td></td> <td>Ethernet1/0/19</td> <td>Ethernet1/0/20</td> </tr> <tr> <td></td> <td></td> <td></td> <td></td> <td>Ethernet1/0/21</td> <td>Ethernet1/0/22</td> </tr> <tr> <td></td> <td></td> <td></td> <td></td> <td>Ethernet1/0/23</td> <td>Ethernet1/0/24</td> </tr> <tr> <td></td> <td></td> <td></td> <td></td> <td>Ethernet1/0/25</td> <td>Ethernet1/0/26</td> </tr> <tr> <td></td> <td></td> <td></td> <td></td> <td>Ethernet1/0/27</td> <td>Ethernet1/0/28</td> </tr> </tbody> </table>	VLAN Name	Type	Media	Ports	1	default	Static	ENET	Ethernet1/0/2	Ethernet1/0/8					Ethernet1/0/9	Ethernet1/0/10					Ethernet1/0/11	Ethernet1/0/12					Ethernet1/0/13	Ethernet1/0/14					Ethernet1/0/15	Ethernet1/0/16					Ethernet1/0/17	Ethernet1/0/18					Ethernet1/0/19	Ethernet1/0/20					Ethernet1/0/21	Ethernet1/0/22					Ethernet1/0/23	Ethernet1/0/24					Ethernet1/0/25	Ethernet1/0/26					Ethernet1/0/27	Ethernet1/0/28
VLAN Name	Type	Media	Ports																																																																				
1	default	Static	ENET	Ethernet1/0/2	Ethernet1/0/8																																																																		
				Ethernet1/0/9	Ethernet1/0/10																																																																		
				Ethernet1/0/11	Ethernet1/0/12																																																																		
				Ethernet1/0/13	Ethernet1/0/14																																																																		
				Ethernet1/0/15	Ethernet1/0/16																																																																		
				Ethernet1/0/17	Ethernet1/0/18																																																																		
				Ethernet1/0/19	Ethernet1/0/20																																																																		
				Ethernet1/0/21	Ethernet1/0/22																																																																		
				Ethernet1/0/23	Ethernet1/0/24																																																																		
				Ethernet1/0/25	Ethernet1/0/26																																																																		
				Ethernet1/0/27	Ethernet1/0/28																																																																		

---

100	VLAN0100	Static	ENET	Ethernet1/0/1	Ethernet1/0/3
				Ethernet1/0/4	Ethernet1/0/5
				Ethernet1/0/6	Ethernet1/0/7

Switch#

---

## 7.1.4 switchport forbidden vlan

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



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

---

## 7.1.5 switchport mode

<b>Syntax</b>	switchport mode ( access   hybrid   trunk   tunnel )
<b>Parameter</b>	access                      Access port.
	hybrid                      Hybrid port.
	trunk                      Trunk port.
	tunnel                      Tunnel port.
<b>Default</b>	The port is in Access mode by default.
<b>Mode</b>	Port Mode.
<b>Usage</b>	<p>Ports in trunk mode is called Trunk ports. Trunk ports can allow traffic of multiple VLANs to pass through. VLAN in different switches can be interconnected with the Trunk ports. Ports under access mode are called Access ports. An access port can be assigned to one and only one VLAN at a time. Hybrid ports can allow traffic of multiple VLANs to pass through, receive and send the packets of multiple VLANs, used to connect switch, or user's computer. When Hybrid ports and Trunk ports receive the data, the deal way is same, but the deal way is different in sending the data. Because Hybrid ports can allow the packets of multiple VLANs to send with no tag, however, Trunk ports can only allow the packets of the default VLAN to send with no tag. The attribute of ports can not directly convert between Hybrid and Trunk, it must configure to be access at first, then configure to be Hybrid or Trunk. When the Trunk or Hybrid attribute is cancelled, the port attribute restores the default (access) attribute and belongs to vlan1.</p> <p>show switchport interface display setting</p>
<b>Example</b>	<p>Set port 1 to hybrid mode.</p> <pre>Switch#config Switch(config)#interface ethernet 1/0/1 Switch(config-if-ethernet1/0/1)# switchport mode hybrid Set the port Ethernet1/0/1 mode Hybrid successfully Switch(config-if-ethernet1/0/1)#show switchport interface ethernet 1/0/1</pre> <pre>Ethernet1/0/1 Type :Universal Mode :Hybrid Port VID :1 Switch(config-if-ethernet1/0/1)#</pre>

## 7.1.6 switchport hybrid native vlan

<b>Syntax</b>	switchport hybrid native vlan <vlan-id> no switchport hybrid native vlan
<b>Parameter</b>	<vlan-id> VLAN ID (e.g. 100), PVID of Hybrid port.
<b>Default</b>	The default PVID of Hybrid port is 1.
<b>Mode</b>	Port Mode.
<b>Usage</b>	When an untagged frame enters a Hybrid port, it will be added a tag of the native PVID which is set by this command, and is forwarded to the native VLAN. show switchport interface display setting °
<b>Example</b>	Set the native vlan to 100 for a Hybrid port. Switch#config Switch(config) # interface ethernet 1/0/2 Switch(config-if-ethernet1/0/2)#switchport mode hybrid Switch(config-if-ethernet1/0/2)#switchport hybrid native vlan 100 Switch# show switchport interface ethernet 1/0/2  Ethernet1/0/2 Type :Universal Mode :Hybrid Port VID :100 Switch#

## 7.1.7 switchport hybrid allowed vlan

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

## 7.1.8 switchport access vlan

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

## 7.1.9 switchport trunk allowed vlan

<b>Syntax</b>	switchport trunk allowed vlan (WORD   all   add WORD   except WORD   remove WORD ) (tag   untag)  no switchport trunk allowed vlan
<b>Parameter</b>	WORD specified VIDs ,the range from 1 to 4094; all all VIDs add WORD add assigned VIDs behind allow vlan; except WORD all VID add to allow vlan except assigned VIDs; Remove WORD delete assigned allow vlan from allow vlan list.
<b>Default</b>	Trunk port allows all VLAN traffic by default.
<b>Mode</b>	Port Mode.
<b>Usage</b>	The user can use this command to set the VLAN traffic allowed to passthrough the Trunk port; traffic of VLANs not included are prohibited.  show switchport interface display setting.
<b>Example</b>	Set Trunk port to allow traffic of VLAN1, 3-5 Switch#config Switch(config)#interface ethernet 1/0/1 Switch(config-if-ethernet1/0/1)# switchport trunk allowed vlan 1;3-5 set the trunk port Ethernet1/0/1 allowed vlan successfully. Switch#show switchport interface ethernet 1/0/1  Ethernet1/0/1 Type :Universal Mode :Trunk Port VID :1 Trunk allowed Vlan: 1;3-5 Switch#

## 7.1.10 switchport trunk native vlan

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

## 7.1.11 switchport mode trunk allow-null

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



## 7.1.12 vlan ingress enable

<b>Syntax</b>	<pre>vlan ingress enable no vlan ingress enable</pre>
<b>Parameter</b>	none
<b>Default</b>	Enable VLAN ingress filtering function.
<b>Mode</b>	Port Mode.
<b>Usage</b>	<p>After VLAN ingress filtering is enabled on the port, when the system receives data it will check source port first, and forwards the data to the destination port if it is the VLAN member port, or else drop the data.</p> <p><u>show running-config display setting</u></p>
<b>Example</b>	<pre>Disable VLAN ingress rules on the port. Switch#config Switch(config)#interface ethernet 1/0/1 Switch(config-if-ethernet1/0/1)# no vlan ingress enable Switch# show running-config ! no service password-encryption ! hostname Switch sysLocation Default sysContact Default ! username admin privilege 15 password 0 admin ! authentication line console login local ! snmp-server enable ! ! vlan 1 ! Interface Ethernet1/0/1     no vlan ingress enable ! Interface Ethernet1/0/2 Switch#</pre>

### 7.1.13 vlan-translation enable

---

<b>Syntax</b>	vlan-translation enable no vlan-translation enable
---------------	---

---

<b>Parameter</b>	none
------------------	------

---

<b>Default</b>	VLAN translation has not been enabled on the port by default.
----------------	---

---

<b>Mode</b>	Port Mode.
-------------	------------

---

<b>Usage</b>	vlan-translation and dot1q-tunnel are mutually exclusive, it is recommended to enable vlan-translation on trunk port and manually disable port filtering.  show vlan-translation display setting
--------------	--

---

<b>Example</b>	Enable VLAN translation function on port1.  Switch#config Switch(config)#interface ethernet 1/0/1 Switch(config-if-ethernet1/0/1)# vlan-translation enable Switch# show vlan-translation Interface Ethernet1/0/1: vlan-translation is enable, miss drop is not set  Switch#
----------------	--

---

## 7.1.14 vlan-translation

<b>Syntax</b>	<pre>vlan-translation &lt;old-valn-id&gt; to &lt;new-vlan-id&gt; {in   out} no vlan-translation &lt;old-valn-id&gt; {in   out}</pre>								
<b>Parameter</b>	<table border="1"> <tr> <td>old-valn-id</td> <td>original VLAN ID</td> </tr> <tr> <td>new-vlan-id</td> <td>translated VLAN ID</td> </tr> <tr> <td>in</td> <td>ingress translation</td> </tr> <tr> <td>out</td> <td>outgress translation.</td> </tr> </table>	old-valn-id	original VLAN ID	new-vlan-id	translated VLAN ID	in	ingress translation	out	outgress translation.
old-valn-id	original VLAN ID								
new-vlan-id	translated VLAN ID								
in	ingress translation								
out	outgress translation.								
<b>Default</b>	There is no VLAN translation relation.								
<b>Mode</b>	Port Mode.								
<b>Usage</b>	<p>The command is for configuring the translation relation of the VLAN translation function. The data packets will be matched according to the configured translation relations, and its VLAN ID will be changed to the one in the configured item once matched, while forward the packets of the original VLAN if not match. This command cannot be used with dot1q-tunnel enable at the same time.</p> <p><code>show vlan-translation display setting</code></p>								
<b>Example</b>	<pre>Move the VLAN100 data entered from the port1 to VLAN2 after ingress translation. Switch#config Switch(config)#interface ethernet 1/0/1 Switch(config-if-ethernet1/0/1)# vlan-translation enable Switch(config-if-ethernet1/0/1)#vlan-translation 100 to 2 in Switch# show vlan-translation Interface Ethernet1/0/1:     vlan-translation is enable, miss drop is not set     vlan-translation 100 to 2 in Switch#</pre>								

## 7.1.15 vlan-translation miss drop

<b>Syntax</b>	<pre>vlan-translation miss drop {in out both} no vlan-translation miss drop {in out both}</pre>						
<b>Parameter</b>	<table border="1"> <tr> <td>in</td> <td>entrance</td> </tr> <tr> <td>out</td> <td>export</td> </tr> <tr> <td>both</td> <td>two-way</td> </tr> </table>	in	entrance	out	export	both	two-way
in	entrance						
out	export						
both	two-way						
<b>Default</b>	Not miss drop when translation failed.						
<b>Mode</b>	Port Mode.						
<b>Usage</b>	<p>During translate the mapping relation between original VID and present VID, if not configure related translation, the default is not packets miss. After using the command, it will miss data packets when translation failed.</p> <p><code>show vlan-translation display setting</code></p>						
<b>Example</b>	<pre>set port 1 translation failed and miss packets in entrance. Switch#config Switch(config)#interface ethernet 1/0/1 Switch(config-if-ethernet1/0/1)# vlan-translation enable Switch(config-if-ethernet1/0/1)#vlan-translation miss drop in Switch# show vlan-translation Interface Ethernet1/0/1:     vlan-translation is enable, miss drop is set in  Switch#</pre>						

## 7.1.16 dot1q-tunnel enable

<b>Syntax</b>	dot1q-tunnel enable no dot1q-tunnel enable
<b>Parameter</b>	none
<b>Default</b>	Dot1q-tunnel function disabled on the port by default.
<b>Mode</b>	Port Mode.
<b>Usage</b>	<p>After enabling dot1q-tunnel on the port, data packets without VLAN tag (referred to as tag) will be packed with a tag when entering through the port; those with tag will be packed with an external tag. The TPID in the tag is the global configuration TPID. its default value is 0x8100, and the VLAN ID is the VLAN ID the port belongs to. Data packets with double tags will be forwarded according to MAC address and external tag, till the external tag is removed when transmitted outside from the access port. Since the length of the data packet may be over sized when packed with external tag, it is recommended to use this command associating the Jumbo function. Normally this command is used on access ports. This command can not be used when vlan-translation enabled.</p> <p><code>show dot1q-tunnel display setting</code></p>
<b>Example</b>	<p>Join port1 into VLAN3, enable dot1q-tunnel function.</p> <pre>Switch#config Switch(config)#vlan 3 Switch(config-vlan3)#switchport interface ethernet 1/0/1 Switch(config-vlan3)#exit Switch(config)#interface ethernet 1/0/1 Switch(config-if-ethernet1/0/1)# dot1q-tunnel enable Switch# show dot1q-tunnel Interface Ethernet1/0/1: dot1q-tunnel is enable  Switch#</pre>

## 7.1.17 dot1q-tunnel selective enable

<b>Syntax</b>	dot1q-tunnel selective enable no dot1q-tunnel selective enable
<b>Parameter</b>	none
<b>Default</b>	Do not enable selective QinQ.
<b>Mode</b>	Port mode
<b>Usage</b>	Enable selective QinQ command should associates with hybrid mode, and it should not be used with dot1q-tunnel enable synchronously.  show running-config display setting
<b>Example</b>	Enable dot1q-tunnel selective enable of port1.  Switch#config Switch(config)#interface ethernet 1/0/1 Switch(config-if-ethernet1/0/1)# dot1q-tunnel selective enable Switch# show running-config no service password-encryption hostname Switch sysLocation Default sysContact Default ! username admin privilege 15 password 0 admin ! authentication line console login local ! snmp-server enable ! vlan 1;3 ! Interface Ethernet1/0/1 dot1q-tunnel selective enable ! Interface Ethernet1/0/2 ! Interface Ethernet1/0/3 ! Switch#

## 7.1.18 dot1q-tunnel selective s-vlan

<b>Syntax</b>	dot1q-tunnel selective s-vlan <s-vlan> c-vlan <c-vid-list> no dot1q-tunnel selective s-vlan <s-vlan> c-vlan <c-vid-list>
<b>Parameter</b>	<s-vlan> SP VLAN ID <c-vid-list> range of user's VLAN ID.
<b>Default</b>	There is no mapping relation.
<b>Mode</b>	Port mode
<b>Usage</b>	This command is used to configure the mapping relation for selective QinQ. If packets match the mapping relation, they will be tagged with SP vlan tag as the outer VLAN tag.  show running-config display setting
<b>Example</b>	<p>Packets of VLAN 3 through VLAN 5 are tagged with the tag of VLAN 1 as the outer VLAN tag on Ethernet1/0/1.</p> <pre> Switch#config Switch(config)#interface ethernet 1/0/1 Switch(config-if-ethernet1/0/1)# dot1q-tunnel selective s-vlan 1 c-vlan 3-5 Switch(config-if-Ethernet1/0/1)# dot1q-tunnel selective enable Switch# show running-config ! no service password-encryption ! hostname Switch sysLocation Default sysContact Default username admin privilege 15 password 0 admin authentication line console login local snmp-server enable vlan 1,3 Interface Ethernet1/0/1 dot1q-tunnel selective s-vlan 1 c-vlan 3-5 dot1q-tunnel selective enable Interface Ethernet1/0/2 Interface Ethernet1/0/3 Interface Ethernet1/0/4 Interface Ethernet1/0/5 Interface Ethernet1/0/6 Switch# </pre>

## 7.1.19 garp timer join

<b>Syntax</b>	garp timer join <200-500>	
<b>Parameter</b>	<200-500>	millisecond
<b>Default</b>	200 ms	
<b>Mode</b>	Global mode	
<b>Usage</b>	<p>Check whether the value satisfy the range. If so, modify the value of garp timer to the specified value, otherwise return a configuration error.</p> <p><u>show garp timer display setting</u></p>	
<b>Example</b>	<p>Set the value of garp join timer as 210ms.</p> <pre>Switch#config Switch(config)# garp timer join 210 Switch#show garp timer GARP join timer value is : 210 (ms) GARP leave timer value is : 600 (ms) GARP leaveall timer value is : 10000 (ms)</pre> <p><u>Switch#</u></p>	



## 7.1.20 garp timer leave

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

## 7.1.21 garp timer leaveall

<b>Syntax</b>	garp timer leaveall <5000-60000>	
<b>Parameter</b>	<500-60000>	millisecond
<b>Default</b>	10000ms	
<b>Mode</b>	Global mode	
<b>Usage</b>	<p>Check whether the value satisfy the range. If so, modify the value of garp leaveAll timer to the specified value, otherwise return a configuration error.</p> <p><code>show garp timer display setting</code></p>	
<b>Example</b>	<p>Set the value of garp leaveAll as 20000ms.</p> <pre>Switch#config Switch(config)#garp time leaveall 20000 Switch(config)#show garp timer GARP join timer value is : 210 (ms) GARP leave timer value is : 700 (ms) GARP leaveall timer value is : 20000 (ms)</pre> <p><code>Switch#</code></p>	

## 7.1.22 no garp timer

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

### 7.1.23 gvrp(Global)

<b>Syntax</b>	gvrp no gvrp
<b>Parameter</b>	none
<b>Default</b>	Disabled.
<b>Mode</b>	Global mode
<b>Usage</b>	Enable GVRP function globally and only in this way GVRP module can work normally. show running-config display setting
<b>Example</b>	<pre> Enable GVRP function globally. Switch#config Switch(config)#gvrp Switch(config)#show running-config ! no service password-encryption ! hostname Switch sysLocation Default sysContact Default ! username admin privilege 15 password 0 admin ! authentication line console login local ! snmp-server enable ! !! vlan 1 ! gvrp ! Interface Ethernet1/0/1 Switch# </pre>

## 7.1.24 gvrp(Port)

<b>Syntax</b>	gvrp no gvrp
<b>Parameter</b>	none
<b>Default</b>	Disabled
<b>Mode</b>	Port mode
<b>Usage</b>	GVRP function can only be enabled on trunk and hybrid ports, and enabling GVRP will return an error on access port. After GVRP enabled on port, this port will be added to GVRP (i.e. adding corresponding state machine to GVRP of the port). <u>show gvrp port-member display setting</u>
<b>Example</b>	Enable GVRP of port. Switch#config Switch(config)# interface ethernet 1/0/1 Switch(config-if-ethernet1/0/1)#switchport mode hybrid Set the port Ethernet1/0/1 mode Hybrid successfully Switch(config-if-ethernet1/0/1)#gvrp Switch#show gvrp port-member Ports which were enabled gvrp included: Ethernet1/0/1 Switch#

## 7.1.25 private-vlan

<b>Syntax</b>	private-vlan {primary   isolated   community} no private-vlan												
<b>Parameter</b>	primary set current VLAN to Primary VLAN isolated set current VLAN to Isolated VLAN community set current VLAN to Community VLAN												
<b>Default</b>	Private VLAN is not configured by default.												
<b>Mode</b>	VLAN mode												
<b>Usage</b>	<p>There are three Private VLANs: Primary VLAN, Isolated VLAN and Community VLAN. Ports in Primary there are three Private VLANs: Primary VLAN, Isolated VLAN and Community VLAN can communicate with ports of Isolated VLAN and Community VLAN related to this Primary VLAN; Ports in Isolated VLAN are isolated between each other and only communicate with ports in Primary VLAN they related to; ports in Community VLAN can communicate both with each other and with Primary VLAN ports they related to; there is no communication between ports in Community VLAN and port in Isolated VLAN.</p> <p>Only VLANs containing empty Ethernet ports can be set to Private VLAN, and only the Private VLANs configured with associated private relationships can set the Access Ethernet ports their member ports. Normal VLAN will clear its Ethernet ports when set to Private VLAN.</p> <p>It is to be noted Private VLAN messages will not be transmitted by GVRP.</p> <p>show vlan private-vlan display setting</p>												
<b>Example</b>	<p>Set VLAN100, 200, 300 to private vlans, with respectively primary, Isolated, Community types.</p> <pre>Switch#config Switch(config)#vlan 100;200;300 Switch(config)#vlan 100 Switch(config-vlan100)#private-vlan primary Note:This will remove all the access ports from vlan 100 Switch(config-vlan100)#vlan 200 Switch(config-vlan200)#private-vlan isolated Note:This will remove all the access ports from vlan 200 Switch(config-vlan200)#vlan 300 Switch(config-vlan300)#private-vlan community Note:This will remove all the access ports from vlan 300 Switch# show vlan private-vlan</pre> <table border="1"> <thead> <tr> <th>VLAN Name</th> <th>Type</th> <th>Asso VLAN Ports</th> </tr> </thead> <tbody> <tr> <td>100 VLAN0100</td> <td>Primary</td> <td></td> </tr> <tr> <td>200 VLAN0200</td> <td>Isolate</td> <td></td> </tr> <tr> <td>300 VLAN0300</td> <td>Community</td> <td></td> </tr> </tbody> </table> <p>Switch#</p>	VLAN Name	Type	Asso VLAN Ports	100 VLAN0100	Primary		200 VLAN0200	Isolate		300 VLAN0300	Community	
VLAN Name	Type	Asso VLAN Ports											
100 VLAN0100	Primary												
200 VLAN0200	Isolate												
300 VLAN0300	Community												

## 7.1.26 private-vlan association

<b>Syntax</b>	private-vlan association <secondary-vlan-list> no private-vlan association												
<b>Parameter</b>	<secondary-vlan-list> Sets Secondary VLAN list which is associated to Primary VLAN. There are two types of Secondary VLAN: Isolated VLAN and Community VLAN. Users can set multiple Secondary VLANs by ','.												
<b>Default</b>	There is no Private VLAN association by default.												
<b>Mode</b>	VLAN Mode.												
<b>Usage</b>	<p>This command can only used for Private VLAN. The ports in Secondary VLANs which are associated to Primary VLAN can communicate to the ports in Primary VLAN.</p> <p>Before setting Private VLAN association, three types of Private VLANs should have no member ports; the Private VLAN with Private VLAN association can't be deleted. When users delete Private VLAN association, all the member ports in the Private VLANs whose association is deleted are removed from the Private VLANs.</p> <p>show vlan private-vlan display setting</p>												
<b>Example</b>	<p>Associate Isolated VLAN200 and Community VLAN300 to Primary VLAN100.</p> <pre>Switch#config Switch(config)# vlan 100 Switch(config-vlan100)#private-vlan association 200;300 Set vlan 100 associated vlan successfully Switch(config-vlan100)#show vlan private-vlan</pre> <table border="1"> <thead> <tr> <th>VLAN Name</th> <th>Type</th> <th>Asso VLAN Ports</th> </tr> </thead> <tbody> <tr> <td>100 VLAN0100</td> <td>Primary</td> <td>200 300</td> </tr> <tr> <td>200 VLAN0200</td> <td>Isolate</td> <td>100</td> </tr> <tr> <td>300 VLAN0300</td> <td>Community</td> <td>100</td> </tr> </tbody> </table> <pre>Switch#</pre>	VLAN Name	Type	Asso VLAN Ports	100 VLAN0100	Primary	200 300	200 VLAN0200	Isolate	100	300 VLAN0300	Community	100
VLAN Name	Type	Asso VLAN Ports											
100 VLAN0100	Primary	200 300											
200 VLAN0200	Isolate	100											
300 VLAN0300	Community	100											

## 7.1.27 show dot1q-tunnel

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



## 7.1.28 show garp timer

<b>Syntax</b>	Show garp timer [join   leave   leaveall ]						
<b>Parameter</b>	<table border="1"> <tr> <td>join</td> <td>join timer</td> </tr> <tr> <td>leave</td> <td>leave timer</td> </tr> <tr> <td>leaveall</td> <td>leaveAll timer</td> </tr> </table>	join	join timer	leave	leave timer	leaveall	leaveAll timer
join	join timer						
leave	leave timer						
leaveall	leaveAll timer						
<b>Default</b>	200 600 10000 milliseconds for join   leave   leaveAll timer respectively.						
<b>Mode</b>	Admin mode						
<b>Usage</b>	Show the corresponding value of the timer specified in the command.						
<b>Example</b>	<p>Show the value of all garp timers currently.</p> <pre>Switch# show garp timer GARP join timer value is : 200 (ms) GARP leave timer value is : 600 (ms) GARP leaveall timer value is : 10000 (ms)</pre> <p>Switch#</p>						

### 7.1.29 show gvrp fsm information

<b>Syntax</b>	show gvrp fsm information interface (ethernet   port-channel   IFNAME)								
<b>Parameter</b>	ethernet                      physical port								
	port-channel                  aggregate port								
	IFNAME                         port name								
<b>Default</b>	MT for registered machine and VO for request state machine.								
<b>Mode</b>	Admin mode								
<b>Usage</b>	Show the corresponding state of all registered machines and request state machines.								
<b>Example</b>	Show the state of all state machines.								
	Switch# show gvrp fsm information interface ethernet 1/0/1								
	<p>VA:Very anxious Active member, AA:Anxious Active member, QA:Quiet Active member          VP:Very anxious Passive member, AP:Anxious Passive member, QP:Quiet Passive member          VO:Very anxious Observer, AO:Anxious Observer, QO:Quiet Observer          LA:Leaving Active member, LO:leaving Observer          IN:In, LV:Leaving, MT:Empty          INR:In Registration fixed, LVR:Leaving Registration fixed, MTR:Empty Registration fixed          INF:In, registration forbidden, LVF:Leaving, registration forbidden, MTF:Empty, registration forbidden</p> <p>Ethernet1/0/1 gvrp fsm information:</p> <table border="1"> <thead> <tr> <th>Index</th> <th>VLANID</th> <th>Applicant</th> <th>Registrar</th> </tr> </thead> <tbody> <tr> <td>1</td> <td>1</td> <td>Qa</td> <td>MT</td> </tr> </tbody> </table> <p>Switch#</p>	Index	VLANID	Applicant	Registrar	1	1	Qa	MT
Index	VLANID	Applicant	Registrar						
1	1	Qa	MT						

### 7.1.30 show gvrp leaveAll fsm information

<b>Syntax</b>	show gvrp leaveAll fsm information interface (ethernet   port-channel   IFNAME)
<b>Parameter</b>	ethernet                      physical port
	port-channel                      aggregate port
	IFNAME                      port name
<b>Default</b>	Passive
<b>Mode</b>	Admin mode
<b>Usage</b>	Check the state of leaveAll state machine
<b>Example</b>	Show the state of leaveAll state machine on port.
	Switch# show gvrp fsm information interface ethernet 1/0/1
	Interface                      LeaveAll fsm
	-----                      -----
	Ethernet1/0/1                      Passive
Switch#	

### 7.1.31 show gvrp leavetimer running information

<b>Syntax</b>	show gvrp leavetimer running information [vlan <1-4094> ]interface (ethernet   port-channel   IFNAME)									
<b>Parameter</b>	<table border="1"> <tr> <td>&lt;1-4094&gt;</td> <td>Vlan tag</td> </tr> <tr> <td>ethernet</td> <td>physical port</td> </tr> <tr> <td>port-channel</td> <td>aggregate port</td> </tr> <tr> <td>IFNAME</td> <td>port name</td> </tr> </table>	<1-4094>	Vlan tag	ethernet	physical port	port-channel	aggregate port	IFNAME	port name	
<1-4094>	Vlan tag									
ethernet	physical port									
port-channel	aggregate port									
IFNAME	port name									
<b>Default</b>	leavetimer is disabled.									
<b>Mode</b>	Admin mode									
<b>Usage</b>	Show running state and expiration time of each leave timer.									
<b>Example</b>	<p>Show running state and expiration time of each leave timer on current port.</p> <pre>Switch# show gvrp leavetimer running information interface ethernet 1/0/1</pre> <table border="1"> <thead> <tr> <th>VLANID</th> <th>running state</th> <th>expired time</th> </tr> <tr> <th>----</th> <th>-----</th> <th>-----</th> </tr> </thead> <tbody> <tr> <td>Switch#</td> <td></td> <td></td> </tr> </tbody> </table>	VLANID	running state	expired time	----	-----	-----	Switch#		
VLANID	running state	expired time								
----	-----	-----								
Switch#										

### 7.1.32 show gvrp port-member

---

<b>Syntax</b>	show gvrp [active  ] port-member
<b>Parameter</b>	active port is in active state
<b>Default</b>	GVRP is disabled on port.

---

<b>Mode</b>	Admin mode
<b>Usage</b>	Show all ports (enable GVRP) saved in GVRP.
<b>Example</b>	Show all ports with GVRP enabled. Switch#show gvrp port-member Ports which were enabled gvrp included: Ethernet1/0/1 Switch#

---

### 7.1.33 show gvrp port registerd vlan

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

## 7.1.34 show gvrp timer running information

---

<b>Syntax</b>	show gvrp timer (join   leaveall) running information interface (ethernet   port-channel   IFNAME)
<b>Parameter</b>	join                                join timer
	leaveall                            leaveAll timer
	Ethernet                            physical port
	port-channel                        aggregate port
	port IFNAME                        port name
<b>Default</b>	Join timer is disabled and leaveAll timer is enabled
<b>Mode</b>	Admin mode
<b>Usage</b>	Check running state of join leaveAll timer on port.
<b>Example</b>	Show running state and expiration time of each timer.
	Switch#show gvrp timer join running information interface ethernet 1/0/1
	Current port's jointimer running state is: UP
	Current port's jointimer expired time is: 0.2 s
	Switch#

---

### 7.1.35 show gvrp vlan registerd port

---

<b>Syntax</b>	show gvrp vlan <1-4094> registerd port
<b>Parameter</b>	<1-4094>                                  Vlan tag
<b>Default</b>	No ports with specified VLAN registered.

---

<b>Mode</b>	admin mode
<b>Usage</b>	none

---

<b>Example</b>	Show all ports with current VLAN registered. Switch#show gvrp vlan 100 registerd port Ethernet1/0/3 (T) Ethernet1/0/4 (T) Ethernet1/0/5 (T) Ethernet1/0/6 (T) Ethernet1/0/7 (T) Ethernet1/0/8 (T) Ethernet1/0/9 (T) Ethernet1/0/10 (T) Switch#
----------------	--

---



## 7.1.36 show vlan

<b>Syntax</b>	show vlan [brief   summary] [id <vlan-id>] [name <vlan-name>] [internal usage [id <vlan-id>   name <vlan-name>]]									
<b>Parameter</b>	<table border="1"> <tr> <td>brief</td> <td>brief information;</td> </tr> <tr> <td>summary</td> <td>VLAN statistics</td> </tr> <tr> <td>&lt;vlan-id&gt;</td> <td>for VLAN ID of the VLAN to display status information, the valid range is 1 to 4094;</td> </tr> <tr> <td>&lt;vlan-name&gt;</td> <td>is the VLAN name for the VLAN to display status information, valid length is 1 to 11 characters.</td> </tr> </table>	brief	brief information;	summary	VLAN statistics	<vlan-id>	for VLAN ID of the VLAN to display status information, the valid range is 1 to 4094;	<vlan-name>	is the VLAN name for the VLAN to display status information, valid length is 1 to 11 characters.	
brief	brief information;									
summary	VLAN statistics									
<vlan-id>	for VLAN ID of the VLAN to display status information, the valid range is 1 to 4094;									
<vlan-name>	is the VLAN name for the VLAN to display status information, valid length is 1 to 11 characters.									
<b>Default</b>	none									
<b>Mode</b>	Admin Mode and Configuration Mode.									
<b>Usage</b>	If no <vlan-id> or <vlan-name> is specified, then information for all VLANs in the switch will be displayed.									
<b>Example</b>	<p>Display the status for the current VLAN; display statistics for the current VLAN.</p> <pre>Switch#show vlan</pre> <table border="1"> <thead> <tr> <th>VLAN Name</th> <th>Type</th> <th>Media</th> <th>Ports</th> </tr> </thead> <tbody> <tr> <td>1</td> <td>default</td> <td>Static</td> <td>ENET</td> <td>Ethernet1/0/2 Ethernet1/0/3 Ethernet1/0/4 Ethernet1/0/5 Ethernet1/0/6 Ethernet1/0/7 Ethernet1/0/8 Ethernet1/0/9 Ethernet1/0/10 Ethernet1/0/11 Ethernet1/0/12 Ethernet1/0/13 Ethernet1/0/14 Ethernet1/0/15 Ethernet1/0/16 Ethernet1/0/17 Ethernet1/0/18 Ethernet1/0/19 Ethernet1/0/20 Ethernet1/0/21 Ethernet1/0/22 Ethernet1/0/23 Ethernet1/0/24 Ethernet1/0/25 Ethernet1/0/26 Ethernet1/0/27 Ethernet1/0/28</td> </tr> </tbody> </table> <pre>Switch#show vlan summary</pre> <p>The max. Vlan entries: 4094</p> <p>Existing Vlan: Universal Vlan: 1 Private Vlan:</p>	VLAN Name	Type	Media	Ports	1	default	Static	ENET	Ethernet1/0/2 Ethernet1/0/3 Ethernet1/0/4 Ethernet1/0/5 Ethernet1/0/6 Ethernet1/0/7 Ethernet1/0/8 Ethernet1/0/9 Ethernet1/0/10 Ethernet1/0/11 Ethernet1/0/12 Ethernet1/0/13 Ethernet1/0/14 Ethernet1/0/15 Ethernet1/0/16 Ethernet1/0/17 Ethernet1/0/18 Ethernet1/0/19 Ethernet1/0/20 Ethernet1/0/21 Ethernet1/0/22 Ethernet1/0/23 Ethernet1/0/24 Ethernet1/0/25 Ethernet1/0/26 Ethernet1/0/27 Ethernet1/0/28
VLAN Name	Type	Media	Ports							
1	default	Static	ENET	Ethernet1/0/2 Ethernet1/0/3 Ethernet1/0/4 Ethernet1/0/5 Ethernet1/0/6 Ethernet1/0/7 Ethernet1/0/8 Ethernet1/0/9 Ethernet1/0/10 Ethernet1/0/11 Ethernet1/0/12 Ethernet1/0/13 Ethernet1/0/14 Ethernet1/0/15 Ethernet1/0/16 Ethernet1/0/17 Ethernet1/0/18 Ethernet1/0/19 Ethernet1/0/20 Ethernet1/0/21 Ethernet1/0/22 Ethernet1/0/23 Ethernet1/0/24 Ethernet1/0/25 Ethernet1/0/26 Ethernet1/0/27 Ethernet1/0/28						

---

100 200 300

Total Existing Vlan:4

Switch#

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

---

## 7.1.37 show vlan-translation

---

<b>Syntax</b>	show vlan-translation
<b>Parameter</b>	None
<b>Default</b>	none

---

<b>Mode</b>	Admin and Configuration Mode.
<b>Usage</b>	Display the information of all the ports at VLAN-translation state.
<b>Example</b>	Display current VLAN translation state information. Switch#show vlan-translation Interface Ethernet1/0/1: vlan-translation is enable, miss drop is not set

---

## 7.1.38 vlan-translation n-to-1

<b>Syntax</b>	<pre> vlan-translation n-to-1 &lt;WORD&gt; to &lt;new-vlan-id&gt; no vlan-translation n-to-1 &lt;WORD&gt; </pre>
<b>Parameter</b>	<p>&lt;WORD&gt; original VLAN ID, its range from 1 to 4094, connect them with ',' and '-'. If there are two VLANs with different range are translated into different VLAN ID in the same port, two VLAN ranges should not be superposed.</p> <hr/> <p>&lt;new-vlan-id&gt; translated VLAN ID, its range from 1 to 4094.</p>
<b>Default</b>	Disable
<b>Mode</b>	Port mode
<b>Usage</b>	<p>Multi-to-One VLAN translation is used to network edge to map multiple VLANs to one VLAN of backbone network. When data traffic returns from backbone network to network edge, it will restore VLAN of network edge to implement Multi-to-One VLAN translation and save VLAN resource of backbone network. Note: When using this function, the device must establish the original and the translated VLAN firstly, and enabling the downlink port of this function and the uplink port for connecting backbone network, which must be join in the original and the translated VLAN with tagged mode. This function should not be used with dot1q-tunnel and VLAN translation at the same time Note: Multi-to-One VLAN translation should be enabled after MAC learning.</p> <p>show vlan-translation n-to-1 display setting ◦</p>
<b>Example</b>	<p>On Ethernet 1/0/1, translate the data traffic from VLAN with the range between 1 to 5 into VLAN 100, and translate the data traffic (belongs to VLAN with the range between 1 to 5) out from VLAN100 into the corresponding VLAN ID, connect the uplink port of the backbone network as Ethernet 1/0/5.</p> <pre> Switch#config Switch(config)#vlan 1;5;100 Switch(config)#vlan 2-4 Switch(config)#interface ethernet 1/0/1 Switch(config-if-ethernet1/0/1)#switchport mode trunk Set the port Ethernet1/0/1 mode Trunk successfully Switch(config-if-ethernet1/0/1)#vlan-translation n-to-1 1-5 to 100 Switch(config-if-ethernet1/0/1)#interface ethernet 1/0/5 Switch(config-if-ethernet1/0/5)#switchport mode trunk Set the port Ethernet1/0/5 mode Trunk successfully Switch#show vlan-translation n-to-1 Ethernet1/0/1: vlan-translation n-to-1 enable vlan-translation n-to-1 1-5 to 100 </pre>

### 7.1.39 show vlan-translation n-to-1

---

<b>Syntax</b>	show vlan-translation n-to-1 <interface-name>
<b>Parameter</b>	<interface-name> Specify the name of the port which will be shown. If there is no parameter, show all port configurations with this function.
<b>Default</b>	There is no Multi-to-One VLAN translation information.
<b>Mode</b>	Admin mode.
<b>Usage</b>	If appointed vlan when show, it will display the n-to-1 translation of specified vlan, if not appointed vlan, it will display all n-to-1 information.
<b>Example</b>	Show all port configurations with Multi-to-One VLAN translation function. Switch#show vlan-translation n-to-1 Ethernet1/0/1: vlan-translation n-to-1 enable vlan-translation n-to-1 1-5 to 100

---

## 7.1.40 dynamic-vlan mac-vlan prefer

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

## 7.1.41 dynamic-vlan subnet-vlan prefer

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

## 7.1.42 mac-vlan vlan

<b>Syntax</b>	<pre>mac-vlan vlan &lt;vlan-id&gt; no mac-vlan vlan &lt;vlan-id&gt;</pre>																		
<b>Parameter</b>	<vlan-id>	<vlan-id> is the number of the specified VLAN.																	
<b>Default</b>	No MAC VLAN is configured by default.																		
<b>Mode</b>	Global Mode.																		
<b>Usage</b>	<pre>Set specified VLAN for MAC VLAN. show mac-vlan display setting.</pre>																		
<b>Example</b>	<pre>Set VLAN100 to MAC VLAN. Switch#config Switch(config)#mac-vlan vlan 100 Switch#show vlan</pre> <table border="1"> <thead> <tr> <th>VLAN Name</th> <th>Type</th> <th>Media</th> <th>Ports</th> </tr> </thead> <tbody> <tr> <td>1</td> <td>default</td> <td>Static</td> <td>ENET</td> <td>Ethernet1/0/1 Ethernet1/0/2 Ethernet1/0/3 Ethernet1/0/4 Ethernet1/0/5 Ethernet1/0/6 Ethernet1/0/7 Ethernet1/0/8 Ethernet1/0/9 Ethernet1/0/10 Ethernet1/0/11 Ethernet1/0/12 Ethernet1/0/13 Ethernet1/0/14 Ethernet1/0/15 Ethernet1/0/16 Ethernet1/0/17 Ethernet1/0/18 Ethernet1/0/19 Ethernet1/0/20 Ethernet1/0/21 Ethernet1/0/22 Ethernet1/0/23 Ethernet1/0/24 Ethernet1/0/25 Ethernet1/0/26 Ethernet1/0/27 Ethernet1/0/28</td> </tr> <tr> <td>100</td> <td>VLAN0100</td> <td>UserDynam</td> <td>ENET</td> <td></td> </tr> </tbody> </table>					VLAN Name	Type	Media	Ports	1	default	Static	ENET	Ethernet1/0/1 Ethernet1/0/2 Ethernet1/0/3 Ethernet1/0/4 Ethernet1/0/5 Ethernet1/0/6 Ethernet1/0/7 Ethernet1/0/8 Ethernet1/0/9 Ethernet1/0/10 Ethernet1/0/11 Ethernet1/0/12 Ethernet1/0/13 Ethernet1/0/14 Ethernet1/0/15 Ethernet1/0/16 Ethernet1/0/17 Ethernet1/0/18 Ethernet1/0/19 Ethernet1/0/20 Ethernet1/0/21 Ethernet1/0/22 Ethernet1/0/23 Ethernet1/0/24 Ethernet1/0/25 Ethernet1/0/26 Ethernet1/0/27 Ethernet1/0/28	100	VLAN0100	UserDynam	ENET	
VLAN Name	Type	Media	Ports																
1	default	Static	ENET	Ethernet1/0/1 Ethernet1/0/2 Ethernet1/0/3 Ethernet1/0/4 Ethernet1/0/5 Ethernet1/0/6 Ethernet1/0/7 Ethernet1/0/8 Ethernet1/0/9 Ethernet1/0/10 Ethernet1/0/11 Ethernet1/0/12 Ethernet1/0/13 Ethernet1/0/14 Ethernet1/0/15 Ethernet1/0/16 Ethernet1/0/17 Ethernet1/0/18 Ethernet1/0/19 Ethernet1/0/20 Ethernet1/0/21 Ethernet1/0/22 Ethernet1/0/23 Ethernet1/0/24 Ethernet1/0/25 Ethernet1/0/26 Ethernet1/0/27 Ethernet1/0/28															
100	VLAN0100	UserDynam	ENET																



## 7.1.43 mac-vlan

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

## 7.1.44 protocol-vlan

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

## 7.1.45 show dynamic-vlan prefer

---

<b>Syntax</b>	show dynamic-vlan prefer
<b>Parameter</b>	None
<b>Default</b>	Mac Vlan/Voice Vlan

---

<b>Mode</b>	Admin Mode and Configuration Mode.
<b>Usage</b>	Display the dynamic VLAN preference.
<b>Example</b>	Display current dynamic VLAN preference. Switch#show dynamic-vlan prefer Mac Vlan/Voice Vlan IP Subnet Vlan Protocol Vlan

---

## 7.1.46 show mac-vlan interface

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

## 7.1.47 show protocol-vlan

<b>Syntax</b>	show protocol-vlan																		
<b>Parameter</b>	None																		
<b>Default</b>	None																		
<b>Mode</b>	Admin Mode and Configuration Mode																		
<b>Usage</b>	Display the configuration of Protocol-based VLAN on the switch.																		
<b>Example</b>	<p>Display the configuration of the current Protocol-based VLAN.</p> <pre>Switch#show protocol-vlan</pre> <table border="1"> <thead> <tr> <th>Protocol_Type</th> <th>VLAN_ID</th> <th>Priority</th> </tr> <tr> <th>-----</th> <th>-----</th> <th>-----</th> </tr> </thead> <tbody> <tr> <td>mode ethernetii etype 0x600</td> <td>200</td> <td>0</td> </tr> <tr> <td>mode ethernetii etype 0x60e</td> <td>1</td> <td>7</td> </tr> <tr> <td>mode snap etype 0x613</td> <td>1</td> <td>1</td> </tr> <tr> <td>mode llc dsap 0x1 ssap 0x1</td> <td>1</td> <td>0</td> </tr> </tbody> </table>	Protocol_Type	VLAN_ID	Priority	-----	-----	-----	mode ethernetii etype 0x600	200	0	mode ethernetii etype 0x60e	1	7	mode snap etype 0x613	1	1	mode llc dsap 0x1 ssap 0x1	1	0
Protocol_Type	VLAN_ID	Priority																	
-----	-----	-----																	
mode ethernetii etype 0x600	200	0																	
mode ethernetii etype 0x60e	1	7																	
mode snap etype 0x613	1	1																	
mode llc dsap 0x1 ssap 0x1	1	0																	

## 7.1.48 show subnet-vlan

<b>Syntax</b>	show subnet-vlan												
<b>Parameter</b>	None												
<b>Default</b>	None												
<b>Mode</b>	Admin Mode and other Configuration Mode.												
<b>Usage</b>	Display the configuration of the IP-subnet-based VLAN on the switch.												
<b>Example</b>	<p>Display the configuration of the current IP-subnet-based VLAN.</p> <pre>Switch#show subnet-vlan</pre> <table border="1"> <thead> <tr> <th>IP-Address</th> <th>Mask</th> <th>VLAN_ID</th> <th>Priority</th> </tr> <tr> <th>-----</th> <th>-----</th> <th>-----</th> <th>-----</th> </tr> </thead> <tbody> <tr> <td>192.168.5.2</td> <td>255.255.255.0</td> <td>100</td> <td>0</td> </tr> </tbody> </table>	IP-Address	Mask	VLAN_ID	Priority	-----	-----	-----	-----	192.168.5.2	255.255.255.0	100	0
IP-Address	Mask	VLAN_ID	Priority										
-----	-----	-----	-----										
192.168.5.2	255.255.255.0	100	0										

## 7.1.49 show subnet-vlan interface

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

## 7.1.50 subnet-vlan

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



## 7.1.51 switchport mac-vlan enable

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

## 7.1.52 switchport subnet-vlan enable

<b>Syntax</b>	<pre>switchport subnet-vlan enable no switchport subnet-vlan enable</pre>
<b>Parameter</b>	none
<b>Default</b>	The IP-subnet-based VLAN is enabled on the port by default.
<b>Mode</b>	Port Mode.
<b>Usage</b>	<p>After adding the IP subnet to specified VLAN, the IP-subnet-based VLAN function will be globally enabled. This command can disable the IP-subnet-based VLAN function on specified port to meet special user applications.</p> <p><code>show subnet-vlan interface display setting.</code></p>
<b>Example</b>	<p>Disable the IP-subnet-based VLAN function on port2.</p> <pre>Switch#config Switch(config)# interface ethernet 1/0/2 Switch(config-if-ethernet1/0/2)#no switchport subnet-vlan enable Switch(config-if-ethernet1/0/2)#show subnet-vlan interface</pre> <p>Ports</p> <pre>----- Ethernet1/0/1(A)  Ethernet1/0/3(A) Ethernet1/0/4(A)  Ethernet1/0/5(A) Ethernet1/0/6(A)  Ethernet1/0/7(A) Ethernet1/0/8(A)  Ethernet1/0/9(A) Ethernet1/0/10(A) Ethernet1/0/11(A) Ethernet1/0/12(A) Ethernet1/0/13(A) Ethernet1/0/14(A) Ethernet1/0/15(A) Ethernet1/0/16(A) Ethernet1/0/17(A) Ethernet1/0/18(A) Ethernet1/0/19(A) Ethernet1/0/20(A) Ethernet1/0/21(A) Ethernet1/0/22(A) Ethernet1/0/23(A) Ethernet1/0/24(A) Ethernet1/0/25(A) Ethernet1/0/26(A) Ethernet1/0/27(A) Ethernet1/0/28(A)</pre>

### 7.1.53 show voice-vlan

<b>Syntax</b>	show voice-vlan															
<b>Parameter</b>	None															
<b>Default</b>	None															
<b>Mode</b>	Admin Mode and other Configuration Mode.															
<b>Usage</b>	Display Voice VLAN Configuration.															
<b>Example</b>	<p>Display the Current Voice VLAN Configuration.</p> <pre>Switch#show subnet-vlan</pre> <table border="1"> <thead> <tr> <th>IP-Address</th> <th>Mask</th> <th></th> <th>VLAN_ID</th> <th>Priority</th> </tr> <tr> <th>-----</th> <th>-----</th> <th>-----</th> <th>-----</th> <th></th> </tr> </thead> <tbody> <tr> <td>192.168.5.2</td> <td>255.255.255.0</td> <td></td> <td>100</td> <td>0</td> </tr> </tbody> </table>	IP-Address	Mask		VLAN_ID	Priority	-----	-----	-----	-----		192.168.5.2	255.255.255.0		100	0
IP-Address	Mask		VLAN_ID	Priority												
-----	-----	-----	-----													
192.168.5.2	255.255.255.0		100	0												

## 7.1.54 switchport voice-vlan enable

<b>Syntax</b>	switchport voice-vlan enable no switchport voice-vlan enable
<b>Parameter</b>	none
<b>Default</b>	Voice VLAN is enabled by default.
<b>Mode</b>	Port Mode.
<b>Usage</b>	When voice equipment is added to the Voice VLAN, the Voice VLAN is enabled globally by default. This command disables Voice VLAN on specified port to meet specified application of the user. show voice-vlan display setting °
<b>Example</b>	<p>Disable the Voice VLAN function on port2.</p> <pre>Switch#config Switch(config)# interface ethernet 1/0/2 Switch(config-if-ethernet1/0/2)# no switchport voice-vlan enable Switch(config-if-ethernet1/0/2)# show voice-vlan Voice VLAN ID:100 Ports ----- Ethernet1/0/1(A)  Ethernet1/0/3(A) Ethernet1/0/4(A)  Ethernet1/0/5(A) Ethernet1/0/6(A)  Ethernet1/0/7(A) Ethernet1/0/8(A)  Ethernet1/0/9(A) Ethernet1/0/10(A) Ethernet1/0/11(A) Ethernet1/0/12(A) Ethernet1/0/13(A) Ethernet1/0/14(A) Ethernet1/0/15(A) Ethernet1/0/16(A) Ethernet1/0/17(A) Ethernet1/0/18(A) Ethernet1/0/19(A) Ethernet1/0/20(A) Ethernet1/0/21(A) Ethernet1/0/22(A) Ethernet1/0/23(A) Ethernet1/0/24(A) Ethernet1/0/25(A) Ethernet1/0/26(A) Ethernet1/0/27(A) Ethernet1/0/28(A)  Voice name      Mac-Address      Mask      Priority -----</pre>

## 7.1.55 voice-vlan

<b>Syntax</b>	voice-vlan mac <mac-address> mask <mac-mask> priority <priority-id> [name <voice-name>] no voice-vlan {mac <mac-address> mask <mac-mask>   name <voice-name>   all}								
<b>Parameter</b>	<table border="1"> <tr> <td>&lt;mac-address&gt;</td> <td>Mac-address is the voice equipment MAC address, shown in "xx-xx-xx-xx-xx-xx" format;</td> </tr> <tr> <td>&lt;mac-mask&gt;</td> <td>mac-mask is the last eight digit of the mask code of the MAC address, the valid values are: 0xff, 0xfe, 0xfc, 0xf8, 0xf0, 0xe0, 0xc0, 0x80, 0x0;</td> </tr> <tr> <td>&lt;priority-id&gt;</td> <td>priority-id is the priority of the voice traffic, the valid range is 0–7;</td> </tr> <tr> <td>&lt;voice-name&gt;</td> <td>the voice-name is the name of the voice equipment, which is to facilitate the equipment management;</td> </tr> </table>	<mac-address>	Mac-address is the voice equipment MAC address, shown in "xx-xx-xx-xx-xx-xx" format;	<mac-mask>	mac-mask is the last eight digit of the mask code of the MAC address, the valid values are: 0xff, 0xfe, 0xfc, 0xf8, 0xf0, 0xe0, 0xc0, 0x80, 0x0;	<priority-id>	priority-id is the priority of the voice traffic, the valid range is 0–7;	<voice-name>	the voice-name is the name of the voice equipment, which is to facilitate the equipment management;
<mac-address>	Mac-address is the voice equipment MAC address, shown in "xx-xx-xx-xx-xx-xx" format;								
<mac-mask>	mac-mask is the last eight digit of the mask code of the MAC address, the valid values are: 0xff, 0xfe, 0xfc, 0xf8, 0xf0, 0xe0, 0xc0, 0x80, 0x0;								
<priority-id>	priority-id is the priority of the voice traffic, the valid range is 0–7;								
<voice-name>	the voice-name is the name of the voice equipment, which is to facilitate the equipment management;								
<b>Default</b>	This command will add a specified voice equipment into the Voice VLAN, if a non VLAN labeled data packet from the specified voice equipment enters through the switch port, then no matter through which port the packet enters, it will belongs to Voice VLAN. The command will not interfere with the packets of VLAN labels.								
<b>Mode</b>	Global Mode.								
<b>Usage</b>	<p>This command will add a specified voice equipment into the Voice VLAN, if a non VLAN labeled data packet from the specified voice equipment enters through the switch port, then no matter through which port the packet enters, it will belongs to Voice VLAN. The command will not interfere with the packets of VLAN labels.</p> <p>show voice-vlan display setting.</p>								
<b>Example</b>	<p>Add the 256 sets of voice equipments of the R&amp;D department with MAC address ranging from 00-03-0f-11-22-00 to 00-03-0f-11-22-ff to the Voice VLAN.</p> <pre>Switch#config Switch(config)#vlan 100 Switch(config-vlan100)#exit Switch(config)#voice-vlan vlan 100 Switch(config)#voice-vlan mac 00-03-0f-11-22-00 mask 0 priority 5 name R&amp;D Switch(config)#show voice-vlan Voice VLAN ID:100 Ports ----- Ethernet1/0/1(A)  Ethernet1/0/3(A) Ethernet1/0/4(A)  Ethernet1/0/5(A) Ethernet1/0/6(A)  Ethernet1/0/7(A) Ethernet1/0/8(A)  Ethernet1/0/9(A) Ethernet1/0/10(A) Ethernet1/0/11(A) Ethernet1/0/12(A) Ethernet1/0/13(A) Ethernet1/0/14(A) Ethernet1/0/15(A) Ethernet1/0/16(A) Ethernet1/0/17(A)</pre>								

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

Voice name	Mac-Address	Mask	Priority
-----	-----	-----	-----
R&D	00-03-0f-11-22-00	00-00-00-00-00-00	5

## 7.1.56 voice-vlan vlan

<b>Syntax</b>	voice-vlan vlan <vlan-id> no voice-vlan
<b>Parameter</b>	<vlan-id>                      Vlan id is the number of the specified VLAN.
<b>Default</b>	No Voice VLAN is configured by default.
<b>Mode</b>	Global Mode.
<b>Usage</b>	Set specified VLAN for Voice VLAN, There can be only one Voice VLAN at the same time. The voice VLAN can not be applied concurrently with MAC-based VLAN.  show voice-vlan display setting.
<b>Example</b>	<pre>Set VLAN100 to Voice VLAN. Switch#config Switch(config)#vlan 100 Switch(config-vlan100)#exit Switch(config)#voice-vlan vlan 100 Switch(config)#show voice-vlan Voice VLAN ID:100 Ports ----- Ethernet1/0/1(A)  Ethernet1/0/3(A) Ethernet1/0/4(A)  Ethernet1/0/5(A) Ethernet1/0/6(A)  Ethernet1/0/7(A) Ethernet1/0/8(A)  Ethernet1/0/9(A) Ethernet1/0/10(A) Ethernet1/0/11(A) Ethernet1/0/12(A) Ethernet1/0/13(A) Ethernet1/0/14(A) Ethernet1/0/15(A) Ethernet1/0/16(A) Ethernet1/0/17(A) Ethernet1/0/18(A) Ethernet1/0/19(A) Ethernet1/0/20(A) Ethernet1/0/21(A) Ethernet1/0/22(A) Ethernet1/0/23(A) Ethernet1/0/24(A) Ethernet1/0/25(A) Ethernet1/0/26(A) Ethernet1/0/27(A) Ethernet1/0/28(A)  Voice name            Mac-Address            Mask                    Priority -----</pre>

# Chapter 8 Anti-ring Protocol

## 8.1 MSTP

### 8.1.1 abort

---

<b>Command</b>	abort
<b>parameter</b>	-
<b>default</b>	-
<b>Mode</b>	MSTP Region Mode

---

**Usage Guide** This command is to quit MSTP region mode without saving the current configuration. The previous MSTP region configuration is valid.

---

**Example** Quit MSTP region mode without saving the current configuration.  
Switch(Config-Mstp-Region)#abort  
Switch(config)#



## 8.1.2 exit

<b>Command</b>	<b>exit</b>
<b>parameter</b>	-
<b>default</b>	-
<b>Mode</b>	MSTP Region Mode
<b>Usage Guide</b>	This command is to quit MSTP region mode with saving the current configuration.
<b>Example</b>	Quit MSTP region mode with saving the current configuration. Switch(Config-Mstp-Region)#exit Switch(config)#

### 8.1.3 instance vlan

<b>Command</b>	<b>instance &lt;instance-id&gt; vlan &lt;vlan-list&gt;</b> <b>no instance &lt;instance-id&gt; [vlan &lt;vlan-list&gt;]</b>	
<b>parameter</b>	<b>instance-id</b>	sets the instance number. The valid range is from 0 to 64
	<b>vlan-list</b>	sets consecutive or non-consecutive VLAN numbers. "-" refers to consecutive numbers, and ";" refers to non-consecutive numbers
<b>default</b>	Before creating any Instances, there is only the instance 0, and VLAN 1~4094 all belong to the instance 0.	
<b>Mode</b>	MSTP Region Mode	
<b>Usage Guide</b>	<p>This command sets the mappings between VLANs and instances. Only if all the mapping relationships and other attributes are same, the switches are considered in the same MSTP region. Before setting any instances, all the VLANs belong to the instance 0.</p> <p>MSTP can support maximum 64 MSTIs (except for CISTs). CIST can be treated as MSTI 0.</p> <p>All the other instances are considered as instance 1 to 64.</p>	
<b>Example</b>	<p>Map VLAN1-10 and VLAN 100-110 to Instance 1.</p> <pre>Switch(config)#spanning-tree mst configuration Switch(Config-Mstp-Region)#instance 1 vlan 1-10;100-110</pre>	

## 8.1.4 Name

<b>Command</b>	<b>name &lt;name&gt;</b> <b>no name</b>
<b>parameter</b>	<b>name</b> is the MSTP region name. The length of the name should be less than 32 characters
<b>default</b>	Default MSTP region name is the MAC address of this bridge.
<b>Mode</b>	MSTP Region Mode
<b>Usage Guide</b>	This command is to set MSTP region name. The bridges with same MSTP region name and same other attributes are considered in the same MSTP region.
<b>Example</b>	Set MSTP region name to mstp-test. Switch(config)#spanning-tree mst configuration Switch(Config-Mstp-Region)#name mstp-test

## 8.1.5 revision-level

<b>Command</b>	<b>revision-level &lt;level&gt;</b> <b>no revision-level</b>
<b>parameter</b>	<b>level</b> is revision level. The valid range is from 0 to 65535
<b>default</b>	The default revision level is 0.
<b>Mode</b>	MSTP Region Mode
<b>Usage Guide</b>	This command is to set revision level for MSTP configuration. The bridges with same MSTP revision level and same other attributes are considered in the same MSTP region.
<b>Example</b>	Set revision level to 2000. Switch(config)#spanning-tree mst configuration Switch(Config-Mstp-Region)# revision-level 2000

## 8.1.6 spanning-tree

<b>Command</b>	spanning-tree <b>no spanning-tree</b>
<b>parameter</b>	-
<b>default</b>	MSTP is not enabled by default.
<b>Mode</b>	Global Mode and Port Mode
<b>Usage Guide</b>	If the MSTP is enabled in global mode, the MSTP is enabled in all the ports except for the ports which are set to disable the MSTP explicitly
<b>Example</b>	Enable the MSTP in global mode, and disable the MSTP in the interface1/0/2. Switch(config)#spanning-tree Switch(config)#interface ethernet 1/0/2 Switch(Config-If-Ethernet1/0/2)#no spanning-tree

## 8.1.7 spanning-tree cost

<b>Command</b>	<b>spanning-tree cost &lt;cost&gt;</b> <b>no spanning-tree cost</b>
<b>parameter</b>	<b>cost</b> sets path cost. The valid range is from 1 to 200,000,000.

**default** By default, the port cost is relevant to the port bandwidth.

For the aggregation ports, the default costs are as below:	Default Path Cost	Suggested Range
10Mbps	2000000	2000000-20000000
100Mbps	200000	200000-2000000
1GMbps	20000	20000-200000

For the aggregation ports, the default costs are as below:

Port Type	Allowed Number Of Aggregation Ports	Default Port Cost	默认端口
10Mbps	N	2000000/N	2000000
100Mbps	N	200000/N	200000/N
1GMbps	N	20000/N	20000/N

**Mode** Port Mode

**Usage Guide** By setting the port cost, users can control the cost from the current port to the root bridge in order to control the elections of port and the designated port of the instance.

**Example** On the port1/0/2, set the port cost is 3000000.  
Switch(Config-If-Ethernet1/0/2)#spanning-tree cost 3000000

## 8.1.8 spanning-tree digest-snooping

<b>Command</b>	<p><b>spanning-tree digest-snooping</b></p> <p><b>no spanning-tree digest-snooping</b></p>
<b>parameter</b>	-
<b>default</b>	Don't use the authentication string of partner port.
<b>Mode</b>	Port Mode
<b>Usage Guide</b>	<p>According to MSTP protocol, the region authentication string is generated by MD5 algorithm with public authentication key, instance ID, VLAN ID. Some manufacturers don't use the public authentication key, this causes the incompatibility. After the command is executed the port can use the authentication string of partner port, realize compatibility with these manufacturers equipment.</p> <p>Because the authentication string is related to instance ID and VLAN ID, the command may cause recognizing the equipment that with different instance and VLAN relation as in the same region. Before the command is executed, make sure that instance and VLAN relation is accord for all the equipment. If there are more than one equipment connected, all the connected ports should execute this command.</p>
<b>Example</b>	<p>Configure the authentication string of partner port.</p> <pre>Switch(config)#interface ethernet 1/0/2 Switch(Config-If-Ethernet1/0/2)#spanning-tree digest-snooping Switch(Config-If-Ethernet1/0/2)#</pre>

### 8.1.9 spanning-tree format

<b>Command</b>	<b>spanning-tree format {standard   privacy   auto}</b> <b>no spanning-tree format</b>	
<b>parameter</b>	<b>standard</b>	The packet format provided by IEEE
	<b>privacy</b>	Privacy packet format, which is compatible with CISCO equipments.
	<b>auto</b>	Auto identified packet format, which is determined by checking the format of the received packets.
<b>default</b>	Auto Packet Format.	
<b>Mode</b>	Port Mode	
<b>Usage Guide</b>	<p>As the CISCO has adopted the packet format different with the one provided by IEEE, while many companies also adopted the CISCO format to be CISCO compatible, we have to provide support to both formats. The standard format is originally the one provided by IEEE, and the privacy packet format is CISCO compatible. In case we are not sure about which the packet format is on partner, the AUTO configuration will be preferred so to identify the format by the packets they sent. The AUTO packet format is set by default in the concern of better compatibility with previous products and the leading companies. The packet format will be privacy format before receiving the partner packet when configured to AUTO.</p> <p>When the format is not AUTO and the received packet format from the partner does not match the configured format, we set the state of the port which receives the unmatched packet to DISCARDING to prevent both sides consider themselves the root which leads to circuits.</p> <p>When the AUTO format is set, and over one equipment which is not compatible with each other are connected on the port (e.g. a equipment running through a HUB or Transparent Transmission BPDU is connected with several equipments running MSTP), the format alter counts will be recorded and the port will be disabled at certain count threshold. The port can only be re-enabled by the administrator.</p>	



**Example** Configure port message format as the message format of IEEE.  
Switch(config)#interface ethernet 1/0/2  
Switch(Config-If-Ethernet1/0/2)#spanning-tree format standard  
Switch(Config-If-Ethernet1/0/2)#

### 8.1.10 spanning-tree forward-time

**Command** spanning-tree forward-time <time>  
no spanning-tree forward-time

**parameter** *time* is forward delay time in seconds. The valid range is from 4 to 30

**default** The forward delay time is 15 seconds by default

**Mode** Global Mode

**Usage Guide** When the network topology changes, the status of the port is changed from blocking to forwarding. This delay is called the forward delay. The forward delay is co working with hello time and max age. The parameters should meet the following conditions. Otherwise, the MSTP may work incorrectly .

$$2 * (\text{Bridge\_Forward\_Delay} - 1.0 \text{ seconds}) \geq \text{Bridge\_Max\_Age}$$

$$\text{Bridge\_Max\_Age} \geq 2 * (\text{Bridge\_Hello\_Time} + 1.0 \text{ seconds})$$

**Example** In global mode, set MSTP forward delay time to 20 seconds.  
Switch(config)#spanning-tree forward-time 20

## 8.1.11 spanning-tree hello-time

<b>Command</b>	<p>spanning-tree hello-time &lt;<i>time</i>&gt; no spanning-tree hello-time</p>
<b>parameter</b>	<p><i>time</i> is Hello time in seconds. The valid range is from 1 to 10</p>
<b>default</b>	<p>Hello Time is 2 seconds by default</p>
<b>Mode</b>	<p>Global Mode</p>
<b>Usage Guide</b>	<p>This command is used to set the interval bpduswitch sending, command "no spanning-tree hello-time" restore default configuration. Hello time is the interval that the switch sends BPDUs. Hello time is co working with forward delay and max age. The parameters should meet the following conditions. Otherwise, the MSTP may work incorrectly.</p> <p><math>2 * (\text{Bridge\_Forward\_Delay} - 1.0 \text{ seconds}) \geq \text{Bridge\_Max\_Age}</math>  <math>\text{Bridge\_Max\_Age} \geq 2 * (\text{Bridge\_Hello\_Time} + 1.0 \text{ seconds})</math></p>
<b>Example</b>	<p>Set MSTP hello time to 5 seconds in global mode. Switch(config)#spanning-tree hello-time 5</p>

## 8.1.12 spanning-tree link-type p2p

<b>Command</b>	<b>spanning-tree link-type p2p {auto   force-true   force-false}</b> <b>no spanning-tree link-type</b>	
<b>parameter</b>	<b>auto</b>	sets auto-negotiation
	<b>force-true</b>	forces the link as point-to-point type
	<b>force-false</b>	forces the link as non point-to-point type.
<b>default</b>	The link type is auto by default; The MSTP detects the link type automatically.	
<b>Mode</b>	Port Mode	
<b>Usage Guide</b>	For configuring port link types, command "no spanning-tree link-type" restore default configuration. When the port is full-duplex, MSTP sets the port link type as point-to-point; When the port is half-duplex, MSTP sets the port link type as shared.	
<b>Example</b>	Force the port 1/0/7-8 as point-to-point type. Switch(config)#interface ethernet 1/0/7-8 Switch(Config-Port-Range)#spanning-tree link-type p2p force-true	

### 8.1.13 spanning-tree maxage

<b>Command</b>	<code>spanning-tree maxage &lt;time&gt;</code> <code>no spanning-tree maxage</code>
<b>parameter</b>	<i>time</i> is max aging time in seconds. The valid range is from 6 to 40.
<b>default</b>	The max age is 20 seconds by default.
<b>Mode</b>	Global Mode
<b>Usage Guide</b>	<p>this command is used to configure bpdu maximum aging time, command "no spanning-tree maxage" restore default configuration. The lifetime of BPDU is called max age time. The max age is co working with hello time and forward delay. The parameters should meet the following conditions. Otherwise, the MSTP may work incorrectly.</p> $2 * (\text{Bridge\_Forward\_Delay} - 1.0 \text{ seconds}) \geq \text{Bridge\_Max\_Age}$ $\text{Bridge\_Max\_Age} \geq 2 * (\text{Bridge\_Hello\_Time} + 1.0 \text{ seconds})$
<b>Example</b>	<p>In global mode, set max age time to 25 seconds.</p> <pre>Switch(config)#spanning-tree maxage 25</pre>

## 8.1.14 spanning-tree max-hop

<b>Command</b>	<b>spanning-tree max-hop &lt;hop-count&gt;</b> <b>no spanning-tree max-hop</b>
<b>parameter</b>	<b>hop-count</b> sets maximum hops. The valid range is from 1 to 40
<b>default</b>	The max hop is 20 by default.
<b>Mode</b>	Global Mode
<b>Usage Guide</b>	This command is used to set BPDU maximum number of hops, and the command " <b>no spanning-tree max-hop</b> " is used to restore the default configuration. The MSTP uses max-age to count BPDU lifetime. In addition, MSTP also uses max-hop to count BPDU lifetime. The max-hop is degressive in the network. The BPDU has the max value when it initiates from MSTI root bridge. Once the BPDU is received, the value of the max-hop is reduced by 1. When a port receives the BPDU with max-hop as 0, it drops this BPDU and sets itself as designated port to send the BPDU.
<b>Example</b>	Set max hop to 32. Switch(config)#spanning-tree max-hop 32

## 8.1.15 spanning-tree mcheck

<b>Command</b>	<code>spanning-tree mcheck</code>
<b>parameter</b>	-
<b>default</b>	The port is in the MSTP mode by default
<b>Mode</b>	Port Mode
<b>Usage Guide</b>	<p>If a network which is attached to the current port is running IEEE 802.1D STP, the port converts itself to run in STP mode. The command is used to force the port to run in the MSTP mode. But once the port receives STP messages, it changes to work in the STP mode again.</p> <p>This command can only be used when the switch is running in IEEE802.1s MSTP mode. If the switch is running in IEEE802.1D STP mode, this command is invalid.</p>
<b>Example</b>	<p>Force the port 1/0/2 to run in the MSTP mode.</p> <pre>Switch(Config-If-Ethernet1/0/2)#spanning-tree mcheck</pre>

## 8.1.16 spanning-tree mode

<b>Command</b>	<b>spanning-tree mode {mstp   stp   rstp}</b> <b>no spanning-tree mode</b>						
<b>parameter</b>	<table border="1"> <tr> <td><b>mstp</b></td> <td>sets the switch in IEEE802.1s MSTP mode</td> </tr> <tr> <td><b>stp</b></td> <td>sets the switch in IEEE802.1D STP mode</td> </tr> <tr> <td><b>rstp</b></td> <td>sets the switch in IEEE802.1D RSTP mode</td> </tr> </table>	<b>mstp</b>	sets the switch in IEEE802.1s MSTP mode	<b>stp</b>	sets the switch in IEEE802.1D STP mode	<b>rstp</b>	sets the switch in IEEE802.1D RSTP mode
<b>mstp</b>	sets the switch in IEEE802.1s MSTP mode						
<b>stp</b>	sets the switch in IEEE802.1D STP mode						
<b>rstp</b>	sets the switch in IEEE802.1D RSTP mode						
<b>default</b>	The switch is in the MSTP mode by default						
<b>Mode</b>	Global Mode						
<b>Usage Guide</b>	This command is used to configure the spanning tree mode and the command " <b>no spanning-tree mode</b> " is used to restore the default mode. When the switch is in IEEE802.1D STP mode, it only sends standard IEEE802.1D BPDU and TCN BPDU. It drops any MSTP BPDUs.						
<b>Example</b>	Set the switch in the STP mode. Switch(config)#spanning-tree mode stp						

## 8.1.17 spanning-tree mst configuration

---

<b>Command</b>	<b>spanning-tree mst configuration</b> <b>no spanning-tree mst configuration</b>
<b>parameter</b>	-
<b>default</b>	-
<b>Mode</b>	Global Mode

---

<b>Usage Guide</b>	Whether the switch is in the MSTP region mode or not, users can enter the MSTP mode, configure the attributes, and save the configuration. When the switch is running in the MSTP mode, the system will generate the MST configuration identifier according to the MSTP configuration. Only if the switches with the same MST configuration identifier are considered as in the same MSTP region.
--------------------	---

---

<b>Example</b>	Enter MSTP region mode. Switch(config)#spanning-tree mst configuration Switch(Config-Mstp-Region)#
----------------	--



## 8.1.18 panning-tree mst cost

<b>Command</b>	<b>spanning-tree mst &lt;instance-id&gt; cost &lt;cost&gt;</b> <b>no spanning-tree mst &lt;instance-id&gt; cost</b>	
<b>parameter</b>	<b>instance-id</b>	sets the instance ID. The valid range is 0-64
	<b>cost</b>	sets path cost, different cost formats have different ranges. For the default dot1t mode the valid range is 1-200,000,000, and for dot1d is 1-65535.

**default** By default, the port cost is relevant to the port bandwidth.

Port Type	Default Path Cost	Suggested Range
10Mbps	2000000	2000000-20000000
100Mbps	200000	200000-2000000
1GMbps	20000	20000-200000

For the aggregation ports, the default costs are as below:

Port Type	Allowed Number Of Aggregation Ports	Default Port Cost
10Mbps	N	2000000/N
100Mbps	N	200000/N
1GMbps	N	20000/N

Port Speed	Port Type	Port Cost	
		802.1D-2008	802.1T
0		65535	200000000
10Mbps	Half- duplex	100	2,000,000
	Full- duplex	99	1,999,999
	aggregation link	95	1,000,000
	with 2 ports	95	666,666
	aggregation link with 3 ports	95	500,000

	aggregation link with 4 ports		
100Mbps	Half- duplex	19	200,000
	Full- duplex	18	199,999
	aggregation link	15	100,000
	with	15	66,666
	2 ports	15	50,000
1000Mbps	aggregation link with 3 ports		
	aggregation link with 4 ports		
	Full- duplex	4	20,000
	aggregation link	3	10,000
	with	3	6,666
	2 ports	3	5,000
	aggregation link with 3 ports		
	aggregation link with 4 ports		

---

**Mode**

Port Mode

---

**Usage Guide**

By setting the port cost, users can control the cost from the current port to the root bridge in order to control the elections of root port and the designated port of the instance.

---

**Example**

On the port1/0/2, set the MSTP port cost in the instance 2 to 3000000.  
Switch(Config-If-Ethernet1/0/2)#spanning-tree mst 2 cost 3000000

## 8.1.19 spanning-tree cost-format

<b>Command</b>	<code>spanning-tree cost-format {dot1d   dot1t}</code>
	-
<b>default</b>	count path-cost with dot1t format.
<b>Mode</b>	Global mode.
<b>Usage Guide</b>	There are two formats about cost value: they are dot1d marked on IEEE802.1d-2008 and dot1t marked on IEEE802.1t, but path-cost ranges of them are different, dot1d range from 1 to 65535, and dot1t range from 1 to 200,000,000.
<b>Example</b>	Set the cost format in global mode. <code>Switch(config)#spanning-tree cost-format dot1d</code>

## 8.1.20 spanning-tree mst loopguard

<b>Command</b>	<b>spanning-tree [mst &lt;instance-id&gt;] loopguard</b> <b>no spanning-tree [mst &lt;instance-id&gt;] loopguard</b>	
<b>parameter</b>	<b>instance-id</b>	MSTP instance ID.
<b>default</b>	Disable loopguard function	
<b>Mode</b>	Port Mode	
<b>Usage Guide</b>	<p>The command can avoid root port or alternate port to be changed as designated port due to invalid unilateralism link. When the receiving timer is time, the configured port with loopguard is set as block state.</p>	
<b>Example</b>	<p>Configure port 1/0/2 as loopguard mode for instance 0.</p> <pre>Switch(Config)#interface ethernet 1/0/2 Switch(Config-Ethernet-1/0/2)#spanning-tree mst 0 loopguard Switch(Config-Ethernet-1/0/2)#</pre>	

## 8.1.21 spanning-tree mst port-priority

<b>Command</b>	<b>spanning-tree mst &lt;instance-id&gt; port-priority &lt;port-priority&gt;</b> <b>no spanning-tree mst &lt;instance-id&gt; port-priority</b>	
<b>parameter</b>	<b>instance-id</b>	sets the instance ID. The valid range is from 0 to 64
	<b>port-priority</b>	sets port priority. The valid range is from 0 to 240. The value should be the multiples of 16, such as 0, 16, 32...240.
<b>default</b>	The default port priority is 128	
<b>Mode</b>	Port Mode	
<b>Usage Guide</b>	By setting the port priority, users can control the port ID of the instance in order to control the root port and designated port of the instance. The lower the value of the port priority is, the higher the priority is.	
<b>Example</b>	Set the port priority as 32 on the port 1/0/2 for the instance 1. Switch(config)#interface ethernet 1/0/2 Switch(Config-If-Ethernet1/0/2)#spanning-tree mst 1 port-priority 32	

## 8.1.22 spanning-tree mst priority

<b>Command</b>	<b>spanning-tree mst &lt;instance-id&gt; priority &lt;bridge-priority&gt;</b> <b>no spanning-tree mst &lt;instance-id&gt; priority</b>	
<b>parameter</b>	<b><i>instance-id</i></b>	sets instance ID. The valid range is from 0 to 64;
	<b><i>port-priority</i></b>	sets the switch priority. The valid range is from 0 to 61440. The value should be the multiples of 4096, such as 0, 4096, 8192...61440
<b>default</b>	The default bridge priority is 32768	
<b>Mode</b>	Global Mode	
<b>Usage Guide</b>	By setting the bridge priority, users can change the bridge ID for the specified instance. And the bridge ID can influence the elections of root bridge and designated port for the specified instance.	
<b>Example</b>	Set the priority for Instance 2 to 4096. Switch(config)#spanning-tree mst 2 priority 4096	

### 8.1.23 spanning-tree mst rootguard

<b>Command</b>	<code>spanning-tree [mst &lt;instance-id&gt;] rootguard</code> <code>no spanning-tree [mst &lt;instance-id&gt;] rootguard</code>		
<b>parameter</b>	<table border="1"> <tr> <td><i>instance-id</i></td> <td>MSTP instance ID</td> </tr> </table>	<i>instance-id</i>	MSTP instance ID
<i>instance-id</i>	MSTP instance ID		
<b>default</b>	Disable rootguard function		
<b>Mode</b>	Port Mode		
<b>Usage Guide</b>	<p>The command is used in Port Mode, if the port is configured to be a rootguard port, it is forbidden to be a MSTP root port. If superior BPDU packet is received from a rootguard port, MSTP did not recalculate spanning-tree, and just set the status of the port to be root_inconsistent (blocked). If no superior BPDU packet is received from a blocked rootguard port, the port status will restore to be forwarding. The rootguard function can maintain a relative stable spanning-tree topology when a new switch is added to the network.</p>		
<b>Example</b>	<p>Enable rootguard function for port 1/0/2 in instance 0.</p> <pre>Switch(config)#interface ethernet 1/0/2 Switch(Config-If-Ethernet1/0/2)#spanning-tree mst 0 rootguard Switch(Config-If-Ethernet1/0/2)#</pre>		

## 8.1.24 spanning-tree portfast

<b>Command</b>	<b>spanning-tree portfast [bpdufilter   bpduguard] [recovery &lt;30-3600&gt;]</b> <b>no spanning-tree portfast</b>	
<b>parameter</b>	<b>bpdufilter</b>	configure the border port mode as BPDU filter
	<b>bpduguard</b>	configure the border port mode as BPDU guard
	<b>recovery</b>	configure the border port can be recovered automatically after implement bpduguard violation operation
	<b>&lt;30-3600&gt;</b>	the recovery time, do not recover it by default
<b>default</b>	All the ports are non-boundary ports by default when enabling MSTP	
<b>Mode</b>	Port Mode	
<b>Usage Guide</b>	<p>Set the current port as boundary port, and BPDU filter. BPDU guard as specified mode or default mode; the command “no spanning-tree portfast” sets the current port as non-boundary port.</p> <p>When a port is set to be a boundary port, the port converts its status from discarding to forwarding without bearing forward delay. Once the boundary port receives the BPDU, the port becomes a non-boundary port.</p>	
<b>Example</b>	<p>Configure the border port mode as BPDU guard, the recovery time as 60s.</p> <pre>Switch(config)#interface ethernet 1/0/2 Switch(Config-If-Ethernet1/0/2)#spanning-tree portfast bpduguard recovery 60 Switch(Config-If-Ethernet1/0/2)#</pre>	



## 8.1.25 spanning-tree port-priority

<b>Command</b>	<code>spanning-tree port-priority &lt;port-priority&gt;</code> <code>no spanning-tree port-priority</code>
<b>parameter</b>	<b><i>port-priority</i></b> sets port priority. The valid range is from 0 to 240. The value should be the multiples of 16, such as 0, 16, 32, 48...240
<b>default</b>	The default port priority is 32768
<b>Mode</b>	Port Mode
<b>Usage Guide</b>	By setting the port priority to designated port. The lower the value of the port priority is, the higher the priority is.
<b>Example</b>	Set the port priority as 4096 on the port 1. Switch(Config-If-Ethernet1/0/1)#spanning-tree port-priority 4096

## 8.1.26 spanning-tree priority

<b>Command</b>	<b>spanning-tree priority &lt;bridge-priority&gt;</b> <b>no spanning-tree priority</b>
<b>parameter</b>	<b>bridge-priority</b> is the priority of the bridging switch. Its value should be round times of 4096 between 0 and 61440, such as 0, 4096, 8192... 61440.
<b>default</b>	Default priority is 32768
<b>Mode</b>	Global Mode
<b>Usage Guide</b>	The bridge ID can be altered by changing the priority of the switch. Further, the priority information can also be used for voting of the root bridge and the specified ports. The bridge priority value of the switch is smaller, however the priority is higher.
<b>Example</b>	Configure the priority is 4096. Switch(config)#spanning-tree priority 4096

## 8.1.27 spanning-tree rootguard

---

<b>Command</b>	<b>spanning-tree rootguard</b> <b>no spanning-tree rootguard</b>
<b>parameter</b>	-
<b>default</b>	Port is non-root port
<b>Mode</b>	Port Mode
<b>Usage Guide</b>	<p>The command is used in Port Mode, if the port is configured to be a rootguard port, it is forbidden to be a MSTP root port. If superior BPDU packet is received from a rootguard port, MSTP did not recalculate spanning-tree, and just set the status of the port to be root_inconsistent (blocked). If no superior BPDU packet is received from a blocked rootguard port, the port status will restore to be forwarding. The rootguard function can maintain a relative stable spanning-tree topology when a new switch is added to the network.</p>
<b>Example</b>	<p>Set the port 1 is root port.</p> <pre>Switch(Config-If-Ethernet1/0/1)#spanning-tree rootguard</pre>

### 8.1.28 spanning-tree tflush (Global mode)

<b>Command</b>	<b>spanning-tree tflush {enable  disable  protect}</b> <b>no spanning-tree tflush</b>	
<b>parameter</b>	<b>enable</b>	The spanning-tree flush once the topology changes.
	<b>disable</b>	The spanning tree don't flush when the topology changes.
	<b>protect</b>	the spanning-tree flush not more than one time every ten seconds.
<b>default</b>	Enable	
<b>Mode</b>	Global mode	
<b>Usage Guide</b>	<p>Configure the spanning-tree flush mode once the topology changes. "<b>no spanning-tree tflush</b>" restores to default setting.</p> <p>According to MSTP, when topology changes, the port that send change message clears MAC/ARP table (FLUSH). In fact it is not needed for some network environment to do FLUSH with every topology change. At the same time, as a method to avoid network assault, we allow the network administrator to configure FLUSH mode by the command.</p>	
<b>Example</b>	<p>Configure the spanning-tree flush mode once the topology changes is not flush to TC.</p> <pre>Switch(config)#spanning-tree tflush disable Switch(config)#</pre>	

### 8.1.29 spanning-tree tcflush (Port mode)

<b>Command</b>	<b>spanning-tree tcflush {enable  disable  protect}</b> <b>no spanning-tree tcflush</b>	
<b>parameter</b>	<b>enable</b>	The spanning-tree flush once the topology changes
	<b>disable</b>	The spanning tree don't flush when the topology changes
	<b>protect</b>	the spanning-tree flush not more than one time every ten seconds
<b>default</b>	Default enable mode	
<b>Mode</b>	Port Mode	
<b>Usage Guide</b>	<p>Configure the spanning-tree flush mode for port once the topology changes. “<b>no spanning-tree tcflush</b>” restores to default setting.</p> <p>According to MSTP, when topology changes, the port that send change message clears MAC/ARP table (FLUSH). In fact it is not needed for some network environment to do FLUSH with every topology change. At the same time, as a method to avoid network assault, we allow the network administrator to configure FLUSH mode by the command.</p>	
<b>Example</b>	<p>Configure the spanning-tree flush mode once the topology change is not flush to TC.</p> <pre>Switch(config)#spanning-tree tcflush disable</pre>	

### 8.1.30 spanning-tree transmit-hold-count

<b>Command</b>	<b>spanning-tree transmit-hold-count &lt;tx-hold-count-value&gt;</b> <b>no spanning-tree transmit-hold-count</b>	
<b>parameter</b>	<b>tx-hold-count-value</b>	ranging from 1 to 20, the default value is 10
<b>default</b>	10	
<b>Mode</b>	Global Mode	
<b>Usage Guide</b>	Set the max number for sending BPDU within the Hello Time interval to control BPDU flow. The variable is used to whole MST bridge.	
<b>Example</b>	Set the max transmit-hold-count as 20. Switch(config)#spanning-tree transmit-hold-count 20	

### 8.1.31 show mst-pending

<b>Command</b>	show mst-pending
<b>parameter</b>	-
<b>default</b>	-
<b>Mode</b>	Admin Mode
<b>Usage Guide</b>	In the MSTP region mode, display the configuration of the current MSTP region such as MSTP name, revision, VLAN and instance mapping.
<b>Example</b>	<p>Display the configuration of the current MSTP region.</p> <pre>Switch(config)#spanning-tree mst configuration Switch(Config-Mstp-Region)#show mst-pending Name switch Revision 0 Instance Vlans Mapped ----- 00 1-29, 31-39, 41-4093 03 30 04 40 05 4094 ----- Switch(Config-Mstp-Region)#</pre>

### 8.1.32 show spanning-tree

<b>Command</b>	<b>show spanning-tree [mst [&lt;instance-id&gt;]] [interface &lt;interface-list&gt;] [detail]</b>					
<b>parameter</b>	<b>instance-id</b>	sets interface list				
	<b>interface-list</b>	sets the instance ID. The valid range is from 0 to 64				
	<b>detail</b>	sets the detailed spanning-tree information				
<b>default</b>	-					
<b>Mode</b>	Admin and Configuration Mode					
<b>Usage Guide</b>	This command can display the MSTP information of the instances in the current bridge.					
<b>Example</b>	<pre> Display the bridge MSTP. Switch#sh spanning-tree ***** Process 0 ***** -- MSTP Bridge Config Info --  Standard      : IEEE 802.1s Bridge MAC    : 00:1f:ce:10:b0:1b Bridge Times  : Max Age 20, Hello Time 2, Forward Delay 15 Force Version: 3  ##### Instance 0 ##### Self Bridge Id  : 32768.00:1f:ce:10:b0:1b Root Id        : this switch Ext.RootPathCost : 0 Region Root Id  : this switch Int.RootPathCost : 0 Root Port ID   : 0 Current port list in Instance 0: Ethernet1/0/12 Ethernet1/0/20 (Total 2)        PortName      ID      ExtRPC  IntRPC  State Role      DsgBridge ----- Ethernet1/0/12 128.012      0        0 FWD  DSGN 32768.001fce10b01b 128.012 Ethernet1/0/20 128.020      0        0 FWD  DSGN 32768.001fce10b01b 128.020 </pre>					



Display information	describe
<b>MSTP Bridge Config Info</b>	
Standard	STP version
Bridge MAC	Bridge MAC address
Bridge Times	Max Age, Hello Time and Forward Delay of the bridge
Force Version	Version of STP
<b>Instance 0</b>	
Self Bridge Id	The priority and the MAC address of the current bridge for the current instance
Root Id	The priority and the MAC address of the root bridge for the current instance
Ext.RootPathCost	Total cost from the current bridge to the root of the entire network
Int.RootPathCost	Cost from the current bridge to the region root of the current instance
Root Port ID	Root port of the current instance on the current bridge
<b>Current port list in Instance 0</b>	
PortName	Port name
ID	Port priority and port index
ExtRPC	Port cost to the root of the entire network
IntRPC	Cost from the current port to the region root of the current instance
State Role	Port status of current instance
DsgBridge	Upward designated bridge of the current port in the current instance
DsgPort	Upward designated port of the current port in the current instance

### 8.1.33 show spanning-tree mst config

---

<b>Command</b>	show spanning-tree mst config
<b>parameter</b>	-
<b>default</b>	-
<b>Mode</b>	Admin Mode

---

**Usage Guide** In the Admin mode, this command can show the parameters of the MSTP configuration such as MSTP name, revision, VLAN and instance mapping.

**Example** Display the configuration of the MSTP on the switch.  
Switch#show spanning-tree mst config

```
Name
Revision    0
Instance    Vlans Mapped
-----
00          1-4094
-----
```

### 8.1.34 spanning-tree process

<b>Command</b>	<code>spanning-tree process &lt;process-id&gt;</code> <code>no spanning-tree process &lt;process-id&gt;</code>
<b>parameter</b>	<b>process-id</b> the range is 1-31
<b>default</b>	-
<b>Mode</b>	Global Mode
<b>Usage Guide</b>	Create the new mstp process. Multiple mstp processes can be configured on one device and each process is standalone. The process 0 exists only as default.
<b>Example</b>	Create the new mstp process 1. Switch(config)#spanning-tree process 1

### 8.1.35 spanning-tree tc-notify process0

<b>Command</b>	<code>spanning-tree tc-notify process0</code> <code>no spanning-tree tc-notify process0</code>
<b>parameter</b>	-
<b>default</b>	-
<b>Mode</b>	mstp process mode
<b>Usage Guide</b>	When there is a change in mstp process N, the device will receive the tc packet, at the same time, the process N will notify tc to the instance in mstp process 0 on the shared link. It makes the process 0 refresh the table entry for ensuring the traffic not to break off.
<b>Example</b>	Configure to notify TC of process 1 to process 0. Switch(Config-Mstp-Process-1)#spanning-tree tc-notify process0

### 8.1.36 spanning-tree binding-process

<b>Command</b>	<code>spanning-tree binding-process &lt;process-id&gt;</code> <code>no spanning-tree binding-process &lt;process-id&gt;</code>
<b>parameter</b>	<b>process-id</b> the range is 1-31.
<b>default</b>	All the ports belong to process 0
<b>Mode</b>	Port Mode
<b>Usage Guide</b>	Configure the port to join the appointed mstp process N. The port will enter into process N from the process 0. This command is mutually exclusive to the shared port configuration command (link-share).
<b>Example</b>	Add the Ethernet1/0/2 into process 1. Switch(Config-If-Ethernet1/0/2)#spanning-tree binding-process 1

### 8.1.37 spanning-tree binding-process link-share

<b>Command</b>	<code>spanning-tree binding-process &lt; process-id &gt; link-share</code> <code>no spanning-tree binding-process &lt; process-id &gt; link-share</code>
<b>parameter</b>	<b>process-id</b> the range is 1-31
<b>default</b>	The port is only in the mstp calculating of process 0
<b>Mode</b>	Port Mode
<b>Usage Guide</b>	Configure the port belong to the shared port of process N. Except for process 0, the configured port can be in the mstp calculating of multiple processes, but the port status can be only configured by process 0. This command can be configured for more than once.
<b>Example</b>	Configure the Ethernet1/0/2 as the shared port of process 1 and 0. Switch(Config-If-Ethernet1/0/2)#spanning-tree binding-process 1 link-share

## 8.2 ERPS Configuration

### 8.2.1 ethernet tcn-propagation erps

<b>Command</b>	<b>ethernet tcn-propagation erps to {erps   stp}</b> <b>no ethernet tcn-propagation erps to</b>	
<b>parameter</b>	<b>erps</b>	topology changing sends the R-APS event packets to notify the connection ring of this device
	<b>stp</b>	topology changing sends the stp packets to notify the stp topology connected to this device
<b>default</b>	ERPS ring topology changing only takes effect in this ring but does not send the notification packets	
<b>Mode</b>	Global Mode	
<b>Usage Guide</b>	Configure the topology changing transmission notification method supported by this device as the appointed method. The ERPS ring instance detects the changing, it will send the notification packets. If configured erps method, it will send the R-APS event packets to other ERPS rings; if configured stp method, it will send the stp packets outward.	
<b>Example</b>	Configure to send R-APS event notification to the interconnection ring after the topology changing. Switch(config)#ethernet tcn-propagation erps to erps Configure to send STP notification to the interconnection ring after the topology changing. Switch(config)#ethernet tcn-propagation erps to stp Delete the topology changing transmission notification method. Switch(config)#no ethernet tcn-propagation erps to	

## 8.2.2 erps-ring

<b>Command</b>	<code>erps-ring &lt; ring-name &gt;</code> <code>no erps-ring &lt; ring-name &gt;</code>
<b>parameter</b>	<b>ring-name</b> the ERPS ring name created. The maximum character number is 64 and it is made up with letters, numbers and the underlines. The first and last character cannot be the underline
<b>default</b>	Do not configure any ERPS ring.
<b>Mode</b>	Global Mode
<b>Usage Guide</b>	Create a ERPS ring and enter ERPS ring configuration mode. enter ERPS ring configuration mode if the ERPS ring already exists. no command delete ERPS ring.
<b>Example</b>	Create the ERPS ring of ring1 Switch(config)#erps-ring 1 Switch(config-erps-ring)# Delete the EPRS ring of ring1 Switch(config)#no erps-ring 1



### 8.2.3 version

<b>Command</b>	<b>version {v1   v2}</b> <b>no version</b>
<b>parameter</b>	<p><b>v1</b> means to support v1 which is released in 2008-06 and the amendment (2009-04)</p> <p><b>v2</b> means to support v2 which is released in 2010-03 and the amendment (2010-06)</p>
<b>default</b>	<b>V2</b>
<b>Mode</b>	ERPS Ring Configuration Mode
<b>Usage Guide</b>	<p>This command is used to configure the supporting version of the ERPS loop, no the command is restored to the default state of the v2.</p> <p>If configured ERPS ring to support v1, this ring will not support multi-instance. ERPS ring instance does not support the management commands of MS, FS, etc. and the non-revertive switch is not effective. It only support revertive switch.</p> <p>If configured ERPS ring to support v1, the instance of this ring will deal with the ERPS packets according to the v1 format. Package the R-APS packets and resolve the fields according to v1 format. The fields defined by v2 will not be dealt.</p>
<b>Example</b>	<pre>Configure the ERPS ring of ring1 to support v1 Switch(config)#erps-ring ring1 Switch(config-erps-ring)#version v1 Delete v1 supported by the ERPS ring of ring1 Switch(config)#erps-ring ring1 Switch(config-erps-ring)#no version</pre>

## 8.2.4 open-ring

<b>Command</b>	<code>open-ring</code> <code>no open-ring</code>
<b>parameter</b>	-
<b>default</b>	Default Configuration ERPS Subrings
<b>Mode</b>	ERPS Ring Configuration Mode
<b>Usage Guide</b>	If the ERPS ring instance has been configured on the ring, there will be the message of <b>“Can’t config open-ring on ERPS ring which has ERPS instance, please delete ERPS instance firstly!”</b> Otherwise, enter into the next step. Configure this ERPS ring type as sub ring.
<b>Example</b>	Configure the ERPS ring of ring1 as sub ring of open type. <code>Switch(config)#erps-ring 1</code> <code>Switch(config-erps-ring)#open-ring</code> Delete the configuration of the sub ring of open type. <code>Switch(config)#erps-ring 1</code> <code>Switch(config-erps-ring)#no open-ring</code>

## 8.2.5 raps-virtual-channel

<b>Command</b>	<b>raps-virtual-channel {with   without}</b>
<b>parameter</b>	<p><b>with</b> the R-APS virtual channel is existed in this ERPS ring</p> <p><b>without</b> the R-APS virtual channel is not existed in this ERPS ring</p>
<b>default</b>	The R-APS virtual channel is not existed in ERPS ring
<b>Mode</b>	ERPS Ring Configuration Mode
<b>Usage Guide</b>	<p>Configure if there is the R-APS virtual channel in ERPS ring according to the configuration.</p> <p>Inputting: Success or error. If there is not R-APS virtual channel on the ERPS ring, the R-APS channel of all the instances of ERPS ring will be unblocked forever and it only blocks the data channel; otherwise, the R-APS channel and the data channel will be blocked at the same time.</p>
<b>Example</b>	<p>Configure that there is R-APS virtual channel in the ERPS sub ring of ring1.</p> <pre>Switch(config)#erps-ring ring1 Switch(config-erps-ring)#raps-virtual-channel with</pre>

## 8.2.6 erps-ring

<b>Command</b>	<b>erps-ring &lt;ring-name&gt; port0 [port1]</b> <b>no erps-ring &lt;ring-name&gt; port0</b>	
<b>parameter</b>	<b>ring-name</b>	ERPS ring name, the maximum string is 64, and it is made up with letters, numbers and underlines; the first and last characters cannot be underlines
	<b>port1-none</b>	there is only the port0 on this ERPS ring node, no port1 and it is the interconnection node
<b>default</b>	Do not configure port0 on ERPS ring	
<b>Mode</b>	Port Mode	
<b>Usage Guide</b>	<p>this command is used to configure the port as the port of the specified ERPS ring. If this ERPS ring is not open-ring type, the port1-none cannot be configured. Check if the ERPS ring configuration is integral; if it is integral, check if the ERPS instance configuration is integral; if it is integral, activate the instance as active and run the protocol.</p>	
<b>Example</b>	<pre> Configure e 1/0/1 as the port0 of ERPS ring1 Switch(config)#interface ethernet 1/0/1 Switch(config-if-ethernet1/0/1)#erps-ring ring1 port0 Delete the e 1/0/1 as port0 of ERPS ring1 Switch(config)#interface ethernet 1/0/1 Switch(config-if-ethernet1/0/1)#no erps-ring ring1 port0 </pre>	

## 8.2.7 failure-detect

<b>Command</b>	<pre>{port0   port1} failure-detect {cc   physical-link-or-cc} domain &lt;domain-name&gt; service {&lt; ma-name &gt;   number &lt; ma-num &gt;   pvlan &lt; vlan-id &gt;} mep &lt;mep-id&gt; rmep&lt;rmep-id&gt; no {port0   port1} failure-detect</pre>	
<b>parameter</b>	<b>{port0   port1}</b>	parameter selection. Port0 means the fault detection type of port0. Port1 means the fault detection type of port1
	<b>{cc physical-link-or-cc}</b>	parameter selection. cc means that the ERPS ring port detection is cc report fault. physical-link-or-cc means that the ERPS ring port detection is cc report fault and physical link fault.
	<b>&lt;domain-name&gt;</b>	the cfm domain name of ERPS ring port detection
	<b>&lt; ma-name &gt;</b>	the service name that cfm belongs to of ERPS ring port detection.
	<b>&lt;mep-id&gt;</b>	the local mep id that cfm monitored of ERPS ring port detection
	<b>&lt;rmep-id&gt;</b>	the remote mep id that cfm monitored of ERPS ring port detection
<b>default</b>	ERPS ring port only detects the physical link fault as default	
<b>Mode</b>	ERPS Ring Configuration Mode	
<b>Usage Guide</b>	<p>Configure the fault detection type of ERPS ring ports. If it is detected as cc type, the maintenance domain, maintenance set that cc belongs to and the monitoring link (it is conditioned with (mep-id, rmep-id)) should be appointed. The premise of this configuration is that the corresponding ring port has been joined into ERPS ring. The no command deletes</p> <p>the fault detection type of ERPS ring ports.</p> <p>Configure the fault detection type of ERPS ring ports as the appointed type. If the type is cc,</p> <p>save the configured md, ma, mep and rmep information to use for matching after receiving</p> <p>the cfm fault notification.</p>	
<b>Example</b>	<p>Configure the detection type of ERPS ring1 port0as cc.</p> <pre>Switch(config)#erps-ring 1</pre>	

```
Switch(config-erps-ring)#port0 failure-defect cc domain domain1 service service1 mep 1
rmep 2
Delete this configuration.
Switch(config)#erps-ring 1
Switch(config-erps-ring)#no port0 failure-defect
```

## 8.2.8 erps-instance

<b>Command</b>	<b>erps-instance &lt;instance-id&gt;</b> <b>no erps-instance &lt;instance-id&gt;</b>
<b>parameter</b>	<b>instance-id</b> id of ERPS ring, the range is 1 to 48
<b>default</b>	Do not configure any ERPS ring instance
<b>Mode</b>	ERPS Ring Configuration Mode
<b>Usage Guide</b>	Create the ERPS ring instance and enter into the ERPS ring instance configuration Mode. If the ERPS ring supports v1, there will be the message of "Doesn't support multiple ERPS instance capability on the ring running version 1!" when configured more than one ERPS instance.
<b>Example</b>	Configure the ERPS ring instance 1 on ERPS ring1. Switch(config)#erps-ring 1 Switch(config-erps-ring)#erps-instance 1 Switch(config-erps-ring-inst-1)# Delete the ERPS ring instance 1 on ERPS ring1. Switch(config)#erps-ring 1 Switch(config-erps-ring)#no erps-instance 1

## 8.2.9 description

<b>Command</b>	<b>description &lt;instance-name&gt;</b> <b>no description &lt;instance-name&gt;</b>
<b>parameter</b>	<b>instance-name</b> ERPS instance name, the maximum string is 64, and it is made up with letters, numbers and underlines; the first and last characters cannot be underlines. The no command deletes the ERPS instance name.
<b>default</b>	Do not configure the ERPS instance name as default
<b>Mode</b>	ERPS Instance Configuration Mode
<b>Usage Guide</b>	Configure the description string for the ERPS instance.
<b>Example</b>	Configure the ERPS instance1 name on ring1 as instance1. Switch(config)#erps-ring ring1 Switch(config-erps-ring)#erps-instance 1 Switch(config-erps-ring-inst-1)# description instance1 Delete this name of instance1. Switch(config)#erps-ring ring1 Switch(config-erps-ring)#erps-instance 1 Switch(config-erps-ring-inst-1)# no description

## 8.2.10 ring-id

<b>Command</b>	<p>ring-id &lt;ring-id&gt; no ring-id &lt;ring-id&gt;</p>
<b>parameter</b>	<p><b>ring-id</b> ERPS ring id and the range is 1 to 64</p>
<b>default</b>	<p>The MAC address is 01-19-A7-00-00-01 as default</p>
<b>Mode</b>	<p>ERPS Instance Configuration Mode.</p>
<b>Usage Guide</b>	<p>Configure the last byte of R-APS packets destination MAC address sent by ERPS ring node to carry ring-id. If ERPS ring supports v1, ring-id only can be configured as 1. The no command configures it not to carry the ring-id, it means that the MAC is 01-19-A7-00-00-01.</p>
<b>Example</b>	<p>Configure the last byte of R-APS packets destination MAC address sent by ERPS ring1 instance2 to carry the ring-id 2.</p> <pre>Switch(config)#erps-ring 1 Switch(config-erps-ring)#erps-instance 2 Switch(config-erps-ring-inst-2)#ring-id 2</pre> <p>Configure the last byte of R-APS packets destination MAC address sent by ERPS ring1 instance2 not to carry the ring-id, it means the destination MAC is 01-19-A7-00-00-01.</p> <pre>Switch(config)#erps-ring 1 Switch(config-erps-ring)#erps-instance 2 Switch(config-erps-ring-inst-2)#no ring-id</pre>



## 8.2.11 rpl

<b>Command</b>	<code>rpl {port0   port1} {owner   neighbour}</code> <code>no rpl {port0   port1}</code>				
<b>parameter</b>	<table border="1"> <tr> <td><code>{port0   port1}</code></td> <td>ERPS ring member ports</td> </tr> <tr> <td><code>{owner   neighbour}</code></td> <td><b>Owner</b> : RPL owner <b>Neighbour</b> : RPL owner</td> </tr> </table>	<code>{port0   port1}</code>	ERPS ring member ports	<code>{owner   neighbour}</code>	<b>Owner</b> : RPL owner <b>Neighbour</b> : RPL owner
<code>{port0   port1}</code>	ERPS ring member ports				
<code>{owner   neighbour}</code>	<b>Owner</b> : RPL owner <b>Neighbour</b> : RPL owner				
<b>default</b>	None, it is the ordinary transmission node type.				
<b>Mode</b>	ERPS Instance Configuration Mode				
<b>Usage Guide</b>	Configure the member port of ERPS ring instance as RPL owner or RPL neighbour, the RPL node roles of different instances on the same ERPS ring cannot be configured on the same member port. The no command configures the member port of ERPS ring instance as the ordinary transmission port member.				
<b>Example</b>	<pre>Configure the port0 of ERPS ring1 instance1 as RPL owner node. Switch(config)#erps-ring 1 Switch(config-erps-ring)#erps-instance 1 Switch(config-erps-ring-inst-1)# rpl port0 owner</pre>				

## 8.2.12 non-revertive

<b>Command</b>	<b>non-revertive</b> <b>no non-revertive</b>
<b>parameter</b>	-
<b>default</b>	ERPS ring instance supports the revertive as default
<b>Mode</b>	ERPS Instance Configuration Mode
<b>Usage Guide</b>	Configure the ERPS ring instance as non-revertive. If this ERPS ring supports v1, this command is null and cannot be configured. The no command configures the ERPS ring instance as revertive. If this ERPS ring supports v1, this command is null. This command can be configured only on the RPL owner node of the sub ring.
<b>Example</b>	Configure the ERPS ring1 instance1 to support the non-revertive. Switch(config)#erps-ring 1 Switch(config-erps-ring)#erps-instance 1 Switch(config-erps-ring-inst-1)#non-revertive

### 8.2.13 guard-timer

<b>Command</b>	<code>guard-timer &lt;guard-times&gt;</code> <code>no guard-timer</code>
<b>parameter</b>	<b>guard-times</b> the interval is 10ms and the range is 10ms to 2s
<b>default</b>	500ms
<b>Mode</b>	ERPS Instance Configuration Mode
<b>Usage Guide</b>	Configure the Guard timer. The guard timer is used for the Ethernet node to avoid the error handling and the close loop according to the outdated R-APS packets. In the starting time of the timer, any R-APS packets received (the R-APS packets that the Request/State="1110" are except) will be dropped. The no command configures the guard timer as the default value.
<b>Example</b>	Configure the guard timer of ERPS ring1 instance1 as 1s. Switch(config)#erps-ring 1 Switch(config-erps-ring)#erps-instance 1 Switch(config-erps-ring-inst-1)guard-timer 100

## 8.2.14 holdoff-timer

<b>Command</b>	<b>holdoff -timer &lt;holdoff-times&gt;</b> <b>no holdoff -timer</b>
<b>parameter</b>	<b>holdoff-times</b> the interval is 1s and the range is 0 to 10s
<b>default</b>	0s
<b>Mode</b>	ERPS Instance Configuration Mode
<b>Usage Guide</b>	This command is used to configure the delay timer, and the default configuration is restored in the form of No
<b>Example</b>	Configure the Holdoff timer of ERPS ring1 instance1 as 5s. Switch(config)#erps-ring ring1 Switch(config-erps-ring)#erps-instance 1 Switch(config-erps-ring-inst-1)#holdoff -timer 5

## 8.2.15 wtr-timer

<b>Command</b>	<b>wtr-timer &lt;wtr-times&gt;</b> <b>no wtr-timer</b>
<b>parameter</b>	<b>wtr-times</b> the interval is 1min and the range is from 1 to 12min
<b>default</b>	5min
<b>Mode</b>	ERPS Instance Configuration Mode
<b>Usage Guide</b>	Configure the WTR timer. WTR timer is used to avoid the frequent protection switching of RPL owner node because of the periodic (intermittent) default. When RPL owner port received the default recovery packets, after some time, and then check if the default still existed on the other nodes and prevent blocking RPL owner port immediately to cause the chokepoint shocking. The no command configures the WTR timer as the default.
<b>Example</b>	Configure the WTR timer of ERPS ring1 instance1 as 10min. Switch(config)#erps-ring 1 Switch(config-erps-ring)#erps-instance 1 Switch(config-erps-ring-inst-1)#wtr-timer 10

## 8.2.16 protected-instance

<b>Command</b>	<code>protected-instance &lt;instance-list&gt;</code> <code>no protected-instance &lt;instance-list&gt;</code>
<b>parameter</b>	<b>instance-list</b> the MSTP instance list protected by ERPS ring instance, such as i, j-k. The number of the instances in the list is not limited.
<b>default</b>	ERPS ring instance does not protect any MSTP instance
<b>Mode</b>	ERPS Instance Configuration Mode
<b>Usage Guide</b>	Configure the protection instance of ERPS ring instance. ERPS ring instance can protect all the MSTP instances. The same instance cannot be quoted by multiple ERPS ring instances under the same topology. Under the same ERPS ring instance, run this command more than once to protect instance, the result will be accumulated. The no command deletes the protection instance of ERPS ring instance.
<b>Example</b>	Configure the protection instance of ERPS ring1 instance1 as instance 2. Switch(config)#erps-ring ring1 Switch(config-erps-ring)#erps-instance 1 Switch(config-erps-ring-inst-1)#protected-instance 2

## 8.2.17 raps-mel

<b>Command</b>	<b>raps-mel &lt;level-value&gt;</b> <b>no raps-mel</b>
<b>parameter</b>	<b>level-value</b> the level value of APS packets, range is from 0 to 7
<b>default</b>	Level is 7
<b>Mode</b>	ERPS Instance Configuration Mode
<b>Usage Guide</b>	<p>Configure the level of R-APS channel of ERPS ring instance as the appointed level. If configured successfully, the mel field of the R-APS packet sent by this ERPS ring instance will be added as the appointed level and only the R-APS packets with the level that is larger than or same as the appointed level can be allowed passing by, or notify the error.</p> <p>The no command configures the level as the default of 7. The MEL field in the protocol packets is used to detect if the current packet can pass by.</p>
<b>Example</b>	<p>Configure the level of R-APS channel of ERPS ring1 instance1 as 5.</p> <pre>Switch(config)#erps-ring ring1 Switch(config-erps-ring)#erps-instance 1 Switch(config-erps-ring-inst-1)raps-mel 5</pre>

## 8.2.18 control-vlan

<b>Command</b>	<code>control-vlan &lt;vlan-id&gt;</code> <code>no control-vlan</code>
<b>parameter</b>	<b>vlan-id</b> vlan id of R-APS packets, range is from 2 to 4094
<b>default</b>	Do not configure any control vlan
<b>Mode</b>	ERPS Instance Configuration Mode
<b>Usage Guide</b>	<p>Configure the control vlan of R-APS packets of R-APS channel. In the ERPS ring instance, this vlan is only used to transmit ERPS protocol packets but not to forward the user business packets. It improves the ERPS protocol security. User makes sure the configuration uniqueness. This vlan is as the vlan tag when sending R-APS packets. The protection VLAN configuration of all the nodes in the instance must be identical. The no command deletes the control vlan.</p>
<b>Example</b>	<p>Configure the control vlan of ERPS ring1 instance1 as vlan10.</p> <pre>Switch(config)#erps-ring ring1 Switch(config-erps-ring)#erps-instance 1 Switch(config-erps-ring-inst-1)control-vlan 10</pre>



## 8.2.19 forced-switch

<b>Command</b>	<b>forced-switch {port0   port1}</b>
<b>parameter</b>	<p><b>port0</b> means to run the forced switch configuration on port0 of the ring node</p> <p><b>port1</b> means to run the forced switch configuration on port1 of the ring node</p>
<b>default</b>	No forced switch in ERPS ring instance
<b>Mode</b>	ERPS Instance Configuration Mode
<b>Usage Guide</b>	<p>Run the forced switch on the port of ERPS ring node. Two or more forced switch are allowed existing at the same time in one ERPS ring instance. But only one forced switch command can be existed on one ring node. User should avoid using multiple forced switch in ERPS ring instance to cause the ERPS ring instance splitting.</p> <p>If the forced switch is on the current highest priority, block the data channel and R-APS channel of this ERPS ring instance on the appointed member port (port0 or port1), and unblock the other member port of this ring node;</p> <p>If this instance configuration is not integral, it is on the status of unactive, there will be the message of "The request is rejected because the ERP instance in unactive state!" otherwise, enter into the next step;</p>
<b>Example</b>	<p>Run the forced switch configuration on the port0 of ERPS ring1 instance1.</p> <pre>Switch(config)#erps-ring ring1 Switch(config-erps-ring)#erps-instance 1 Switch(config-erps-ring-inst-1)#force-switch port0</pre>

## 8.2.20 manual-switch

<b>Command</b>	<code>manual-switch {port0   port1}</code>
<b>parameter</b>	<p><b>port0</b> means to run the manual switch configuration on port0 of the ring node</p> <p><b>port1</b> means to run the manual switch configuration on port1 of the ring node</p>
<b>default</b>	No manual switch in ERPS ring instance
<b>Mode</b>	ERPS Instance Configuration Mode
<b>Usage Guide</b>	<p>Run the manual switch on the port of ERPS ring node. Only one manual switch is allowed existing in one ERPS ring instance, and the premise is that there is no SF fault or FS command in ERPS ring instance.</p> <p>If this instance configuration is not integral, it is on the status of unactive, there will be the message of "The request is rejected because the ERP instance in unactive state!" otherwise, enter into the next step;</p>
<b>Example</b>	<p>Run the manual switch configuration on the port0 of ERPS ring1 instance1.</p> <pre>Switch(config)#erps-ring ring1 Switch(config-erps-ring)#erps-instance 1 Switch(config-erps-ring-inst-1)#manual-switch port0</pre>

## 8.2.21 clear command

<b>Command</b>	<b>clear command</b>
<b>parameter</b>	-
<b>default</b>	No clear command in ERPS ring instance.
<b>Mode</b>	ERPS Instance Configuration Mode
<b>Usage Guide</b>	<p>Run the clear command to the member port of ERPS ring node, it can clear the management command of the local activity: forced switch command and manual switch command; it can be also used to trigger the link switch under the revertive mode before WTR or WTB is time out; and trigger the link to switch from the standby link RPL back to the intrinsic link under the non-revertive mode after the fault recovery.</p> <p>If the forced or manual switch command has existed on the node of this ring instance, clear the switch command and keep the block status of the data channel and R-APS channel of the blocked member ports. And send the P-APS (NR) packets on the two member ports stably and steadily until received R-APS (NR, RB) packets and known the RPL is blocked. Or the higher level request happens on the ring (such as SF);</p> <p>If the local forced or manual switch has existed on the node of this ring instance, clear the command and then receive the R-APS (NR) packets whose node ID is larger than the local node ID. Unblock all the ring ports without SF fault and stop sending the R-APS (NR) packets on the two member ports.</p>
<b>Example</b>	<p>Run clear configuration on ERPS ring1 instance1.</p> <pre>Switch(config)#erps-ring ring1 Switch(config-erps-ring)#erps-instance 1 Switch(config-erps-ring-inst-1)#clear command</pre>

## 8.2.22 show erps ring

<b>Command</b>	show erps ring {<ring-name>   brief}			
<b>parameter</b>	<b>ring-name</b>	ERPS ring name		
	<b>brief</b>	Show the ERPS ring main information		
<b>default</b>	-			
<b>Mode</b>	Admin Mode			
<b>Usage Guide</b>	Read the ERPS ring information.			
<b>Example</b>	<pre> show all the ERPS rings information. Switch#show erps ring brief ethernet tcn-propagation erps to none. Ring-Name                                     Ring-topo Port0          Port1          Version  Inst-Coun t ----- ----- -- ring1                                     major-ring  - -          V2          0 </pre>			

## 8.2.23 show erps instance

<b>Command</b>	<b>show erps instance [ring &lt;ring-name&gt; [instance &lt;instance-id&gt;]]</b>	
<b>parameter</b>	<b>ring-name</b>	ERPS ring name
	<b>instance-id</b>	ID of ERPS ring instance, range is from 1 to 48. If it is not appointed, show all the ERPS ring instances information.
<b>default</b>	-	
<b>Mode</b>	Admin Mode	
<b>Usage Guide</b>	Show the ERPS ring instance information.	

**Example**

Show all the ERPS ring instances information.

```
Switch#show erps instance
ERPS Ring: 1
  Instance: 1
  Description: -
  Protected Instance: -
  Revertive mode: revertive
  R-APS MEL: 7
  R-APS Virtual-Channel: with
  Control Vlan: -
  Ring ID: 1
  Guard Timer(10ms): 50
  Holdoff Timer(seconds): 0
  WTR Timer(min): 5

-----
Port      Role          Port-Status
-----
Port0     common       blocked
Port1     common       blocked
```

Display content	analyze
Description	ERPS ring instance name
Protected Instance	MSTP instance protected by ERPS ring instance
Revertive mode	ERPS ring link mode: revertive, non-revertive

R-APS MEL	Level of R-APS channel, package R-APS packets
R-APS Virtual-Channel	If the ERPS ring is the sub ring, the R-APS virtual channel of the inherited ring: with, without
Ring ID	The ring-id number carried by the packets sent by ERPS ring instance, range is from 1 to 64.
Contral Vlan	R-APS channel vlan, package R-APS packet of tag
WTR_Timer	Wait to Restore timer, range is from 1 to 12min
Guard_Timer	Guard timer, range is from 10ms to 2s
Holdoff_Timer	Holdoff timer, range is from 0 to 10
Port	ERPS ring port information: port0, port1
Role	ERPS ring node roles: RPL Owner, RPL neighbor, Common
Port-Status	Blocked: port is in block status forwarding: port is in forwarding status

## 8.2.24 show erps status

<b>Command</b>	<b>show erps status [ring &lt;ring-name&gt; [instance &lt;instance-id&gt;]]</b>	
<b>parameter</b>	<b>ring-name</b>	ERPS ring name
	<b>instance-id</b>	ID of ERPS ring instance, range is from 1 to 48. If it is not appointed, show all the ERPS ring instances status information.
<b>default</b>	-	
<b>Mode</b>	Admin Mode	
<b>Usage Guide</b>	Show the status information of ERPS ring instance.	

<b>Example</b>	<p>Show all the ERPS ring instances status information.</p> <pre>Switch#show erps status ERPS ring: 1 instance: 1 status: Active: 0 Node State: - Time last topology change:Jan 00 00:00:00 1900</pre> <table border="1"> <thead> <tr> <th>Port</th> <th>Interface</th> <th>Port-Status</th> <th>Signal-Status</th> <th>R-APS-NodeId</th> <th>BPR</th> </tr> </thead> <tbody> <tr> <td>Port0</td> <td>-</td> <td>-</td> <td>-</td> <td>-</td> <td>-</td> </tr> <tr> <td>Port1</td> <td>-</td> <td>-</td> <td>-</td> <td>-</td> <td>-</td> </tr> </tbody> </table> <p>ERPS ring: 1 instance: 2 status:</p> <pre>Active: 0 Node State: - Time last topology change:Jan 00 00:00:00 1900</pre> <table border="1"> <thead> <tr> <th>Port</th> <th>Interface</th> <th>Port-Status</th> <th>Signal-Status</th> <th>R-APS-NodeId</th> <th>BPR</th> </tr> </thead> <tbody> <tr> <td>Port0</td> <td>-</td> <td>-</td> <td>-</td> <td>-</td> <td>-</td> </tr> <tr> <td>Port1</td> <td>-</td> <td>-</td> <td>-</td> <td>-</td> <td>-</td> </tr> </tbody> </table> <table border="1"> <tr> <td>Display content</td> <td>analyze</td> </tr> <tr> <td>Active</td> <td>Current active status of ERPS ring instance: 1, 0</td> </tr> <tr> <td>Node State</td> <td>Current status of ERPS ring instance: Idle,</td> </tr> </table>		Port	Interface	Port-Status	Signal-Status	R-APS-NodeId	BPR	Port0	-	-	-	-	-	Port1	-	-	-	-	-	Port	Interface	Port-Status	Signal-Status	R-APS-NodeId	BPR	Port0	-	-	-	-	-	Port1	-	-	-	-	-	Display content	analyze	Active	Current active status of ERPS ring instance: 1, 0	Node State	Current status of ERPS ring instance: Idle,
Port	Interface	Port-Status	Signal-Status	R-APS-NodeId	BPR																																							
Port0	-	-	-	-	-																																							
Port1	-	-	-	-	-																																							
Port	Interface	Port-Status	Signal-Status	R-APS-NodeId	BPR																																							
Port0	-	-	-	-	-																																							
Port1	-	-	-	-	-																																							
Display content	analyze																																											
Active	Current active status of ERPS ring instance: 1, 0																																											
Node State	Current status of ERPS ring instance: Idle,																																											

	Protection, Forced-switch, Manual-switch, Pending
Time last topology change	Topology switching last time
Port-Status	Blocked: the port is in block status Forwarding: the port is in forwarding status
Signal-Status	ERPS ring port fault status: Non-failed: no fault Failed: fault happened
R-APS-NodeId	The node ID information is the last bit of the MAC address
BPR	The block link information carried by the receiving last R-APS saved by ERPS ring port, it is port0 or port1 which was blocked.



## 8.2.25 show erps statistics

<b>Command</b>	<b>show erps statistics [ring &lt;ring-name&gt; [instance &lt;instance-id&gt;]]</b>	
<b>parameter</b>	<b>ring-name</b>	ERPS ring name
	<b>instance-id</b>	ID of ERPS ring instance, range is from 1 to 48. If it is not appointed, show the statistic information of all the ERPS ring instances of this device.
<b>default</b>	-	
<b>Mode</b>	Admin Mode	
<b>Usage Guide</b>	Show the statistic information of ERPS ring instance.	

**Example**

Show the statistic information of ERPS ring instance.

```
Switch#show erps statistics
Statistics for ERPS ring: 1 instance 1:
R-APS  Port0(Tx/Rx)          Port1(Tx/Rx)
-----
NR:     0          /0          0          /0
NR,RB:  0          /0          0          /0
SF:     0          /0          0          /0
MS:     0          /0          0          /0
FS:     0          /0          0          /0
EVENT:  0          /0          0          /0
-----
TOTAL:  0          /0          0          /0

Statistics for ERPS ring: 1 instance 2:
R-APS  Port0(Tx/Rx)          Port1(Tx/Rx)
-----
NR:     0          /0          0          /0
NR,RB:  0          /0          0          /0
SF:     0          /0          0          /0
MS:     0          /0          0          /0
FS:     0          /0          0          /0
EVENT:  0          /0          0          /0
-----
TOTAL:  0          /0          0          /0
```

## 8.2.26 clear erps statistics

<b>Command</b>	clear erps statistics [ring <ring-name> [instance <instance-id>]]	
<b>parameter</b>	<b>ring-name</b>	ERPS ring name
	<b>instance-id</b>	ID of ERPS ring instance, range is from 1 to 48. If it is not appointed, clear the statistic information of all the ERPS ring instances of this device
<b>default</b>	-	
<b>Mode</b>	Admin Mode	
<b>Usage Guide</b>	Clear the statistic information of ERPS.	
<b>Example</b>	Clear the statistic information of ERPS ring1 instance1. Switch#clear erps statistics ring 1 instance 1	

# Chapter 9 QOS and Flow-based Redirection

## 9.1 QOS

### 9.1.1 accounting

Syntax	Accounting no accounting
Parameter	none
Default	Do not set statistic function.
Mode	Policy map configuration mode
Usage	Set statistic function for the classified traffic. After enable this function, add statistic function to the traffic of the policy class map, the messages can only red or green when passing policy. When print statistic information, in packets means classify packets numbers and not support the classify of color.
Example	Count the packets which satisfy c1 rule. Switch#config Switch(config)#class-map c1 Switch(config-classmap-c1)#exit Switch(config)#policy-map p1 Switch(config-policymap-p1)#class c1 Switch(config-policymap-p1-class-c1)#accounting Switch(config-policymap-p1-class-c1)#exit Switch(config-policymap-p1)#exit Switch(config)#

## 9.1.2 class

Syntax	<pre>class &lt;class-map-name&gt; [insert-before &lt;class-map-name&gt;] no class &lt;class-map-name&gt;</pre>
Parameter	<p>&lt;class-map-name&gt;      &lt;class-map-name&gt; is the class map name used by the class.</p> <p>insert-before &lt;class-      insert-before &lt;class-map-name&gt; insert a new configured class to the map-name&gt;                      front of a existent class to improve the priority of the new class.</p>
Default	No policy class is configured by default.
Mode	Policy map configuration mode
Usage	<p>Associates a class to a policy map and enters the policy class map mode; the no command deletes the specified class.</p> <p>Before setting up a policy class, a policy map should be created and the policy map mode entered. In the policy map mode, classification and nexthop configuration can be performed on packet traffic classified by class map.</p>
Example	<p>After add a policy class map c1 to the policy map, add a policy class map c2 and insert it to the front of c1.</p> <pre>Switch(config)#class-map c1 Switch(config-classmap-c1)#exit Switch(config)#class-map c2 Switch(config-classmap-c2)#exit Switch(config)#policy-map p1 Switch(config-policymap-p1)#class c1 Switch(config-policymap-p1-class-c1)#exit Switch(config-policymap-p1)#class c2 insert-before c1 Switch(config-policymap-p1-class-c2)#exit</pre>

### 9.1.3 class-map

Syntax	<code>class-map &lt;class-map-name&gt;</code> <code>no class-map &lt;class-map-name&gt;</code>
Parameter	<code>&lt;class-map-name&gt;</code> class map name
Default	No class map is configured by default.
Mode	Global Mode
Usage	<u>Creates a class map and enters class map mode; the no command deletes the specified class map.</u>
Example	Creating and then deleting a class map named "c1". Switch#config Switch(config)#class-map c1 Switch(config-classmap-c1)#exit Switch(config)#no class-map c1

### 9.1.4 clear mls qos statistics

Syntax	clear mls qos statistics (interface [ethernet] <interface-name>   (vlan <vlan-id>)
Parameter	<vlan-id> VLAN ID <interface-name> interface name
Default	Do not set action.
Mode	Admin Mode
Usage	Clear accounting data of the specified ports or VLAN Policy Map. If there are no parameters, clear accounting data of all policy map.
Example	Clear the Policy Map statistic of VLAN 100. Switch#clear mls qos statistics vlan 100

## 9.1.5 drop

Syntax	drop no drop
Parameter	none
Default	None
Mode	Policy class map configuration mode
Usage	Drop the specified packet after configure this command.
Example	Drop the packet which satisfy c1. Switch#config Switch(config)#policy-map p1 Switch(config-policy-map-p1)#class c1 Switch(config-policy-map-p1-class-c1)#drop Switch(config-policy-map-p1-class-c1)#exit Switch(config-policy-map-p1)#exit

## 9.1.6 match

Syntax	<pre>match (access-group &lt;acl-index-or-name&gt;   ip dscp &lt;dscp-list&gt;   ip precedence &lt;ip-precedence-list&gt;   ipv6 access-group &lt;acl-index-or-name&gt;   ipv6 dscp &lt;dscp-list&gt;   ipv6 flowlabel &lt;flowlabel-list&gt;   vlan &lt;vlan-list&gt;   cos &lt;cos-list&gt; ) no match {access-group   ip dscp   ip precedence  ipv6 access-group  ipv6 dscp   ipv6 flowlabel   vlan   cos }</pre>														
Parameter	<table border="1"> <tr> <td>&lt;acl-index-or-name&gt;</td> <td>match specified IP ACL, MAC ACL or IPv6 standard ACL or MAC-IP ACL, the parameters are the number or name of the ACL;</td> </tr> <tr> <td>&lt;dscp-list&gt;</td> <td>match specified DSCP value, the parameter is a list of DSCP consisting of maximum 8 DSCP values, the range is 0~63;</td> </tr> <tr> <td>&lt;ip-precedence-list&gt;</td> <td>match specified IP Precedence, the parameter is a IP Precedence list consisting of maximum 8 IP Precedence values with a valid range of 0~7;</td> </tr> <tr> <td>ipv6 access-group &lt;acl-index-or-name&gt;</td> <td>match specified IPv6 ACL, the parameter is the number or name of the IPv6 ACL;</td> </tr> <tr> <td>&lt;flowlabel-list&gt;</td> <td>match specified IPv6 flow label, the parameter is IPv6 flow label value, the range is 0~1048575;</td> </tr> <tr> <td>&lt;vlan-list&gt;</td> <td>match specified VLAN ID, the parameter is a VLAN ID list consisting of maximum 8 VLAN IDs, the range is 1~4094;</td> </tr> <tr> <td>&lt;cos-list&gt;</td> <td>match specified CoS value, the parameter is a CoS list consisting of maximum 8 CoS, the range is 0~7;</td> </tr> </table>	<acl-index-or-name>	match specified IP ACL, MAC ACL or IPv6 standard ACL or MAC-IP ACL, the parameters are the number or name of the ACL;	<dscp-list>	match specified DSCP value, the parameter is a list of DSCP consisting of maximum 8 DSCP values, the range is 0~63;	<ip-precedence-list>	match specified IP Precedence, the parameter is a IP Precedence list consisting of maximum 8 IP Precedence values with a valid range of 0~7;	ipv6 access-group <acl-index-or-name>	match specified IPv6 ACL, the parameter is the number or name of the IPv6 ACL;	<flowlabel-list>	match specified IPv6 flow label, the parameter is IPv6 flow label value, the range is 0~1048575;	<vlan-list>	match specified VLAN ID, the parameter is a VLAN ID list consisting of maximum 8 VLAN IDs, the range is 1~4094;	<cos-list>	match specified CoS value, the parameter is a CoS list consisting of maximum 8 CoS, the range is 0~7;
<acl-index-or-name>	match specified IP ACL, MAC ACL or IPv6 standard ACL or MAC-IP ACL, the parameters are the number or name of the ACL;														
<dscp-list>	match specified DSCP value, the parameter is a list of DSCP consisting of maximum 8 DSCP values, the range is 0~63;														
<ip-precedence-list>	match specified IP Precedence, the parameter is a IP Precedence list consisting of maximum 8 IP Precedence values with a valid range of 0~7;														
ipv6 access-group <acl-index-or-name>	match specified IPv6 ACL, the parameter is the number or name of the IPv6 ACL;														
<flowlabel-list>	match specified IPv6 flow label, the parameter is IPv6 flow label value, the range is 0~1048575;														
<vlan-list>	match specified VLAN ID, the parameter is a VLAN ID list consisting of maximum 8 VLAN IDs, the range is 1~4094;														
<cos-list>	match specified CoS value, the parameter is a CoS list consisting of maximum 8 CoS, the range is 0~7;														
Default	No match standard by default														
Mode	Class-map Mode														
Usage	<p>Configure the match standard of the class map; the no form of this command deletes the specified match standard.</p> <p>Only one match standard can be configured in a class map. When configuring the match ACL, permit rule as the match option, apply Policy Map action. Deny rule as the excluding option, do not apply Policy Map action. (The deny rule is not supported issuing in PBR, please pay attention to avoid it.)</p> <p>If configure another match rule after one was configured, the operation fails, but configure the same match rule will cover the previous.</p>														
Example	<pre>Create a class-map named c1, and configure the class rule of this class-map to match packets with IP Precedence of 0. Switch(config)#class-map c1 Switch(config-classmap-c1)#match ip precedence 0 Switch(config-classmap-c1)#exit</pre>														



### 9.1.7 mls qos aggregate-policy

Syntax	mls qos aggregate-policy <policer_name> <bits_per_second> burst-group <normal_burst_bytes> no mls qos aggregate-policy <policer_name>
Parameter	<p>&lt;policer_name&gt; it is the aggregate policy name.</p> <p>&lt;bits_per_second&gt; it define the information rate, namely CIR, the unit is kbit per second, and it ranges from 1 to 10000000;</p> <p>&lt;normal_burst_bytes&gt; it define the committed burst size, namely CBS, the unit is kilobyte, and it ranges from 1 to 8192, when the CBS more than the maximum of chips , it uses the biggest value that chip support to set hardware, CLI have not notice information;</p>
Default	The default is no policy action.
Mode	Global Mode
Usage	Define a aggregate policy command. The no command delete mode configuration. It only supports single cylinder configuration, when configuring, if configured CBS, not support configure color, green packets only supports transmit, red packets only supports drop.
Example	<p>Set 10000 as CIR, CBS is 512.</p> <p>Switch (config)#policy burst 1 512</p> <p>Switch(config)# mls qos aggregate-policy 1 1000 burst-group 1</p>

## 9.1.8 mls qos cos

Syntax	mls qos cos <default-cos> no mls qos cos
Parameter	<default-cos> default CoS value for the port, the valid range is 0 to 7
Default	The default CoS value is 0
Mode	Port Configuration Mode
Usage	Configures the default CoS value of the port; the "no mls qos cos" command restores the default setting. Configure the default CoS value for switch port. In default configuration, the message ingress cos from this port are default value whether the message with tag. If the message without tag, the message cos value for tag is enacted.
Example	Setting the default CoS value of ethernet port 1/0/1 to 7, i.e., packets coming in through this port will be assigned a default CoS value of 7 if no CoS value present . Switch(config)#interface ethernet 1/0/1 Switch(config-if-ethernet1/0/1)#mls qos cos 7

### 9.1.9 mls qos map

Syntax	<pre>mls qos map (cos-intp &lt;intp1...intp8&gt;   cos-dp &lt;dp1...dp8&gt;   dscp-intp &lt;in-dscp list&gt; to &lt;intp&gt;   dscp-dp &lt;in-dscp list&gt; to &lt;dp&gt;   dscp-dscp &lt;in-dscp list&gt; to &lt;out-dscp&gt;) no mls qos map (cos-intp   cos-dp   dscp-intp   dscp-dp   dscp-dscp)</pre>
Parameter	<p><b>cos-intp &lt;intp1...intp8&gt;</b> defines the mapping from CoS to intp (queue) value, &lt;intp1..intp8&gt; are 8 intp value corresponding to the 0 to 7 CoS value, each intp value is delimited with space, ranging from 0 to 7;</p> <hr/> <p><b>cos-dp&lt;dp1...dp8&gt;</b> defines the mapping from cos to intp (queue), &lt;dp1...dp8&gt; is 8 drop priority and it corresponding to the Cos value from 0 to 7, every drop priority is separated by space, and it ranges from 0 to 2;</p> <hr/> <p><b>dscp-intp</b> defines the mapping from DSCP to intp (queue).</p> <hr/> <p><b>dscp-dp</b> defines the mapping from dscp to drop priority.</p> <hr/> <p><b>dscp-dscp</b> defines the mapping from entrance dscp to export dscp, &lt;in-dscp list&gt; is the input dscp value, the most is 8 and it separated by space from each other, and it ranges from 0 to 63, &lt;out-dscp&gt; is output dscp value and it ranges from 0 to 63.</p>
Default	<p>Default mapping values are:</p> <p>Default CoS-TO-INTP Map</p> <pre>COS: 0 1 2 3 4 5 6 7 INTP: 0 1 2 3 4 5 6 7</pre> <p>Default CoS-TO-DP Map</p> <pre>CoS 0 1 2 3 4 5 6 7 DP 0 0 0 0 0 0 0 0</pre> <p>Default DSCP-TO-INTP Map</p> <pre>d1 : d2 0 1 2 3 4 5 6 7 8 9 0: 0 0 0 0 0 0 0 0 0 1 1 1: 1 1 1 1 1 1 2 2 2 2 2: 2 2 2 2 3 3 3 3 3 3 3: 3 3 4 4 4 4 4 4 4 4 4: 5 5 5 5 5 5 5 5 6 6 5: 6 6 6 6 6 6 7 7 7 7 6: 7 7 7 7</pre> <p>Default DSCP-TO-DP Map</p> <pre>d1 : d2 0 1 2 3 4 5 6 7 8 9 0: 0 0 0 0 0 0 0 0 0 0 1: 0 0 0 0 0 0 0 0 0 0 2: 0 0 0 0 0 0 0 0 0 0</pre>

```

3:    0  0  0  0  0  0  0  0  0  0  0
4:    0  0  0  0  0  0  0  0  0  0  0
5:    0  0  0  0  0  0  0  0  0  0  0
6:    0  0  0  0

```

Default DSCP-TO-DSCP Map

```

d1 : d2  0  1  2  3  4  5  6  7  8  9
0:    0  1  2  3  4  5  6  7  8  9
1:   10 11 12 13 14 15 16 17 18 19
2:   20 21 22 23 24 25 26 27 28 29
3:   30 31 32 33 34 35 36 37 38 39
4:   40 41 42 43 44 45 46 47 48 49
5:   50 51 52 53 54 55 56 57 58 59
6:   60 61 62 63

```

---

Mode

Global Mode

---

Usage

INTP means the chip internal priority setting. Because of the internal DSCP value have 64 and the chip internal priority (queue) only 8, the dscp-intp mapping need 8 continuum internal dscp mapping to the same INTP.

---

Example

Setting the CoS-to-INTP mapping value to the default 0 8 16 24 32 40 48 56 to 0 1 2 3 4 5 6 7 °

```
Switch(config)#mls qos map cos-intp 0 1 2 3 4 5 6 7
```

---

## 9.1.10 mls qos queue algorithm

Syntax	mls qos queue algorithm (sp   wrr   wdr)
	no mls qos queue algorithm
Parameter	sp The strict priority, the queue number of bigger, then the priority is higher
	wrr Select wrr algorithm
	wdr Select wdr algorithm.
Default	WRR
Mode	Port Configuration Mode
Usage	After configure this command, the queue management algorithm is set.
Example	Setting the queue management algorithm as sp. switch#config Switch(config)#interface ethernet 1/0/1 Switch(config-if-ethernet1/0/1)#mls qos queue algorithm sp

### 9.1.11 mls qos queue wdr weight

Syntax	mls qos queue wdr weight <weight1..weight8> no mls qos queue wdr weight
Parameter	<weight1..weight8> defines the queue weight, in Kbytes. For WDRR algorithm, this configuration is valid, but for SP algorithm, it is invalid. When the weight is 0, this queue adopts SP algorithm to manage, and WDRR algorithm turns into SP+WDRR algorithm. range:0-32767
Default	The queue weight is 10 20 40 80 160 320 640 1280.
Mode	Port Configuration Mode
Usage	If the queue weight is configured as 0, it uses SP algorithm to manage, while WRR turns into SWDRR. When removing the queue, the system will manage SP queue at first, then manage WDRR queue, SP queue executes the strict priority management mode, WDRR queue executes the weight rotation management mode.
Example	Configure the queue weight as 10 10 20 20 40 40 80 80. Switch(interface-ethernet1/0/1)#mls qos queue wdr weight 10 10 20 20 40 40 80 80

## 9.1.12 mls qos queue wrr weight

Syntax	mls qos queue wrr weight <weight1..weight8> no mls qos queue wrr weight
Parameter	<weight1..weight8> defines the queue weight, range: 0-127
Default	The queue weight is 1 2 3 4 5 6 7 8 °
Mode	Port Configuration Mode
Usage	If the queue weight is configured as 0, it uses SP algorithm to manage, while WRR turns into SWDRR. When removing the queue, the system will manage SP queue at first, then manage WDRR queue, SP queue executes the strict priority management mode, WDRR queue executes the weight rotation management mode.
Example	Configure the queue weight as 127 8 9 6 3 4 2 0 ° Switch(interface-ethernet1/0/1)#mls qos queue wrr weight 127 8 9 6 3 4 2 0

### 9.1.13 mls qos queue bandwidth

Syntax	mls qos queue <queue-id> bandwidth <maximum-bandwidth> no mls qos queue <queue-id> bandwidth
Parameter	<p>&lt;queue-id&gt; queue ID to configure the bandwidth guarantee, the different chip supports the different queue count, the range is different too, and the ranging from 1 to 8.</p> <p>&lt;maximum-bandwidth&gt; maximum-bandwidth, ranging from 0 to 128000, when input 0, it means the max-bandwidth function is not take effect. The minimum-bandwidth must not bigger than maximum-bandwidth.</p>
Default	The queue bandwidth have no guarantee
Mode	Port Configuration Mode
Usage	The minimum-bandwidth guarantee and maximum-bandwidth limit can be configured at the different or same queue. The queue bandwidth pledge for egress is relative to management mode, for example: one port is the strict priority-queue, the highest priority is queue 8 now, it will satisfy this queue traffic when block is happened. But if user want the lower priority of queue having bandwidth, it can remain bandwidth via this command, the lower priority queue's minimum-bandwidth will be satisfied at first, then the excess bandwidth is managed according to SP.
Example	<p>Configure the maximum-bandwidth is 128kbps for ethernet1/0/2 queue1.</p> <pre>Switch(config)#interface ethernet 1/0/2 Switch(config-if-ethernet1/0/2)# mls qos queue 1 bandwidth 128</pre>



## 9.1.14 mls qos trust

Syntax	mls qos trust (cos   dscp) no mls qos trust (cos   dscp)
Parameter	dscp                                      configures the port to trust DSCP status cos    configures the COS port to trust status.
Default	the default is trust COS value.
Mode	Port Configuration Mode
Usage	Configures the current port trust; the no command disables the current trust status of the port. trust dscp mode: Set the intp field based dscp-to-intp mapping. trust cos mode: Set the intp field based cos-to-intp mapping.
Example	Set trust dscp of port 1/0/1, not trust cos. Switch(config)#interface ethernet 1/0/1 Switch(config-if-ehternet1/1)# mls qos trust dscp Switch(config-if-ehternet1/1)#no mls qos trust cos

### 9.1.15 Policy burst

Syntax	policy burst <burst_group> <normal_burst_bytes>
Parameter	<p>&lt;burst_group&gt; burst_group id ranges from 1 to 2</p> <p>&lt;normal_burst_bytes&gt; The committed burst size – CBS (Committed Burst Size), in byte, ranging from 1 to 8192. When the configured CBS value exceeds the max limit of the chip, configure the hardware with max number supported by the chip without any CLI prompt;</p>
Default	The default of normal_burst_bytes is 1024.
Mode	Global Mode
Usage	Configure burst-group in global mode and it supports 2 burst-group, then it can use burst-group in strategy classify table mode. It can return default configuration by set 1024 as default value.
Example	<p>Set burst-group 1 to define CBS as 512 bits</p> <p>Switch(config)#policy burst 1 512</p>

## 9.1.16 Policy

Syntax	policy <bits_per_second> burst-group <burst-group-id> no policy
Parameter	<bits_per_second>            The committed information rate – CIR (Committed Information Rate), in Kbps, ranging from 1 to 10000000;  <burst-group-id>            It is CBS burst-group id and it ranges from 1 to 2.
Default	No policy action.
Mode	Policy class map configuration mode
Usage	Support non-aggregate policy command of double color, the no command delete mode configuration.  Configure information rate in policy class map configuration mode. Not support the color configuration and the default green packets is transmit, red packets drop.
Example	Set information rate 1000 in policy class map configuration mode, the CBS is 512, the more than cir rate will send and do nothing for packets.  Switch(config)#policy burst 1 512  Switch(config)#class-map cm  Switch(config-classmap-cm)#match cos 0  Switch(config-classmap-cm)#exit  Switch(config)#policy-map 1  Switch(config-policymap-1)#class cm  Switch(config-policymap-1-class-cm)# policy 1000 burst-group 1

## 9.1.17 Policy aggregate

Syntax	<p>policy aggregate &lt;aggregate-policy-name&gt;</p> <p>no policy aggregate &lt;aggregate-policy-name&gt;</p>
Parameter	<p>&lt;aggregate-policy-name&gt; is the policy set name.</p>
Default	No policy is configured by default
Mode	Policy class map configuration mode
Usage	<p>Police Map reference aggregate policy, applies an aggregate policy to classified traffic; the no command deletes the specified aggregate policy.</p> <p>The same policy set can be referred to by different policy class maps.</p>
Example	<p>Create class-map, the match rule is the cos value is 0; policy-map is 1, enter the policy map mode, set the Policy and choose the color policy for the current list.</p> <pre>Switch(config)#class-map cm Switch(config-classmap-cm)#match cos 0 Switch(config-classmap-cm)#exit Switch(config)#policy-map 1 Switch(config-policymap-1)#class cm Switch(config-policymap-1-class-cm)#policy aggregate color</pre>

## 9.1.18 Policy-map

Syntax	<p>policy-map &lt;policy-map-name&gt;</p> <p>no policy-map &lt;policy-map-name&gt;</p>
Parameter	<policy-map-name>      policy map name.
Default	No policy map is configured by default.
Mode	Global Mode
Usage	<p>Creates a policy map and enters the policy map mode; the "no policy-map &lt;policy-map-name&gt;" command deletes the specified policy map.</p> <p><u>Policy class map operation can be done in policy map configuration mode.</u></p>
Example	<p>Creating and deleting a policy map named "p1".</p> <pre>Switch(config)#policy-map p1 Switch(config-policy-map-p1)#exit Switch(config)#no policy-map p1</pre>

## 9.1.19 service-policy input

Syntax	<pre>service-policy input &lt;policy-map-name&gt; no service-policy input {&lt;policy-map-name&gt;}</pre>
Parameter	<pre>input &lt;policy-map-name&gt; input &lt;policy-map-name&gt;</pre> <p>applies the specified policy map to the ingress direction of switch port. no command will delete all the policy maps applied on the ingress direction of the port if there is not the specified policy map name.</p>
Default	No policy map is bound to port by default.
Mode	Port Configuration Mode
Usage	<p>Applies a policy map to the specified port; the no command deletes the specified policy map applied to the port or deletes all the policy maps applied on the ingress direction of the port .</p> <p>Only one policy map can be applied to each direction of each port or VLAN interface.</p>
Example	<pre>Bind policy p1 to ingress Ethernet port1/1. Switch(config)#interface ethernet 1/0/1 Switch(config-if-ethernet1/0/1)#service-policy input p1</pre>

## 9.1.20 service-policy input vlan

Syntax	<pre>service-policy input &lt;policy-map-name&gt; vlan &lt;vlan-list&gt; no service-policy input {&lt;policy-map-name&gt;} vlan &lt; vlan-list&gt;</pre>
Parameter	<pre>input &lt;policy-map- name&gt; input &lt;policy-map-name&gt; applies the specified policy map to the ingress direction of switch VLAN interface. vlan &lt; vlan-list&gt; vlan &lt;vlan-list&gt; the vlan list of binding policy map.</pre>
Default	No policy map is bound to VLAN interface by default.
Mode	Global Mode
Usage	<p>Applies a policy map to the specified VLAN interface; the no command deletes the specified policy map applied to the VLAN interface or deletes all the policy maps applied in the ingress direction of the vlan interface .</p> <p>Only one policy map can be applied to each direction of each port or VLAN interface. °</p>
Example	<pre>Bind policy p1 to ingress of VLAN interface 2-4,6 Switch(config)#service-policy input p1 vlan 2-4;6</pre>

## 9.1.21 set

Syntax	<pre>set (ip dscp &lt;new-dscp&gt;   ip precedence &lt;new-precedence&gt;   internal priority &lt;new-inp&gt;   drop precedence &lt;new-dp&gt;   cos &lt;new-cos&gt;) no set (ip dscp   ip precedence   internal priority   drop precedence   cos)</pre>
Parameter	<pre>ip dscp &lt;new-dscp&gt;          new DSCP value, do not distinguish v4 and v6. ip precedence &lt;new- precedence&gt;                new IP Precedence. cos &lt;new-cos&gt;              new IP Precedence.</pre>
Default	Not assigning by default.
Mode	Policy Class-map Mode
Usage	<p>Assign a new DSCP, IP Precedence for the classified traffic; the no form of this command delete assigning the new values.</p> <p><u>Only the classified traffic which matches the matching standard will be assigned with the new values.</u></p>
Example	<pre>Set the IP Precedence of the packets matching c1 class rule to 3. Switch(config)#policy-map p1 Switch(Config-PolicyMap-p1)#class c1 Switch(Config-PolicyMap-p1-Class-c1)#set ip precedence 3 Switch(Config-PolicyMap-p1-Class-c1)#exit Switch(Config-PolicyMap-p1)#exit</pre>



## 9.1.22 show class-map

Syntax	show class-map [<class-map-name>]								
Parameter	[<class-map-name>] class map name								
Default	None								
Mode	Admin Mode.								
Usage	Displays all configured class-map or specified class-map information.								
Example	<pre>Switch#show class-map Class map name:cm, used by 1 time(s)   match cos: 0  Class map name:color, used by 0 time(s)   match cos: 0</pre> <table border="1"> <thead> <tr> <th>Displayed information</th> <th>Explanation</th> </tr> </thead> <tbody> <tr> <td>Class map name:c1</td> <td>Name of the Class map</td> </tr> <tr> <td>used by 1 times</td> <td>Used times</td> </tr> <tr> <td>match acl name:1</td> <td>Classifying rule for the class map</td> </tr> </tbody> </table>	Displayed information	Explanation	Class map name:c1	Name of the Class map	used by 1 times	Used times	match acl name:1	Classifying rule for the class map
Displayed information	Explanation								
Class map name:c1	Name of the Class map								
used by 1 times	Used times								
match acl name:1	Classifying rule for the class map								

### 9.1.23 show policy-map

Syntax	show policy-map [<policy-map-name>]
Parameter	<policy-map-name>      policy map name
Default	None

Mode                      Admin Mode.

Usage                     Displays all configured policy-map or specified policy-map information.

Example

```
Switch#show policy-map
Policy Map 1, used by 0 time(s)
  Class Map name: cm

Policy Map p1, used by 0 time(s)
  Class Map name: c1
    drop
    set ip precedence 3
      policy CIR: 2000 CBS: 512
    conform-action:
      transmit
    exceed-action:
      drop
```

Displayed information	Explanation
Policy map name:c1	Name of policy map
Class Map name: c1	Class Map name
policy 20000 512	Policy implemented
used by 0 port	Number of port that use the policy

### 9.1.24 show mls qos interface

Syntax	show mls qos {interface [<interface-id>] [policy   queuing]   vlan <vlan-id>}   [begin   include   exclude <regular-expression>]						
Parameter	<table border="1"> <tr> <td>&lt;interface-id&gt;</td> <td>port ID</td> </tr> <tr> <td>&lt;vlan-id&gt;</td> <td>VLAN ID</td> </tr> <tr> <td>&lt;regular-expression&gt;</td> <td>Regular expression</td> </tr> </table>	<interface-id>	port ID	<vlan-id>	VLAN ID	<regular-expression>	Regular expression
<interface-id>	port ID						
<vlan-id>	VLAN ID						
<regular-expression>	Regular expression						
Default	None						
Mode	Admin Mode.						
Usage	<p>Displays QoS configuration information on a port.</p> <p>There is only red or green when packets passing police. In the print information, in packets means classify packets numbers and not supports the statistic information of color.</p>						
Example	<pre>Switch#show mls qos interface ethernet 1/0/1 Ethernet1/0/1: Default COS: 0 Trust: DSCP Attached Policy Map for Ingress: p1  Egress Internal-Priority-TO-Queue map: INTP:  0  1  2  3  4  5  6  7 ----- Queue: 0  1  2  3  4  5  6  7  Queue Algorithm: WRR Queue weights: Queue   1    2    3    4    5    6    7    8 ----- WrrWeight 1    2    3    4    5    6    7    8 WdrrWeight 10   10   20   20   40   40   80   80  Bandwidth Guarantee Configuration: Queue   1    2    3    4    5    6    7    8 ----- MinBW(K) 0    0    0    0    0    0    0    0 MaxBW(K) 0    0    0    0    0    0    0    0</pre> <table border="1"> <tr> <td>Displayed information</td> <td>Explanation</td> </tr> <tr> <td>Ethernet1/0/1</td> <td>Port name</td> </tr> </table>	Displayed information	Explanation	Ethernet1/0/1	Port name		
Displayed information	Explanation						
Ethernet1/0/1	Port name						

default cos:0	Default CoS value of the port
Trust: COS	The trust state of the port
Attached Policy Map for Ingress: p1	Policy name bound to port
ClassMap	ClassMap name
classified	Total data packets match this ClassMap. If there is no Accounting for Class Map, show NA
in-profile	Total in-profile data packets match this ClassMap. If there is no Accounting for Class Map, show NA
out-profile	Total out-profile data packets match this ClassMap. If there is no Accounting for Class Map, show NA
Internal-Priority-TO-Queue map::	Internal-Priority to queue mapping
Queue Algorithm:	WRR , WDDR or PQ queue out method
Queue weights	Queue weights Configuration
Bandwidth Guarantee Configuration	Bandwidth Guarantee Configuration

Switch(config)#show mls qos interface ethernet 1/0/1 queuing

Ethernet1/0/1:

Egress Internal-Priority-TO-Queue map:

INTP: 0 1 2 3 4 5 6 7

-----

Queue: 0 1 2 3 4 5 6 7

Queue Algorithm: WRR

Queue weights:

Queue 1 2 3 4 5 6 7 8

-----

WrrWeight 1 2 3 4 5 6 7 8

WdrrWeight 10 10 20 20 40 40 80 80

Bandwidth Guarantee Configuration:

Queue 1 2 3 4 5 6 7 8

-----

MinBW(K) 0 0 0 0 0 0 0 0

MaxBW(K) 0 0 0 0 0 0 0 0

Displayed information	Explanation
Internal-Priority-TO-Queue map::	Internal-Priority to queue mapping
Queue Algorithm:	WRR, WDDR or PQ queue out method
Queue weights	Queue weights configuration
Bandwidth Guarantee Configuration	Bandwidth Guarantee Configuration

Switch # show mls qos interface ethernet 1/0/1 policy

Ethernet1/0/1:

Attached Policy Map for Ingress: p1

Displayed information	Explanation
Ethernet1/0/1	Port name
Attached Policy Map for Ingress: p1	Policy name bound to port
ClassMap	ClassMap name
classified	Total data packets match this ClassMap.
in-profile	Total in-profile data packets match this ClassMap.
out-profile	Total out-profile data packets match this ClassMap.

### 9.1.25 show mls qos

Syntax	show mls qos in (interface <interface-name> policy)   (vlan <vlan-id>)
Parameter	<interface-name> port name. <vlan-id> VLAN ID
Default	None
Mode	Admin Mode.
Usage	Show the policy configuration information of the in direction of port or vlan. Show the policy configuration information of the in direction.
Example	Show the policy configuration information of the in direction. Switch#show mls qos in interface ethernet1/0/1 policy Ethernet1/0/1: Attached Policy Map for Ingress: p1

## 9.1.26 show mls qos maps

Syntax	show mls qos maps [cos-intp   cos-dp   dscp-intp   dscp-dp   dscp-dscp]   [begin   include   exclude <regular-expression> ]										
Parameter	<table border="1"> <tr> <td>cos-intp</td> <td>The mapping from ingress L2 CoS to internal priority</td> </tr> <tr> <td>cos-dp</td> <td>The mapping from ingress L2 CoS to drop priority</td> </tr> <tr> <td>dscp-intp</td> <td>The mapping from ingress DSCP to internal priority</td> </tr> <tr> <td>dscp-dp</td> <td>The mapping from ingress DSCP to drop priority</td> </tr> <tr> <td>dscp-dscp</td> <td>The mapping from outgress internal to DSCP priority</td> </tr> </table>	cos-intp	The mapping from ingress L2 CoS to internal priority	cos-dp	The mapping from ingress L2 CoS to drop priority	dscp-intp	The mapping from ingress DSCP to internal priority	dscp-dp	The mapping from ingress DSCP to drop priority	dscp-dscp	The mapping from outgress internal to DSCP priority
cos-intp	The mapping from ingress L2 CoS to internal priority										
cos-dp	The mapping from ingress L2 CoS to drop priority										
dscp-intp	The mapping from ingress DSCP to internal priority										
dscp-dp	The mapping from ingress DSCP to drop priority										
dscp-dscp	The mapping from outgress internal to DSCP priority										
Default	None										
Mode	Admin and Configuration Mode.										
Usage	Display the map configuration information of QoS.										
Example	<p>Display configuration information of the mapping table.</p> <pre>Switch#show mls qos maps</pre> <p>Ingress COS-TO-Internal-Priority map:</p> <pre>COS:  0  1  2  3  4  5  6  7 ----- INTP: 0  1  2  3  4  5  6  7</pre> <p>Ingress DSCP-TO-Internal-Priority map:</p> <pre>d1 : d2  0  1  2  3  4  5  6  7  8  9 0:      7  1  7  7  7  0  7  7  7  1 1:      1  1  1  1  1  1  2  1  2  2 2:      2  2  2  2  3  1  3  3  3  3 3:      3  3  4  1  4  4  4  4  4  4 4:      5  1  5  5  5  5  5  5  6  1 5:      6  6  6  6  6  6  7  1  7  7 6:      7  7  7  7</pre> <p>Ingress COS-TO-Drop-Precedence map:</p> <pre>COS:  0  1  2  3  4  5  6  7 ----- DP:   0  0  0  0  0  0  0  0</pre>										

Ingress DSCP-TO-DSCP map:

d1 : d2	0	1	2	3	4	5	6	7	8	9
0:	0	1	2	3	4	5	6	7	8	9
1:	10	11	12	13	14	15	16	17	18	19
2:	20	21	22	23	24	25	26	27	28	29
3:	30	31	32	33	34	35	36	37	38	39
4:	40	41	42	43	44	45	46	47	48	49
5:	50	51	52	53	54	55	56	57	58	59
6:	60	61	62	63						

Ingress DSCP-TO-Drop-Precedence map:

d1 : d2	0	1	2	3	4	5	6	7	8	9
0:	0	0	0	0	0	0	0	0	0	0
1:	0	0	0	0	0	0	0	0	0	0
2:	0	0	0	0	0	0	0	0	0	0
3:	0	0	0	0	0	0	0	0	0	0
4:	0	0	0	0	0	0	0	0	0	0
5:	0	0	0	0	0	0	0	0	0	0
6:	0	0	0	0						

---



### 9.1.27 show mls qos vlan

Syntax	show mls qos vlan <v-id>
Parameter	<v-id> VLAN ID
Default	None
Mode	Admin Mode.
Usage	Display configuration information of the QOS VLAN.
Example	Switch#show mls qos vlan 1 Vlan 1: Attached Policy Map for Ingress: 1 Classmap classified(in packets) c1 0 Rule ID classified(in packets)

## 9.1.28 show mls qos aggregate-policy

Syntax	show mls qos aggregate-policy [<aggregate-policy-name>]						
Parameter	<aggregate-policy-name> aggregate policy name						
Default	None						
Mode	Admin mode and configuration mode.						
Usage	Display all configured aggregate-policy or appointed aggregate-policy information.						
Example	<pre>Switch#show mls qos aggregate-policy a2 aggregate policy a2 CIR: 1000 CBS: 1024 conform-action: transmit exceed-action: drop Not used by any policy map</pre> <table border="1" data-bbox="422 1003 1455 1245"> <thead> <tr> <th>Displayed information</th> <th>Explanation</th> </tr> </thead> <tbody> <tr> <td>aggregate policy a2 CIR: 1000 CBS: 1024 conform-action: transmit exceed-action: drop</td> <td>The configuration of aggregate policy.</td> </tr> <tr> <td>Not used by any Policy Map</td> <td>The referenced times of aggregate policy.</td> </tr> </tbody> </table>	Displayed information	Explanation	aggregate policy a2 CIR: 1000 CBS: 1024 conform-action: transmit exceed-action: drop	The configuration of aggregate policy.	Not used by any Policy Map	The referenced times of aggregate policy.
Displayed information	Explanation						
aggregate policy a2 CIR: 1000 CBS: 1024 conform-action: transmit exceed-action: drop	The configuration of aggregate policy.						
Not used by any Policy Map	The referenced times of aggregate policy.						

## 9.1.29 transmit

---

Syntax	transmit no transmit
Parameter	none
Default	Do not set the action.
Mode	Policy class map configuration mode
Usage	Send the packet directly after configure this command.
Example	Send the packet which satisfy c1. Switch#config Switch(config)#policy-map p1 Switch(config-policymap-p1)#class c1 Switch(config-policymap-p1-class-c1)#transmit Switch(config-policymap-p1-class-c1)#exit Switch(config-policymap-p1)#exit

---

### 9.1.30 access-group redirect to interface ethernet

Syntax	access-group <aclname> redirect to interface [ethernet] <IFNAME> no access-group <aclname> redirect
Parameter	<p>&lt;aclname&gt; name of the flow , only supports digital standard IP ACL, digital extensive IP ACL, nomenclatural standard IP ACL, nomenclatural extensive IP ACL, digital standard MAC ACL, digital extensive MAC ACL, nomenclatural standard MAC ACL, nomenclatural extensive MAC, digital standard IPv6 ACL, and nomenclatural standard IPv6 ACL. Parameters of Timerange and Portrange cannot be set in ACL; the type of ACL should be Permit.</p> <hr/> <p>&lt;IFNAME&gt; &lt;IFNAME&gt; the destination port of redirection</p>
Default	None
Mode	Port Configuration Mode
Usage	<p>Specify flow-based redirection; “no access-group &lt;aclname&gt; redirect” command is used to delete flow-based redirection.</p> <p>Flow-based redirection function enables the switch to transmit the data frames meeting some special condition to another specified port. Notice: Redirect does not support redirect flow to the port.</p>
Example	<p>Redirecting the frames whose source IP is 192.168.1.111 received from port 1 to port 6</p> <pre>Switch(config)#access-list 1 permit host 192.168.1.111 Switch(config)# interface ethernet 1/0/1 Switch(config-if-ethernet1/0/1)#access-group 1 redirect to interface ethernet 1/0/6</pre>

### 9.1.31 show flow-based-redirect

Syntax	<code>show flow-based-redirect [interface [ethernet] &lt;IFNAME&gt;]</code>
Parameter	<IFNAME> display the information of the flow-based redirection configured in the ports listed in the interface-list.
Default	none
Mode	Admin Mode and Configuration Mode.
Usage	This command is used to display the information of current flow-based redirection in the system/port
Example	Switch(config)#show flow-based-redirect Flow-based-redirect config on interface Ethernet1/0/1: RX flow (access-list 1) is redirected to interface Ethernet1/0/6

## 9.1.32 add

Syntax	add s-vid <new-vid> no add s-vid
Parameter	s-vid <new-vid>                      s-vid <new-vid> appointed VID of tunnel VLAN Tag.
Default	The default is not add tag.
Mode	Policy classify table configuration mode
Usage	<p>Add specified tunnel tag for data packets of mapped classify table, the no command cancel configuration.</p> <p>After configured the command, add appointed tunnel tag or inner tag for packets of mapping classify table. When use QinQ function, the data packets that sent only have inner VLAN Tag or no Tag, it needs add s-vid commands to add appointed tunnel VLAN Tag, otherwise data have not tunnel VLAN in switch.</p>
Example	<p>Add a VLAN Tag that VID is 2 to satisfied c1 classify rule packets.</p> <pre>Switch#config Switch(config)#policy-map p1 Switch(config-policy-map-p1)#class c1 Switch(config-policy-map-p1-class-c1)#add s-vid 2</pre>

### 9.1.33 match

Syntax	<pre>match {access-group &lt;acl-index-or-name&gt;   ip dscp &lt;dscp-list&gt;  ip precedence &lt;ip-precedence-list&gt;  ipv6 access-group &lt;acl-index-or-name&gt;   ipv6 dscp &lt;dscp-list&gt;   ipv6 flowlabel &lt;flowlabel-list&gt;   vlan &lt;vlan-list&gt;   cos &lt;cos-list&gt; } no match {access-group   ip dscp   ip precedence   ipv6 access-group   ipv6 dscp no match {access-group   ip dscp   ip precedence   ipv6 access-group   ipv6 dscp   ipv6 flowlabel   vlan   cos }}</pre>														
Parameter	<table border="1"> <tr> <td>access-group &lt;acl-index-or-name&gt;</td> <td>match the specified IP ACL or MAC-IP ACL or standard IPV6 ACL, the parameters are the number or name of ACL</td> </tr> <tr> <td>ip dscp &lt;dscp-list&gt;</td> <td>match the specified DSCP value, the parameter is a list of DSCP consisting of maximum 8 DSCP values, the ranging is 0 to 63</td> </tr> <tr> <td>ip precedence &lt;ip-precedence-list&gt;</td> <td>match the specified IP Precedence, the parameter is a IP Precedence list consisting of maximum 8 IP Precedence values with a valid range of 0 to 7</td> </tr> <tr> <td>ipv6 access-group &lt;acl-index-or-name&gt;</td> <td>match the specified IPv6 ACL, the parameter is the number or name of IPv6 ACL</td> </tr> <tr> <td>ipv6 flowlabel &lt;flowlabel-list&gt;</td> <td>match the specified IPv6 flow label, the parameter is IPv6 flow label value, the ranging is 0 to 1048575</td> </tr> <tr> <td>vlan &lt;vlan-list&gt;</td> <td>match the specified VLAN ID of the external VLAN Tag, the parameter is a VLAN ID list consisting of maximum 8 VLAN IDs, the ranging is 1 to 4094</td> </tr> <tr> <td>cos &lt;cos-list&gt;</td> <td>match the specified CoS value, the parameter is a CoS list consisting of maximum 8 CoS values, the ranging is 0 to 7</td> </tr> </table>	access-group <acl-index-or-name>	match the specified IP ACL or MAC-IP ACL or standard IPV6 ACL, the parameters are the number or name of ACL	ip dscp <dscp-list>	match the specified DSCP value, the parameter is a list of DSCP consisting of maximum 8 DSCP values, the ranging is 0 to 63	ip precedence <ip-precedence-list>	match the specified IP Precedence, the parameter is a IP Precedence list consisting of maximum 8 IP Precedence values with a valid range of 0 to 7	ipv6 access-group <acl-index-or-name>	match the specified IPv6 ACL, the parameter is the number or name of IPv6 ACL	ipv6 flowlabel <flowlabel-list>	match the specified IPv6 flow label, the parameter is IPv6 flow label value, the ranging is 0 to 1048575	vlan <vlan-list>	match the specified VLAN ID of the external VLAN Tag, the parameter is a VLAN ID list consisting of maximum 8 VLAN IDs, the ranging is 1 to 4094	cos <cos-list>	match the specified CoS value, the parameter is a CoS list consisting of maximum 8 CoS values, the ranging is 0 to 7
access-group <acl-index-or-name>	match the specified IP ACL or MAC-IP ACL or standard IPV6 ACL, the parameters are the number or name of ACL														
ip dscp <dscp-list>	match the specified DSCP value, the parameter is a list of DSCP consisting of maximum 8 DSCP values, the ranging is 0 to 63														
ip precedence <ip-precedence-list>	match the specified IP Precedence, the parameter is a IP Precedence list consisting of maximum 8 IP Precedence values with a valid range of 0 to 7														
ipv6 access-group <acl-index-or-name>	match the specified IPv6 ACL, the parameter is the number or name of IPv6 ACL														
ipv6 flowlabel <flowlabel-list>	match the specified IPv6 flow label, the parameter is IPv6 flow label value, the ranging is 0 to 1048575														
vlan <vlan-list>	match the specified VLAN ID of the external VLAN Tag, the parameter is a VLAN ID list consisting of maximum 8 VLAN IDs, the ranging is 1 to 4094														
cos <cos-list>	match the specified CoS value, the parameter is a CoS list consisting of maximum 8 CoS values, the ranging is 0 to 7														
Default	There is no match standard.														
Mode	Class-map Mode														
Usage	<p>Configure the match standard of the class map; the no command deletes the specified match standard.</p> <p>Only one match standard can be configured in a class map. When configuring the ACL match, permit rule is the match option, it will apply Policy Map action. Deny rule is the excluding option, it does not apply Policy Map action. If it has been configured other match rule, the operation is failure, but configuring the same match rule will cover the previous.</p>														
Example	<pre>Create a class-map named c1, and configure the class rule of the class-map to match packets with IP Precedence of 0. Switch(config)#class-map c1 Switch(config-classmap-c1)#match ip precedence 0 Switch(config-classmap-c1)#exit</pre>														

### 9.1.34 service-policy

Syntax	<pre>service-policy &lt;policy-map-name&gt; in no service-policy &lt;policy-map-name&gt; in</pre>
Parameter	<policy-map-name> The specified policy-map name of flexible QinQ
Default	No policy map is bound to port
Mode	Port Configuration Mode
Usage	<p>Bind the specified policy of flexible QinQ to the ingress of the port, the no command cancels the binding.</p> <p>Only one policy map can be bound to each port, the function takes effect after the policy map is bound to a port. At present, do not support the configuration with add command and delete command in policy.</p>
Example	<pre>Apply policy-map p1 (p1 corresponds with the action that modify s-vid) to Ethernet port 1/0/1 for flexible QinQ. Switch(config-if-ethernet1/0/1)#dot1q-tunnel enable Switch(config-if-ethernet1/0/1)#service-policy p1 in</pre>



## 9.1.35 set

Syntax	<pre>set {s-vid &lt;new-vid&gt;   cos &lt;cos-list&gt;   drop-precedence &lt;dp-list&gt;   internal-priority &lt;inp-list&gt;   ip {dscp &lt;dscp-list&gt;   precedence &lt;pri-list&gt;}   s-tpid &lt;tpid-list&gt; }</pre>												
	<pre>no set{s-vid   cos   drop-precedence   internal-priority   ip {dscp   precedence}   s-tpid }</pre>												
Parameter	<table border="1"> <tr> <td>&lt;new-vid&gt;</td> <td>modify tunnel VID of VLAN Tag</td> </tr> <tr> <td>&lt;cos-list&gt;</td> <td>modify cos value of packets</td> </tr> <tr> <td>&lt;dp-list&gt;</td> <td>modify drop priority</td> </tr> <tr> <td>&lt;inp-list&gt;</td> <td>modify inner priority</td> </tr> <tr> <td>&lt;dscp-list&gt; &lt;pri-list&gt;</td> <td>modify ip dscp value or precedence value</td> </tr> <tr> <td>&lt;tpid-list&gt;</td> <td>modify tunnel tpid value of packets</td> </tr> </table>	<new-vid>	modify tunnel VID of VLAN Tag	<cos-list>	modify cos value of packets	<dp-list>	modify drop priority	<inp-list>	modify inner priority	<dscp-list> <pri-list>	modify ip dscp value or precedence value	<tpid-list>	modify tunnel tpid value of packets
<new-vid>	modify tunnel VID of VLAN Tag												
<cos-list>	modify cos value of packets												
<dp-list>	modify drop priority												
<inp-list>	modify inner priority												
<dscp-list> <pri-list>	modify ip dscp value or precedence value												
<tpid-list>	modify tunnel tpid value of packets												
Default	Do not modify the value.												
Mode	Policy class map configuration mode												
Usage	<p>Assign the new cos and vid value to the packets which match the class map, no command cancels the operation.</p> <p>Only modify the new value again for the classified flow that correspond the match standard.</p>												
Example	<pre>Set an external VLAN Tag' VID as 3 for the packet which satisfy c2 class rule.  Switch(config)#policy-map p1 Switch(config-policy-map-p1)#class c2 Switch(config-policy-map-p1-class-c2)#set s-vid 3 Switch(config-policy-map-p1-class-c2)#exit</pre>												

# Chapter 10 Layer 3 Interface and ARP

## 10.1 Layer 3 Interface

### 10.1.1 description

<b>Command</b>	<b>description &lt;text&gt;</b> <b>no description</b>
<b>parameter</b>	<b>text</b> is the description information of VLAN interface, the length should not exceed 256 characters
<b>default</b>	Do not configure
<b>Mode</b>	VLAN interface mode
<b>Usage Guide</b>	The description information of VLAN interface behind description and shown under the configured VLAN.
<b>Example</b>	Configure the description information of VLAN interface as test vlan. Switch(config)#interface vlan 2 Switch(config-if-vlan2)#description test vlan

## 10.1.2 interface vlan

<b>Command</b>	<code>interface vlan &lt;vlan-id&gt;</code> <code>no interface vlan &lt;vlan-id&gt;</code>
<b>parameter</b>	<i>vlan-id</i> is the VLAN ID of the established VLAN, ranging from 1 to 4094.
<b>default</b>	No Layer 3 interface is configured upon switch shipment.
<b>Mode</b>	Global Mode
<b>Usage Guide</b>	this command is used to create the 3-layer interface, no the command is used to delete the 3-layer interface.
<b>Example</b>	Create a VLAN interface (layer 3 interface). Switch(config)#interface vlan 1 Switch(Config-if-Vlan1)#

### 10.1.3 no interface IFNAME

<b>Command</b>	<b>no interface IFNAME</b>
<b>parameter</b>	<b>IFNAME</b> Interface Name
<b>default</b>	-
<b>Mode</b>	Global mode
<b>Usage Guide</b>	This command is used to delete the layer 3 interface. It can deal with the situation that the interface name is spelt in special way. IFNAME can match multiple ways, such as vlan1, Vlan1, v1, V1 and etc.
<b>Example</b>	Delete interface vlan1. (config)# no interface vlan1

### 10.1.4 show ip route

<b>Command</b>	show ip route [ database ]	
<b>parameter</b>	<b>database</b>	is database information.
<b>default</b>	-	
<b>Mode</b>	Admin Mode	

**Usage Guide** Show kernal routing table, include: routing type, destination network, mask, next-hop address, interface, etc.

**Example** shows the routing table.  
 Switch#show ip route  
 Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP  
         O - OSPF, IA - OSPF inter area  
         N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2  
         E1 - OSPF external type 1, E2 - OSPF external type 2  
         i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area  
         \* - candidate default

C       127.0.0.0/8 is directly connected, Loopback tag:0  
 Total routes are : 1 item(s)

Display information	describe
C –connected	Direct route, namely the segment directly connected with the layer 3 switch
S –static	Static route, the route manually configured by users
R - RIP derived	RIP route, acquired by layer 3 switch through the RIP protocol.
O - OSPF derived	OSPF route, acquired by layer 3 switch through the OSPF protocol
A- OSPF ASE	Route introduced by OSPF
B- BGP derived	BGP route, acquired by the BGP protocol.

## 10.2 IPv4/v6 configuration

### 10.2.1 clear ip traffic

<b>Command</b>	clear ip traffic
<b>parameter</b>	-
<b>default</b>	-
<b>Mode</b>	Admin Mode.
<b>Usage Guide</b>	Clear the statistic information of receiving and sending packets for IP kernel protocol, including the statistic of receiving packets, sending packets and dropping packets and the error information of receiving and sending packets for IP protocol, ICMP protocol, TCP protocol and UDP protocol.
<b>Example</b>	Clear statistic information of IP protocol. Switch#clear ip traffic

## 10.2.2 clear ipv6 neighbor

<b>Command</b>	clear ipv6 neighbors
<b>parameter</b>	-
<b>default</b>	-
<b>Mode</b>	Admin Mode.
<b>Usage Guide</b>	This command can not clear static neighbor
<b>Example</b>	Clear neighbor list. Switch#clear ipv6 neighbors

### 10.2.3 ip address

<b>Command</b>	<pre>ip address &lt;ip-address&gt; &lt;mask&gt; [secondary] no ip address [&lt;ip-address&gt; &lt;mask&gt;] [secondary]</pre>						
<b>parameter</b>	<table border="1"> <tr> <td><i>ip-address</i></td> <td>is IP address, dotted decimal notation;</td> </tr> <tr> <td><i>mask</i></td> <td>is subnet mask, dotted decimal notation;</td> </tr> <tr> <td><b>secondary</b></td> <td>indicates that the IP address is configured as secondary IP address.</td> </tr> </table>	<i>ip-address</i>	is IP address, dotted decimal notation;	<i>mask</i>	is subnet mask, dotted decimal notation;	<b>secondary</b>	indicates that the IP address is configured as secondary IP address.
<i>ip-address</i>	is IP address, dotted decimal notation;						
<i>mask</i>	is subnet mask, dotted decimal notation;						
<b>secondary</b>	indicates that the IP address is configured as secondary IP address.						
<b>default</b>	The system default is no IP address configuration.						
<b>Mode</b>	VLAN interface configuration mode						
<b>Usage Guide</b>	<p>This command configures IP address on VLAN interface manually. If optional parameter secondary is not configured, then it is configured as the primary IP address of VLAN interface; if optional parameter secondary is configured, then that means the IP address is the secondary IP address of VLAN. One VLAN interface can only have one primary IP address and more than one secondary IP addresses. Primary IP and Secondary IP all can be used on SNMP/Web/Telnet management. Furthermore, the switch also provides BOOTP/DHCP manner to get IP address.</p>						
<b>Example</b>	<p>The IP address of switch VLAN1 interface is set to 192.168.1.10/24.</p> <pre>Switch(Config-if-Vlan1)#ip address 192.168.1.10 255.255.255.0</pre>						



## 10.2.4 ip default-gateway

<b>Command</b>	<code>ip default-gateway &lt;A.B.C.D&gt;</code> <code>no ip default-gateway &lt;A.B.C.D&gt;</code>
<b>parameter</b>	<b>A.B.C.D</b> is gateway address, for example 10.1.1.10.
<b>default</b>	There is no default gateway.
<b>Mode</b>	Global mode.
<b>Usage Guide</b>	Configure the default gateway of the router to specify the default next hop address to which the packets will be sent.
<b>Example</b>	Specifies the default gateway. Switch(config)# ip default-gateway 10.1.1.10

## 10.2.5 ipv6 address

<b>Command</b>	<code>ipv6 address &lt;ipv6-address prefix-length&gt; [eui-64]</code> <code>no ipv6 address &lt;ipv6-address prefix-length&gt; [eui-64]</code>	
<b>parameter</b>	<b>ipv6-address</b>	is the prefix of IPv6 address, parameter
	<b>prefix-length</b>	is the prefix length of IPv6 address, which is between 3-128
	<b>eui-64</b>	means IPv6 address is generated automatically based on eui64 interface identifier of the interface.
<b>default</b>	-	
<b>Mode</b>	Interface Configuration Mode	
<b>Usage Guide</b>	<p>IPv6 address prefix cannot be multicast address or any other specific IPv6 address, and different layer 3 interfaces cannot configure the same address prefix. For global unicast address, the length of the prefix must be greater than or equal to 3. For site-local address and link-local address, the length of the prefix must be greater than or equal to 10.</p>	
<b>Example</b>	<p>Configure an IPv6 address on VLAN1 Layer 3 interface: the prefix is 2001:3f:ed8::99 and the length of the prefix is 64.</p> <pre>Switch(Config-if-Vlan1)#ipv6 address 2001:3f:ed8::99/64</pre>	

## 10.2.6 ipv6 nd dad attempts

<b>Command</b>	<code>ipv6 nd dad attempts &lt;value&gt;</code> <code>no ipv6 nd dad attempts</code>
<b>parameter</b>	<i>value</i> is the Neighbor Solicitation Message number sent in succession by Duplicate Address Detection and the value of <value> must be in 0-10, NO command restores to default value 1.
<b>default</b>	The default request message number is 1
<b>Mode</b>	Interface Configuration Mode
<b>Usage Guide</b>	When configuring an IPv6 address, it is required to process IPv6 Duplicate Address Detection, this command is used to configure the ND message number of Duplicate Address Detection to be sent, value being 0 means no Duplicate Address Detection is executed.
<b>Example</b>	The Neighbor Solicitation Message number sent in succession by interface when setting Duplicate Address Detection is 3. Switch(Config-if-Vlan1)# ipv6 nd dad attempts 3

## 10.2.7 ipv6 nd ns-interval

<b>Command</b>	<code>ipv6 nd ns-interval &lt;seconds&gt;</code> <code>no ipv6 nd ns-interval</code>
<b>parameter</b>	<b>seconds</b> is the time interval of sending Neighbor Solicitation Message, <seconds> value must be between 1-3600 seconds, no command restores the default value 1 second.
<b>default</b>	The default Request Message time interval is 1 second.
<b>Mode</b>	Interface Configuration Mode
<b>Usage Guide</b>	The value to be set will include the situation in all routing announcement on the interface. Generally, very short time interval is not recommended.
<b>Example</b>	Set Vlan1 interface to send out Neighbor Solicitation Message time interval to be 8 seconds. Switch(Config-if-Vlan1)#ipv6 nd ns-interval 8

## 10.2.8 ipv6 neighbor

<b>Command</b>	<pre>ipv6 neighbor &lt;ipv6-address&gt; &lt;hardware-address&gt; interface &lt;interface-type interface-name&gt; no ipv6 neighbor &lt;ipv6-address&gt;</pre>								
<b>parameter</b>	<table border="1"> <tr> <td><i>ipv6-address</i></td> <td>is static neighbor IPv6 address</td> </tr> <tr> <td><i>hardware-address</i></td> <td>is static neighbor hardware address</td> </tr> <tr> <td><i>interface-type</i></td> <td>is Ethernet type,</td> </tr> <tr> <td><i>interface-name</i></td> <td>is Layer 2 interface name</td> </tr> </table>	<i>ipv6-address</i>	is static neighbor IPv6 address	<i>hardware-address</i>	is static neighbor hardware address	<i>interface-type</i>	is Ethernet type,	<i>interface-name</i>	is Layer 2 interface name
<i>ipv6-address</i>	is static neighbor IPv6 address								
<i>hardware-address</i>	is static neighbor hardware address								
<i>interface-type</i>	is Ethernet type,								
<i>interface-name</i>	is Layer 2 interface name								
<b>default</b>	There is not static neighbor table entry								
<b>Mode</b>	Interface Configuration Mode								
<b>Usage Guide</b>	IPv6 address and multicast address for specific purpose and local address cannot be set as neighbor.								
<b>Example</b>	<p>Set static neighbor 2001:1:2::4 on port E1/0/1, and the hardware MAC address is 00-03-0f-89-44-bc.</p> <pre>Switch(Config-if-Vlan1)#ipv6 neighbor 2001:1:2::4 00-03-0f-89-44-bc interface Ethernet 1/0/1</pre>								

## 10.2.9 show ip interface

<b>Command</b>	<b>show ip interface [<i>&lt;ifname&gt;</i>   vlan <i>&lt;vlan-id&gt;</i>] brief</b>			
<b>parameter</b>	<b><i>ifname</i></b>	Interface name		
	<b><i>vlan-id</i></b>	VLAN ID		
<b>default</b>	Show all brief information of the configured layer 3 interface when no parameter is specified.			
<b>Mode</b>	All modes.			
<b>Usage Guide</b>	This command is used to view brief information on the configured Layer 3 interface.			
<b>Example</b>	view brief information on vlan1 interface configuration.			
	Switch#show ip interface vlan 1 brief			
	Index	Interface	IP-Address	Protocol
	11001	Vlan1	192.168.2.1	up

## 10.2.10 show ip traffic

<b>Command</b>	<b>show ip traffic</b>
<b>parameter</b>	-
<b>default</b>	-
<b>Mode</b>	Admin Mode
<b>Usage Guide</b>	Display statistics for IP, ICMP, TCP, UDP packets received/sent.
<b>Example</b>	<p>Displays statistics for IP packets.</p> <pre>Switch#show ip traffic IP statistics: Rcvd: 3249810 total, 3180 local destination 0 header errors, 0 address errors 0 unknown protocol, 0 discards Frag: 0 reassembled, 0 timeouts 0 fragment rcvd, 0 fragment dropped 0 fragmented, 0 couldn't fragment, 0 fragment sent Sent: 0 generated, 3230439 forwarded 0 dropped, 0 no route ICMP statistics: Rcvd: 0 total 0 errors 0 time exceeded 0 redirects, 0 unreachable, 0 echo, 0 echo replies 0 mask requests, 0 mask replies, 0 quench 0 parameter, 0 timestamp, 0 timestamp replies Sent: 0 total 0 errors 0 time exceeded 0 redirects, 0 unreachable, 0 echo, 0 echo replies 0 mask requests, 0 mask replies, 0 quench 0 parameter, 0 timestamp, 0 timestamp replies TCP statistics: TcpActiveOpens 0, TcpAttemptFails 0 TcpCurrEstab 0, TcpEstabResets 0 TcpInErrs 0, TcpInSegs 3180 TcpMaxConn 0, TcpOutRsts 3 TcpOutSegs 0, TcpPassiveOpens 8 TcpRetransSegs 0, TcpRtoAlgorithm 0 TcpRtoMax 0, TcpRtoMin 0 UDP statics: UdpInDatagrams 0, UdpInErrors 0</pre>

UdpNoPorts 0, UdpOutDatagrams 0

Display content	describe
IP statistics :	IP packet statistics
Rcvd: 3249810 total, 3180 local destination 0 header errors, 0 address errors 0 unknown protocol, 0 discards	Statistics of total packets received, number of packets reached local destination, number of packets have header errors, number of erroneous addresses, number of packets of unknown protocols; number of packets dropped.
Frgs : 0 reassembled, 0 timeouts 0 fragment rcvd, 0 fragment dropped 0 fragmented, 0 couldn't fragment, 0 fragment sent	Fragmentation statistics: number of packets reassembled, timeouts, fragments received, fragments discarded, packets that cannot be fragmented, number of fragments sent, etc.
Sent : 0 generated, 0 forwarded 0 dropped, 0 no route	Statistics for total packets sent, including number of local packets, forwarded packets, dropped packets and packets without route.
ICMP statistics :	ICMP packet statistics.
Rcvd : 0 total 0 errors 0 time exceeded 0 redirects, 0 unreachable, 0 echo, 0 echo replies 0 mask requests, 0 mask replies, 0 quench 0 parameter, 0 timestamp, 0 timestamp replies	Statistics of total ICMP packets received and classified information
Sent : 0 total 0 errors 0 time exceeded 0 redirects, 0 unreachable, 0 echo, 0 echo replies 0 mask requests, 0 mask replies, 0 quench 0 parameter, 0 timestamp, 0 timestamp replies	Statistics of total ICMP packets sent and classified information
TCP statistics:	TCP packet statistics.
UDP statistics:	UDP packet statistics.



## 10.2.11 show ipv6 interface

<b>Command</b>	<code>show ipv6 interface {brief &lt;interface-name&gt;}</code>
<b>parameter</b>	<p><b>brief</b> is the brief summarization of IPv6 status and configuration</p> <p><b>interface-name</b> is Layer 3 interface name</p>
<b>default</b>	-
<b>Mode</b>	Admin and Configuration Mode
<b>Usage Guide</b>	If only brief is specified, then information of all L3 is displayed, and you can also specify a specific Layer 3 interface.
<b>Example</b>	<pre>View information ipv6 the vlan1 interface. Switch#show ipv6 interface Vlan1 Vlan1 is up, line protocol is up, dev index is 2004 Device flag 0x1203(UP BROADCAST ALLMULTI MULTICAST) IPv6 is enabled Link-local address(es): fe80::203:fff:fe00:10 PERMANENT Global unicast address(es): 3001::1 subnet is 3001::1/64 PERMANENT Joined group address(es): ff02::1 ff02::16 ff02::2 ff02::5 ff02::6 ff02::9 ff02::d ff02::1:ff00:10 ff02::1:ff00:1 MTU is 1500 bytes ND DAD is enabled, number of DAD attempts is 1 ND managed_config_flag is unset ND other_config_flag is unset ND NS interval is 1 second(s) ND router advertisements is disabled ND RA min-interval is 200 second(s) ND RA max-interval is 600 second(s)</pre>

ND RA hoplimit is 64

ND RA lifetime is 1800 second(s)

ND RA MTU is 0

ND advertised reachable time is 0 millisecond(s)

ND advertised retransmit time is 0 millisecond(s)

Display content	describe
Vlan1	Layer 3 interface name
[up/up]	Layer 3 interface status
dev index	Internal index No.
fe80::203:fff:fe00:10	Automatically configured IPv6 address of Layer 3 interface
3001::1	Configured IPv6 address of Layer 3 interface

## 10.2.12 show ipv6 route

<b>Command</b>	<b>show ipv6 route [database]</b>
<b>parameter</b>	<b>database</b> is router database
<b>default</b>	-
<b>Mode</b>	Admin and Configuration Mode
<b>Usage Guide</b>	<b>show ipv6 route</b> only shows IPv6 kernal routing table (routing table in tcpip), database shows all routers except the local router.

**Example**

Display IPv6 Routing Table.

```
Switch#show ipv6 route
IPv6 Routing Table
Codes: K - kernel route, C - connected, S - static, R - RIP, O - OSPF,
       I - IS-IS, B - BGP
Timers: Uptime

C   ::1/128 via ::, Loopback, 02:55:37 tag:0
```

Display content	describe
IPv6 Routing Table	IPv6 routing table status
Codes: K - kernel route, C - connected, S - static, R - RIP, O - OSPF, I - IS-IS, B - BGP > - selected route	Abbreviation display sign of every entry

## 10.2.13 show ipv6 neighbors

<b>Command</b>	<b>show ipv6 neighbors</b> [{vlan ethernet} interface-number   interface-name   address <ipv6address>]		
<b>parameter</b>	<b>{vlan ethernet}</b>	specify the lookup based on interface	
	<b>interface-number</b>		
	<b>ipv6address</b>	specifies the lookup based on IPv6 address. It displays the whole neighbor table entry if without parameter.	
<b>default</b>	-		
<b>Mode</b>	Admin and Configuration Mode		
<b>Usage Guide</b>	Displays neighbor table information. If there are no parameters, the entire neighbor table entry is displayed.		

**Example**

Check ipv6 Neighbor Table Information.

```
Switch#show ipv6 neighbors
IPv6 neighbour unicast items: 2, valid: 1, matched: 1, incomplete: 0, delayed: 0,
    manage items: 0
```

IPv6 Address	Hardware Addr	Interface	Port
State Age-time(sec)			
fe80::d8e4:a662:88e4:dc24	00-e0-4c-21-00-34		Vlan1
Ethernet1/0/18	reachable	563	

IPv6 neighbour table: 1 entries

Display content	describe
IPv6 Address	Neighbor IPv6 address
Hardware Addr	Neighbor MAC address
Interface	Exit interface name
Port	Exit interface name
State	Neighbor status (reachable. statle. delay. probe. permanent. incomplete. unknow)

## 10.2.14 show ipv6 traffic

<b>Command</b>	<b>show ipv6 traffic</b>
<b>parameter</b>	-
<b>default</b>	-
<b>Mode</b>	Admin and Configuration Mode
<b>Usage Guide</b>	Display IPv6 transmit packet statistics.
<b>Example</b>	<p>Display IPv6 transmit packet statistics.</p> <pre>Switch#show ipv6 traffic IPv6 statistics:   Rcvd:  27 total, 21 local destination          0 header errors, 0 address errors          0 unknown protocol, 0 discards   Frags: 0 reassembled, 0 timeouts          0 fragment rcvd, 0 fragment dropped          0 fragmented, 0 couldn't fragment, 0 fragment sent   Sent:  24 generated, 0 forwarded          0 dropped, 0 no route ICMPv6 statistics:   Rcvd:  21 total, 0 errors          0 unreachable, 0 too big, 0 time exceeded, 0 parameter problems          0 echo requests, 0 echo replies          0 group queries, 0 group responses, 0 group reduces          0 router solicits, 0 router adverts, 0 redirects          9 neighbor solicits, 12 neighbor adverts   Sent:  24 total, 0 errors          0 unreachable, 0 too big, 0 time exceeded, 0 parameter problems          0 echo requests, 0 echo replies          0 group queries, 0 group responses, 0 group reduces          0 router solicits, 0 router adverts, 0 redirects          9 neighbor solicits, 9 neighbor adverts TCP statistics:   Rcvd:  0 total segments, 0 errors   Sent:  0 total segments, 0 retransmitted segments UDP statics:   Rcvd:  0 total, 0 errors, 0 no port   Sent:  0 total</pre>

Display content	describe
IPv6 statistics:	IPv6 data report statistics
Rcvd: 27 total, 21 local destination 0 header errors, 0 address errors 0 unknown protocol, 0 discards	IPv6 received packets statistics
Frgs: 0 reassembled, 0 timeouts 0 fragment rcvd, 0 fragment dropped 0 fragmented, 0 couldn't fragment, 0 fragment sent	IPv6 fragmenting statistics
Sent: 24 total, 0 errors 0 unreachable, 0 too big, 0 time exceeded, 0 parameter problems 0 echo requests, 0 echo replies 0 group queries, 0 group responses, 0 group reduces 0 router solicits, 0 router adverts, 0 redirects 9 neighbor solicits, 9 neighbor adverts	IPv6 sent packets statistics

## 10.2.15 ip route

<b>Command</b>	<pre>ip route {&lt;ip-prefix&gt; &lt;mask&gt;   &lt;ip-prefix&gt;/&lt;prefix-length&gt;} {&lt;gateway-address&gt;   null0} [&lt;distance&gt;]  no ip route {&lt;ip-prefix&gt; &lt;mask&gt;   &lt;ip-prefix&gt;/&lt;prefix-length&gt;} [&lt;gateway-address&gt;   &lt;gateway-interface&gt;] [&lt;distance&gt;]</pre>												
<b>parameter</b>	<table border="1"> <tr> <td><b><i>ip-prefix</i></b></td> <td>Routing destination address, for example :1.1.1.1</td> </tr> <tr> <td><b><i>mask</i></b></td> <td>Routing destination address subnet mask, for example :255.255.255.0</td> </tr> <tr> <td><b><i>prefix-length</i></b></td> <td>Routing destination address prefix</td> </tr> <tr> <td><b><i>gateway-address</i></b></td> <td>Address IP next hop, for example :1.1.1.1</td> </tr> <tr> <td><b><i>null0</i></b></td> <td>Forwarding interface</td> </tr> <tr> <td><b><i>distance</i></b></td> <td>Routing priority, size range :1-255</td> </tr> </table>	<b><i>ip-prefix</i></b>	Routing destination address, for example :1.1.1.1	<b><i>mask</i></b>	Routing destination address subnet mask, for example :255.255.255.0	<b><i>prefix-length</i></b>	Routing destination address prefix	<b><i>gateway-address</i></b>	Address IP next hop, for example :1.1.1.1	<b><i>null0</i></b>	Forwarding interface	<b><i>distance</i></b>	Routing priority, size range :1-255
<b><i>ip-prefix</i></b>	Routing destination address, for example :1.1.1.1												
<b><i>mask</i></b>	Routing destination address subnet mask, for example :255.255.255.0												
<b><i>prefix-length</i></b>	Routing destination address prefix												
<b><i>gateway-address</i></b>	Address IP next hop, for example :1.1.1.1												
<b><i>null0</i></b>	Forwarding interface												
<b><i>distance</i></b>	Routing priority, size range :1-255												
<b>default</b>	Default static routing has a priority of 1												
<b>Mode</b>	Global mode.												
<b>Usage Guide</b>	This command can be used to configure switch static routing. both the address and the forwarding interface are available by specifying the next hop IP the routing packet when configuring the next hop of the static route.												
<b>Example</b>	<p>Add static routing to the switch.</p> <pre>Switch(config)#ip route 192.168.2.8/24 null0</pre>												

## 10.3 ARP Configuration

### 10.3.1 arp

<b>Command</b>	<code>arp &lt;ip_address&gt; &lt;mac_address&gt; {interface [ethernet] &lt;portName&gt;}</code> <code>no arp &lt;ip_address&gt;</code>								
<b>parameter</b>	<table border="1"> <tr> <td><i>ip_address</i></td> <td>is the IP address, at the same field with interface address</td> </tr> <tr> <td><i>mac_address</i></td> <td>is the MAC address</td> </tr> <tr> <td><i>ethernet</i></td> <td>stands for Ethernet port</td> </tr> <tr> <td><i>portName</i></td> <td>for the name of layer2 port</td> </tr> </table>	<i>ip_address</i>	is the IP address, at the same field with interface address	<i>mac_address</i>	is the MAC address	<i>ethernet</i>	stands for Ethernet port	<i>portName</i>	for the name of layer2 port
<i>ip_address</i>	is the IP address, at the same field with interface address								
<i>mac_address</i>	is the MAC address								
<i>ethernet</i>	stands for Ethernet port								
<i>portName</i>	for the name of layer2 port								
<b>default</b>	No static ARP entry is set by default.								
<b>Mode</b>	VLAN Interface Mode								
<b>Usage Guide</b>	Static ARP entries can be configured in the switch.								
<b>Example</b>	Configuring static ARP for interface VLAN1. Switch(Config-if-Vlan1)#arp 1.1.1.1 00-03-0f-f0-12-34 interface eth 1/0/2								



## 10.3.2 clear arp-cache

<b>Command</b>	clear arp-cache
<b>parameter</b>	-
<b>default</b>	-
<b>Mode</b>	Admin Mode
<b>Usage Guide</b>	this command is used to clear the arp table.
<b>Example</b>	Clear the arp table. Switch#clear arp-cache

### 10.3.3 clear arp traffic

<b>Command</b>	clear arp traffic
<b>parameter</b>	-
<b>default</b>	-
<b>Mode</b>	Admin Mode
<b>Usage Guide</b>	Clear the switch ARP message statistics. box switches, this command only clears the statistics of APP messages received and sent from the current card.
<b>Example</b>	Clear switch ARP message statistics. Switch#clear arp traffic

## 10.3.4 show arp

<b>Command</b>	<b>show arp [&lt;ipaddress&gt;] [&lt;vlan-id&gt;] [&lt;hw-addr&gt;] [type {static   dynamic}] [count] [vrf word]</b>														
<b>parameter</b>	<table border="1"> <tr> <td><b>ipaddress</b></td> <td>is a specified IP address</td> </tr> <tr> <td><b>vlan-id</b></td> <td>Vlan id</td> </tr> <tr> <td><b>hw-addr</b></td> <td>for entry of specified MAC address</td> </tr> <tr> <td><b>static</b></td> <td>for static ARP entry</td> </tr> <tr> <td><b>dynamic</b></td> <td>for dynamic ARP entry</td> </tr> <tr> <td><b>count</b></td> <td>displays number of ARP entries</td> </tr> <tr> <td><b>vrf word</b></td> <td>is the specified vrf name</td> </tr> </table>	<b>ipaddress</b>	is a specified IP address	<b>vlan-id</b>	Vlan id	<b>hw-addr</b>	for entry of specified MAC address	<b>static</b>	for static ARP entry	<b>dynamic</b>	for dynamic ARP entry	<b>count</b>	displays number of ARP entries	<b>vrf word</b>	is the specified vrf name
<b>ipaddress</b>	is a specified IP address														
<b>vlan-id</b>	Vlan id														
<b>hw-addr</b>	for entry of specified MAC address														
<b>static</b>	for static ARP entry														
<b>dynamic</b>	for dynamic ARP entry														
<b>count</b>	displays number of ARP entries														
<b>vrf word</b>	is the specified vrf name														
<b>default</b>	-														
<b>Mode</b>	Admin Mode														
<b>Usage Guide</b>	Displays the content of current ARP table such as IP address, MAC address, hardware type, interface name, etc.														

**Example**

Displays the current ARP table content information.

```
Switch#show arp
ARP Unicast Items: 7, Valid: 7, Matched: 7, Verifying: 0, Incomplete: 0, Failed: 0, None: 0
```

Address	Hardware Addr	Interface	Port	Flag
50.1.1.6	00-0a-eb-51-51-38	Vlan50	Ethernet1/0/11	Dynamic
50.1.1.9	00-00-00-00-00-09	Vlan50	Ethernet1/0/1	Static
150.1.1.2	00-00-58-fc-48-9f	Vlan150	Ethernet1/0/4	Dynamic

Display content	describe
Total arp items	Total number of ARP entries.
Valid	ARP entry number matching the filter conditions and attributing the legality states.
Matched	ARP entry number matching the filter conditions.
Verifying	ARP entry number at verifying again validity for ARP
InCompleted	ARP entry number have ARP request sent without ARP reply.
Failed	ARP entry number at failed state.

None	ARP entry number at begin-found state.
Address	IP address of ARP entries.
Hardware Address	MAC address of ARP entries.
Interface	Layer 3 interface corresponding to the ARP entry.
Port	Physical (Layer2) port corresponding to the ARP entry.
Flag	Describes whether ARP entry is dynamic or static.

### 10.3.5 show arp traffic

<b>Command</b>	<b>show arp traffic</b>
<b>parameter</b>	-
<b>default</b>	-
<b>Mode</b>	Admin and Config Mode
<b>Usage Guide</b>	Display statistics information of received and sent APP messages.
<b>Example</b>	<p>Displays current ARP statistics.</p> <p>Switch#show arp traffic</p> <p>ARP statistics:</p> <p>Rcvd: 0 request, 0 response</p> <p>Sent: 0 request, 0 response</p>

## 10.4 ARP Scanning Prevention

### 10.4.1 anti-arpscan enable

---

<b>Command</b>	<b>anti-arpscan enable</b> <b>no anti-arpscan enable</b>
<b>parameter</b>	-
<b>default</b>	Disable ARP scanning prevention function.
<b>Mode</b>	Global configuration mode
<b>Usage Guide</b>	When remotely managing a switch with a method like telnet, users should set the uplink port as a Super Trust port before enabling anti-ARP-scan function, preventing the port from being shutdown because of receiving too many ARP messages. After the anti-ARP-scan function is disabled, this port will be reset to its default attribute, that is, Untrust port.
<b>Example</b>	Enable the ARP scanning prevention function of the switch. Switch(config)#anti-arpscan enable

## 10.4.2 anti-arpscan port-based threshold

<b>Command</b>	<code>anti-arpscan port-based threshold &lt;threshold-value&gt;</code> <code>no anti-arpscan port-based threshold</code>
<b>parameter</b>	<i>threshold-value</i> rate threshold, ranging from 2 to 200.
<b>default</b>	10 packets /second.
<b>Mode</b>	Global Configuration Mode
<b>Usage Guide</b>	the threshold of port-based ARP scanning prevention should be larger than the threshold of IP-based ARP scanning prevention, or, the IP-based ARP scanning prevention will fail.
<b>Example</b>	Set the threshold of port-based ARP scanning prevention as 10 packets/second. Switch(config)#anti-arpscan port-based threshold 10

### 10.4.3 anti-arpscan ip-based threshold

<b>Command</b>	<code>anti-arpscan ip-based threshold &lt;threshold-value&gt;</code> <code>no anti-arpscan ip-based threshold</code>
<b>parameter</b>	<b><i>threshold-value</i></b> rate threshold, ranging from 1 to 200.
<b>default</b>	3 packets/second.
<b>Mode</b>	Global configuration mode
<b>Usage Guide</b>	The threshold of port-based ARP scanning prevention should be larger than the threshold of IP-based ARP scanning prevention, or, the IP-based ARP scanning prevention will fail.
<b>Example</b>	Set the threshold of IP-based ARP scanning prevention as 6 packets/second. Switch(config)#anti-arpscan ip-based threshold 6

## 10.4.4 anti-arpscan trust

<b>Command</b>	<code>anti-arpscan trust [port   supertrust-port]</code> <code>no anti-arpscan trust [port   supertrust-port]</code>
<b>parameter</b>	-
<b>default</b>	By default all the ports are non- trustful.
<b>Mode</b>	Port configuration mode
<b>Usage Guide</b>	If a port is configured as a trusted port, then the ARP scanning prevention function will not deal with this port, even if the rate of received ARP messages exceeds the set threshold, this port will not be closed, but the non- trustful IP of this port will still be checked. If a port is set as a super trusted port, then neither the port nor the IP of the port will be dealt with. If the port is already closed by ARP scanning prevention, it will be opened right after being set as a trusted port.
<b>Example</b>	Set port ethernet 4/5 of the switch as a trusted port. Switch(Config-If-Ethernet4/5)# anti-arpscan trust port



## 10.4.5 anti-arpscan trust ip

<b>Command</b>	anti-arpscan trust ip <ip-address> [<netmask>] no anti-arpscan trust ip <ip-address> [<netmask>]	
<b>parameter</b>	<i>ip-address</i>	Configure trusted IP address
	<i>netmask</i>	Net mask of the IP.
<b>default</b>	By default all the IP are non-trustful. Default mask is 255.255.255.255	
<b>Mode</b>	Global configuration mode	
<b>Usage Guide</b>	If a port is configured as a trusted port, then the ARP scanning prevention function will not deal with this port, even if the rate of received ARP messages exceeds the set threshold, this port will not be closed. If the port is already closed by ARP scanning prevention, its traffic will be recovered right immediately.	
<b>Example</b>	Set 192.168.1.0/24 as trusted IP Switch(config)#anti-arpscan trust ip 192.168.1.0 255.255.255.0	

## 10.4.6 anti-arp scan recovery enable

---

<b>Command</b>	<b>anti-arp scan recovery enable</b> <b>no anti-arp scan recovery enable</b>
<b>parameter</b>	-
<b>default</b>	Enable the automatic recovery function
<b>Mode</b>	Global configuration mode
<b>Usage Guide</b>	If the users want the normal state to be recovered after a while the port is closed or the IP is disabled, they can configure this function.
<b>Example</b>	Enable the automatic recovery function of the switch. Switch(config)#anti-arp scan recovery enable

## 10.4.7 anti-arp scan recovery time

<b>Command</b>	<code>anti-arp scan recovery time &lt;seconds&gt;</code> <code>no anti-arp scan recovery time</code>
<b>parameter</b>	<b>seconds</b> Automatic recovery time, in second ranging from 5 to 86400.
<b>default</b>	300s
<b>Mode</b>	Global configuration mode
<b>Usage Guide</b>	this command is used to configure automatic recovery time, no command is used to restore default configuration.
<b>Example</b>	Set the automatic recovery time as 3600 seconds. Switch(config)#anti-arp scan recovery time 3600

## 10.4.8 anti-arpscan log enable

<b>Command</b>	<b>anti-arpscan log enable</b> <b>no anti-arpscan log enable</b>
<b>parameter</b>	-
<b>default</b>	Enable ARP scanning prevention log function.
<b>Mode</b>	Global configuration mode
<b>Usage Guide</b>	After enabling ARP scanning prevention log function, users can check the detailed information of ports being closed or automatically recovered by ARP scanning prevention or IP being disabled and recovered by ARP scanning prevention. The level of the log is "Warning".
<b>Example</b>	Enable ARP scanning prevention log function of the switch. Switch(config)#anti-arpscan log enable

## 10.4.9 anti-arpscan trap enable

<b>Command</b>	<b>anti-arpscan trap enable</b> <b>no anti-arpscan trap enable</b>
<b>parameter</b>	-
<b>default</b>	Disable ARP scanning prevention SNMP Trap function.
<b>Mode</b>	Global configuration mode
<b>Usage Guide</b>	After enabling ARP scanning prevention SNMP Trap function, users will receive Trap message whenever a port is closed or recovered by ARP scanning prevention, and whenever IP t is closed or recovered by ARP scanning prevention.
<b>Example</b>	Enable ARP scanning prevention SNMP Trap function of the switch. Switch(config)#anti-arpscan trap enable

## 10.4.10 show anti-arpscan

<b>Command</b>	<b>show anti-arpscan [trust [ip   port   supertrust-port]  prohibited [ip   port]]</b>																																																																																												
<b>parameter</b>	-																																																																																												
<b>default</b>	Display every port to tell whether it is a trusted port and whether it is closed. If the port is closed, then display how long it has been closed. Display all the trusted IP and disabled IP.																																																																																												
<b>Mode</b>	Admin Mode																																																																																												
<b>Usage Guide</b>	Use "show anti-arpscan trust port" if users only want to check trusted ports. The reset follow the same rule.																																																																																												
<b>Example</b>	<p>Check the operating state of ARP scanning prevention function after enabling it.</p> <pre>Switch#show anti-arpscan</pre> <p>Total port: 28</p> <table border="1"> <thead> <tr> <th>Name</th> <th>Port-property</th> <th>beShut</th> <th>shutTime(seconds)</th> </tr> </thead> <tbody> <tr><td>Ethernet1/0/1</td><td>untrust</td><td>N</td><td>0</td></tr> <tr><td>Ethernet1/0/2</td><td>untrust</td><td>N</td><td>0</td></tr> <tr><td>Ethernet1/0/3</td><td>untrust</td><td>N</td><td>0</td></tr> <tr><td>Ethernet1/0/4</td><td>trust</td><td>N</td><td>0</td></tr> <tr><td>Ethernet1/0/5</td><td>trust</td><td>N</td><td>0</td></tr> <tr><td>Ethernet1/0/6</td><td>untrust</td><td>N</td><td>0</td></tr> <tr><td>Ethernet1/0/7</td><td>untrust</td><td>N</td><td>0</td></tr> <tr><td>Ethernet1/0/8</td><td>untrust</td><td>N</td><td>0</td></tr> <tr><td>Ethernet1/0/9</td><td>untrust</td><td>N</td><td>0</td></tr> <tr><td>Ethernet1/0/10</td><td>untrust</td><td>N</td><td>0</td></tr> <tr><td>Ethernet1/0/11</td><td>untrust</td><td>N</td><td>0</td></tr> <tr><td>Ethernet1/0/12</td><td>untrust</td><td>N</td><td>0</td></tr> <tr><td>Ethernet1/0/13</td><td>untrust</td><td>N</td><td>0</td></tr> <tr><td>Ethernet1/0/14</td><td>untrust</td><td>N</td><td>0</td></tr> <tr><td>Ethernet1/0/15</td><td>untrust</td><td>N</td><td>0</td></tr> <tr><td>Ethernet1/0/16</td><td>untrust</td><td>N</td><td>0</td></tr> <tr><td>Ethernet1/0/17</td><td>untrust</td><td>N</td><td>0</td></tr> <tr><td>Ethernet1/0/18</td><td>untrust</td><td>N</td><td>0</td></tr> <tr><td>Ethernet1/0/19</td><td>untrust</td><td>N</td><td>0</td></tr> <tr><td>Ethernet1/0/20</td><td>untrust</td><td>N</td><td>0</td></tr> <tr><td>Ethernet1/0/21</td><td>untrust</td><td>N</td><td>0</td></tr> <tr><td>Ethernet1/0/22</td><td>untrust</td><td>N</td><td>0</td></tr> </tbody> </table>	Name	Port-property	beShut	shutTime(seconds)	Ethernet1/0/1	untrust	N	0	Ethernet1/0/2	untrust	N	0	Ethernet1/0/3	untrust	N	0	Ethernet1/0/4	trust	N	0	Ethernet1/0/5	trust	N	0	Ethernet1/0/6	untrust	N	0	Ethernet1/0/7	untrust	N	0	Ethernet1/0/8	untrust	N	0	Ethernet1/0/9	untrust	N	0	Ethernet1/0/10	untrust	N	0	Ethernet1/0/11	untrust	N	0	Ethernet1/0/12	untrust	N	0	Ethernet1/0/13	untrust	N	0	Ethernet1/0/14	untrust	N	0	Ethernet1/0/15	untrust	N	0	Ethernet1/0/16	untrust	N	0	Ethernet1/0/17	untrust	N	0	Ethernet1/0/18	untrust	N	0	Ethernet1/0/19	untrust	N	0	Ethernet1/0/20	untrust	N	0	Ethernet1/0/21	untrust	N	0	Ethernet1/0/22	untrust	N	0
Name	Port-property	beShut	shutTime(seconds)																																																																																										
Ethernet1/0/1	untrust	N	0																																																																																										
Ethernet1/0/2	untrust	N	0																																																																																										
Ethernet1/0/3	untrust	N	0																																																																																										
Ethernet1/0/4	trust	N	0																																																																																										
Ethernet1/0/5	trust	N	0																																																																																										
Ethernet1/0/6	untrust	N	0																																																																																										
Ethernet1/0/7	untrust	N	0																																																																																										
Ethernet1/0/8	untrust	N	0																																																																																										
Ethernet1/0/9	untrust	N	0																																																																																										
Ethernet1/0/10	untrust	N	0																																																																																										
Ethernet1/0/11	untrust	N	0																																																																																										
Ethernet1/0/12	untrust	N	0																																																																																										
Ethernet1/0/13	untrust	N	0																																																																																										
Ethernet1/0/14	untrust	N	0																																																																																										
Ethernet1/0/15	untrust	N	0																																																																																										
Ethernet1/0/16	untrust	N	0																																																																																										
Ethernet1/0/17	untrust	N	0																																																																																										
Ethernet1/0/18	untrust	N	0																																																																																										
Ethernet1/0/19	untrust	N	0																																																																																										
Ethernet1/0/20	untrust	N	0																																																																																										
Ethernet1/0/21	untrust	N	0																																																																																										
Ethernet1/0/22	untrust	N	0																																																																																										

---

Ethernet1/0/23	untrust	N	0
Ethernet1/0/24	untrust	N	0
Ethernet1/0/25	untrust	N	0
Ethernet1/0/26	untrust	N	0
Ethernet1/0/27	untrust	N	0
Ethernet1/0/28	untrust	N	0

No prohibited IP.

Trust IP:

192.168.1.0      255.255.255.0

## 10.5 Preventing ARP Spoofing

### 10.5.1 ip arp-security updateprotect

<b>Command</b>	<code>ip arp-security updateprotect</code> <code>no ip arp-security updateprotect</code>
<b>parameter</b>	-
<b>default</b>	ARP table automatic update.
<b>Mode</b>	Global Mode/ Interface configuration.
<b>Usage Guide</b>	Forbid ARP table automatic update, the ARP packets conflicting with current ARP item (e.g. with same IP but different MAC or port) will be dropped, the others will be received to update aging timer or create a new item; so, the current ARP item keep unchanged and the new item can still be learned.
<b>Example</b>	Automatic update of ARP table is prohibited. Switch(Config-if-Vlan1)#ip arp-security updateprotect. Switch(config)#ip arp-security updateprotect



## 10.5.2 ip arp-security learnprotect

<b>Command</b>	<code>ip arp-security learnprotect</code> <code>no ip arp-security learnprotect</code>
<b>parameter</b>	-
<b>default</b>	ARP learning enabled.
<b>Mode</b>	Global Mode/ Interface Configuration
<b>Usage Guide</b>	This command is for preventing the automatic learning and updating of ARP. Unlike ip arp-security updateprotect, once this command implemented, there will still be timeout even if the switch keeps sending Request/Reply messages.
<b>Example</b>	Prohibit IPv4 version of the ARP learning function. Switch(config)# ip arp-security learnprotect

### 10.5.3 ip arp-security convert

---

<b>Command</b>	<b>ip arp-security convert</b>
<b>parameter</b>	-
<b>default</b>	-
<b>Mode</b>	Global Mode/ Interface configuration

---

<b>Usage Guide</b>	This command will convert the dynamic ARP entries to static ones, which, in combination with disabling automatic learning, can prevent ARP binding. Once implemented, this command will lose its effect.
--------------------	--

---

<b>Example</b>	To change all dynamic ARP to static ARP. Switch(config)#ip arp -security convert
----------------	---

## 10.5.4 clear ip arp dynamic

<b>Command</b>	clear ip arp dynamic
<b>parameter</b>	-
<b>default</b>	-
<b>Mode</b>	Interface Configuration
<b>Usage Guide</b>	This command will clear dynamic entries before binding ARP. Once implemented, this command will lose its effect.
<b>Example</b>	Clear all dynamic ARP. on the interface. Switch(Config-if-Vlan1)#clear ip arp dynamic

## 10.5.5 clear ipv6 nd dynamic

<b>Command</b>	clear ipv6 nd dynamic
<b>parameter</b>	-
<b>default</b>	-
<b>Mode</b>	Vlan Interface Mode
<b>Usage Guide</b>	It used in dynamic table when use ND bind function to clear. After executeit, the command will be useless.
<b>Example</b>	Clear all dynamic ND. in ports. Switch(Config-if-Vlan1)#clear ipv6 nd dynamic

## 10.6 ARP GUARD

### 10.6.1 arp-guard ip

<b>Command</b>	<pre>arp-guard ip &lt;addr&gt; no arp-guard ip &lt;addr&gt;</pre>
<b>parameter</b>	<p><b>Addr</b> is the protected IP address, in dotted decimal notation</p>
<b>default</b>	There is no ARP GUARD address by default
<b>Mode</b>	Port configuration mode
<b>Usage Guide</b>	<p>After configuring the ARP GUARD address, the ARP messages received from the ports configured ARP GUARD will be filtered. If the source IP addresses of the ARP message match the ARP GUARD address configured on this port, these messages will be judged as ARP cheating messages, which will be directly dropped instead of sending to the CPU of the switch or forwarding. 16 ARP GUARD addresses can be configured on each port.</p>
<b>Example</b>	<pre>Configure the ARP GUARD address on port ethernet1/0/1 as 100.1.1.1 switch(config)#interface ethernet1/0/1 switch(Config-If-Ethernet 1/0/1)#arp-guard ip 100.1.1.1</pre>

## 10.7 Gratuitous ARP Configuration

### 10.7.1 ip gratuitous-arp

<b>Command</b>	<pre>ip gratuitous-arp [&lt;interval-time&gt;] no ip gratuitous-arp</pre>
<b>parameter</b>	<p><i>interval-time</i> is the update interval for gratuitous ARP with its value limited between 5 and 1200 seconds and with default value as 300 seconds.</p>
<b>default</b>	Gratuitous ARP is disabled by default.
<b>Mode</b>	Global configuration mode and vlan interface configuration mode
<b>Usage Guide</b>	<p>When configuring gratuitous ARP in global configuration mode, all the Layer 3 interfaces in the switch will be enabled to send gratuitous ARP request. If gratuitous ARP is configured in interface configuration mode, then only the specified interface is able to send gratuitous ARP requests. When configuring the gratuitous ARP, the update interval configuration from interface configuration mode has higher preference than that from the global configuration mode.</p>
<b>Example</b>	<p>To enable gratuitous ARP in global configuration mode, and set the update interval to be 400 seconds.</p> <pre>Switch#config Switch(config)#ip gratuitous-arp 400</pre>

## 10.7.2 show ip gratuitous-arp

<b>Command</b>	<code>show ip gratuitous-arp [interface vlan &lt;vlan-id&gt;]</code>
<b>parameter</b>	<b><i>vlan-id</i></b> VLAN ID
<b>default</b>	-
<b>Mode</b>	All the Configuration Modes.
<b>Usage Guide</b>	Displays gratuitous ARP configuration information.
<b>Example</b>	Displays gratuitous ARP configuration information. Switch#show ip gratuitous-arp Gratuitous ARP send is Global enabled, Interval-Time is 300(s) Gratuitous ARP send enabled interface vlan information: Name Interval-Time(seconds) Vlan1 400 Vlan10 350

## 10.8 Dynamic ARP Inspection

### 10.8.1 ip arp inspection

<b>Command</b>	<pre>ip arp inspection vlan &lt;vlan-id&gt; no ip arp inspection vlan &lt;vlan-id&gt;</pre>
<b>parameter</b>	<p><b>vlan-id</b> is the vlan which is enabled the dynamic ARP inspection function</p>
<b>default</b>	Disable.
<b>Mode</b>	Global Mode.
<b>Usage Guide</b>	<p>After configured the dynamic ARP inspection function in global mode, the administrator can intercept, record and drop the ARP data packets which have the invalid MAC address/IP address.</p>
<b>Example</b>	<p>Enable the dynamic ARP inspection function of vlan10.</p> <pre>Switch(config)# Switch(config)#ip arp inspection vlan 10 Switch(config)#exit</pre>



## 10.8.2 ip arp inspection trust

<b>Command</b>	<b>ip arp inspection trust</b> <b>no ip arp inspection trust</b>
<b>parameter</b>	-
<b>default</b>	All the ports are the untrusted ports as default.
<b>Mode</b>	Port Mode
<b>Usage Guide</b>	After configured this command under the port mode, the configured port will not inspect the received ARP packet and it will forward it directly. If the ARP data packet is received from the untrusted port, the switch will only forward the lawful data packet. For the illegal data, it will drop the data directly and record this action.
<b>Example</b>	Configure the port 1/0/1 as the trusted port. Switch(config)# Switch(config)#in e 1/0/1 Switch(config-if-ethernet1/0/1)#ip arp inspection trust

### 10.8.3 ip arp inspection limit-rate

<b>Command</b>	<code>ip arp inspection limit-rate &lt;rate&gt;</code> <code>no ip arp inspection limit-rate</code>
<b>parameter</b>	<b>rate</b> is the configured limited rate of the ARP packet of the untrusted port, the unit is pps
<b>default</b>	Do not limit the rate for the ARP packets of the trusted or untrusted ports.
<b>Mode</b>	Port Mode
<b>Usage Guide</b>	This command can limit the ARP packet rate of the untrusted port. The rate of the lawful ARP data packets forwarding is in the limited range.
<b>Example</b>	Configure the rate of the ARP packet of the untrusted port 1/0/1 as 100pps. Switch(config)# Switch(config)#in e 1/0/1 Switch(config-if-ethernet1/0/1)# ip arp inspection limit-rate 100 Switch(config-if-ethernet1/0/1)#exit

# Chapter 11 DHCP Server Configuration

## 11.1 DHCP

### 11.1.1 bootfile

<b>Syntax</b>	<b>Bootfile &lt;filename&gt;</b> <b>no bootfile</b>
<b>Parameter</b>	<b>&lt;filename&gt;</b> name of the file to be imported, up to 255 characters are allowed.
<b>Default</b>	None
<b>Mode</b>	DHCP Address Pool Mode
<b>Usage</b>	Specify the name of the file to be imported for the client. This is usually used for diskless workstations that need to download a configuration file from the server on boot up. This command is together with the "next sever".
<b>Example</b>	The path and filename for the file to be imported is "temp\nos.img" Switch#config Switch(config)#ip dhcp pool 1 Switch(dhcp-1-config)#bootfile \temp\nos.img

## 11.1.2 clear ip dhcp binding

<b>Syntax</b>	<b>clear ip dhcp binding (&lt;A.B.C.D&gt;   all)</b>
<b>Parameter</b>	<b>&lt;A.B.C.D&gt;</b> IP address that has a binding record in decimal format <b>all</b> all IP addresses that have a binding record
<b>Default</b>	None
<b>Mode</b>	Admin Mode
<b>Usage</b>	“ <b>show ip dhcp binding</b> ” command can be used to view binding information for IP addresses and corresponding DHCP client hardware addresses. If the DHCP server is informed that a DHCP client is not using the assigned IP address for some reason before the lease period expires, the DHCP server would not remove the binding information automatically. The system administrator can use this command to delete that IP address-client hardware address binding manually, if “all” is specified, then all auto binding records will be deleted, thus all addresses in the DHCP address pool will be reallocated.
<b>Example</b>	Removing all IP-hardware address binding records Switch#clear ip dhcp binding all

### 11.1.3 clear ip dhcp conflict

<b>Syntax</b>	<code>clear ip dhcp binding (&lt;A.B.C.D&gt;   all)</code>
<b>Parameter</b>	<code>&lt;A.B.C.D&gt;</code> IP address that has a conflict record;
	<code>all</code> All stands for all addresses that have conflict records.
<b>Default</b>	None
<b>Mode</b>	Admin Mode
<b>Usage</b>	<p>show ip dhcp conflict" command can be used to check which IP addresses are conflicting for use. The "clear ip dhcp conflict" command can be used to delete the conflict record for an address. If "all" is specified, then all conflict records in the log will be removed. When records are removed from the log, the addresses are available for allocation by the DHCP server</p>
<b>Example</b>	<p>The network administrator finds 10.1.128.160 that has a conflict record in the log and is no longer used by anyone, so he deletes the record from the address conflict log.</p> <pre>Switch#clear ip dhcp conflict 10.1.128.160</pre>

### 11.1.4 clear ip dhcp server statistics

<b>Syntax</b>	<code>clear ip dhcp server statistics</code>
<b>Parameter</b>	None
<b>Default</b>	None
<b>Mode</b>	Admin Mode
<b>Usage</b>	DHCP count statistics can be viewed with “ <b>show ip dhcp server statistics</b> ” command, all information is accumulated. You can use the “ <b>clear ip dhcp server statistics</b> ” command to clear the count for easier statistics checking
<b>Example</b>	Clearing the count for DHCP server. Switch#clear ip dhcp server statistics

### 11.1.5 client-identifier

<b>Syntax</b>	<b>client-identifier &lt;unique-identifier&gt;</b> <b>no client-identifier</b>
<b>Parameter</b>	<b>&lt;unique-identifier&gt;</b> user identifier, in dotted Hex format
<b>Default</b>	None
<b>Mode</b>	DHCP Address Pool Mode
<b>Usage</b>	This command is used with "host" when binding an address manually. If the requesting client identifier matches the specified identifier, DHCP server assigns the IP address defined in "host" command to the client.
<b>Example</b>	Specifying the IP address 10.1.128.160 to be bound to user with the unique id of 00-10-5a-60-af-12 in manual address binding. Switch#config Switch(config)#ip dhcp pool 1 Switch(dhcp-1-config)#client-identifier 00-10-5a-60-af-12 Switch(dhcp-1-config)#host 10.1.128.160 24

## 11.1.6 default-router

<b>Syntax</b>	<code>default-router &lt;A.B.C.D&gt; [&lt;A.B.C.D&gt;[...&lt;A.B.C.D&gt;]]</code> <code>no default-router</code>
<b>Parameter</b>	<code>&lt;A.B.C.D&gt;</code> IP addresses, in decimal format.
<b>Default</b>	No default gateway is configured for DHCP clients by default.
<b>Mode</b>	DHCP Address Pool Mode
<b>Usage</b>	The IP address of default gateway(s) should be in the same subnet as the DHCP client IP, the switch supports up to 8 gateway addresses. The gateway address assigned first has the highest priority, and therefore address1 has the highest priority, and address2 has the second, and so on.
<b>Example</b>	Configuring the default gateway for DHCP clients to be 10.1.128.2 and 10.1.128.100. Switch#config Switch(config) # ip dhcp pool 1 Switch(dhcp-1-config)#default-router 10.1.128.2 10.1.128.100



## 11.1.7 dns-server

---

<b>Syntax</b>	<code>dns-server &lt;A.B.C.D&gt; [&lt;A.B.C.D&gt;[...&lt;A.B.C.D&gt;]]</code> <code>no dns-server</code>
<b>Parameter</b>	<code>&lt;A.B.C.D&gt;</code> IP addresses, in decimal format.
<b>Default</b>	No DNS server is configured for DHCP clients by default.
<b>Mode</b>	DHCP Address Pool Mode
<b>Usage</b>	Up to 8 DNS server addresses can be configured. The DNS server address assigned first has the highest priority, therefore address 1 has the highest priority, and address 2 has the second, and so on.
<b>Example</b>	Set 10.1.128.2 as the DNS server address for DHCP clients. Switch#config Switch(config) # ip dhcp pool 1 Switch(dhcp-1-config)#dns-server 10.1.128.2

---

## 11.1.8 domain-name

<b>Syntax</b>	<b>domain-name &lt;domain&gt;</b> <b>no domain-name</b>
<b>Parameter</b>	<b>&lt;domain&gt;</b> domain name, up to 255 characters are allowed.
<b>Default</b>	None
<b>Mode</b>	DHCP Address Pool Mode
<b>Usage</b>	Specifies a domain name for the client.
<b>Example</b>	Specifying "switch.com.cn" as the DHCP clients' domain name. Switch#config Switch(config)#ip dhcp pool 1 Switch(dhcp-1-config)#domain-name switch.com.cn

## 11.1.9 hardware-address

<b>Syntax</b>	<code>hardware-address &lt;hardware-address&gt; [Ethernet   IEEE802   &lt;type-number&gt; ]</code> <code>no hardware-address</code>						
<b>Parameter</b>	<table border="0"> <tr> <td><code>&lt;hardware-address&gt;</code></td> <td>hardware address in Hex</td> </tr> <tr> <td><code>Ethernet   IEEE802</code></td> <td>Ethernet protocol type</td> </tr> <tr> <td><code>&lt;type-number&gt;</code></td> <td>RFC number defined for protocol types, from 1 to 255, e.g., 0 for Ethernet and 6 for IEEE 802.</td> </tr> </table>	<code>&lt;hardware-address&gt;</code>	hardware address in Hex	<code>Ethernet   IEEE802</code>	Ethernet protocol type	<code>&lt;type-number&gt;</code>	RFC number defined for protocol types, from 1 to 255, e.g., 0 for Ethernet and 6 for IEEE 802.
<code>&lt;hardware-address&gt;</code>	hardware address in Hex						
<code>Ethernet   IEEE802</code>	Ethernet protocol type						
<code>&lt;type-number&gt;</code>	RFC number defined for protocol types, from 1 to 255, e.g., 0 for Ethernet and 6 for IEEE 802.						
<b>Default</b>	The default protocol type is Ethernet						
<b>Mode</b>	DHCP Address Pool Mode						
<b>Usage</b>	This command is used with the "host" when binding address manually. If the requesting client hardware address matches the specified hardware address, the DHCP server assigns the IP address defined in "host" command to the client.						
<b>Example</b>	<p>Specify IP address 10.1.128.160 to be bound to the user with hardware address 00-00-e2-3a-26-04 in manual address binding.</p> <pre>Switch#config Switch(config)#ip dhcp pool 1 Switch(dhcp-1-config)#hardware 00-00-e2-3a-26-04 Switch(dhcp-1-config)#host 10.1.128.160 24</pre>						

## 11.1.10 host

<b>Syntax</b>	<code>host &lt;address&gt; [&lt;mask&gt;   &lt;prefix-length&gt;]</code> <code>no host</code>						
<b>Parameter</b>	<table border="1"> <tr> <td><code>&lt;address&gt;</code></td> <td>IP address in decimal format</td> </tr> <tr> <td><code>&lt;mask&gt;</code></td> <td>subnet mask in decimal format</td> </tr> <tr> <td><code>&lt;prefix-length&gt;</code></td> <td>mask is indicated by prefix. For example, mask 255.255.255.0 in prefix is "24", and mask 255.255.255.252 in prefix is "30".</td> </tr> </table>	<code>&lt;address&gt;</code>	IP address in decimal format	<code>&lt;mask&gt;</code>	subnet mask in decimal format	<code>&lt;prefix-length&gt;</code>	mask is indicated by prefix. For example, mask 255.255.255.0 in prefix is "24", and mask 255.255.255.252 in prefix is "30".
<code>&lt;address&gt;</code>	IP address in decimal format						
<code>&lt;mask&gt;</code>	subnet mask in decimal format						
<code>&lt;prefix-length&gt;</code>	mask is indicated by prefix. For example, mask 255.255.255.0 in prefix is "24", and mask 255.255.255.252 in prefix is "30".						
<b>Default</b>	None						
<b>Mode</b>	DHCP Address Pool Mode						
<b>Usage</b>	<p>If no mask or prefix is configured when configuring the IP address, and no information in the IP address pool indicates anything about the mask, the system will assign a mask automatically according to the IP address class.</p> <p>This command is used with "hardware address" command or "client identifier" command when binding addresses manually. If the identifier or hardware address of the requesting client matches the specified identifier or hardware address, the DHCP server assigns the IP address defined in "host" command to the client.</p>						
<b>Example</b>	<p>Specifying IP address 10.1.128.160 to be bound to user with hardware address 00-10-5a-60-af-12 in manual address binding.</p> <pre>Switch#config Switch(config)#ip dhcp pool 1 Switch(dhcp-1-config)#hardware-address 00-10-5a-60-af-12 Switch(dhcp-1-config)#host 10.1.128.160 24</pre>						

### 11.1.11 ip dhcp conflict logging

<b>Syntax</b>	<b>ip dhcp conflict logging</b> <b>no ip dhcp conflict logging</b>
<b>Parameter</b>	none
<b>Default</b>	Logging for address conflict is enabled by default.
<b>Mode</b>	Global Mode
<b>Usage</b>	When logging is enabled, once the address conflict is detected by the DHCP server, the conflicting address will be logged. Addresses present in the log for conflicts will not be assigned dynamically by the DHCP server until the conflicting records are deleted.
<b>Example</b>	Disable logging for DHCP server. Switch#config Switch(config)#no ip dhcp conflict logging

### 11.1.12 ip dhcp disable

<b>Syntax</b>	<code>ip dhcp disable</code> <code>no ip dhcp disable</code>
<b>Parameter</b>	none
<b>Default</b>	Enable
<b>Mode</b>	Port mode
<b>Usage</b>	After the port disables DHCP services, directly drop all DHCP packets sent by the port.
<b>Example</b>	The port disables DHCP services. Switch#config Switch(config)#interface ethernet 1/0/1 Switch(config-if-ethernet1/0/1)#ip dhcp disable

### 11.1.13 ip dhcp excluded-address

---

<b>Syntax</b>	<code>ip dhcp excluded-address &lt;low-address&gt; [&lt;high-address&gt;]</code> <code>no ip dhcp excluded-address &lt;low-address&gt; [&lt;high-address&gt;]</code>
<b>Parameter</b>	<code>&lt;low-address&gt;</code> starting IP address <code>&lt;high-address&gt;</code> ending IP address
<b>Default</b>	Only individual address is excluded by default
<b>Mode</b>	Global Mode
<b>Usage</b>	This command can be used to exclude one or several consecutive addresses in the pool from being assigned dynamically so that those addresses can be used by the administrator for other purposes.
<b>Example</b>	Reserving addresses 1.1.1.1 from dynamic assignment. Switch#config Switch(config)#ip dhcp excluded-address 1.1.1.1

---

### 11.1.14 ip dhcp pool

---

<b>Syntax</b>	<code>ip dhcp pool &lt;name&gt;</code> <code>no ip dhcp pool &lt;name&gt;</code>
<b>Parameter</b>	<code>&lt;name&gt;</code> address pool name, up to 32 characters are allowed
<b>Default</b>	None
<b>Mode</b>	Global Mode
<b>Usage</b>	This command is used to configure a DHCP address pool under Global
<b>Example</b>	Defining an address pool named "1". Switch#config Switch(config)#ip dhcp pool 1 Switch(dhcp-1-config)#

---



### 11.1.15 ip dhcp conflict ping-detection enable

<b>Syntax</b>	<code>ip dhcp conflict ping-detection enable</code> <code>no ip dhcp conflict ping-detection enable</code>
<b>Parameter</b>	None
<b>Default</b>	By default, Ping-detection of conflict is disabled.
<b>Mode</b>	Global Mode
<b>Usage</b>	To enable Ping-detection of conflict, one should enable the log of conflict addresses, when which is disabled, so will the ping-detection of conflict. When a client is unable to receive Ping request messages (when blocked by firewall, for example), this function will check local ARP according to allocated IP: if a designated IP has a corresponding ARP, then an address conflict exists; otherwise, allocate it to the client.
<b>Example</b>	Enable Ping-detection of conflict. Switch#config Switch(config)#ip dhcp conflict ping-detection enable

### 11.1.16 ip dhcp ping packets

<b>Syntax</b>	<b>ip dhcp ping packets &lt;request-num&gt;</b> <b>no ip dhcp ping packets</b>
<b>Parameter</b>	<request num>                      number of Ping request message to be sent in Ping-detection of conflict.
<b>Default</b>	No more than 2 Ping request messages will be sent by default.
<b>Mode</b>	Global Mode
<b>Usage</b>	Set the max number of Ping request (Echo Request) message to be sent in Ping-detection of conflict on DHCP server, whose default value is 2; the no operation of this command will restore the default value.
<b>Example</b>	Set the max number of Ping request (Echo Request) message to be sent in Ping-detection of conflict on DHCP server as 3.  Switch#config Switch(config)#ip dhcp ping packets 3

### 11.1.17 ip dhcp ping timeout

<b>Syntax</b>	ip dhcp ping timeout <timeout-value> no ip dhcp ping timeout
<b>Parameter</b>	<timeout-value>      <timeout-value> is the timeout period of waiting for a reply message after each Ping request message in Ping-detection of conflict.
<b>Default</b>	The timeout period is 500ms by default.
<b>Mode</b>	Global Mode
<b>Usage</b>	Set the timeout period (in ms) of waiting for a reply message (Echo Request) after each Ping request message (Echo Request) in Ping-detection of conflict on DHCP server, whose default value is 500ms. The no operation of this command will restore the default value.
<b>Example</b>	Set the timeout period (in ms) of waiting for each reply message (Echo Request) in Ping-detection of conflict on DHCP server as 600ms.  Switch#config Switch(config)#ip dhcp ping timeout 600

### 11.1.18 lease

<b>Syntax</b>	lease (<days> [<hours>][<minutes>]   infinite ) no lease								
<b>Parameter</b>	<table border="1"> <tr> <td>&lt;days&gt;</td> <td>number of days from 0 to 365;</td> </tr> <tr> <td>&lt;hours&gt;</td> <td>number of hours from 0 to 23</td> </tr> <tr> <td>&lt;minutes&gt;</td> <td>number of minutes from 0 to 59</td> </tr> <tr> <td>infinite</td> <td>perpetual use</td> </tr> </table>	<days>	number of days from 0 to 365;	<hours>	number of hours from 0 to 23	<minutes>	number of minutes from 0 to 59	infinite	perpetual use
<days>	number of days from 0 to 365;								
<hours>	number of hours from 0 to 23								
<minutes>	number of minutes from 0 to 59								
infinite	perpetual use								
<b>Default</b>	The default lease duration is 1 day.								
<b>Mode</b>	DHCP Address Pool Mode								
<b>Usage</b>	DHCP is the protocol to assign network addresses dynamically instead of permanently, hence the introduction of lease duration. Lease settings should be decided based on network conditions: too long lease duration offsets the flexibility of DHCP, while too short duration results in increased network traffic and overhead. The default lease duration of switch is 1 day.								
<b>Example</b>	<p>Setting the lease of DHCP pool "sd" to 3 days 12 hours and 30 minutes.</p> <pre>Switch#config Switch(config)#ip dhcp pool sd Switch(dhcp-sd-config)#lease 3 12 30</pre>								

## 11.1.19 max-lease-time

<b>Syntax</b>	max-lease-time (<days> [<hours>][<minutes>]   infinite ) no max-lease-time								
<b>Parameter</b>	<table border="1"> <tr> <td>&lt;days&gt;</td> <td>number of days from 0 to 365;</td> </tr> <tr> <td>&lt;hours&gt;</td> <td>number of hours from 0 to 23</td> </tr> <tr> <td>&lt;minutes&gt;</td> <td>number of minutes from 0 to 59</td> </tr> <tr> <td>infinite</td> <td>perpetual use</td> </tr> </table>	<days>	number of days from 0 to 365;	<hours>	number of hours from 0 to 23	<minutes>	number of minutes from 0 to 59	infinite	perpetual use
<days>	number of days from 0 to 365;								
<hours>	number of hours from 0 to 23								
<minutes>	number of minutes from 0 to 59								
infinite	perpetual use								
<b>Default</b>	The default lease time is 1 day.								
<b>Mode</b>	DHCP Address Pool Mode								
<b>Usage</b>	This command is used to DHCP request packets with option51. If the lease time (user requests the address) exceeds the maximum lease time configured, the lease that DHCP server assigns the address is the maximum lease time configured. If the lease time requested by the user is less than the maximum lease time configured, the lease that DHCP server assigns the address is the lease time requested by the user. The maximum lease time is able to be set by the administrator according to the actual network condition, and the maximum lease time is 1 day by default.								
<b>Example</b>	<p>Set the maximum lease time of DHCP address pool1 to 3 days 12 hours and 30 minutes.</p> <pre>Switch#config Switch(config)#ip dhcp pool 1 Switch(dhcp-1-config)#max-lease-time 3 12 30</pre>								

## 11.1.20 netbios-name-server

<b>Syntax</b>	<code>netbios-name-server &lt;address1&gt; [address2[...&lt;address8&gt;]]</code> <code>no netbios-name-server</code>
<b>Parameter</b>	<code>&lt;address1&gt;...&lt;address8&gt;</code> IP addresses, in decimal format.
<b>Default</b>	No WINS server is configured by default.
<b>Mode</b>	DHCP Address Pool Mode
<b>Usage</b>	This command is used to specify WINS server for the client, up to 8 WINS server addresses can be configured. The WINS server address assigned first has the highest priority. Therefore, address 1 has the highest priority, and address 2 the second, and so on.
<b>Example</b>	Setting the server address of DHCP pool "1" to 192.168.1.1. Switch#config Switch(config)#ip dhcp pool 1 Switch(dhcp-1-config)#netbios-name-server 192.168.1.1

## 11.1.21 netbios-node-type

<b>Syntax</b>	<code>netbios-node-type {b-node   h-node   m-node   p-node   &lt;type-number&gt;}</code> <code>no netbios-node-type</code>										
<b>Parameter</b>	<table border="1"> <tr> <td><b>b-node</b></td> <td>broadcasting node</td> </tr> <tr> <td><b>h-node</b></td> <td>hybrid node that broadcasts after point-to-point communication</td> </tr> <tr> <td><b>m-node</b></td> <td>hybrid node to communicate in point-to-point after broadcast;</td> </tr> <tr> <td><b>p-node</b></td> <td>point-to-point node</td> </tr> <tr> <td><b>&lt;type-number&gt;</b></td> <td>node type in Hex from 0 to FF</td> </tr> </table>	<b>b-node</b>	broadcasting node	<b>h-node</b>	hybrid node that broadcasts after point-to-point communication	<b>m-node</b>	hybrid node to communicate in point-to-point after broadcast;	<b>p-node</b>	point-to-point node	<b>&lt;type-number&gt;</b>	node type in Hex from 0 to FF
<b>b-node</b>	broadcasting node										
<b>h-node</b>	hybrid node that broadcasts after point-to-point communication										
<b>m-node</b>	hybrid node to communicate in point-to-point after broadcast;										
<b>p-node</b>	point-to-point node										
<b>&lt;type-number&gt;</b>	node type in Hex from 0 to FF										
<b>Default</b>	No client node type is specified by default.										
<b>Mode</b>	DHCP Address Pool Mode										
<b>Usage</b>	If client node type is to be specified, it is recommended to set the client node type to h-node that broadcasts after point-to-point communication.										
<b>Example</b>	<p>Setting the node type for client of pool 1 to broadcasting node.</p> <pre>Switch#config Switch(config)#ip dhcp pool 1 Switch(dhcp-1-config)#netbios-node-type-node</pre>										

## 11.1.22 network-address

<b>Syntax</b>	<code>network-address &lt;network-number&gt; [&lt;mask&gt;   &lt;prefix-length&gt;]</code> <code>no network-address</code>						
<b>Parameter</b>	<table border="1"> <tr> <td><code>&lt;network-number&gt;</code></td> <td>network number;</td> </tr> <tr> <td><code>&lt;mask&gt;</code></td> <td>subnet mask in the decimal format</td> </tr> <tr> <td><code>&lt;prefix-length&gt;</code></td> <td>mask in prefix form. For example, mask 255.255.255.0 in prefix is "24", and mask 255.255.255.252 in prefix is "30". Note: When using DHCP server, the pool mask should be longer or equal to that of layer 3 interface IP address in the corresponding segment.</td> </tr> </table>	<code>&lt;network-number&gt;</code>	network number;	<code>&lt;mask&gt;</code>	subnet mask in the decimal format	<code>&lt;prefix-length&gt;</code>	mask in prefix form. For example, mask 255.255.255.0 in prefix is "24", and mask 255.255.255.252 in prefix is "30". Note: When using DHCP server, the pool mask should be longer or equal to that of layer 3 interface IP address in the corresponding segment.
<code>&lt;network-number&gt;</code>	network number;						
<code>&lt;mask&gt;</code>	subnet mask in the decimal format						
<code>&lt;prefix-length&gt;</code>	mask in prefix form. For example, mask 255.255.255.0 in prefix is "24", and mask 255.255.255.252 in prefix is "30". Note: When using DHCP server, the pool mask should be longer or equal to that of layer 3 interface IP address in the corresponding segment.						
<b>Default</b>	If no mask is specified, default mask will be assigned according to the address class.						
<b>Mode</b>	DHCP Address Pool Mode						
<b>Usage</b>	This command sets the scope of addresses that can be used for dynamic assignment by the DHCP server; one address pool can only have one corresponding segment. This command is exclusive with the manual address binding command "hardware address" and "host".						
<b>Example</b>	<p>Configuring the assignable address in pool 1 to be 10.1.128.0/24.</p> <pre>Switch#config Switch(config)#ip dhcp pool 1 Switch(dhcp-1-config)#network-address 10.1.128.0 24</pre>						



### 11.1.23 next-server

<b>Syntax</b>	<code>next-server &lt;address1&gt;[&lt;address2&gt;[...&lt;address8&gt;]]</code> <code>no next-server</code>
<b>Parameter</b>	<code>&lt;address1&gt;...&lt;address8&gt;</code> IP addresses, in the decimal format
<b>Default</b>	None
<b>Mode</b>	DHCP Address Pool Mode
<b>Usage</b>	This command configures the address for the server hosting client import file. This is usually used for diskless workstations that need to download configuration files from the server on boot up. This command is used together with "bootfile".
<b>Example</b>	Setting the hosting server address as 10.1.128.4. Switch#config Switch(config)#ip dhcp pool 1 Switch(dhcp-1-config)#next-server 10.1.128.4

## 11.1.24 option

<b>Syntax</b>	<code>option &lt;code&gt; {ascii &lt;string&gt;   hex &lt;hex&gt;   ipaddress &lt;ipaddress&gt;}</code> <code>no option &lt;code&gt;</code>								
<b>Parameter</b>	<table border="1"> <tr> <td><code>&lt;code&gt;</code></td> <td>code for network parameters</td> </tr> <tr> <td><code>&lt;string&gt;</code></td> <td>ASCII string up to 255 characters</td> </tr> <tr> <td><code>&lt;hex&gt;</code></td> <td>a value in Hex that is no greater than 510 and must be of even length</td> </tr> <tr> <td><code>&lt;ipaddress&gt;</code></td> <td>IP address in decimal format, up to 63 IP addresses can be configured.</td> </tr> </table>	<code>&lt;code&gt;</code>	code for network parameters	<code>&lt;string&gt;</code>	ASCII string up to 255 characters	<code>&lt;hex&gt;</code>	a value in Hex that is no greater than 510 and must be of even length	<code>&lt;ipaddress&gt;</code>	IP address in decimal format, up to 63 IP addresses can be configured.
<code>&lt;code&gt;</code>	code for network parameters								
<code>&lt;string&gt;</code>	ASCII string up to 255 characters								
<code>&lt;hex&gt;</code>	a value in Hex that is no greater than 510 and must be of even length								
<code>&lt;ipaddress&gt;</code>	IP address in decimal format, up to 63 IP addresses can be configured.								
<b>Default</b>	none								
<b>Mode</b>	DHCP Address Pool Mode								
<b>Usage</b>	The switch provides common commands for network parameter configuration as well as various commands useful in network configuration to meet different user needs. The definition of option code is described in detail in RFC2123.								
<b>Example</b>	Setting the WWW server address as 10.1.128.240. <pre>Switch#config Switch(config)# ip dhcp pool 1 Switch(dhcp-1-config)#option 72 ip 10.1.128.240</pre>								

## 11.1.25 service dhcp

<b>Syntax</b>	<code>service dhcp</code> <code>no service dhcp</code>
<b>Parameter</b>	None
<b>Default</b>	DHCP service is disabled by default.
<b>Mode</b>	Global Mode
<b>Usage</b>	Both DHCP server and DHCP relay are included in the DHCP service. When DHCP services are enabled, both DHCP server and DHCP relay are enabled. Switch can only assign IP address for the DHCP clients and enable DHCP relay when DHCP server function is enabled.
<b>Example</b>	Enabling DHCP server. Switch#config Switch(config)#service dhcp

## 11.1.26 show ip dhcp binding

<b>Syntax</b>	<code>show ip dhcp binding [[&lt;ip-addr&gt;] [type {all   manual   dynamic}] [count] ]</code>										
<b>Parameter</b>	<table border="1"> <tr> <td><code>&lt;ip-addr&gt;</code></td> <td>a specified IP address in decimal format</td> </tr> <tr> <td><code>all</code></td> <td>all binding types (manual binding and dynamic assignment)</td> </tr> <tr> <td><code>manual</code></td> <td>manual binding</td> </tr> <tr> <td><code>dynamic</code></td> <td>dynamic assignment</td> </tr> <tr> <td><code>count</code></td> <td>displays statistics for DHCP address binding entries.</td> </tr> </table>	<code>&lt;ip-addr&gt;</code>	a specified IP address in decimal format	<code>all</code>	all binding types (manual binding and dynamic assignment)	<code>manual</code>	manual binding	<code>dynamic</code>	dynamic assignment	<code>count</code>	displays statistics for DHCP address binding entries.
<code>&lt;ip-addr&gt;</code>	a specified IP address in decimal format										
<code>all</code>	all binding types (manual binding and dynamic assignment)										
<code>manual</code>	manual binding										
<code>dynamic</code>	dynamic assignment										
<code>count</code>	displays statistics for DHCP address binding entries.										

**Default** None

**Mode** Admin and Configuration Mode

**Usage** Displays IP-MAC binding information.

**Example**

```
Switch# show ip dhcp binding
IP address Hardware address Lease expiration Type
10.1.1.233 00-00-E2-3A-26-04 Infinite Manual
10.1.1.254 00-00-E2-3A-5C-D3 60 Automatic
```

Displayed information	Explanation
IP address	IP address IP address assigned to a DHCP client
Hardware address	MAC address of a DHCP client
Lease expiration	Valid time for the DHCP client to hold the IP address
Type	Type of assignment: manual binding or dynamic assignment

## 11.1.27 show ip dhcp conflict

<b>Syntax</b>	<code>show ip dhcp conflict</code>								
<b>Parameter</b>	none								
<b>Default</b>	none								
<b>Mode</b>	Admin and Configuration Mode								
<b>Usage</b>	Displays log information for addresses that have a conflict record.								
<b>Example</b>	<pre>Switch# show ip dhcp conflict IP Address Detection method Detection Time 10.1.1.1 Ping FRI JAN 02 00:07:01 2002</pre> <table border="1"> <thead> <tr> <th>Displayed information</th> <th>Explanation</th> </tr> </thead> <tbody> <tr> <td>IP Address</td> <td>Conflicting IP address</td> </tr> <tr> <td>Detection method</td> <td>Method in which the conflict is detected</td> </tr> <tr> <td>Detection Time</td> <td>Time when the conflict is detected.</td> </tr> </tbody> </table>	Displayed information	Explanation	IP Address	Conflicting IP address	Detection method	Method in which the conflict is detected	Detection Time	Time when the conflict is detected.
Displayed information	Explanation								
IP Address	Conflicting IP address								
Detection method	Method in which the conflict is detected								
Detection Time	Time when the conflict is detected.								

## 11.1.28 show ip dhcp relay information option

<b>Syntax</b>	<code>show ip dhcp relay information option</code>
<b>Parameter</b>	<code>none</code>
<b>Default</b>	none
<b>Mode</b>	Admin and Configuration Mode
<b>Usage</b>	Show the relative configuration for DHCP relay option82
<b>Example</b>	Switch#show ip dhcp relay information option ip dhcp server relay information option(i.e. option 82) is enabled ip dhcp relay information option(i.e. option 82) is enabled

## 11.1.29 show ip dhcp server statistics

<b>Syntax</b>	<b>show ip dhcp server statistics</b>
<b>Parameter</b>	<b>none</b>
<b>Default</b>	none
<b>Mode</b>	Admin and Configuration Mode
<b>Usage</b>	Displays statistics of all DHCP packets for a DHCP server
<b>Example</b>	<pre>Switch# show ip dhcp server statistics  Address pools          1 Database agents       0 Automatic bindings    0 Manual bindings       0 Conflict bindings     0 Expired bindings      0 Malformed message     0  Message                Received BOOTREQUEST           0 DHCPDISCOVER          0 DHCPREQUEST           0 DHCPDECLINE           0 DHCPRELEASE           0 DHCPINFORM            0  Message                Send BOOTREPLY             0 DHCPOFFER             0 DHCPACK               0 DHCPNAK               0 DHCPRELAY             0 DHCPFORWARD           0  Switch#  Displayed information  Explanation Address pools         Number of DHCP address pools configured. Database agents       Number of database agents. Automatic bindings    Number of addresses assigned automatically Manual bindings       Number of addresses bound manually Conflict bindings     Number of conflicting addresses</pre>

---

Expired bindings	Number of addresses whose leases are expired
Malformed message	Number of error messages.
Message Received	Statistics for DHCP packets received
BOOTREQUEST	Total packets received
DHCPDISCOVER	Number of DHCPDISCOVER packets
DHCPREQUEST	Number of DHCPREQUEST packets
DHCPDECLINE	Number of DHCPDECLINE packets
DHCPRELEASE	Number of DHCPRELEASE packets
DHCPINFORM	Number of DHCPINFORM packets
Message Send	Statistics for DHCP packets sent
BOOTREPLY	Total packets sent
DHCPOFFER	Number of DHCPOFFER packets
DHCPACK	Number of DHCPACK packets
DHCPNAK	Number of DHCPNAK packets
DHCPRELAY	Number of DHCPRELAY packets
DHCPFORWARD	Number of DHCPFORWARD packets

---



### 11.1.30 ip dhcp broadcast suppress

---

<b>Syntax</b>	<code>ip dhcp broadcast suppress</code> <code>no ip dhcp broadcast suppress</code>
<b>Parameter</b>	<code>none</code>
<b>Default</b>	Disable
<b>Mode</b>	Global Mode
<b>Usage</b>	Enable DHCP broadcast suppress function, the no command disables the function Suppress the forwarding about DHCP broadcast packets, namely, drop or copy DHCP broadcast packets to CPU.
<b>Example</b>	Enable DHCP broadcast suppress function. Switch# config Switch(config)#ip dhcp broadcast suppress

---

### 11.1.31 ip dhcp relay share-vlan

<b>Syntax</b>	<code>ip dhcp relay share-vlan &lt;vlanid&gt; sub-vlan &lt;vlanlist&gt;</code> <code>no ip dhcp relay share-vlan</code>				
<b>Parameter</b>	<table border="1"> <tr> <td><code>&lt;vlanid&gt;</code></td> <td>VLAN ID of share-vlan</td> </tr> <tr> <td><code>&lt;vlanlist&gt;</code></td> <td>sub-vlan list</td> </tr> </table>	<code>&lt;vlanid&gt;</code>	VLAN ID of share-vlan	<code>&lt;vlanlist&gt;</code>	sub-vlan list
<code>&lt;vlanid&gt;</code>	VLAN ID of share-vlan				
<code>&lt;vlanlist&gt;</code>	sub-vlan list				
<b>Default</b>	None				
<b>Mode</b>	Global Mode				
<b>Usage</b>	<p>Specify sub-vlan of a share-vlan, the no command cancels sub-vlan.</p> <p>share-vlan may include many sub-vlan, but a sub-vlan only corresponds to a share-vlan. When layer 2 device of DHCP Relay receive DHCP Request, firstly judge whether VLAN with layer 3 interface for receiving package. If there is layer 3 interface in package, use the interface to process DHCP Relay, or else use layer 3 interface of share-vlan to process DHCP Relay when the vlan is sub-vlan of share-vlan.</p>				
<b>Example</b>	<pre>Switch#config Switch(config)#ip dhcp relay share-vlan 2 sub-vlan 2-4</pre>				

### 11.1.32 ip forward-protocol udp bootps

<b>Syntax</b>	<code>ip forward-protocol udp bootps</code> <code>no ip forward-protocol udp bootps</code>
<b>Parameter</b>	none
<b>Default</b>	Not forward UPD broadcast packets by default.
<b>Mode</b>	Global Mode
<b>Usage</b>	Sets DHCP relay to forward UPD broadcast packets on the port; the “ <b>no ip forward-protocol udp bootps</b> ”command cancels the service. The forwarding destination address is set in the “ <b>ip helper-address</b> ” command and described later
<b>Example</b>	Setting DHCP packets to be forwarded to 192.168.1.5. Switch#config Switch(config)#ip forward-protocol udp bootps Switch(config)#interface vlan 1 Switch(config-if-vlan1)#ip helper-address 192.168.1.5

### 11.1.33 ip helper-address

<b>Syntax</b>	<code>ip helper-address &lt;ip-address&gt;</code> <code>no ip helper-address &lt;ip-address&gt;</code>
<b>Parameter</b>	<b>ip-address</b> IP addresses, in the decimal format
<b>Default</b>	none
<b>Mode</b>	Port mode
<b>Usage</b>	<p>Specifies the destination address for the DHCP relay to forward UDP packets. The “<b>no ip helper-address &lt;ip-address&gt;</b>” command cancels the setting.</p> <p>The DHCP relay forwarding server address corresponds to the port forwarding UDP, i.e. DHCP relay forwards corresponding UDP packets only to the corresponding server instead of all UDP packets to all servers. When this command is run after “ip forward-protocol udp &lt;port&gt;” command, the forwarding address configured by this command receives the UDP packets from &lt;port&gt;. The combination of “ip forward-protocol udp &lt;port&gt;” command and this command should be used for configuration.</p>
<b>Example</b>	<pre>Switch#config Switch(config)#ip forward-protocol udp bootps Switch(config)#interface vlan 1 Switch(config-if-vlan1)#ip helper-address 192.168.2.5</pre>

### 11.1.34 show ip forward-protocol

<b>Syntax</b>	<b>show ip forward-protocol</b>
<b>Parameter</b>	<b>none</b>
<b>Default</b>	none
<b>Mode</b>	Admin and Configuration Mode
<b>Usage</b>	Show the configured port ID of the protocol which support the forwarding of broadcast packets, it means the port ID for forwarding DHCP packets.
<b>Example</b>	Switch#show ip forward-protocol Forward protocol(UDP port): 67(active)

### 11.1.35 show ip helper-address

<b>Syntax</b>	<b>show ip helper-address</b>		
<b>Parameter</b>	none		
<b>Default</b>	none		
<b>Mode</b>	Admin and Configuration Mode		
<b>Usage</b>	Show the configuration relation for the port ID of the protocol (It can forward broadcast packets), the interface (It supports forwarding function) and the forwarded destination IP.		
<b>Example</b>	Switch#show ip helper-address		
	Forward protocol	Interface	Forward server
	67(active)	Vlan1	192.168.2.5

### 11.1.36 clear ipv6 dhcp binding

<b>Syntax</b>	<code>clear ipv6 dhcp binding [&lt;ipv6-address&gt;] [pd &lt;ipv6-prefix   prefix-length&gt;]</code>				
<b>Parameter</b>	<table border="0"> <tr> <td><code>&lt;ipv6-address&gt;</code></td> <td>specified IPv6 address with binding record</td> </tr> <tr> <td><code>&lt;ipv6-prefix   prefix-length&gt;</code></td> <td>specified IPv6 prefix with binding record; To clear all IPv6 address binding record if there is no specified record.</td> </tr> </table>	<code>&lt;ipv6-address&gt;</code>	specified IPv6 address with binding record	<code>&lt;ipv6-prefix   prefix-length&gt;</code>	specified IPv6 prefix with binding record; To clear all IPv6 address binding record if there is no specified record.
<code>&lt;ipv6-address&gt;</code>	specified IPv6 address with binding record				
<code>&lt;ipv6-prefix   prefix-length&gt;</code>	specified IPv6 prefix with binding record; To clear all IPv6 address binding record if there is no specified record.				
<b>Default</b>	none				
<b>Mode</b>	Admin Configuration Mode				
<b>Usage</b>	<p>To clear one specified DHCPv6 assigned address binding record or all the IPv6 address binding records.</p> <p>DHCPv6 IPv6 address binding information can be displayed through the command <b>show ipv6 dhcp binding</b>. If DHCPv6 client does not use the DHCPv6 allocated IPv6 address but when the life time of the IPv6 address does not end, the DHCPv6 server will not remove its bind for this address. In this situation, the address binding information can be removed manually through this command; and if no parameter is appended, this command will remove all the address binding information, then all addresses and prefix will be assigned again in the DHCPv6 address pool.</p>				
<b>Example</b>	<p>To delete all binding record of IPv6 address and prefix</p> <pre>Switch#clear ipv6 dhcp binding</pre>				

### 11.1.37 clear ipv6 dhcp conflict

---

<b>Syntax</b>	<b>clear ipv6 dhcp conflict [address]</b>
<b>Parameter</b>	address                      specified address with the conflict record, no specified address will clear all conflict records.
<b>Default</b>	none
<b>Mode</b>	Admin Mode
<b>Usage</b>	Clear the address with the conflict record in address conflict log. With <b>show ipv6 dhcp conflict</b> command, the user can check the conflict in which IP addresses. With this command, the user can clear the conflict record of an address. If no specified address will clear the conflict record of all addresses in log. After the conflict records are cleared in log, these addresses can be used by DHCPv6 server again.
<b>Example</b>	When administrator checks the conflict logs, administrator discovers that address 2001::1 with the conflict record is not used, so its record will be cleared from address conflict files. Switch#clear ipv6 dhcp conflict 2001::1

---



### 11.1.38 clear ipv6 dhcp statistics

<b>Syntax</b>	<code>clear ipv6 dhcp statistics</code>
<b>Parameter</b>	none
<b>Default</b>	none
<b>Mode</b>	Admin Mode
<b>Usage</b>	<p>Clear the statistic records of DHCPv6 packets, the statistic counter of DHCPv6 packets is cleared.</p> <p>With <b>show ipv6 dhcp statistics</b> command, the user can check the statistic information of the counter for DHCPv6 packets, all statistic information is an accumulative value. With this command will clear the counter to check the debugging conveniently.</p>
<b>Example</b>	<p>Clear the counter of DHCPv6 packets.</p> <pre>Switch#clear ipv6 dhcp statistics</pre>

### 11.1.39 dns-server

<b>Syntax</b>	<code>dns-server &lt;ipv6-address&gt;</code> <code>no dns-server &lt;ipv6-address&gt;</code>
<b>Parameter</b>	<code>&lt;ipv6-address&gt;</code> IPv6 address of DNS Server
<b>Default</b>	none
<b>Mode</b>	DHCPv6 Address Pool Configuration Mode.
<b>Usage</b>	To configure the IPv6 address of the DNS server for DHCPv6 client; the no form of this command will remove the DNS configuration.  For each address pool, at most three DNS server can be configured, and the addresses of the DNS server must be valid IPv6 addresses.
<b>Example</b>	To configure the DNS Server address of DHCPv6 client as 2001:da8::1. <code>Switch(dhcp-1-config)#dns-server 2001:da8::1</code>

## 11.1.40 domain-name

---

<b>Syntax</b>	<b>domain-name &lt;domain-name&gt;</b> <b>no domain-name &lt;domain-name&gt;</b>
<b>Parameter</b>	<b>&lt;domain-name&gt;</b> domain name, less than 32 characters
<b>Default</b>	The domain name parameter of address pool is not configured by default
<b>Mode</b>	DHCPv6 Address Pool Configuration Mode.
<b>Usage</b>	To configure domain name of DHCPv6 client; the no form of this command will delete the domain name. At most 3 domain names can be configured for each address pool.
<b>Example</b>	To set the domain name of DHCPv6 client as test.com.cn Switch(dhcp-1-config)#domain-name test.com.cn

---

### 11.1.41 excluded-address

<b>Syntax</b>	<code>excluded-address &lt;ipv6-address&gt;</code> <code>no excluded-address &lt;ipv6-address&gt;</code>
<b>Parameter</b>	<code>&lt;ipv6-address&gt;</code> IPv6 address to be excluded from being allocated to hosts in the address pool
<b>Default</b>	Disabled
<b>Mode</b>	DHCPv6 Address Pool Configuration Mode.
<b>Usage</b>	To configure the specified IPv6 address to be excluded from the address pool, the excluded address will not be allocated to any hosts; the no form of this command will remove the configuration. <u>This command is used to preserve the specified address from DHCPv6 address allocation.</u>
<b>Example</b>	To configure to exclude 2001:da8:123::1 from DHCPv6 address allocation. <code>Switch(config)#excluded-address 2001:da8:123::1</code>

## 11.1.42 ipv6 address

<b>Syntax</b>	<code>ipv6 address &lt;prefix-name&gt; &lt;ipv6-prefix/prefix-length&gt;</code> <code>no ipv6 address &lt;prefix-name&gt; &lt;ipv6-prefix/prefix-length&gt;</code>	
<b>Parameter</b>	<b>&lt;prefix-name&gt;</b>	a string with its length no more than 32, designating or manual configuring the name of the address prefix defined in the prefix pool
	<b>&lt;ipv6-prefix/prefix-length&gt;</b>	latter part of the IPv6 address excluding the address prefix, as well as its length.
<b>Default</b>	No global address is configured for interfaces by default.	
<b>Mode</b>	Port mode	
<b>Usage</b>	<p>To configure the specified interface to use prefix delegation for address allocation. The no form of this command will disable the using of prefix delegation for address allocation.</p> <p>The IPv6 address of an interface falls into two parts: <b>&lt;prefix-name&gt;</b> and <b>&lt;ipv6-prefix&gt;/&lt;prefix-length&gt;</b>. If routing advertisement has been enabled, the first 64 bits of the addresses will be advertised. The address generated by <b>&lt;prefix-name&gt;</b> and <b>&lt;ipv6-prefix/prefix-length&gt;</b> combination will be removed, and the advertising of the prefix will be disabled. Only one <b>&lt;ipv6-prefix/prefix-length&gt;</b> can be configured for one prefix name.</p>	
<b>Example</b>	<p>If the prefix name my-prefix designates 2001:da8:221::/48, then the following command will add the address 2001:da8:221:2008::2008 to interface VLAN1.</p> <pre>Switch(Config-if-Vlan1)# ipv6 address my-prefix 0:0:0:2008::2008/64</pre>	

## 11.1.43 ipv6 dhcp client pd

<b>Syntax</b>	<pre>ipv6 dhcp client pd &lt;prefix-name&gt; [rapid-commit] no ipv6 dhcp client pd</pre>
<b>Parameter</b>	<p><b>&lt;prefix-name&gt;</b> &lt;prefix-name&gt; is the string with its length no more than 32, which designates the name of the address prefix.</p> <hr/> <p><b>rapid-commit</b> If <b>rapid-commit</b> optional is specified and the prefix delegation server enables the rapid-commit function, then the prefix delegation server will reply the prefix delegation client with the REPLY message directly. And the prefix delegation request will be accomplished by exchanging messages once.</p>
<b>Default</b>	DHCPv6 prefix delegation client is not enabled by default.
<b>Mode</b>	Port mode
<b>Usage</b>	<p>To configure DHCPv6 prefix delegation client for the specified interface. The no form of this command will disable the DHCPv6 prefix delegation client and remove the allocated address prefix.</p> <p>This command is used to configure the prefix delegation client on the specified interface, an interface with prefix delegation client enabled will send SOLICIT packets to try to get address prefix from the server. If the prefix is retrieved correctly, the address prefix in the global address pool can be used by the <b>ipv6 address</b> command to generate a valid IPv6 address. This command is exclusive with <b>ipv6 dhcp server</b> and <b>ipv6 dhcp relay destination</b>. If the prefix delegation client is disabled for an interface, then the address prefix which is get from this interface through prefix delegation client, will be removed from the global address pool. Also the interface address which is generated by the prefix delegation client will be removed, and routing advertisement with the prefix will be disabled. If any general prefix has been configured by the <b>ipv6 general-prefix</b> command, the same prefix learnt from prefix delegation will be disagreed.</p>
<b>Example</b>	<pre>Switch(Config-if-Vlan1)#ipv6 dhcp client pd ClientA rapid-commit</pre>

### 11.1.44 ipv6 dhcp client pd hint

<b>Syntax</b>	<code>ipv6 dhcp client pd hint &lt;prefix prefix-length&gt;</code> <code>no ipv6 dhcp client pd hint &lt;prefix prefix-length&gt;</code>
<b>Parameter</b>	<code>&lt;prefix prefix-length&gt;</code> prefix demanded by the client and its length.
<b>Default</b>	There is no such configuration in the system by default.
<b>Mode</b>	Port mode
<b>Usage</b>	<p>Designate the prefix demanded by the client and its length. The no operation of this command will delete that prefix and its length from the specified interface.</p> <p>The system designates a prefix and its length on the interface for a client. If client prefix-proxy demanding function is enabled on the interface and hint function is enabled on the switch, the user will have prior claim to the prefix it demands and the prefix length when the server allocates them. Only one hint prefix is allowed in the system.</p>
<b>Example</b>	<code>Switch(vlan-1-config)#ipv6 dhcp client pd hint 2001::/48</code>

## 11.1.45 ipv6 dhcp pool

<b>Syntax</b>	<pre>ipv6 dhcp pool &lt;poolname&gt; no ipv6 dhcp pool &lt;poolname&gt;</pre>
<b>Parameter</b>	<poolname> address pool name of DHCPv6 with its length no more than 32.
<b>Default</b>	Any DHCPv6 address pool are not configured by default.
<b>Mode</b>	Global Mode
<b>Usage</b>	<p>To configure the address pool for DHCPv6, and enter the DHCPv6 address pool configuration mode. In this mode, information such as the address prefix to be allocated, the DNS server addresses, and domain names, can be configured for the DHCPv6 client. The no form of this command will remove the configuration of the address pool.</p> <p>This command should be launched in global configuration mode, and falls in DHCPv6 address pool configuration mode if launched successfully. To remove a configured address pool, interface bindings related to the address pool, as well as the related address bindings will be removed.</p>
<b>Example</b>	<p>To define an address pool, named 1.</p> <pre>Switch#config Switch(config)#ipv6 dhcp pool 1</pre>



## 11.1.46 ipv6 dhcp relay destination

<b>Syntax</b>	<pre>ipv6 dhcp relay destination {[&lt;ipv6-address&gt;] [interface { &lt;interface-name&gt;   vlan &lt;1-4096&gt; } ] ] } no ipv6 dhcp relay destination { [ &lt;ipv6-address&gt;] [ interface { &lt;interface-name&gt;   vlan &lt;1-4096&gt; } ] ] }</pre>						
<b>Parameter</b>	<table border="1"> <tr> <td><b>&lt;ipv6-address&gt;</b></td> <td>address of the destination to which the DHCPv6 relay forwards;</td> </tr> <tr> <td><b>&lt;interface-name&gt;</b></td> <td>interface name which is used for forwarding of DHCPv6 requests</td> </tr> <tr> <td><b>&lt;1-4096&gt;</b></td> <td>VLAN ID</td> </tr> </table> <p>If <b>&lt;ipv6-address&gt;</b> is a global unicast address, the <b>interface</b> parameter should not be configured; If <b>&lt;ipv6-address&gt;</b> is an local address, the <b>interface</b> parameter is required be configured; The destination address for the DHCPv6 server will be the multicast address of <b>ALL_DHCP_Servers (FF05::1:3)</b>, if the interface parameter is configured only.</p>	<b>&lt;ipv6-address&gt;</b>	address of the destination to which the DHCPv6 relay forwards;	<b>&lt;interface-name&gt;</b>	interface name which is used for forwarding of DHCPv6 requests	<b>&lt;1-4096&gt;</b>	VLAN ID
<b>&lt;ipv6-address&gt;</b>	address of the destination to which the DHCPv6 relay forwards;						
<b>&lt;interface-name&gt;</b>	interface name which is used for forwarding of DHCPv6 requests						
<b>&lt;1-4096&gt;</b>	VLAN ID						
<b>Default</b>	By default, destination address for DHCPv6 relay is not configured.						
<b>Mode</b>	Port mode						
<b>Usage</b>	<p>To configure the destination to which the DHCPv6 relay forwards the DHCPv6 requests from the clients, the destination should be the address of an external DHCPv6 relay or the DHCPv6 server. The no form of this command will remove the configuration.</p> <p>This command is used to configure the DHCPv6 relay for the specified interface, the address should be the address of another DHCPv6 relay or the address DHCPv6 server. At most three relay addresses can be configured for an interface. To be mentioned, the DHCPv6 relay stops working only if all the relay destination address configurations have been removed. This command is mutually exclusive to "ipv6 dhcp server" and "ipv6 dhcp client pd" commands.</p>						
<b>Example</b>	<pre>Switch#config Switch(config)#interface vlan 1 Switch(config-if-vlan1)#ipv6 dhcp relay destination 2001:da8::1</pre>						

## 11.1.47 ipv6 dhcp server

<b>Syntax</b>	<code>ipv6 dhcp server &lt;poolname&gt; [preference &lt;value&gt;] [rapid-commit] [allow-hint]</code> <code>no ipv6 dhcp server &lt;poolname&gt;</code>
<b>Parameter</b>	<b>&lt;poolname&gt;</b> Name of the created DHCPv6 address pool
	<b>&lt;value&gt;</b> The priority of the DHCPv6 server, the larger the value, the higher the priority, the range: 0-255, the default is 0.
	<b>rapid-commit</b> The DHCPv6 server sends the REPLY packet to the client immediately after receiving the SOLICIT packet
	<b>allow-hint</b> Append the client's expected parameter value to its request packet
<b>Default</b>	DHCPv6 address pool based on port is not configured by default.
<b>Mode</b>	Port mode
<b>Usage</b>	<p>This command configures the address pool which will be allocated by the DHCPv6 server through the specified interface. The no form of this command will remove the address pool configuration.</p> <p>This command configure the DHCPv6 address pool which is applied by the DHCPv6 server for the specified interface, as well as optional parameters. One VLAN can bind many DHCPv6 address pools and assign the address for DHCPv6 request packet from direct-link and relay delegation.</p>
<b>Example</b>	<pre>Switch#config Switch(config)#interface vlan 1 Switch(config-if-vlan1)#ipv6 dhcp server PoolA preference 80 rapid-commit allow-hint</pre>

### 11.1.48 ipv6 general-prefix

<b>Syntax</b>	<pre>ipv6 general-prefix &lt;prefix-name&gt; &lt;ipv6-prefix/prefix-length&gt; no ipv6 general-prefix &lt;prefix-name&gt;</pre>
<b>Parameter</b>	<p><b>&lt;prefix-name&gt;</b>                    <b>&lt;prefix-name&gt;</b> is a character string less than 32 characters, to use as IPv6 general prefix name.</p> <hr/> <p><b>&lt;ipv6-prefix/prefix-length&gt;</b>    <b>&lt;ipv6-prefix/prefix-length&gt;</b> is defined as IPv6 general prefix.</p>
<b>Default</b>	IPv6 general prefix is not configured by default.
<b>Mode</b>	Global Mode
<b>Usage</b>	<p>To define an IPv6 general prefix. The no form of this command will delete the configuration. If IPv6 general prefix is configured, the interface will use the configured prefix for IPv6 address generating. Commonly, the general prefix is used for enterprise IPv6 prefix, and when entering an IPv6 address, users can simply add the address suffix of to the name of the general prefix. The configured address prefix will be reserved in the general address prefix pool. At most 8 general prefix can be configured at the same time. When trying to remove a configured general prefix name, the operation will fail if any interfaces used the configured prefix. Only one general prefix for a prefix name. The general prefix cannot use the same prefix definition with prefixes learnt from prefix delegation.</p>
<b>Example</b>	<p>To set the prefix of 2001:da8:221::/48 to general prefix my-prefix.</p> <pre>Switch#config Switch(config)# ipv6 general-prefix my-prefix 2001:da8:221::/48</pre>

## 11.1.49 ipv6 local pool

<b>Syntax</b>	<pre>ipv6 local pool &lt;poolname&gt; &lt;prefix/prefix-length&gt; &lt;assigned-length&gt; no ipv6 local pool &lt;poolname&gt;</pre>	
<b>Parameter</b>	<b>&lt;poolname&gt;</b>	<b>&lt;poolname&gt;</b> is the name for the IPv6 address pool of the prefix delegation, the length name string should be less than 32.
	<b>&lt;prefix/prefix-length&gt;</b>	<b>&lt;prefix/prefix-length&gt;</b> is the address prefix and its length of the prefix delegation.
	<b>&lt;assigned-length&gt;</b>	<b>&lt;assigned-length&gt;</b> is the length of the prefix in the address pool which can be retrieved by the client, the assigned prefix length should be no less than the value of <b>&lt;prefix-length&gt;</b>
<b>Default</b>	No IPv6 prefix delegation address pool is configured by default.	
<b>Mode</b>	Global Mode	
<b>Usage</b>	<p>To configure the address pool for prefix delegation. The no form of this command will remove the IPv6 prefix delegation configuration.</p> <p>This command should be used with the “<b>prefix delegation pool</b>” command to allocate address prefixes to the clients. If IPv6 prefix delegation is removed, the associated “<b>prefix delegation</b>” command will be in-effective either.</p>	
<b>Example</b>	<pre>Switch#config Switch(config)#ipv6 local pool 1 1100::1/24 24</pre>	

## 11.1.50 lifetime

<b>Syntax</b>	lifetime {<valid-time>   infinity} {<preferred-time>   infinity} no lifetime	
<b>Parameter</b>	<valid-time>	The valid lifetime of the IPv6 address allocated in the local address pool, 1-31536000 seconds, must be greater than <preferred-time>
	<preferred-time>	The preferred lifetime of the IPv6 address allocated in the local address pool, 1-31536000 seconds, must be less than <valid-time>
	<b>infinity</b>	Longest service life
<b>Default</b>	The default valid life time and preferred life time are 2592000 seconds (30 days) and 604800 seconds (7 days) respectively	
<b>Mode</b>	DHCPv6 Address Pool Configuration Mode.	
<b>Usage</b>	To configure the life time for the addresses or the address prefixes allocated by DHCPv6. The no form of this command will restore the default setting.	
<b>Example</b>	To configure the valid life time as 1000 seconds, and the preferred life time as 600 seconds. Switch#config Switch(config)#lifetime 1000 600	

## 11.1.51 network-address

<b>Syntax</b>	<code>network-address &lt;ipv6-pool-start-address&gt; &lt;ipv6-pool-end-address&gt;   &lt;prefix-length&gt; [eui-64])</code> <code>no network-address</code>								
<b>Parameter</b>	<table border="1"> <tr> <td><code>&lt;ipv6-pool-start-address&gt;</code></td> <td>start of the address pool;</td> </tr> <tr> <td><code>&lt;ipv6-pool-end-address&gt;</code></td> <td>end of the address pool</td> </tr> <tr> <td><code>&lt;prefix-length&gt;</code></td> <td>The length of the address prefix, ranging from 3 to 128, the default is 64</td> </tr> <tr> <td><code>eui-64</code></td> <td>According to the eui-64 standard, IPv6 addresses are allocated, not designated as being allocated in order</td> </tr> </table>	<code>&lt;ipv6-pool-start-address&gt;</code>	start of the address pool;	<code>&lt;ipv6-pool-end-address&gt;</code>	end of the address pool	<code>&lt;prefix-length&gt;</code>	The length of the address prefix, ranging from 3 to 128, the default is 64	<code>eui-64</code>	According to the eui-64 standard, IPv6 addresses are allocated, not designated as being allocated in order
<code>&lt;ipv6-pool-start-address&gt;</code>	start of the address pool;								
<code>&lt;ipv6-pool-end-address&gt;</code>	end of the address pool								
<code>&lt;prefix-length&gt;</code>	The length of the address prefix, ranging from 3 to 128, the default is 64								
<code>eui-64</code>	According to the eui-64 standard, IPv6 addresses are allocated, not designated as being allocated in order								
<b>Default</b>	No address pool is configured by default. °								
<b>Mode</b>	DHCPv6 Address Pool Configuration Mode.								
<b>Usage</b>	<p>To configure the DHCPv6 address pool; the no form of this command will remove the address pool configuration.</p> <p>This command configures the address pool for the DHCPv6 server to allocate addresses, only one address range can be configured for each address pool. To be noticed, if the DHCPv6 server has been enabled, and the length of the IPv6 address prefix has been configured, the length of the prefix in the address pool should be no less than the length of the prefix of the IPv6 address of the respective layer three interfaces in the switch. If <code>&lt;ipv6-pool-end-address&gt;</code> is bigger than <code>&lt;ipv6-pool-start-address&gt;</code>, this command returns at once.</p>								
<b>Example</b>	<p>To configure the address range for address pool as 2001:da8:123::100-2001:da8:123::200.</p> <pre>Switch#config Switch(config)#ipv6 dhcp pool 1 Switch(dhcp-1-config)#network-address 2001:da8:123::100 2001:da8:123::200</pre>								

## 11.1.52 prefix-delegation

<b>Syntax</b>	<pre>prefix-delegation &lt;ipv6-prefix/prefix-length&gt; &lt;client-DUID&gt; [iaid &lt;iaid&gt;] [lifetime &lt;valid-time&gt; &lt;preferred-time&gt; ] no prefix-delegation &lt;ipv6-prefix/prefix-length&gt; &lt;client-DUID&gt; [iaid &lt;iaid&gt;]</pre>										
<b>Parameter</b>	<table border="1"> <tr> <td><b>&lt;ipv6-prefix/prefix-length&gt;</b></td> <td><b>&lt;ipv6-prefix/prefix-length&gt;</b> is the length of the prefix to be allocated to the client.</td> </tr> <tr> <td><b>&lt;client-DUID&gt;</b></td> <td><b>&lt;client-DUID&gt;</b> is the DUID of the client. DUID with the type of DUID-LLT and DUID-LL are supported, the DUID of DUID-LLT type should be of 14 characters.</td> </tr> <tr> <td><b>&lt;iaid&gt;</b></td> <td><b>&lt;iaid&gt;</b> is the value to be appended in the IA_PD field of the clients' requests.</td> </tr> <tr> <td><b>&lt;valid-time&gt;</b></td> <td>The valid life cycle (in seconds) of the IPv6 address assigned to the client, the range is 1-31536000, the default is 2592000, and it must be greater than the preferred-time</td> </tr> <tr> <td><b>&lt;preferred-time&gt;</b></td> <td>The preferred lifetime of the IPv6 address assigned to the client (in seconds), the range is 1-31536000, the default is 604800, and it must be less than valid-time</td> </tr> </table>	<b>&lt;ipv6-prefix/prefix-length&gt;</b>	<b>&lt;ipv6-prefix/prefix-length&gt;</b> is the length of the prefix to be allocated to the client.	<b>&lt;client-DUID&gt;</b>	<b>&lt;client-DUID&gt;</b> is the DUID of the client. DUID with the type of DUID-LLT and DUID-LL are supported, the DUID of DUID-LLT type should be of 14 characters.	<b>&lt;iaid&gt;</b>	<b>&lt;iaid&gt;</b> is the value to be appended in the IA_PD field of the clients' requests.	<b>&lt;valid-time&gt;</b>	The valid life cycle (in seconds) of the IPv6 address assigned to the client, the range is 1-31536000, the default is 2592000, and it must be greater than the preferred-time	<b>&lt;preferred-time&gt;</b>	The preferred lifetime of the IPv6 address assigned to the client (in seconds), the range is 1-31536000, the default is 604800, and it must be less than valid-time
<b>&lt;ipv6-prefix/prefix-length&gt;</b>	<b>&lt;ipv6-prefix/prefix-length&gt;</b> is the length of the prefix to be allocated to the client.										
<b>&lt;client-DUID&gt;</b>	<b>&lt;client-DUID&gt;</b> is the DUID of the client. DUID with the type of DUID-LLT and DUID-LL are supported, the DUID of DUID-LLT type should be of 14 characters.										
<b>&lt;iaid&gt;</b>	<b>&lt;iaid&gt;</b> is the value to be appended in the IA_PD field of the clients' requests.										
<b>&lt;valid-time&gt;</b>	The valid life cycle (in seconds) of the IPv6 address assigned to the client, the range is 1-31536000, the default is 2592000, and it must be greater than the preferred-time										
<b>&lt;preferred-time&gt;</b>	The preferred lifetime of the IPv6 address assigned to the client (in seconds), the range is 1-31536000, the default is 604800, and it must be less than valid-time										
<b>Default</b>	Disabled										
<b>Mode</b>	Port mode										
<b>Usage</b>	<p>To configure dedicated prefix delegation for the specified user. The no form of this command will remove the dedicated prefix delegation.</p> <p>This command configures the specified IPv6 address prefix to bind with the specified client. If no IAID is configured, any IA of any clients will be able get this address prefix. At most eight static binding address prefix can be configured for each address pool. For prefix delegation, static binding is of higher priority than the prefix address pool.</p>										
<b>Example</b>	<p>The following command will allocate 2001:da8::/48 to the client with DUID as 0001000600000005000BBFAA2408, and IAID as 12.</p> <pre>Switch#config Switch(config)#ipv6 dhcp pool 1 Switch(dhcp-1-config)#prefix-delegation 2001:da8::/48 0001000600000005000BBFAA240812</pre>										

### 11.1.53 prefix-delegation pool

<b>Syntax</b>	<pre>prefix-delegation pool &lt;poolname&gt; [lifetime &lt;valid-time&gt; &lt;preferred-time&gt;] no prefix-delegation pool &lt;poolname&gt;</pre>						
<b>Parameter</b>	<table border="1"> <tr> <td><b>&lt;poolname&gt;</b></td> <td><b>&lt;poolname&gt;</b> is the name of the address prefix pool, the length name string should be less than 32.</td> </tr> <tr> <td><b>&lt;valid-time&gt;</b></td> <td>The valid life cycle (in seconds) of the IPv6 address assigned to the client, the range is 1-31536000, the default is 2592000, and it must be greater than the preferred-time</td> </tr> <tr> <td><b>&lt;preferred-time&gt;</b></td> <td>The preferred lifetime of the IPv6 address assigned to the client (in seconds), the range is 1-31536000, the default is 604800, and it must be less than valid-time</td> </tr> </table>	<b>&lt;poolname&gt;</b>	<b>&lt;poolname&gt;</b> is the name of the address prefix pool, the length name string should be less than 32.	<b>&lt;valid-time&gt;</b>	The valid life cycle (in seconds) of the IPv6 address assigned to the client, the range is 1-31536000, the default is 2592000, and it must be greater than the preferred-time	<b>&lt;preferred-time&gt;</b>	The preferred lifetime of the IPv6 address assigned to the client (in seconds), the range is 1-31536000, the default is 604800, and it must be less than valid-time
<b>&lt;poolname&gt;</b>	<b>&lt;poolname&gt;</b> is the name of the address prefix pool, the length name string should be less than 32.						
<b>&lt;valid-time&gt;</b>	The valid life cycle (in seconds) of the IPv6 address assigned to the client, the range is 1-31536000, the default is 2592000, and it must be greater than the preferred-time						
<b>&lt;preferred-time&gt;</b>	The preferred lifetime of the IPv6 address assigned to the client (in seconds), the range is 1-31536000, the default is 604800, and it must be less than valid-time						
<b>Default</b>	The prefix delegation name used by DHCPv6 address pool is not configured.						
<b>Mode</b>	DHCPv6 Address Pool Configuration Mode.						
<b>Usage</b>	<p>To configure prefix delegation name used by DHCPv6 address pool. The no form of this command deletes the configuration.</p> <p>This command configures the name of the address prefix pool for address allocation. If configured, the addresses in the prefix address pool will be allocated to the clients. This command can be used in association with the <b>ipv6 local pool</b> command. For one address pool, only one prefix delegation pool can be bound. When trying to remove the prefix name configuration, the prefix delegation service of the server will be unavailable, if both the address pool is not associated with the prefix delegation pool and no static prefix delegation binding is enabled.</p>						
<b>Example</b>	<pre>Switch#show subnet-vlan Switch(config)#ipv6 dhcp pool 1 Switch(dhcp-1-config)#prefix-delegation pool abc</pre>						



## 11.1.54 service dhcpv6

<b>Syntax</b>	<code>service dhcpv6</code> <code>no service dhcpv6</code>
<b>Parameter</b>	none
<b>Default</b>	Disabled
<b>Mode</b>	Global Mode
<b>Usage</b>	<p>To enable DHCPv6 server function; the no form of this command disables the configuration.</p> <p>The DHCPv6 services include DHCPv6 server function, DHCPv6 relay function, DHCPv6 prefix delegation function. All of the above services are configured on ports. Only when DHCPv6 server function is enabled, the IP address assignment of DHCPv6 client, DHCPv6 relay and DHCPv6 prefix delegation functions enabled can be configured on ports.</p>
<b>Example</b>	<p>To enable DHCPv6 server.</p> <pre>Switch#config</pre> <pre>Switch(config)# service dhcpv6</pre>

## 11.1.55 show ipv6 dhcp

<b>Syntax</b>	<code>show ipv6 dhcp</code>
<b>Parameter</b>	none
<b>Default</b>	none
<b>Mode</b>	Admin and Configuration Mode
<b>Usage</b>	To show the enable switch and DUID of DHCPv6 service To show the enable switch and DUID of DHCPv6 service, server identifier options only use DUID of DUID-LLT type.
<b>Example</b>	Switch#show ipv6 dhcp DHCPv6 is enabled LLT DUID is <00:01:00:01:43:b7:1b:81:00:03:0f:01:5f:9d> LL DUID is <00:03:00:01:00:03:0f:01:5f:9d>

## 11.1.56 show ipv6 dhcp binding

<b>Syntax</b>	<code>show ipv6 dhcp binding [&lt;ipv6-address&gt;  pd &lt;ipv6-prefix prefix-length&gt; count]</code>				
<b>Parameter</b>	<table border="1"> <tr> <td><b>ipv6-address</b></td> <td>specified IPv6 address;</td> </tr> <tr> <td><b>count</b></td> <td>show the number of DHCPv6 address bindings</td> </tr> </table>	<b>ipv6-address</b>	specified IPv6 address;	<b>count</b>	show the number of DHCPv6 address bindings
<b>ipv6-address</b>	specified IPv6 address;				
<b>count</b>	show the number of DHCPv6 address bindings				
<b>Default</b>	none				
<b>Mode</b>	Admin and Configuration Mode				
<b>Usage</b>	To show all the address and prefix binding information of DHCPv6, include type, DUID, IAID, prefix, valid time and so on.				
<b>Example</b>	<pre>Switch#show ipv6 dhcp binding Client: iatype IANA, iaaid 0x0e001d92 DUID: 00:01:00:01:0f:55:82:4f:00:19:e0:3f:d1:83 IANA leased address: 2001:da8::10 Preferred lifetime 604800 seconds, valid lifetime 2592000 seconds Lease obtained at %Jan 01 01:34:44 1970 Lease expires at %Jan 31 01:34:44 1970 (2592000 seconds left)  The number of DHCPv6 bindings is 1</pre>				

## 11.1.57 show ipv6 dhcp conflict

<b>Syntax</b>	<code>show ipv6 dhcp conflict</code>
<b>Parameter</b>	none
<b>Default</b>	none
<b>Mode</b>	Admin and Configuration Mode
<b>Usage</b>	Show the log for the address that have a conflict record.
<b>Example</b>	Switch#show ipv6 dhcp DHCPv6 is enabled LLT DUID is <00:01:00:01:43:b7:1b:81:00:03:0f:01:5f:9d> LL DUID is <00:03:00:01:00:03:0f:01:5f:9d>

## 11.1.58 show ipv6 dhcp interface

<b>Syntax</b>	<code>show ipv6 dhcp interface [&lt;interface-name&gt;]</code>
<b>Parameter</b>	<p><b>&lt;interface-name&gt;</b>      <b>&lt;interface-name&gt;</b> is the name and number of interface, if the <b>&lt;interface-name&gt;</b> parameter is not provided, then all the DHCPv6 interface information will be shown.</p>
<b>Default</b>	none
<b>Mode</b>	Admin and Configuration Mode
<b>Usage</b>	To show the information for DHCPv6 interface, include Port Mode (Prefix delegation client. DHCPv6 server. DHCPv6 relay) , and the relative conformation information under all kinds of mode.
<b>Example</b>	<pre>Switch#show ipv6 dhcp interface vlan10 Vlan10 is in server mode Using pool: poolv6 Preference value: 20 Rapid-Commit is disabled</pre>

## 11.1.59 show ipv6 dhcp pool

<b>Syntax</b>	<b>show ipv6 dhcp pool [poolname]</b>	
<b>Parameter</b>	<b>[poolname]</b>	<b>&lt;poolname&gt;</b> is the DHCPv6 address pool name which configured already, and the length less than 32 characters. If the <b>&lt;poolname&gt;</b> parameter is not provided, then all the DHCPv6 address pool information will be shown.
<b>Default</b>	none	
<b>Mode</b>	Admin and Configuration Mode	
<b>Usage</b>	To display the configuration and dynamic assignment information for DHCPv6 address pool, include the name of DHCPv6 address pool, the prefix of DHCPv6 address pool, excluded address, DNS server configuration, relative prefix information and so on. To display assigned address binding number of address pool that is used as address assignment server. To display assigned prefix number of address pool that is used as prefix delegation server	
<b>Example</b>	Switch#show ipv6 dhcp pool poolv6	

## 11.1.60 show ipv6 dhcp statistics

<b>Syntax</b>	<code>show ipv6 dhcp statistics</code>
<b>Parameter</b>	none
<b>Default</b>	none
<b>Mode</b>	Admin and Configuration Mode
<b>Usage</b>	To show the statistic of all kinds of DHCPv6 packets by DHCPv6 server.

**Example**

```
Switch#show ipv6 dhcp statistics
```

Address pools	1		
Active bindings	0		
Expiried bindings	0		
Malformed message	0		

Message	Received	Send
DHCP6SOLICIT	0	0
DHCP6ADVERTISE	0	0
DHCP6REQUEST	0	0
DHCP6REPLY	0	0
DHCP6RENEW	0	0
DHCP6REBIND	0	0
DHCP6RELEASE	0	0
DHCP6DECLINE	0	0
DHCP6CONFIRM	0	0
DHCP6RECONFIGURE	0	0
DHCP6INFORMREQ	0	0
DHCP6RELAYFORW	0	0
DHCP6RELAYREPLY	0	0

Show information	Explanation
Address pools	To configure the number of DHCPv6 address pools;
Active bindings	The number of auto assign addresses;
Expiried bindings	The number of expired bindings;
Malformed message	The number of malformed messages;
Message Recieved	The statistic of received DHCPv6 packets.
DHCP6SOLICIT	The number of DHCPv6 SOLICIT packets.
DHCP6ADVERTISE	The number of DHCPv6 ADVERTISE packets

---

DHCPv6REQUEST	The number of DHCPv6 REQUEST packets
DHCP6REPLY	The number of DHCPv6 REPLY packets
DHCP6RENEW	The number of DHCPv6 RENEW packets
DHCP6REBIND	The number of DHCPv6 REBIND packets
DHCP6RELEASE	The number of DHCPv6 RELEASE packets
DHCP6DECLINE	The number of DHCPv6 DECLINE packets
DHCP6CONFIRM	The number of DHCPv6 CONFIRM packets
DHCP6RECONFIGURE	The number of DHCPv6 RECONFIGURE packets
DHCP6INFORMREQ	The number of DHCPv6 INFORMREQ packets
DHCP6RELAYFORW	The number of DHCPv6 RELAYFORW packets
DHCP6RELAYREPLY	The number of DHCPv6 RELAYREPLY packets

---



## 11.1.61 show ipv6 general-prefix

<b>Syntax</b>	<code>show ipv6 general-prefix</code>
<b>Parameter</b>	none
<b>Default</b>	none
<b>Mode</b>	Admin and Configuration Mode
<b>Usage</b>	To show the IPv6 general prefix pool information, include the prefix number in general prefix pool, the name of every prefix, the interface of prefix obtained, and the prefix value.
<b>Example</b>	Switch#show ipv6 general-prefix  IPv6 Prefix my, acquired via Manual configuration  2001:da8:221::/48

## 11.1.62 show ipv6 local pool

<b>Syntax</b>	<code>show ipv6 local pool</code>
<b>Parameter</b>	none
<b>Default</b>	none
<b>Mode</b>	Admin and Configuration Mode
<b>Usage</b>	To show the statistic information of DHCPv6 prefix pool, include the name of prefix pool, the prefix and prefix length as well as assigned prefix length, the number of assigned prefix and information in DHCPv6 address pool.
<b>Example</b>	Switch#show ipv6 local pool Pool Prefix Free In use a 2010::1/0/48 65536 0

## 11.1.63 ip dhcp relay information option

<b>Syntax</b>	<code>ip dhcp relay information option</code> <code>no ip dhcp relay information option</code>
<b>Parameter</b>	<code>none</code>
<b>Default</b>	The system disables the option82 function by default
<b>Mode</b>	Global Mode
<b>Usage</b>	<p>Set this command to enable the option82 function of the switch Relay Agent. The “<b>no ip dhcp relay information option</b>” command is used to disable the option82 function of the switch Relay Agent.</p> <p>Only the DHCP Relay Agents configuring with this command can add option82 to the DHCP request message, and let the server to process it. Before enabling this function, users should make sure that the DHCP service is enabled and the Relay Agent will transmit the udp broadcast messages whose destination port is 67.</p>
<b>Example</b>	<p>Enable the option82 function of the Relay Agent.</p> <pre>Switch#config Switch(config)#service dhcp Switch(config)# ip forward-protocol udp bootps Switch(config)# ip dhcp relay information option</pre>

### 11.1.64 ip dhcp relay information option delimiter

<b>Syntax</b>	ip dhcp relay information option delimiter [colon   dot   slash   space] no ip dhcp relay information option delimiter
<b>Parameter</b>	none
<b>Default</b>	Slash("/")
<b>Mode</b>	Global Mode
<b>Usage</b>	Set the delimiter of each parameter for suboption of option82 in global mode, no command restores the delimiter as slash. Divide the parameters with the configured delimiters after users have defined them which are used to create suboption (remot-de, circuit-id) of option82 in global mode.
<b>Example</b>	Set the parameter delimiters as dot (".") for suboption of option82. Switch#config Switch(config)#ip dhcp relay information option delimiter dot

### 11.1.65 ip dhcp relay information option remote-id

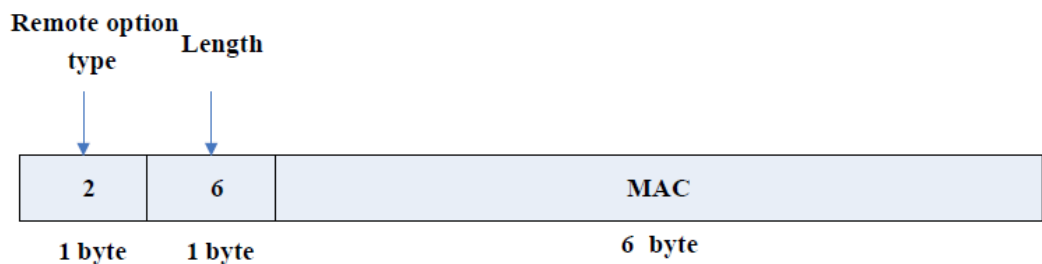
<b>Syntax</b>	<code>ip dhcp relay information option remote-id {standard   &lt;remote-id&gt;}</code> <code>no ip dhcp relay information option remote-id</code>				
<b>Parameter</b>	<table border="0"> <tr> <td><b>standard</b></td> <td><b>standard</b> means the default VLAN MAC format.</td> </tr> <tr> <td><b>&lt;remote-id&gt;</b></td> <td>&lt;remote-id&gt; means the remote-id content of option 82 specified by users, its length cannot exceed 64 characters.</td> </tr> </table>	<b>standard</b>	<b>standard</b> means the default VLAN MAC format.	<b>&lt;remote-id&gt;</b>	<remote-id> means the remote-id content of option 82 specified by users, its length cannot exceed 64 characters.
<b>standard</b>	<b>standard</b> means the default VLAN MAC format.				
<b>&lt;remote-id&gt;</b>	<remote-id> means the remote-id content of option 82 specified by users, its length cannot exceed 64 characters.				
<b>Default</b>	Use standard format to set remote-id of option 82				
<b>Mode</b>	Global Mode				
<b>Usage</b>	<p>Set the suboption2 (remote ID option) content of option 82 added by DHCP request packets (They are received by the interface). The no command sets the additive suboption2 (remote ID option) format of option 82 as standard.</p> <p>The additive option 82 information needs to associate with third-party DHCP server, it is used to specify the remote-id content by users when the standard remote-id format cannot satisfy server's request.</p>				
<b>Example</b>	<p>Set the suboption remote-id of DHCP option82 as street-1-1.</p> <pre>Switch#config Switch(config)#ip dhcp relay information option remote-id street-1-1</pre>				

### 11.1.66 ip dhcp relay information option remote-id format

<b>Syntax</b>	<code>ip dhcp relay information option remote-id format {default   vs-hp}</code>	
<b>Parameter</b>	<b>default</b>	default means that remote-id is the VLAN MAC address with hexadecimal format.
	<b>vs-up</b>	vs-hp means that remote-id is compatible with the remote-id format of HP manufacturer.
<b>Default</b>	default	
<b>Mode</b>	Global Mode	

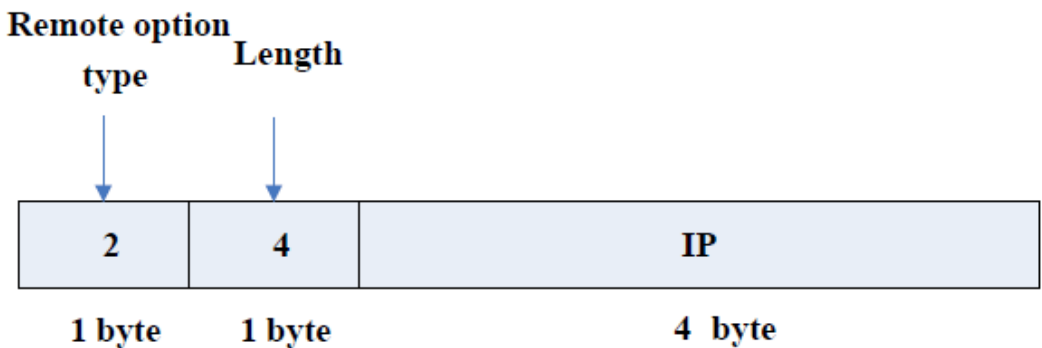
**Usage**

Set remote-id format of Relay Agent option82.  
 The default remote-id format defined as below:



MAC means VLAN MAC address.

The compatible remote-id format with HP manufacturer defined as below:



IP means the primary IP address of layer 3 interface where DHCP packets from.

**Example**

Set remote-id of Relay Agent option82 as the compatible format with HP manufacturer.  
 Switch#config  
 Switch(config)#ip dhcp relay information option remote-id format vs-hp

### 11.1.67 ip dhcp relay information option self-defined remote-id

<b>Syntax</b>	<code>ip dhcp relay information option self-defined remote-id {hostname   mac   string WORD}</code> <code>no ip dhcp relay information option self-defined remote-id</code>
<b>Parameter</b>	<b>WORD</b> WORD the defined character string of remote-id by themselves, the maximum length is 64.
<b>Default</b>	Using standard method.
<b>Mode</b>	Global Mode
<b>Usage</b>	Set creation method for option82, users can define the parameters of remote-id suboption by themselves. After configure this command, if users do not configure remote-id on interface, it will create remote-id suboption for option82 according to self-defined method. For mac, use the format such as 00-02-d1-2e-3a-0d if it is filled to packets with ascii format, but hex format occupies 6 bytes. Each option will be filled to packets according to the configured order of the commands and divide them with delimiter (delimiter is <b>ip dhcp relay information option delimiter</b> configuration).
<b>Example</b>	Set self-defined method and character string of remote-id suboption are hostname and abc respectively for option82. Switch#config Switch(config)# ip dhcp relay information option self-defined remote-id hostname string abc

### 11.1.68 ip dhcp relay information option self-defined remote-id format

<b>Syntax</b>	<code>ip dhcp relay information option self-defined remote-id format [ascii   hex]</code>
<b>Parameter</b>	none
<b>Default</b>	ascii
<b>Mode</b>	Global Mode
<b>Usage</b>	Set self-defined format of remote-id for relay option82. self-defined format use ip dhcp relay information option type self-defined remote-id to create remote-id format.
<b>Example</b>	Set self-defined method of remote-id as hex for relay option82. Switch#config Switch(config)# ip dhcp relay information option self-defined remote-id format hex



### 11.1.69 ip dhcp relay information option self-defined subscriber-id

<b>Syntax</b>	<code>ip dhcp relay information option self-defined subscriber-id {vlan   port   id (switch-id (mac   hostname)  remote-mac)  string WORD }</code> <code>no ip dhcp relay information option self-defined subscriber-id</code>
<b>Parameter</b>	<b>WORD</b> WORD the defined character string of circuit-id by themselves, the maximum length is 64.
<b>Default</b>	Using standard method.
<b>Mode</b>	Global Mode
<b>Usage</b>	<p>Set creation method for option82, users can define the parameters of circute-id suboption by themselves.</p> <p>After configure this command, if users do not configure circuit-id on interface, it will create circuit-id suboption for option82 according to self-defined method. Self-defined format of circuit-id: if self-defined format is ascii, the filled format of vlan such as "Vlan2", the format of port such as "Ethernet1/0/1", the format of mac and remote-mac such as "00-02-d1-2e-3a-0d". If self-defined format is hex, the filled format of vlan occupies 2 bytes, port occupies 4 bytes, a byte means slot (for chassis switch, it means slot ID, for box switch, it is 1), a byte means Module (the default is 0), two bytes means port ID beginning from 1, mac and remote-mac occupy 6 bytes. Each option will be filled to packets according to the configured order of the commands and divide them with delimiter (delimiter is <b>ip dhcp relay information option delimiter</b> configuration).</p>
<b>Example</b>	<p>Set self-defined method of circuit-id suboption as port, mac for option82.</p> <pre>Switch#config Switch(config)#ip dhcp relay information option self-defined subscriber-id port id switch-id mac</pre>

## 11.1.70 ip dhcp relay information option self-defined subscriber-id format

<b>Syntax</b>	<code>ip dhcp relay information option self-defined subscriber-id format [ascii   hex]</code>
<b>Parameter</b>	none
<b>Default</b>	ascii
<b>Mode</b>	Global Mode
<b>Usage</b>	Set self-defined format of circuit-id for relay option82. self-defined format use ip dhcp relay information option type self-defined subscriber-id to create circuit-id format.
<b>Example</b>	Set self-defined format of circuit-id as hex for relay option82. Switch#config Switch(config)#ip dhcp relay information option self-defined subscriber-id format hex

### 11.1.71 ip dhcp relay information option subscriber-id

<b>Syntax</b>	<code>ip dhcp relay information option subscriber-id {standard   &lt;circuit-id&gt;}</code> <code>no ip dhcp relay information option subscriber-id</code>
<b>Parameter</b>	<p><b>&lt;circuit-id&gt;</b>                      <b>&lt;circuit-id&gt;</b> is the circuit-id contents of option82 specified by users, which is a string no longer than 64 characters.</p> <p><b>standard</b>                              <b>standard</b> means the standard vlan name and physical port name format</p>
<b>Default</b>	The system uses the standard format to set the circuit-id of option 82 by default.
<b>Mode</b>	Port mode
<b>Usage</b>	Because the option 82 information added for the switch should cooperate with the third party DHCP server, if the standard circuit-id format of the switch cannot satisfy the server's request, this method will be provided for users to specify the contents of circuit-id according to the situation of the server.
<b>Example</b>	<p>Set the sub-option circuit-id of DHCP option82 as foobar.</p> <pre>Switch#config Switch(config)#interface vlan 1 Switch(config-if-vlan1)#ip dhcp relay information option subscriber-id foobar</pre>

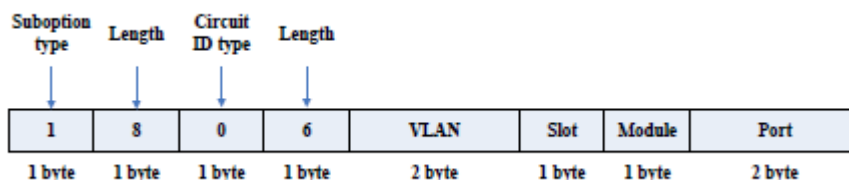
### 11.1.72 ip dhcp relay information option subscriber-id format

<b>Syntax</b>	<code>ip dhcp relay information option subscriber-id format {hex   ascii   vs-hp}</code>	
<b>Parameter</b>	<b>hex</b>	hex means that subscriber-id is VLAN and port information with hexadecimal format
	<b>ascii</b>	ascii means that subscriber-id is VLAN and port information with ACSII format.
	<b>vs-hp</b>	vs-hp means that subscriber-id is compatible with the format of HP manufacturer.

**Default**      ascii

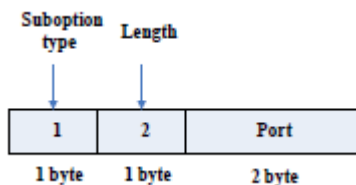
**Mode**          Global Mode

**Usage**          Set subscriber-id format of Relay Agent option82.  
 VLAN and port information with ASCII format, such as "Vlan1+Ethernet1/0/11", VLAN and port information with hexadecimal format defined as below:



VLAN field fills in VLAN ID. For chassis switch, Slot means slot number, for box switch, Slot is 1; default Module is 0; Port means port number which begins from 1.

The compatible subscriber-id format with HP manufacturer defined as below:



Port means port number which begins from 1.

**Example**          Set subscriber-id format of Relay Agent option82 as hexadecimal format.  
 Switch#config  
 Switch(config)#ip dhcp relay information option subscriber-id format hex

### 11.1.73 ip dhcp relay information policy

<b>Syntax</b>	<code>ip dhcp relay information policy {drop   keep   replace}</code> <code>no ip dhcp relay information policy</code>
<b>Parameter</b>	<p><b>drop</b> drop mode means that if the message has option82, then the system will drop it without processing;</p> <p><b>keep</b> keep mode means that the system will keep the original option82 segment in the message, and forward it to the server to process</p> <p><b>replace</b> replace mode means that the system will replace the option 82 segment in the existing message with its own option 82, and forward the message to the server to process</p>
<b>Default</b>	The system uses replace mode to replace the option 82 segment in the existing message with its own option 82.
<b>Mode</b>	Port mode
<b>Usage</b>	<p>This command is used to set the retransmitting policy of the system for the received DHCP request message which contains option82.</p> <p>The “no ip dhcp relay information policy” will set the retransmitting policy of the option 82 DHCP message as “replace”.</p> <p>Since the DHCP client messages might go through several DHCP Relay Agents when passed to the DHCP server, the latter Relay Agents on the path should set policies to decide how to process the option82 added by Relay Agents before them. The selection of option 82 retransmitting policies should take the configuration policy of the DHCP server into account.</p>
<b>Example</b>	<p>Set the retransmitting policy of DHCP messages option 82 as keep.</p> <pre>Switch#config Switch(config)#interface vlan 1 Switch(Config-if-Vlan1)#ip dhcp relay information policy keep</pre>

### 11.1.74 ip dhcp server relay information enable

<b>Syntax</b>	<code>ip dhcp server relay information enable</code> <code>no ip dhcp server relay information enable</code>
<b>Parameter</b>	none
<b>Default</b>	The system disable the option82 identifying function by default.
<b>Mode</b>	Global Mode
<b>Usage</b>	This command is used to enable the switch DHCP server to identify option82. The “no ip dhcp server relay information enable” command will make the server ignore the option 82. If the users want the switch DHCP server to identify option82 and return option 82 information in the reply message, this command needs to be set, or, the switch DHCP server will ignore the option82.
<b>Example</b>	Set the DHCP server to support option82 Switch#config Switch(config)#interface vlan 1 Switch(Config-if-Vlan1)#ip dhcp server relay information enable

## 11.1.75 show ip dhcp relay information option

<b>Syntax</b>	<code>show ip dhcp relay information option</code>
<b>Parameter</b>	none
<b>Default</b>	none
<b>Mode</b>	Admin and Configuration Mode
<b>Usage</b>	<p>This command will display the state information of the DHCP option 82 in the system, including option82 enabling switch, the interface retransmitting policy, the circuit ID mode and the switch DHCP server option82 enabling switch.</p> <p><u>Use this command to check the state information of Relay Agent option82 during operation.</u></p>
<b>Example</b>	<pre>Switch#show ip dhcp relay information option ip dhcp server relay information option(i.e. option 82) is disabled ip dhcp relay information option(i.e. option 82) is enabled Vlan2: ip dhcp relay information policy keep ip dhcp relay information option subscriber-id standard Vlan3: ip dhcp relay information policy replace ip dhcp relay information option subscriber-id foobar</pre>

## 11.1.76 option 43 ascii LINE

<b>Syntax</b>	<b>option 43 ascii LINE</b> <b>no option 43</b>
<b>Parameter</b>	<b>LINE</b> The configured option 43 character string with ascii format, its length range between 1 and 255.
<b>Default</b>	No option 43 character string is configured.
<b>Mode</b>	DHCP Address Pool Mode
<b>Usage</b>	Configure option 43 character string with ascii format in ip dhcp pool mode. The no command deletes the configured option 43.
<b>Example</b>	Configure option 43 with ascii format to be "AP 1000". Switch#config Switch(config)#ip dhcp pool a switch (dhcp-a-config)#option 43 ascii AP 1000



### 11.1.77 option 43 hex WORD

<b>Syntax</b>	<b>option 43 hex WORD</b> <b>no option 43</b>
<b>Parameter</b>	<b>WORD</b> The configured option 43 character string with hex format, such as a1241b.
<b>Default</b>	No option 43 is configured.
<b>Mode</b>	DHCP Address Pool Mode
<b>Usage</b>	<p>Configure option 43 character string with hex format in ip dhcp pool mode. The no command deletes the configured option 43.</p> <p>When using hex method to configure option 43, the string needs to be written according to TLV (Type-Length-Value) format. For example, issue ip address of 10.1.1.1 through option 43, then the hex string here should be 01040A010101; Type=0x01, it means IP address; Length=0x04, it means the length of IP address is 4 Bytes; Value=0x0A010101, it means the hexadecimal format of 10.1.1.1.</p>
<b>Example</b>	<p>Configure option 43 with hex format to be "01040a010101".</p> <pre>Switch#config Switch(config)#ip dhcp pool a switch (dhcp-a-config)#option 43 hex 01040a010101</pre>

## 11.1.78 option 43 ip A.B.C.D

<b>Syntax</b>	<b>option 43 ip A.B.C.D</b> <b>no option 43</b>
<b>Parameter</b>	<b>A.B.C.D</b> The configured option 43 with IP format, such as 192.168.1.1.
<b>Default</b>	No option 43 is configured.
<b>Mode</b>	DHCP Address Pool Mode
<b>Usage</b>	Configure option 43 character string with IP format in ip dhcp pool mode. The no command deletes the configured option 43. Using this command to configure option 43, such as "192.168.1.1", then option 43 filled in packets is "C0A80101".
<b>Example</b>	Configure option 43 with IP format to be "192.168.1.1". Switch#config Switch(config)#ip dhcp pool a switch (dhcp-a-config)#option 43 ip 192.168.1.1

### 11.1.79 option 60 ascii LINE

<b>Syntax</b>	<b>option 60 ascii LINE</b> <b>no option 60</b>
<b>Parameter</b>	<b>LINE</b> The configured option 60 character string with ascii format, its length range between 1 and 255.
<b>Default</b>	No option 60 character string is configured.
<b>Mode</b>	DHCP Address Pool Mode
<b>Usage</b>	Configure option 60 character string with ascii format in ip dhcp pool mode. The no command deletes the configured option 60.
<b>Example</b>	Configure option 60 with ascii format to be "AP 1000". Switch#config Switch(config)#ip dhcp pool a switch (dhcp-a-config)#option 60 ascii AP 1000

### 11.1.80 option 60 hex WORD

<b>Syntax</b>	<b>option 60 hex WORD</b> <b>no option 60</b>
<b>Parameter</b>	<b>WORD</b> The configured option 60 character string with hex format, such as a1241b
<b>Default</b>	No option 60 is configured.
<b>Mode</b>	DHCP Address Pool Mode
<b>Usage</b>	Configure option 60 character string with hex format in ip dhcp pool mode. The no command deletes the configured option 60.
<b>Example</b>	Configure option 60 with hex format to be "01040a010101". Switch#config Switch(config)#ip dhcp pool a switch (dhcp-a-config)#option 60 hex 01040a010101

### 11.1.81 option 60 ip A.B.C.D

<b>Syntax</b>	<b>option 60 ip A.B.C.D</b> <b>no option 60</b>
<b>Parameter</b>	<b>A.B.C.D</b> The configured option 60 with IP format, such as 192.168.1.1.
<b>Default</b>	No option 60 is configured.
<b>Mode</b>	DHCP Address Pool Mode
<b>Usage</b>	Configure option 60 character string with IP format in ip dhcp pool mode. The no command deletes the configured option 60. Using this command to configure option 60, such as "192.168.1.1", option 60 of packets matched with the configured option 60 is "C0A80101".
<b>Example</b>	Configure option 60 with IP format to be "192.168.1.1". Switch#config Switch(config)#ip dhcp pool a switch (dhcp-a-config)#option 60 ip 192.168.1.1

## 11.1.82 address range

<b>Syntax</b>	<p>address range &lt;start-ip&gt; &lt;end-ip&gt;</p> <p>no address range &lt;start-ip&gt; &lt;end-ip&gt;</p>
<b>Parameter</b>	<p>&lt;start-ip&gt; defines the start address of the address pool</p> <p>&lt;end-ip&gt; defines the end address of the address pool</p>
<b>Default</b>	None
<b>Mode</b>	DHCPv6 address pool class configuration mode
<b>Usage</b>	<p>This command is used to set address range for a DHCPv6 class in DHCPv6 address pool configuration mode, the no command is used to remove the address range. The prefix/plen form is not supported.</p> <p>It is necessary to check the address range assigned to class in order to make sure that it doesn't exceed the address range of relevant address pool. A class is assigned a single address range and the address range assigned to different class in the same address pool can overlap. If you do not use this command to assign address range for a DHCPv6 class, then the range for it will be the whole subnet of the address pool by default.</p>
<b>Example</b>	<p>Associate a DHCPv6 class named CLASS1 to dhcpv6 pool 1 and assign the address range from 2001:da8:100:1::2 to 2001:da8:100:1::30 for CLASS1.</p> <pre>Switch#config Switch(config)#ipv6 dhcp pool 1 Switch(dhcp-1-config)#class CLASS1 Switch(dhcp-1-class-CLASS1-config)#address range 2001:da8:100:1::2 2001:da8:100:1::30</pre>

## 11.1.83 class

<b>Syntax</b>	<code>class &lt;class-name&gt;</code> <code>no class &lt;class-name&gt;</code>
<b>Parameter</b>	<code>&lt;class-name&gt;</code> name of DHCPv6 class.
<b>Default</b>	none
<b>Mode</b>	DHCPv6 address pool class configuration mode
<b>Usage</b>	<p>This command associates class to address pool in DHCPv6 address pool configuration mode and enters class configuration mode in address pool. Use the no command to remove the link.</p> <p>It is recommended to define this class first using global command of IPv6 DHCP class. No class will be created if you input a class name which doesn't exist.</p>
<b>Example</b>	<p>Associate the DHCPv6 class named CLASS1 to dhcpv6 pool 1.</p> <pre>Switch(Config)#ipv6 dhcp pool 1 Switch(dhcp-1-config)#class CLASS1</pre>

### 11.1.84 ipv6 dhcp class

---

<b>Syntax</b>	<code>ipv6 dhcp class &lt;class-name&gt;</code> <code>no ipv6 dhcp class &lt;class-name&gt;</code>
<b>Parameter</b>	<code>&lt;class-name&gt;</code> the name of DHCPv6 class which is a string with a length of less than 32
<b>Default</b>	none
<b>Mode</b>	Global Mode
<b>Usage</b>	<p>This command defines a DHCPv6 class and enters DHCPv6 class configuration mode, the no operation of this command removes this DHCPv6 class.</p> <p>Configure a group of option 37 or option 38, or configure option 37 and option 38 simultaneously in a DHCPv6 class. This command can be used when the server supports DHCPv6 class only.</p>
<b>Example</b>	<p>Define a DHCPv6 class named CLASS1.</p> <pre>Switch(config)#ipv6 dhcp class CLASS1</pre>

---



### 11.1.85 ipv6 dhcp relay remote-id

<b>Syntax</b>	<pre>ipv6 dhcp relay remote-id &lt;remote-id&gt; no ipv6 dhcp relay remote-id</pre>
<b>Parameter</b>	<pre>&lt;remote-id&gt;          user-defined content of option 37.</pre>
<b>Default</b>	Using vlan MAC address as remote-id content by default such as "00-01-ac-12-23" with '-' hyphen.
<b>Mode</b>	Port mode
<b>Usage</b>	<p>This command is used to set the form of adding option 37 in received DHCPv6 request packets, of which &lt;remote-id&gt; is the remote-id in user-defined option 37 and it is a string with a length of less than 128. The no operation of this command restores remote-id in option 37 to enterprise-number together with vlan MAC address.</p> <p>Because the option 37 information added by switch may associate with third-party DHCPv6 servers, users can specify the remote-id content based on server condition when default remote-id of the switch cannot satisfy the demand of server. The enterprise-number together with vlan MAC address is used as the remote-id by default.</p>
<b>Example</b>	<pre>Enable abc as the remote-id of DHCPv6 option 37.  Switch#config Switch(config)#interface vlan 1 Switch(config-if-vlan1)# ipv6 dhcp relay remote-id abc</pre>

## 11.1.86 ipv6 dhcp relay remote-id option

<b>Syntax</b>	<b>ipv6 dhcp relay remote-id option</b> <b>no ipv6 dhcp relay remote-id option</b>
<b>Parameter</b>	<b>none</b>
<b>Default</b>	Disable the relay option 37.
<b>Mode</b>	Global Mode
<b>Usage</b>	<p>This command enables switch relay to support the option 37, the no form of this command disables it.</p> <p>Only after this command is configured, DHCPv6 relay agent can add option 37 in DHCPv6 request packets before sending it to server or next relay agent. Make sure that DHCPv6 service has been enabled before execute this command.</p>
<b>Example</b>	<p>Enable the switch relay to support option 37.</p> <pre>Switch#config Switch(config)#service dhcpv6 Switch(config)#ipv6 dhcp relay remote-id option</pre>

## 11.1.87 ipv6 dhcp relay subscriber-id

<b>Syntax</b>	<code>ipv6 dhcp relay subscriber-id &lt;subscriber-id&gt;</code> <code>no ipv6 dhcp relay subscriber-id</code>
<b>Parameter</b>	<code>&lt;subscriber-id&gt;</code> user-defined content of option 38
<b>Default</b>	Set subscriber-id in option 38 to vlan name together with port name.
<b>Mode</b>	Port mode
<b>Usage</b>	<p>This command is used to set the form of adding option 38 in received DHCPv6 request packets, of which <code>&lt;subscriber-id&gt;</code> is the subscriber-id in user-defined option 38 and it is a string with a length of less than 128.</p> <p>Because the option 38 information added by switch may associate with third-party DHCPv6 servers, users can specify the subscriber-id content based on server condition when standard subscriber-id of the switch cannot satisfy the demand of server. The vlan name together with physical port name is used as the subscriber-id in option 38 by default.</p>
<b>Example</b>	<p>Enable abc as the subscriber-id of DHCPv6 option 38.</p> <pre>Switch#config Switch(config) # interface vlan 1 Switch(config-if-vlan1)# ipv6 dhcp relay subscriber-id abc</pre>

### 11.1.88 ipv6 dhcp relay subscriber-id option

<b>Syntax</b>	<code>ipv6 dhcp relay subscriber-id option</code> <code>no ipv6 dhcp relay subscriber-id option</code>
<b>Parameter</b>	<code>none</code>
<b>Default</b>	Disable the relay option 38.
<b>Mode</b>	Global Mode
<b>Usage</b>	Only after this command is configured, DHCPv6 relay agent can add option 38 in DHCPv6 request packets before sending it to server or next relay agent. Make sure that DHCPv6 service has been enabled before execute this command. The option 38 of switch relay is disabled by default.
<b>Example</b>	Enable the switch relay to support option 38. <code>Switch#config</code> <code>Switch(config) # service dhcpv6</code> <code>Switch(Config)#ipv6 dhcp relay subscriber-id option</code>

### 11.1.89 ipv6 dhcp relay subscriber-id select delimiter

<b>Syntax</b>	<pre>ipv6 dhcp relay subscriber-id select (sp   sv   pv   spv) delimiter WORD (delimiter WORD )</pre> <pre>no ipv6 dhcp relay subscriber-id select delimiter</pre>
<b>Parameter</b>	<p><b>(sp   sv   pv   spv)</b> a selection in combinations of slot, port and vlan, among which <b>sp</b> represents slot and port, <b>sv</b> represents slot and vlan, <b>pv</b> represents port and vlan, and <b>spv</b> represents slot, port and vlan.</p> <hr/> <p><b>WORD</b> the delimiter between slot, port and vlan which ranges among (# . . ; : / space). Note that there're two <b>delimiter WORDs</b> here, of which the former is the delimiter between slot and port and the latter is the one between port and vlan.</p>
<b>Default</b>	Null
<b>Mode</b>	Global Mode
<b>Usage</b>	<p>Configures user configuration options to generate subscriber-id. The no form of this command restores to its original default configuration, i.e. vlan name together with port name.</p> <p>The command has no effect on ports with self-defined subscriber-id. If user redefines the subscriber-id of the port after using the command, the user-defined one prevails. This configuration is null by default.</p>
<b>Example</b>	<pre>Switch#config</pre> <pre>Switch(config)#ipv6 dhcp relay subscriber-id select sp delimiter #</pre>

## 11.1.90 ipv6 dhcp server remote-id option

<b>Syntax</b>	<code>ipv6 dhcp server remote-id option</code> <code>no ipv6 dhcp server remote-id option</code>
<b>Parameter</b>	None
<b>Default</b>	Do not support option 37.
<b>Mode</b>	Global Mode
<b>Usage</b>	<p>This command enables DHCPv6 server to support the identification of option 37, the no form of this command disables it.</p> <p>Configure this command if option 37 options is expected to be identified and processed by DHCPv6 server, otherwise they will be ignored. Option 37 is not supported by default.</p>
<b>Example</b>	<p>Enable the DHCPv6 server to support option 37.</p> <pre>Switch#config Switch(config)#ipv6 dhcp server remote-id option</pre>

### 11.1.91 ip dhcp server select relay-forw

<b>Syntax</b>	<code>ipv6 dhcp server select relay-forw</code> <code>no ipv6 dhcp server select relay-forw</code>
<b>Parameter</b>	none
<b>Default</b>	Selecting option 37 and option 38 of the original packets.
<b>Mode</b>	Global Mode
<b>Usage</b>	<p>This command enables the DHCPv6 server to support selections when multiple option 37 or option 38 options exist and the option 37 and option 38 of relay-forw in the innermost layer are selected. The no operation of it restores the default configuration, i.e. selecting option 37 and option 38 of the original packets.</p> <p>Make sure that the server has been enabled to support option 37 and option 38 before use this command. The system selects option 37 and option 38 of the original packets by default.</p>
<b>Example</b>	<p>Configure that the vlan1 interface of DHCPv6 server selects option 37 and option 38 of relay-forw in the innermost layer.</p> <pre>Switch#config Switch(config)#interface vlan 1 Switch(config-if-vlan1)# ipv6 dhcp server select relay-forw</pre>

## 11.1.92 ipv6 dhcp server subscriber-id option

<b>Syntax</b>	<code>ipv6 dhcp server subscriber-id option</code> <code>no ipv6 dhcp server subscriber-id option</code>
<b>Parameter</b>	none
<b>Default</b>	Do not support option 38.
<b>Mode</b>	Global Mode
<b>Usage</b>	<p>This command enables DHCPv6 server to support the identification of option 38, the no operation of this command disables it.</p> <p>Configure this command if option 38 is expected to be identified and processed by DHCPv6 server, otherwise they will be ignored. option 38 is not supported by default.</p>
<b>Example</b>	<p>Enable DHCPv6 server to support option 38.</p> <pre>Switch#config Switch(config)#ipv6 dhcp server subscriber-id option</pre>

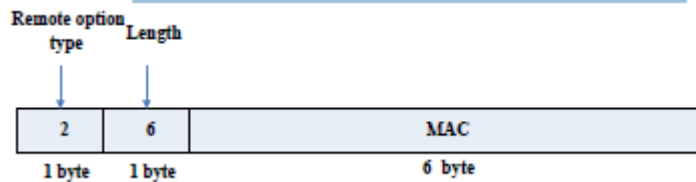


### 11.1.93 ipv6 dhcp snooping information option remote-id format

<b>Syntax</b>	<code>ipv6 dhcp snooping information option remote-id format {hex   ascii }</code>	
<b>Parameter</b>	<b>hex</b>	Hex means that the remote-id is the VLAN MAC address of the hexadecimal switch.
	<b>ascii</b>	ascii means that the remote-id is the VLAN MAC address of the ascii format switch.
<b>Default</b>	ascii	
<b>Mode</b>	Global Mode	

**Usage** This command can configure the remote-id format of the switch relay agent's DHCPv6 option37.

The hexadecimal remote-id format's definition is as below:



The MAC is the VLAN MAC address of the switch.

**Example** Configure the default remote-id format of the switch relay agent's DHCPv6 option37.  
Switch#config  
Switch(config)#ipv6 dhcp snooping information option remote-id format ascii

### 11.1.94 ipv6 dhcp snooping information option subscriber-id format

<b>Syntax</b>	ipv6 dhcp snooping information option subscriber-id format {hex   ascii }																																								
<b>Parameter</b>	<b>hex</b>	hex means that the subscriber-id is the hexadecimal VLAN and port information																																							
	<b>ascii</b>	ascii means that the subscriber-id is the ACSII VLAN and port information.																																							
<b>Default</b>	ascii																																								
<b>Mode</b>	Global Mode																																								
<b>Usage</b>	<p>Configure the default subscribe-id format of the switch DHCPv6 snooping option38. The ACSII VLAN and port information is as Vlan1+Ethernet1/0/11. The hexadecimal VLAN and port information is defined as below:</p> <table border="1" style="margin-left: auto; margin-right: auto;"> <tr> <td style="text-align: center;">Suboption type</td> <td style="text-align: center;">Length</td> <td style="text-align: center;">Circuit ID type</td> <td style="text-align: center;">Length</td> <td></td> <td></td> <td></td> <td></td> <td></td> </tr> <tr> <td style="text-align: center;">↓</td> <td style="text-align: center;">↓</td> <td style="text-align: center;">↓</td> <td style="text-align: center;">↓</td> <td style="text-align: center;">1</td> <td style="text-align: center;">8</td> <td style="text-align: center;">0</td> <td style="text-align: center;">6</td> <td style="text-align: center;">VLAN</td> <td style="text-align: center;">Slot</td> <td style="text-align: center;">Module</td> <td style="text-align: center;">Port</td> </tr> <tr> <td></td> <td></td> <td></td> <td></td> <td style="text-align: center;">1 byte</td> <td style="text-align: center;">1 byte</td> <td style="text-align: center;">1 byte</td> <td style="text-align: center;">1 byte</td> <td style="text-align: center;">2 byte</td> <td style="text-align: center;">1 byte</td> <td style="text-align: center;">1 byte</td> <td style="text-align: center;">2 byte</td> </tr> </table> <p>The VLAN field is written with the switch VLAN ID. For the rackmount switch, Slot means the slot number; for the cassette switch, it is 1. The default module is 0. Port means the port number and starts from 1.</p>								Suboption type	Length	Circuit ID type	Length						↓	↓	↓	↓	1	8	0	6	VLAN	Slot	Module	Port					1 byte	1 byte	1 byte	1 byte	2 byte	1 byte	1 byte	2 byte
Suboption type	Length	Circuit ID type	Length																																						
↓	↓	↓	↓	1	8	0	6	VLAN	Slot	Module	Port																														
				1 byte	1 byte	1 byte	1 byte	2 byte	1 byte	1 byte	2 byte																														
<b>Example</b>	<p>Configure the subscribe-id format of the switch DHCPv6 snooping option38 as the hexadecimal format.</p> <pre>Switch#config Switch(config)#ipv6 dhcp snooping information option subscriber-id format hex</pre>																																								

### 11.1.95 ipv6 dhcp snooping remote-id

<b>Syntax</b>	<pre>ipv6 dhcp snooping remote-id &lt;remote-id&gt; no ipv6 dhcp snooping remote-id</pre>
<b>Parameter</b>	<pre>&lt;remote-id&gt;          user-defined content of option 37.</pre>
<b>Default</b>	Using vlan MAC address as remote-id content by default such as "00-01-ac-12-23" with '-' hyphen.
<b>Mode</b>	Port mode
<b>Usage</b>	<p>This command is used to set the form of adding option 37 in received DHCPv6 request packets, of which &lt;remote-id&gt; is the content of remote-id in user-defined option 37 and it is a string with a length of less than 128. The no form of this command restores remote-id in option 37 to enterprise-number together with vlan MAC address.</p> <p>Because option 37 information added by switch may associate with third-party DHCPv6 servers, users can specify remote-id content based on server condition when standard remote-id of the switch cannot satisfy the demand of server. The enterprise-number together with vlan MAC address is used as the remote-id by default.</p>
<b>Example</b>	<pre>Enable abc as remote-id of DHCPv6 option 37. Switch#config Switch(config)#interface ethernet 1/0/1 Switch(config-if-Ethernet1/0/1)#ipv6 dhcp snooping remote-id abc</pre>

### 11.1.96 ipv6 dhcp snooping remote-id option

<b>Syntax</b>	<code>ipv6 dhcp snooping remote-id option</code> <code>no ipv6 dhcp snooping remote-id option</code>
<b>Parameter</b>	none
<b>Default</b>	Disable.
<b>Mode</b>	Global Mode
<b>Usage</b>	<p>This command enables DHCPv6 SNOOPING to support option 37, the no form of this command disables it.</p> <p>Only after this command is configured, DHCPv6 SNOOPING can add option 37 in DHCPv6 packets before sending it to server or relay agent. Make sure that DHCPv6 SNOOPING has been enabled before execute this command. The system disables option 37 of DHCPv6 SNOOPING by default.</p>
<b>Example</b>	<p>Enable option 37 in DHCPv6 SNOOPING.</p> <pre>Switch#config Switch(config)#ipv6 dhcp snooping enable Switch(config)#ipv6 dhcp snooping remote-id option</pre>

### 11.1.97 ipv6 dhcp snooping remote-id policy

<b>Syntax</b>	<code>ipv6 dhcp snooping remote-id policy {drop   keep   replace}</code> <code>no ipv6 dhcp snooping remote-id policy</code>						
<b>Parameter</b>	<table border="1"> <tr> <td><b>drop</b></td> <td>The system only discards it via option 37</td> </tr> <tr> <td><b>keep</b></td> <td>The system keeps option 37 unchanged and forwards the packet</td> </tr> <tr> <td><b>replace</b></td> <td>The system will replace the option 37 field in the existing message with its own option 37 before forwarding the message to the server.</td> </tr> </table>	<b>drop</b>	The system only discards it via option 37	<b>keep</b>	The system keeps option 37 unchanged and forwards the packet	<b>replace</b>	The system will replace the option 37 field in the existing message with its own option 37 before forwarding the message to the server.
<b>drop</b>	The system only discards it via option 37						
<b>keep</b>	The system keeps option 37 unchanged and forwards the packet						
<b>replace</b>	The system will replace the option 37 field in the existing message with its own option 37 before forwarding the message to the server.						
<b>Default</b>	Using replace mode to replace option 37 of current packets with system's own.						
<b>Mode</b>	Global Mode						
<b>Usage</b>	Since DHCPv6 client packets may already include option 37 information, corresponding processing policy of DHCPv6 SNOOPING is required to develop. If the forwarding policy is set as <b>replace</b> , option 37 has to be enabled in advance. Use replace mode to replace option 37 of current packets with system's own by default.						
<b>Example</b>	<pre>Configure the reforward policy of DHCPv6 packets with option 37 as keep for DHCPv6 SNOOPING Switch#config Switch(config)#ipv6 dhcp snooping remote-id policy keep</pre>						

### 11.1.98 ipv6 dhcp snooping subscriber-id

<b>Syntax</b>	<code>ipv6 dhcp snooping subscriber-id &lt;subscriber-id&gt;</code> <code>no ipv6 dhcp snooping subscriber-id</code>
<b>Parameter</b>	<subscriber-id>                      user-defined content of option 38
<b>Default</b>	Set subscriber-id in option 38 to vlan name together with port name.
<b>Mode</b>	Port mode
<b>Usage</b>	<p>This command is used to set the form of adding option 38 in received DHCPv6 request packets, of which &lt;subscriber-id&gt; is the content of subscriber-id in user-defined option 38 and it is a string with a length of less than 128. The no operation of this command restores subscriber-id in option 38 to vlan name together with port name such as "Vlan2+Ethernet1/0/2".</p> <p>Because option 38 information added by switch may associate with third-party DHCPv6 servers, users can specify subscriber-id content based on server condition when standard subscriber-id of the switch cannot satisfy the demand of server. The vlan name together with physical port name is used as subscriber-id in option 38 by default.</p>
<b>Example</b>	<p>Enable abc as subscriber-id of DHCPv6 option 38.</p> <pre>Switch#config Switch(config)#interface ethernet 1/0/1 Switch(config-if-ethernet1/0/1)#ipv6 dhcp snooping subscriber-id abc</pre>

## 11.1.99 ipv6 dhcp snooping subscriber-id option

<b>Syntax</b>	<code>ipv6 dhcp snooping subscriber-id option</code> <code>no ipv6 dhcp snooping subscriber-id option</code>
<b>Parameter</b>	none
<b>Default</b>	Disable option 38 of DHCPv6 SNOOPING.
<b>Mode</b>	DHCP Address Pool Mode
<b>Usage</b>	<p>This command enables DHCPv6 SNOOPING to support option 38, the no form of this command disables it.</p> <p>Only after this command is configured, DHCPv6 SNOOPING can add option 38 in DHCPv6 packets before sending it to server or relay agent. Make sure that DHCPv6 SNOOPING has been enabled before executing this command. The system disables option 38 of DHCPv6 SNOOPING by default.</p>
<b>Example</b>	<p>Enable option 38 in DHCPv6 SNOOPING.</p> <pre>Switch#config Switch(config)#ipv6 dhcp snooping enable Switch(config)#ipv6 dhcp snooping subscriber-id option</pre>

### 11.1.100 ipv6 dhcp snooping subscriber-id policy

<b>Syntax</b>	<pre>ipv6 dhcp snooping subscriber-id policy {drop   keep   replace} no ipv6 dhcp snooping subscriber-id policy</pre>						
<b>Parameter</b>	<table border="1"> <tr> <td><b>drop</b></td> <td>The system only discards it via option 38</td> </tr> <tr> <td><b>keep</b></td> <td>The system keeps option 38 unchanged and forwards the packet</td> </tr> <tr> <td><b>replace</b></td> <td>The system will replace the option 38 field in the existing message with its own option 38 before forwarding the message to the server.</td> </tr> </table>	<b>drop</b>	The system only discards it via option 38	<b>keep</b>	The system keeps option 38 unchanged and forwards the packet	<b>replace</b>	The system will replace the option 38 field in the existing message with its own option 38 before forwarding the message to the server.
<b>drop</b>	The system only discards it via option 38						
<b>keep</b>	The system keeps option 38 unchanged and forwards the packet						
<b>replace</b>	The system will replace the option 38 field in the existing message with its own option 38 before forwarding the message to the server.						
<b>Default</b>	Using replace mode to replace option 38 of current packets with system's own.						
<b>Mode</b>	Global Mode						
<b>Usage</b>	<p>Since DHCPv6 client packets may already include option 38 information, corresponding processing policy of DHCPv6 SNOOPING is requested to develop. If the reforward policy is set as <b>replace</b>, option 38 has to be enabled in advance. The system disables option 38 of DHCPv6 SNOOPING by default.</p>						
<b>Example</b>	<pre>Set the reforward policy of DHCPv6 packets with option 38 as keep for DHCPv6 SNOOPING.  Switch#config Switch(config)#ipv6 dhcp snooping subscriber-id policy keep</pre>						



### 11.1.101 ipv6 dhcp snooping subscriber-id select delimiter

<b>Syntax</b>	<pre>ipv6 dhcp snooping subscriber-id select (sp   sv   pv   spv) delimiter WORD (delimiter WORD   )</pre>
<hr/>	
<b>no ipv6 dhcp snooping subscriber-id select delimiter</b>	
<b>Parameter</b>	<p><b>(sp   sv   pv   spv)</b> a selection from combinations of slot, port and vlan, among which <b>sp</b> represents slot and port, <b>sv</b> represents slot and vlan, <b>pv</b> represents port and vlan, and <b>spv</b> represents slot, port and vlan.</p> <hr/> <p><b>WORD</b> the delimiter between slot, port and vlan which ranges among (# . . ; : / space). Note that there're two delimiter WORDs here, of which the former is the delimiter between slot and port while the latter is that between port and vlan.</p>
<b>Default</b>	null
<b>Mode</b>	Global Mode
<hr/>	
<b>Usage</b>	<p>Configure user configuration options to generate subscriber-id. The no form of this command restores to its original default configuration, i.e. vlan name together with port name.</p> <p>This command has no effect on ports with self-defined subscriber-id. If a user redefines subscriber-id of the port after configuring the command, the user-defined one prevails.</p> <p>This configuration is null by default.</p>
<b>Example</b>	<pre>Switch#config Switch(config)#ipv6 dhcp snooping subscriber-id select sv delimiter #</pre>

### 11.1.102 ipv6 dhcp use class

---

<b>Syntax</b>	<b>ipv6 dhcp use class</b> <b>no ipv6 dhcp use class</b>
<b>Parameter</b>	none
<b>Default</b>	DHCPv6 server supports DHCPv6 class during address assignment.
<b>Mode</b>	Global Mode
<b>Usage</b>	<p>This command enables DHCPv6 server to support DHCPv6 class during address assignment, the no operation of this command disables it without removing the relative DHCPv6 class information that has been configured.</p> <p>By default, DHCPv6 servers support DHCPv6 class during address assignment and the no form of this command doesn't remove DHCPv6 class information that has been configured. Make sure that DHCPv6 service has been enabled before using this command. DHCPv6 server supports DHCPv6 class during address assignment by default.</p>
<b>Example</b>	<p>Configure DHCPv6 server to support DHCPv6 class during address assignment.</p> <pre>Switch#config Switch(config)# ipv6 dhcp use class</pre>

---

### 11.1.103 remote-id subscriber-id

<b>Syntax</b>	<code>{remote-id [*] &lt;remote-id&gt; [*]   subscriber-id [*] &lt;subscriber-id&gt; [*]}</code> <code>no {remote-id [*] &lt;remote-id&gt; [*]   subscriber-id [*] &lt;subscriber-id&gt; [*]}</code>						
<b>Parameter</b>	<table border="1"> <tr> <td><code>&lt;remote-id&gt;</code></td> <td>a string with a length ranging from 1 to 128 bytes is used to match remote-id in option 37.</td> </tr> <tr> <td><code>&lt;subscriber-id&gt;</code></td> <td>a string with a length ranging from 1 to 128 bytes is used to match subscriber-id in option 38.</td> </tr> <tr> <td><code>[*]</code></td> <td>match zero or more characters.</td> </tr> </table>	<code>&lt;remote-id&gt;</code>	a string with a length ranging from 1 to 128 bytes is used to match remote-id in option 37.	<code>&lt;subscriber-id&gt;</code>	a string with a length ranging from 1 to 128 bytes is used to match subscriber-id in option 38.	<code>[*]</code>	match zero or more characters.
<code>&lt;remote-id&gt;</code>	a string with a length ranging from 1 to 128 bytes is used to match remote-id in option 37.						
<code>&lt;subscriber-id&gt;</code>	a string with a length ranging from 1 to 128 bytes is used to match subscriber-id in option 38.						
<code>[*]</code>	match zero or more characters.						
<b>Default</b>	None						
<b>Mode</b>	IPv6 DHCP Class configuration mode						
<b>Usage</b>	<p>This command configures option 37 and option 38 that match the class in IPv6 DHCP class configuration mode.</p> <p>This command configures a mode which matches with the already-defined DHCPv6 class, and a DHCPv6 class may configure multiple commands. If this command is ignored and no mode configured in IPv6 DHCP Class mode, any remote-id or subscriber-id is considered to match with the DHCPv6 class, however, remote-id or subscriber-id must exist in DHCPv6 packet.</p>						
<b>Example</b>	<pre>Configure some remote-id or subscriber-id belonging to DHCPv6 class named CLASS1. Switch#config Switch(config)#ipv6 dhcp class CLASS1 Switch(dhcpv6-class-class1-config)#remote-id abc* subscriber-id bcd* Switch(dhcpv6-class-class1-config)#remote-id edf* Switch(dhcpv6-class-class1-config)#subscriber-id *mmn</pre>						

## 11.1.104 show ipv6 dhcp relay option

<b>Syntax</b>	<code>show ipv6 dhcp relay option</code>
<b>Parameter</b>	none
<b>Default</b>	none
<b>Mode</b>	Admin and Configuration Mode
<b>Usage</b>	Use this command to check relay agents' configuration status for option 37 and option 38.
<b>Example</b>	Switch#show ipv6 dhcp relay option remote-id option enable subscriber-id option enable Interface Vlan 1: remote-id option configure "abc"

## 11.1.105 show ipv6 dhcp snooping option

<b>Syntax</b>	<code>show ipv6 dhcp snooping option</code>
<b>Parameter</b>	none
<b>Default</b>	none
<b>Mode</b>	Admin and Configuration Mode
<b>Usage</b>	Use this command to check snooping configuration status for option 37 and option 38.
<b>Example</b>	Switch#show ipv6 dhcp snooping option remote-id option enable subscriber-id option enable The slot port vlan select option is : port and vlan The delimiter is : #

### 11.1.106 enable trustview key

<b>Syntax</b>	enable trustview key {0   7} <password> no enable trustview key
<b>Parameter</b>	<password>                      <password> is character string length less than 16, which use as encrypted key.
	{0   7}                              0 for un-encrypted text for the password, while 7 for encrypted.
<b>Default</b>	Disabled
<b>Mode</b>	Global Mode
<b>Usage</b>	<p>To configure DES encrypted key for private packets, this command is also the switch for the private packets encrypt and hash function enabled or not.</p> <p>The switch communicates with the TrustView management system through private protocols. By default these packets are not encrypted. In order to prevent spoofing, it can be configured to encrypt these packets. And at the same time, the same password should be configured on TrustView server.</p>
<b>Example</b>	<p>Enable encrypt or hash function of private message</p> <pre>Switch#config Switch(config)# enable trustview key 0 switch</pre>

### 11.1.107 ip dhcp snooping

<b>Syntax</b>	<code>ip dhcp snooping enable</code> <code>no ip dhcp snooping enable</code>
<b>Parameter</b>	none
<b>Default</b>	DHCP Snooping is disabled by default
<b>Mode</b>	Global Mode
<b>Usage</b>	Enable the DHCP Snooping function. When this function is enabled, it will monitor all the DHCP Server packets of non-trusted ports.
<b>Example</b>	Enable the DHCP Snooping function. Switch#config Switch(config)#ip dhcp snooping enable

### 11.1.108 ip dhcp snooping action

<b>Syntax</b>	<code>ip dhcp snooping action {shutdown   blackhole} [recovery &lt;second&gt;]</code> <code>no ip dhcp snooping action</code>								
<b>Parameter</b>	<table border="1"> <tr> <td><b>shutdown</b></td> <td>When the port detects a fake DHCP Server, it will be shutdown.</td> </tr> <tr> <td><b>blackhole</b></td> <td>When the port detects a fake DHCP Server, the vid and source MAC of the fake packet will be used to block the traffic from this MAC.</td> </tr> <tr> <td><b>recovery</b></td> <td>Users can set to recover after the automatic defense action being executed.(no shut ports or delete correponding blackhole) .</td> </tr> <tr> <td><b>&lt;second&gt;</b></td> <td>Users can set how long after the execution of defense action to recover. The unit is second, and valid range is 10-3600.</td> </tr> </table>	<b>shutdown</b>	When the port detects a fake DHCP Server, it will be shutdown.	<b>blackhole</b>	When the port detects a fake DHCP Server, the vid and source MAC of the fake packet will be used to block the traffic from this MAC.	<b>recovery</b>	Users can set to recover after the automatic defense action being executed.(no shut ports or delete correponding blackhole) .	<b>&lt;second&gt;</b>	Users can set how long after the execution of defense action to recover. The unit is second, and valid range is 10-3600.
<b>shutdown</b>	When the port detects a fake DHCP Server, it will be shutdown.								
<b>blackhole</b>	When the port detects a fake DHCP Server, the vid and source MAC of the fake packet will be used to block the traffic from this MAC.								
<b>recovery</b>	Users can set to recover after the automatic defense action being executed.(no shut ports or delete correponding blackhole) .								
<b>&lt;second&gt;</b>	Users can set how long after the execution of defense action to recover. The unit is second, and valid range is 10-3600.								
<b>Default</b>	No default defense action.								
<b>Mode</b>	Port mode								
<b>Usage</b>	<p>Set or delete the automatic defense action of a port.</p> <p>Only when DHCP Snooping is globally enabled, can this command be set. Trusted port will not detect fake DHCP Server, so, will never trigger the corresponding defense action. When a port turns into a trusted port from a non-trusted port, the original defense action of the port will be automatically deleted.</p>								
<b>Example</b>	<p>Set the DHCP Snooping defense action of port ethernet1/0/1 as setting blackhole, and the recovery time is 30 seconds.</p> <pre>Switch#config Switch(config)#interface ethernet 1/0/1 Switch(Config-Ethernet1/0/1)#ip dhcp snooping action blackhole recovery 30</pre>								



### 11.1.109 ip dhcp snooping action MaxNum

<b>Syntax</b>	<code>ip dhcp snooping action {&lt;maxNum&gt; default}</code>
<b>Parameter</b>	<p><b>&lt;maxNum&gt;</b> the number of defense action on each port, the range of which is 1-200, and the value of which is 10 by default.</p> <p><b>default</b> recover to the default value.</p>
<b>Default</b>	The default value is 10.
<b>Mode</b>	Global Mode
<b>Usage</b>	<p>Set the number of defense action that can be simultaneously took effect.</p> <p>Set the max number of defense actions to avoid the resource exhaustion of the switch caused by attacks. If the number of alarm information is larger than the set value, then the earliest defense action will be recovered forcibly in order to send new defense actions.</p>
<b>Example</b>	<p>Set the number of port defense actions as 100.</p> <pre>Switch#config Switch(config)#ip dhcp snooping action 100</pre>

## 11.1.110 ip dhcp snooping binding

<b>Syntax</b>	<code>ip dhcp snooping binding enable</code> <code>no ip dhcp snooping binding enable</code>
<b>Parameter</b>	<code>none</code>
<b>Default</b>	DHCP Snooping binding is disabled by default.
<b>Mode</b>	Global Mode
<b>Usage</b>	Enable the DHCP Snooping binding function. When the function is enabled, it will record the binding information allocated by DHCP Server of all trusted ports. Only after the DHCP SNOOPING function is enabled, the binding function can be enabled.
<b>Example</b>	Enable the DHCP Snooping binding function. Switch#config Switch(config)#ip dhcp snooping binding enable

### 11.1.111 ip dhcp snooping binding dot1x

<b>Syntax</b>	<code>ip dhcp snooping binding dot1x</code> <code>no ip dhcp snooping binding dot1x</code>
<b>Parameter</b>	<code>none</code>
<b>Default</b>	By default, the binding DOT1X function is disabled on all ports.
<b>Mode</b>	Port mode
<b>Usage</b>	<p>When this function is enabled, DHCP SNOOPING will notify the DOT1X module about the captured binding information as a DOT1X controlled user. This command is mutually exclusive to "ip dhcp snooping binding user-control" command.</p> <p>Only after the DHCP SNOOPING binding function is enabled, the binding dot1x function can be set.</p>
<b>Example</b>	<p>Enable the binding DOT1X function on port ethernet1/0/1.</p> <pre>Switch#config Switch(config) #interface ethernet 1/0/1 switch(Config-Ethernet 1/0/1)# ip dhcp snooping binding dot1x</pre>

### 11.1.112 ip dhcp snooping binding user

<b>Syntax</b>	<pre>ip dhcp snooping binding user &lt;mac&gt; address &lt;ipaddress&gt; vlan &lt;vlan-id&gt; interface [Ethernet] &lt;ifname&gt; no ip dhcp snooping binding user &lt;mac&gt; interface [Ethernet] &lt;ifname&gt;</pre>								
<b>Parameter</b>	<table border="1"> <tr> <td><b>&lt;mac&gt;</b></td> <td>The MAC address of the static binding user, which is the only index of the binding user.</td> </tr> <tr> <td><b>&lt;ipaddress&gt;</b></td> <td>The IP address of the static binding user</td> </tr> <tr> <td><b>&lt;vlan-id&gt;</b></td> <td>The VLAN ID of static binding user</td> </tr> <tr> <td><b>&lt;ifname&gt;</b></td> <td>The access interface of static binding user</td> </tr> </table>	<b>&lt;mac&gt;</b>	The MAC address of the static binding user, which is the only index of the binding user.	<b>&lt;ipaddress&gt;</b>	The IP address of the static binding user	<b>&lt;vlan-id&gt;</b>	The VLAN ID of static binding user	<b>&lt;ifname&gt;</b>	The access interface of static binding user
<b>&lt;mac&gt;</b>	The MAC address of the static binding user, which is the only index of the binding user.								
<b>&lt;ipaddress&gt;</b>	The IP address of the static binding user								
<b>&lt;vlan-id&gt;</b>	The VLAN ID of static binding user								
<b>&lt;ifname&gt;</b>	The access interface of static binding user								
<b>Default</b>	DHCP Snooping has no static binding list entry by default.								
<b>Mode</b>	Global Mode								
<b>Usage</b>	<p>The static binding users is deal in the same way as the dynamic binding users captured by DHCP SNOOPING; the following actions are all allowed: notifying DOT1X to be a controlled user of DOT1X, adding a trusted user list entry directly, adding a binding ARP list entry. The static binding users will never be aged, and have a priority higher than dynamic binding users. Only after the DHCP SNOOPING binding function is enabled, the static binding users can be enabled.</p>								
<b>Example</b>	<pre>Configure static binding users. Switch#config Switch(config)#ip dhcp snooping binding user 00-11-22-33-44-55 address 1.1.1.1 vlan 1 interface ethernet 1/0/14</pre>								

### 11.1.113 ip dhcp snooping binding user-control

<b>Syntax</b>	<pre>ip dhcp snooping binding user-control no ip dhcp snooping binding user-control</pre>
<b>Parameter</b>	None
<b>Default</b>	By default, the binding user function is disabled on all ports.
<b>Mode</b>	Port mode
<b>Usage</b>	<p>When this function is enabled, DHCP SNOOPING will treat the captured binding information as trusted users allowed to access all resources. This command is mutually exclusive to "ip dhcp snooping binding dot1x" command.</p> <p>Only after DHCP SNOOPING binding function is enabled, the binding user function can be set. This command is not limited by "ip dhcp snooping" based on VLAN, but it is only limited by the global "ip dhcp snooping enable" command.</p>
<b>Example</b>	<pre>Enable the binding USER function on port ethernet1/0/1. Switch#config Switch(config)#interface ethernet 1/0/1 Switch(Config-Ethernet 1/0/1)# ip dhcp snooping binding user-control</pre>

### 11.1.114 ip dhcp snooping binding user-control max-user

<b>Syntax</b>	<code>ipv6 dhcp snooping binding user-control max-user &lt;number&gt;</code> <code>no ip dhcp snooping binding user-control max-user</code>
<b>Parameter</b>	<code>&lt;number&gt;</code> <code>&lt;number&gt;</code> the max number of users allowed to access the port, from 0 to 1024.
<b>Default</b>	The max number of users allowed by each port to access is 1024.
<b>Mode</b>	Port mode
<b>Usage</b>	<p>Set the max number of users allowed to access the port when enabling DHCP Snooping binding user function; the no operation of this command will restore default value.</p> <p>This command defines the max number of trust users distributed according to binding information, with <b>ip dhcp snooping binding user-control</b> enabled on the port. By default, the number is 1024. Considering the limited hardware resources of the switch, the actual number of trust users distributed depends on the resource amount. If a bigger max number of users is set using this command, DHCP Snooping will distribute the binding information of untrust users to hardware to be trust users as long as there is enough available resources. Otherwise, DHCP Snooping will change the distributed binding information according to the new smaller max user number. When the number of distributed binding information entries reaches the max limit, no new DHCP will be able to become trust user or to access other network resources via the switch.</p>
<b>Example</b>	<p>Enable DHCP Snooping binding user function on Port ethernet1/0/1, setting the max number of user allowed to access by Port Ethernet1/0/1 as 5.</p> <pre>Switch#config Switch(config)#interface ethernet 1/0/1 Switch(config-ethernet 1/0/1)#ip dhcp snooping binding user-control max-user 5</pre>

## 11.1.115 ip dhcp snooping information enable

<b>Syntax</b>	<p><b>ip dhcp snooping information enable</b></p> <p><b>no ip dhcp snooping information enable</b></p>
<b>Parameter</b>	none
<b>Default</b>	Option 82 function is disabled in DHCP Snooping by default.
<b>Mode</b>	Global Mode
<b>Usage</b>	<p>This command will enable option 82 function of DHCP Snooping on the switch, the no operation of this command will disable that function.</p> <p>Only by implementing this command, can DHCP Snooping add standard option 82 to DHCP request messages and forward the message. The format of option1 in option 82 (Circuit ID option) is standard vlan name plus physical port name, like vlan1+ethernet1/0/12. That of option2 in option 82 (remote ID option) is CPU MAC of the switch, like 00030f023301. If a DHCP request message with option 82 options is received, DHCP Snooping will replace those options in the message with its own. If a DHCP reply message with option 82 options is received, DHCP Snooping will dump those options in the message and forward it.</p>
<b>Example</b>	<p>Enable option 82 function of DHCP Snooping on the switch.</p> <pre>Switch#config Switch(config)#ip dhcp snooping enable Switch(config)# ip dhcp snooping binding enable Switch(config)# ip dhcp snooping information enable</pre>

## 11.1.116 ip dhcp snooping information option allow-untrusted (replace)

<b>Syntax</b>	ip dhcp snooping information option allow-untrusted (replace) no ip dhcp snooping information option allow-untrusted (replace)
<b>Parameter</b>	(replace) When the "replace" is setting, the option82 option is allowed to replace.
<b>Default</b>	Drop DHCP packets with option82 option received by untrusted ports.
<b>Mode</b>	Global Mode
<b>Usage</b>	<p>This command is used to set that allow untrusted ports of DHCP snooping to receive DHCP packets with option82 option. When disabling this command, all untrusted ports will drop DHCP packets with option82 option.</p> <p>Usually the switch with DHCP snooping function connects the terminal user directly, so close allow-untrusted by default to avoid option82 option added by user privately. Please set uplink port as trust port when enabling the uplink of DHCP snooping function.</p>
<b>Example</b>	<p>Enable the function that receives DHCP packets with option82</p> <pre>Switch#config Switch(config)#ip dhcp snooping information option allow-untrusted</pre>



## 11.1.117 ip dhcp snooping information option delimiter

<b>Syntax</b>	<code>ip dhcp snooping information option delimiter [colon   dot   slash   space]</code> <code>no ip dhcp snooping information option delimiter</code>
<b>Parameter</b>	none
<b>Default</b>	slash (“/”)
<b>Mode</b>	Global Mode
<b>Usage</b>	<p>Set the delimiter of each parameter for suboption of option82 in global mode, no command restores the delimiter as slash.</p> <p>Divide parameters with the configured delimiters after users have defined them which are used to create suboption (remote-id, circuit-id) of option82 in global mode.</p>
<b>Example</b>	<p>Set the parameter delimiters as dot (“.”) for suboption of option82.</p> <pre>Switch#config Switch(config)#ip dhcp snooping information option delimiter dot</pre>

### 11.1.118 ip dhcp snooping information option remote-id

<b>Syntax</b>	<code>ip dhcp snooping information option remote-id {standard   &lt;remote-id&gt;}</code> <code>no ip dhcp snooping information option remote-id</code>				
<b>Parameter</b>	<table border="0"> <tr> <td><b>standard</b></td> <td>standard means the default VLAN MAC format</td> </tr> <tr> <td><b>&lt;remote-id&gt;</b></td> <td><b>&lt;remote-id&gt;</b> means the remote-id content of option 82 specified by users, its length can not exceed 64 characters.</td> </tr> </table>	<b>standard</b>	standard means the default VLAN MAC format	<b>&lt;remote-id&gt;</b>	<b>&lt;remote-id&gt;</b> means the remote-id content of option 82 specified by users, its length can not exceed 64 characters.
<b>standard</b>	standard means the default VLAN MAC format				
<b>&lt;remote-id&gt;</b>	<b>&lt;remote-id&gt;</b> means the remote-id content of option 82 specified by users, its length can not exceed 64 characters.				
<b>Default</b>	Use standard format to set remote-id.				
<b>Mode</b>	Global Mode				
<b>Usage</b>	The additive option 82 needs to associate with third-party DHCP server, it is used to specify the remote-id content by users when the standard remote-id format can not satisfy server's request .				
<b>Example</b>	<p>Set the suboption remote-id of DHCP option82 as street-1-1.</p> <pre>Switch#config Switch(config)#ip dhcp snooping information option remote-id street-1-1</pre>				

### 11.1.119 ip dhcp snooping information option self-defined remote-id

<b>Syntax</b>	<code>ip dhcp snooping information option self-defined remote-id {hostname   mac   string WORD}</code> <code>no ip dhcp snooping information option self-defined remote-id</code>
<b>Parameter</b>	<b>WORD</b> the defined character string of remote-id by themselves, the maximum length is 64.
<b>Default</b>	Using standard method.
<b>Mode</b>	Global Mode
<b>Usage</b>	<p>Set creation method for option82, users can define the parameters of remote-id suboption by themselves.</p> <p>After configure this command, if users do not configure ip dhcp snooping information option remote-id globally, it will create remote-id suboption for option82 according to self-defined method. For mac, use the format such as 00-02-d1-2e-3a-0d if it is filled to packets with ascii format, but hex format occupies 6 bytes. Each option will be filled to packets according to the configured order of the commands and divide them with delimiter (delimiter is <b>ip dhcp snooping information option delimiter</b> configuration).</p>
<b>Example</b>	<p>Set self-defined method and character string of remote-id suboption are mac and abc respectively for option82.</p> <pre>Switch#config Switch(config)#ip dhcp snooping information option self-defined remote-id mac string abc</pre>

## 11.1.120 ip dhcp snooping information option self-defined remote-id format

<b>Syntax</b>	<code>ip dhcp snooping information option self-defined remote-id format [ascii   hex]</code>	
<b>Parameter</b>	<b>hex</b>	hex means that the remote-id is the hexadecimal VLAN and port information
	<b>ascii</b>	ascii means that the remote-id is the ACSII VLAN and port information.
<b>Default</b>	ascii	
<b>Mode</b>	Global Mode	
<b>Usage</b>	Set self-defined format of remote-id for snooping option82. self-defined format use <code>ip dhcp snooping information option type self-defined remote-id</code> to create remote-id format.	
<b>Example</b>	Set self-defined format of remote-id as hex for snooping option82.	
	Switch#config	
	Switch(config)#ip dhcp snooping information option self-defined remote-id format hex	

### 11.1.121 ip dhcp snooping information option self-defined subscriber-id

<b>Syntax</b>	<pre>ip dhcp snooping information option self-defined subscriber-id {vlan   port   id (switch-id (mac   hostname)  remote-mac)   string WORD} no ip dhcp snooping information option type self-defined subscriber-id</pre>
<b>Parameter</b>	<p><b>WORD</b>                                  <b>WORD</b> the defined character string of circuit-id by themselves, the maximum length is 64.</p>
<b>Default</b>	Using standard method.
<b>Mode</b>	Global Mode
<b>Usage</b>	<p>Set creation method for option82, users can define the parameters of circute-id suboption by themselves.</p> <p>After configure this command, if users do not configure circuit-id on port, it will create circuit-id suboption for option82 according to self-defined method. Self-defined format of circuit-id: if self-defined subscriber-id format is ascii, the filled format of vlan such as "Vlan2", the format of port such as "Ethernet1/0/1", the format of mac and remote-mac such as "00-02-d1-2e-3a-0d". If self-defined format is hex, the filled format of vlan occupies 2 bytes, port occupies 4 bytes, a byte means slot (for chassis switch, it means slot ID, for box switch, it is 1), a byte means Module (the default is 0), two bytes means port ID beginning from 1, mac and remote-mac occupy 6 bytes. Each option will be filled to packets according to the configured order of the commands and divide them with delimiter (delimiter is <b>ip dhcp snooping information option delimiter</b> configuration).</p>
<b>Example</b>	<p>Set self-defined method of circuit-id suboption as vlan, port, mac and remote-mac for option82.</p> <pre>Switch#config Switch(config)#ip dhcp snooping information option self-defined subscriber-id vlan port id remote- mac</pre>

## 11.1.122 ip dhcp snooping information option self-defined subscriber-id format

<b>Syntax</b>	<b>ip dhcp snooping information option self-defined subscriber-id format [ascii   hex]</b>	
<b>Parameter</b>	<b>hex</b>	hex means that the subscriber-id is the hexadecimal VLAN and port information
	<b>ascii</b>	ascii means that the subscriber-id is the ACSII VLAN and port information.
<b>Default</b>	ascii	
<b>Mode</b>	Global Mode	
<b>Usage</b>	Set self-defined format of circuit-id for snooping option82. self-defined format uses ip dhcp snooping information option type self-defined subscriber-id to create circuit-id format.	
<b>Example</b>	Set self-defined format of circuit-id as hex for snooping option82.	
	Switch#config Switch(config)#ip dhcp snooping information option self-defined subscriber-id format hex	

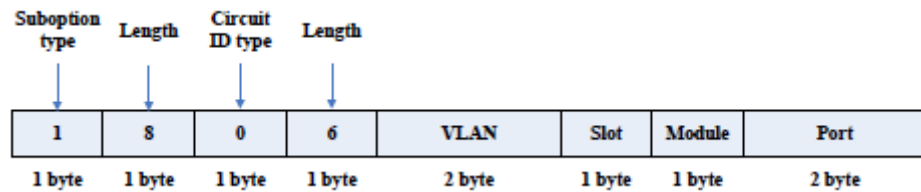
### 11.1.123 ip dhcp snooping information option subscriber-id

<b>Syntax</b>	<code>ip dhcp snooping information option subscriber-id {standard   &lt;circuit-id&gt;}</code> <code>no ip dhcp snooping information option subscriber-id</code>
<b>Parameter</b>	<p><b>standard</b>                      standard means the standard format of VLAN name and physical port name, such as Vlan2+Ethernet1/0/12.</p> <hr/> <p><b>&lt;circuit-id&gt;</b>                      <b>&lt;circuit-id&gt;</b> means the circuit-id content of option 82 specified by users, its length can not exceed 64 characters.</p>
<b>Default</b>	Use standard format to set circuit-id.
<b>Mode</b>	Port mode
<b>Usage</b>	<p>Set the suboption1 (circuit ID option) content of option 82 added by DHCP request packets (they are received by the port). The no command sets the additive suboption1 (circuit ID option) format of option 82 as standard.</p> <p>The additive option 82 needs to associate with third-party DHCP server, it is used to specify the circuit-id content by user when the standard circuit-id format can not satisfy server's request.</p>
<b>Example</b>	<p>Set the suboption circuit-id of DHCP option82 as P2.</p> <pre>Switch#config Switch(config)#interface ethernet 1/0/1 Switch(config-if-ethernet1/0/1)#ip dhcp snooping information option subscriber-id P2</pre>

### 11.1.124 ipv6 dhcp snooping information option subscriber-id format

<b>Syntax</b>	<b>ip dhcp snooping information option subscriber-id format {hex   ascii   vs-hp}</b>	
<b>Parameter</b>	<b>hex</b>	hex means that subscriber-id is VLAN and port information with hexadecimal format
	<b>ascii</b>	ascii means that subscriber-id is VLAN and port information with ASCII format.
	<b>vs-hp</b>	vs-hp means that subscriber-id is compatible with the format of HP manufacturer.
<b>Default</b>	ascii	
<b>Mode</b>	Global Mode	

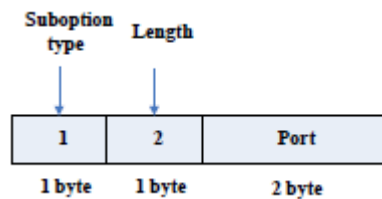
**Usage** This command is used to set subscriber-id format of DHCP snooping option82. VLAN and port information with ASCII format, such as Vlan1+Ethernet1/0/11, VLAN and port



information with hexadecimal format defined as below:

VLAN field fill in VLAN ID. For chassis switch, Slot means slot number, for box switch, Slot is 1; default Module is 0; Port means port number which begins from 1.

The compatible subscriber-id format with HP manufacturer defined as below:



Port means port number which begins from 1.

<b>Example</b>	Set subscriber-id format of DHCP snooping option82 as hexadecimal format. Switch#config Switch(config)#ip dhcp snooping information option subscriber-id format hex
----------------	---



## 11.1.125 ip dhcp snooping limit-rate

<b>Syntax</b>	<code>ip dhcp snooping limit-rate &lt;pps&gt;</code> <code>no ip dhcp snooping limit-rate</code>
<b>Parameter</b>	<code>&lt;pps&gt;</code> The number of DHCP messages transmitted in every minute, ranging from 0 to 100. Its default value is 100. 0 means that no DHCP message will be transmitted.
<b>Default</b>	The default value is 100.
<b>Mode</b>	Global Mode
<b>Usage</b>	Set the DHCP message rate limit After enabling DHCP snooping, the switch will monitor all the DHCP messages and implement software transmission. The software performance of the switch is relative to the type of the switch, its current load and so on.
<b>Example</b>	Set the message transmission rate as 50pps. Switch#config Switch(config)# ip dhcp snooping limit-rate 50

## 11.1.126 ip dhcp snooping trust

<b>Syntax</b>	<code>ip dhcp snooping trust</code> <code>no ip dhcp snooping trust</code>
<b>Parameter</b>	<code>none</code>
<b>Default</b>	By default, all ports are non-trusted ports
<b>Mode</b>	Port mode
<b>Usage</b>	<p>Set or delete the DHCP Snooping trust attributes of a port.</p> <p>Only when DHCP Snooping is globally enabled, can this command be set. When a port turns into a trusted port from a non-trusted port, the original defense action of the port will be automatically deleted; all the security history records will be cleared (except the information in system log)</p>
<b>Example</b>	<p>Set port ethernet1/0/1 as a DHCP Snooping trusted port</p> <pre>Switch#config Switch(config)#interface ethernet 1/0/1 switch(config- ethernet 1/0/1)#ip dhcp snooping trust</pre>

### 11.1.127 ip dhcp snooping vlan

<b>Syntax</b>	<b>ip dhcp snooping vlan (WORD)</b> <b>no ip dhcp snooping vlan (WORD)</b>
<b>Parameter</b>	<b>WORD</b> VLAN ID
<b>Default</b>	Disable
<b>Mode</b>	Global Mode
<b>Usage</b>	Enable the dhcp snooping in vlan. <b>no ip dhcp snooping vlan &lt;vlan-id&gt;</b> means to disable the dhcp snooping function on the appointed vlan.
<b>Example</b>	Enable DHCP snooping function. Switch#config Switch(config)#ip dhcp snooping vlan 10 Switch(config)#no ip dhcp snooping vlan 10

### 11.1.128 ip user helper-address

<b>Syntax</b>	<pre>ip user helper-address &lt;svr_addr&gt; [port &lt;udp_port&gt;] source &lt;src_addr&gt; [secondary] no ip user helper-address [secondary]</pre>								
<b>Parameter</b>	<table border="1"> <tr> <td style="vertical-align: top;"><b>&lt;svr_addr&gt;</b></td> <td>The IP address of HELPER SERVER IP in dotted-decimal notation</td> </tr> <tr> <td style="vertical-align: top;"><b>&lt;udp_port&gt;</b></td> <td>The UDP port of HELPER SERVER, the range of which is 1 – 65535, and its default value is 9119.</td> </tr> <tr> <td style="vertical-align: top;"><b>&lt;src_addr&gt;</b></td> <td>The local management IP address of the switch, in dotted-decimal notation.</td> </tr> <tr> <td style="vertical-align: top;"><b>[secondary]</b></td> <td>Whether it is a secondary SERVER address.</td> </tr> </table>	<b>&lt;svr_addr&gt;</b>	The IP address of HELPER SERVER IP in dotted-decimal notation	<b>&lt;udp_port&gt;</b>	The UDP port of HELPER SERVER, the range of which is 1 – 65535, and its default value is 9119.	<b>&lt;src_addr&gt;</b>	The local management IP address of the switch, in dotted-decimal notation.	<b>[secondary]</b>	Whether it is a secondary SERVER address.
<b>&lt;svr_addr&gt;</b>	The IP address of HELPER SERVER IP in dotted-decimal notation								
<b>&lt;udp_port&gt;</b>	The UDP port of HELPER SERVER, the range of which is 1 – 65535, and its default value is 9119.								
<b>&lt;src_addr&gt;</b>	The local management IP address of the switch, in dotted-decimal notation.								
<b>[secondary]</b>	Whether it is a secondary SERVER address.								
<b>Default</b>	There is no HELPER SERVER address by default.								
<b>Mode</b>	Global Mode								
<b>Usage</b>	<p>Set the address and port of HELPER SERVER.</p> <p>DHCP SNOOPING will send the monitored binding information to HELPER SERVER to save it. If the switch starts abnormally, it can recover the binding data from HELPER SERVER. The HELPER SERVER function usually is integrated into DCBI packet. The DHCP SNOOPING and HELPER SERVER use the UDP protocol to communicate, and guarantee the arrival of retransmitted data. HELPER SERVER configuration can also be used to sent DOT1X user data from the server, the detail of usage is described in the chapter of dot1x configuration.</p> <p>Two HELPER SERVER addresses are allowed, DHCP SNOOPING will try to connect to PRIMARY SERVER in the first place. Only when the PRIMARY SERVER is unreachable, will the switch c HELPER SERVER connects to SECONDARY SERVER.</p> <p><b>Please pay attention:</b> source address is the effective management IP address of the switch, if the management IP address of the switch changes, this configuration should be updated in time.</p>								
<b>Example</b>	<p>Set the local management IP address as 100.1.1.1, primary HELPER SERVER address as 100.1.1.100 and the port as default value.</p> <pre>Switch#config switch(config)#interface vlan 1 Switch(config-if-vlan1)#ip address 100.1.1.1 255.255.255.0 switch(config-if-vlan1)exit switch(config)#ip user helper-address 100.1.1.100 source 100.1.1.1</pre>								

### 11.1.129 ip user private packet version two

<b>Syntax</b>	<p>ip user private packet version two</p> <p>no ip user private packet version two</p>
<b>Parameter</b>	none
<b>Default</b>	The switch choose private packet version one to communicate with DCBI.
<b>Mode</b>	Global Mode
<b>Usage</b>	<p>The switch choose private packet version two to communicate with trustview.</p> <p>If the DCBI access control system is applied, the switch should be configured to use private protocol of version one to communicate with the DCBI server. However, if TrustView is applied, version two should be applied.</p>
<b>Example</b>	<p>To configure the switch choose private packet version two to communicate with inter security management background system.</p> <pre>Switch#config Switch(config)#ip user private packet version two</pre>

### 11.1.130 show ip dhcp snooping

<b>Syntax</b>	<code>show ip dhcp snooping [interface [ethernet] &lt;interfaceName&gt;]</code>																																																																																										
<b>Parameter</b>	<interfaceName>      The name of the specific port.																																																																																										
<b>Default</b>	none																																																																																										
<b>Mode</b>	Admin and Configuration Mode																																																																																										
<b>Usage</b>	If there is no specific port, then display the current configuration information of dhcp snooping, otherwise, display the records of defense actions of the specific port																																																																																										
<b>Example</b>	<pre>Switch#show ip dhcp snooping User primary helper server 1.1.1.1:9119, source 100.1.1.1, socket 0 seq no 0, connection 0, retry 0, renew 0, binding count 0 00:00:00 retry, 01:16:57 keep alive, 00:00:00 dead Get PrivateDESMD5 Ack 0, Get FreeResource Ack 0, Get HttpRedirPage Ack 0, Get Binding Ack 0  DHCP Snooping is enabled DHCP Snooping maxnum of action info:100 DHCP Snooping limit rate is 100 pps, switch ID 10-f0-13-f1-72-3a DHCP Snooping dropped packets 0, discarded packets 0 DHCP Snooping alarm count 0, binding count 1, static binding count 1, from shell 1, from server 0 expired binding 0, request binding 0</pre> <table border="1"> <thead> <tr> <th>interface</th> <th>trust</th> <th>action</th> <th>recovery</th> <th>alarm num</th> <th>bind num</th> </tr> </thead> <tbody> <tr><td>Ethernet1/0/1</td><td>trust</td><td>none</td><td>0</td><td>0</td><td>0</td></tr> <tr><td>Ethernet1/0/2</td><td>untrust</td><td>none</td><td>0</td><td>0</td><td>0</td></tr> <tr><td>Ethernet1/0/3</td><td>untrust</td><td>none</td><td>0</td><td>0</td><td>0</td></tr> <tr><td>Ethernet1/0/4</td><td>untrust</td><td>none</td><td>0</td><td>0</td><td>0</td></tr> <tr><td>Ethernet1/0/5</td><td>untrust</td><td>none</td><td>0</td><td>0</td><td>0</td></tr> <tr><td>Ethernet1/0/6</td><td>untrust</td><td>none</td><td>0</td><td>0</td><td>0</td></tr> <tr><td>Ethernet1/0/7</td><td>untrust</td><td>none</td><td>0</td><td>0</td><td>0</td></tr> <tr><td>Ethernet1/0/8</td><td>untrust</td><td>none</td><td>0</td><td>0</td><td>0</td></tr> <tr><td>Ethernet1/0/9</td><td>untrust</td><td>none</td><td>0</td><td>0</td><td>0</td></tr> <tr><td>Ethernet1/0/10</td><td>untrust</td><td>none</td><td>0</td><td>0</td><td>0</td></tr> <tr><td>Ethernet1/0/11</td><td>untrust</td><td>none</td><td>0</td><td>0</td><td>0</td></tr> <tr><td>Ethernet1/0/12</td><td>untrust</td><td>none</td><td>0</td><td>0</td><td>0</td></tr> <tr><td>Ethernet1/0/13</td><td>untrust</td><td>none</td><td>0</td><td>0</td><td>0</td></tr> <tr><td>Ethernet1/0/14</td><td>untrust</td><td>none</td><td>0</td><td>0</td><td>1</td></tr> </tbody> </table>	interface	trust	action	recovery	alarm num	bind num	Ethernet1/0/1	trust	none	0	0	0	Ethernet1/0/2	untrust	none	0	0	0	Ethernet1/0/3	untrust	none	0	0	0	Ethernet1/0/4	untrust	none	0	0	0	Ethernet1/0/5	untrust	none	0	0	0	Ethernet1/0/6	untrust	none	0	0	0	Ethernet1/0/7	untrust	none	0	0	0	Ethernet1/0/8	untrust	none	0	0	0	Ethernet1/0/9	untrust	none	0	0	0	Ethernet1/0/10	untrust	none	0	0	0	Ethernet1/0/11	untrust	none	0	0	0	Ethernet1/0/12	untrust	none	0	0	0	Ethernet1/0/13	untrust	none	0	0	0	Ethernet1/0/14	untrust	none	0	0	1
interface	trust	action	recovery	alarm num	bind num																																																																																						
Ethernet1/0/1	trust	none	0	0	0																																																																																						
Ethernet1/0/2	untrust	none	0	0	0																																																																																						
Ethernet1/0/3	untrust	none	0	0	0																																																																																						
Ethernet1/0/4	untrust	none	0	0	0																																																																																						
Ethernet1/0/5	untrust	none	0	0	0																																																																																						
Ethernet1/0/6	untrust	none	0	0	0																																																																																						
Ethernet1/0/7	untrust	none	0	0	0																																																																																						
Ethernet1/0/8	untrust	none	0	0	0																																																																																						
Ethernet1/0/9	untrust	none	0	0	0																																																																																						
Ethernet1/0/10	untrust	none	0	0	0																																																																																						
Ethernet1/0/11	untrust	none	0	0	0																																																																																						
Ethernet1/0/12	untrust	none	0	0	0																																																																																						
Ethernet1/0/13	untrust	none	0	0	0																																																																																						
Ethernet1/0/14	untrust	none	0	0	1																																																																																						

Ethernet1/0/15	untrust	none	0	0	0
Ethernet1/0/16	untrust	none	0	0	0
Ethernet1/0/17	untrust	none	0	0	0
Ethernet1/0/18	untrust	none	0	0	0
Ethernet1/0/19	untrust	none	0	0	0
Ethernet1/0/20	untrust	none	0	0	0
Ethernet1/0/21	untrust	none	0	0	0
Ethernet1/0/22	untrust	none	0	0	0
Ethernet1/0/23	untrust	blackhole	30	0	0
Ethernet1/0/24	untrust	none	0	0	0
Ethernet1/0/25	untrust	none	0	0	0
Ethernet1/0/26	untrust	none	0	0	0
Ethernet1/0/27	untrust	none	0	0	0
Ethernet1/0/28	untrust	none	0	0	0

Displayed Information	Explanation
DHCP Snooping is enable	Whether the DHCP Snooping is globally enabled or disabled.
DHCP Snooping binding arp	Whether the ARP binding function is enabled.
DHCP Snooping maxnum of action info	The number limitation of port defense actions
DHCP Snooping limit rate	The rate limitation of receiving packets
switch ID	The switch ID is used to identify the switch, usually using the CPU MAC address
DHCP Snooping dropped packets	The number of dropped messages when the received DHCP messages exceeds the rate limit.
discarded packets	The number of discarded packets caused by the communication failure within the system. If the CPU of the switch is too busy to schedule the DHCP SNOOPING task and thus can not handle the received DHCP messages, such situation might happen.
DHCP Snooping alarm count:	The number of alarm information.
binding count	The number of binding information.
expired binding	The number of binding information which is already expired but has not been deleted. The reason why the expired information is not deleted immediately might be that the

---

	switch needs to notify the helper server about the information, but the helper server has not acknowledged it.
request binding	The number of REQUEST information
interface	The name of port
trust	The trust attributes of the port
action	The automatic defense action of the port
recovery	The automatic recovery time of the port
alarm num	The number of history records of the port automatic defense actions
bind num	The number of port-relative binding information.

---



### 11.1.131 show ip dhcp snooping binding all

<b>Syntax</b>	<code>show ip dhcp snooping binding all</code>										
<b>Parameter</b>	none										
<b>Default</b>	none										
<b>Mode</b>	Admin and Configuration Mode										
<b>Usage</b>	<p>This command can check the global binding information of DHCP snooping, each table entry includes the corresponding MAC address, IP address, port name, VLAN ID and the flag of the binding state. Besides, DHCP Snooping must be enabled globally, this command can be configured.</p>										
<b>Example</b>	<pre>Switch#show ip dhcp snooping binding all ip dhcp snooping static binding count:1, dynamic binding count:0</pre> <table border="1"> <thead> <tr> <th>MAC</th> <th>IP address</th> <th>Interface</th> <th>Vlan ID</th> <th>Flag</th> </tr> </thead> <tbody> <tr> <td>00-11-22-33-44-55</td> <td>1.1.1.1</td> <td>Ethernet1/0/14</td> <td>1</td> <td>SE</td> </tr> </tbody> </table>	MAC	IP address	Interface	Vlan ID	Flag	00-11-22-33-44-55	1.1.1.1	Ethernet1/0/14	1	SE
MAC	IP address	Interface	Vlan ID	Flag							
00-11-22-33-44-55	1.1.1.1	Ethernet1/0/14	1	SE							

### 11.1.132 show trustview status

<b>Syntax</b>	<b>show trust status</b>
<b>Parameter</b>	<b>none</b>
<b>Default</b>	none
<b>Mode</b>	Admin and Configuration Mode
<b>Usage</b>	This command can be used for debugging the communication messages between the switch and the TrustView server, messages such as protocol version notification, encryption negotiation, free resource and web URL redirection, and the number of forced log-off messages, as well as the number of forced accounting update messages, can be displayed.
<b>Example</b>	<pre>Switch#show trustview status Primary trustview Server 1.1.1.1:9119     trustview version2 message inform failed     trustview inform free resource failed     trustview inform web redirect address failed     trustview inform user binding data failed trustview version 2 message encrypt/digest not enabled Rcvd 0 force log-off packets Rcvd 0 force accounting update packets using version two private packet</pre>

### 11.1.133 ip dhcp snooping information enable

<b>Syntax</b>	<p>ip dhcp snooping information enable</p> <p>no ip dhcp snooping information enable</p>
<b>Parameter</b>	none
<b>Default</b>	Option 82 function is disabled in DHCP Snooping by default.
<b>Mode</b>	Global Mode
<b>Usage</b>	<p>Only by implementing this command, can DHCP Snooping add standard option 82 to DHCP request messages and forward the message. The format of option1 in option 82 (Circuit ID option) is standard vlan name plus physical port name, like "vlan1+ethernet1/0/12". That of option2 in option 82 (remote ID option) is CPU MAC of the switch, like "00030f023301". If a DHCP request message with option 82 options is received, DHCP Snooping will replace those options in the message with its own. If a DHCP reply message with option 82 options is received, DHCP Snooping will dump those options in the message and forward it.</p>
<b>Example</b>	<pre> Switch#config Switch(config)#ip dhcp snooping enable Switch(config)#ip dhcp snooping binding enable Switch(config)#ip dhcp snooping information enable </pre>

# Chapter 12 Multicast Protocol

## 12.1 IPv4 Multicast

### 12.1.1 access-list (Multicast Destination Control)

Syntax	<pre>access-list &lt;6000-7999&gt; (((add   delete) profile-id WORD)   ((deny   permit) ip ((&lt;source&gt; &lt;wildcard-bit&gt;)   (host-source &lt;source-host-ip&gt; [range &lt;2-65535&gt;])   any-source) ((&lt;destination&gt; &lt;wildcard-bit&gt;)   (host-destination &lt;destination-host-ip&gt; [range &lt;2-255&gt;])   any-destination))) no access-list &lt;6000-7999&gt; {deny permit} ip ((&lt;source&gt; &lt;source-wildcard&gt;)   (host-source &lt;source-host-ip&gt; [range &lt;2-65535&gt;])   any-source) ((&lt;destination&gt; &lt;destination-wildcard&gt;)   (host-destination &lt;destination-host-ip&gt; [range &lt;2-255&gt;])   any-destination)</pre>																						
Parameter	<table border="1"> <tr> <td>&lt;6000-7999&gt;</td> <td>destination control access-list number.</td> </tr> <tr> <td>add   delete</td> <td>add or delete the profile</td> </tr> <tr> <td>WORD</td> <td>File id</td> </tr> <tr> <td>deny   permit</td> <td>deny or permit</td> </tr> <tr> <td>&lt;source&gt;</td> <td>multicast source address</td> </tr> <tr> <td>&lt;wildcard-bit&gt;</td> <td>Address wildcard</td> </tr> <tr> <td>&lt;source-host-ip&gt;</td> <td>multicast source host address.</td> </tr> <tr> <td>&lt;2-65535&gt;</td> <td>the range of multicast source host.</td> </tr> <tr> <td>&lt;destination&gt;</td> <td>multicast destination address</td> </tr> <tr> <td>&lt;destination-host-ip&gt;</td> <td>multicast destination host address</td> </tr> <tr> <td>&lt;2-255&gt;</td> <td>the range of multicast destination host.</td> </tr> </table>	<6000-7999>	destination control access-list number.	add   delete	add or delete the profile	WORD	File id	deny   permit	deny or permit	<source>	multicast source address	<wildcard-bit>	Address wildcard	<source-host-ip>	multicast source host address.	<2-65535>	the range of multicast source host.	<destination>	multicast destination address	<destination-host-ip>	multicast destination host address	<2-255>	the range of multicast destination host.
<6000-7999>	destination control access-list number.																						
add   delete	add or delete the profile																						
WORD	File id																						
deny   permit	deny or permit																						
<source>	multicast source address																						
<wildcard-bit>	Address wildcard																						
<source-host-ip>	multicast source host address.																						
<2-65535>	the range of multicast source host.																						
<destination>	multicast destination address																						
<destination-host-ip>	multicast destination host address																						
<2-255>	the range of multicast destination host.																						
Default	none																						
Mode	Global Mode																						
Usage	<p>ACL of Multicast destination control list item is controlled by specifical ACL number from 6000 to 7999, the command applies to configure this ACL. ACL of ip Multicast destination control only needs to configure source IP address and destination IP address controlled (group IP address), the configuration mode is basically the same to other ACLs, and use mask length to configure address range, and also specify a host address or all address. Remarkable, "all address" is 224.0.0.0/4 according to group IP address, not 0.0.0.0/0 in other access-list. And adding or deleting the profile-id can be used to change the multicast destination control ACL.</p>																						
Example	<pre>Switch#config Switch(config)#access-list 6000 permit ip 10.1.1.1 0.0.0.255 232.0.0.0 0.0.0.255 Switch(config)#access-list 6000 add profile-id 1 profile id 1 is not exist % Operation failed Switch(config)#</pre>																						

## 12.1.2 access-list (Multicast Source Control)

Syntax	<pre>access-list &lt;5000-5099&gt; (deny   permit) ip ((&lt;source&gt; &lt;wildcard-bit&gt;)   (host &lt;source-host-ip&gt;)   any-source) ((&lt;destination&gt; &lt;wildcard-bit&gt;)   (host-destination &lt;destination-host-ip&gt;)   any-destination} no access-list &lt;5000-5099&gt; (deny   permit) ip ((&lt;source&gt; &lt;wildcard-bit&gt;)   (host &lt;source-host-ip&gt;)   any-source) ((&lt;destination&gt; &lt;wildcard-bit&gt;)   (host-destination &lt;destination-host-ip&gt;)   any-destination)</pre>														
Parameter	<table border="1"> <tr> <td>&lt;5000-5099&gt;</td> <td>source control access-list number</td> </tr> <tr> <td>deny   permit</td> <td>deny or permit.</td> </tr> <tr> <td>&lt;source&gt;</td> <td>multicast source address..</td> </tr> <tr> <td>&lt;wildcard-bit&gt;</td> <td>address wildcard character.</td> </tr> <tr> <td>&lt;source-host-ip&gt;</td> <td>multicast source host address.</td> </tr> <tr> <td>&lt;destination&gt;</td> <td>multicast destination address.</td> </tr> <tr> <td>&lt;destination-host-ip&gt;</td> <td>multicast destination host address.</td> </tr> </table>	<5000-5099>	source control access-list number	deny   permit	deny or permit.	<source>	multicast source address..	<wildcard-bit>	address wildcard character.	<source-host-ip>	multicast source host address.	<destination>	multicast destination address.	<destination-host-ip>	multicast destination host address.
<5000-5099>	source control access-list number														
deny   permit	deny or permit.														
<source>	multicast source address..														
<wildcard-bit>	address wildcard character.														
<source-host-ip>	multicast source host address.														
<destination>	multicast destination address.														
<destination-host-ip>	multicast destination host address.														
Default	None														
Mode	Global Mode														
Usage	<p>ACL of Multicast source control list item is controlled by specific ACL number from 5000 to 5099, the command applies to configure this ACL. ACL of Multicast source control only needs to configure source IP address and destination IP address controlled (group IP address), the configuration mode is basically the same to other ACLs, and use wildcard character to configure address range, and also specify a host address or all address. Remarkable, "all address" is 224.0.0.0/4 according to group IP address, not 0.0.0.0/0 in other access-list.</p>														
Example	<pre>Switch(config)#access-list 5000 permit ip 10.1.1.0 0.0.0.255 232.0.0.0 0.0.0.255</pre>														

### 12.1.3 ip multicast destination-control access-group

Syntax	ip multicast destination-control access-group <6000-7999> no ip multicast destination-control access-group <6000-7999>
Parameter	<6000-7999> destination-control access-list number.
Default	None
Mode	Interface Configuration Mode
Usage	The command is only working under global multicast destination-control enabled, after configuring the command, if IGMP-SPOOPING is enabled, for adding the interface to multicast group, and match configured access-list, such as matching: permit, the interface can be added, otherwise do not be added.
Example	Switch#config Switch(config)#interface ethernet 1/0/4 Switch(config-if-ethernet1/0/4)#ip multicast destination-control access-group 6000 Switch(config-if-ethernet1/0/4)#

## 12.1.4 ip multicast destination-control access-group (sip)

Syntax	ip multicast destination-control <IPADDRESS/M> access-group <6000-7999> no ip multicast destination-control <IPADDRESS/M> access-group <6000-7999>
Parameter	<IPADDRESS/M> IP address and mask length <6000-7999> Destination control access-list number
Default	None
Mode	Global Mode
Usage	The command is only working under global multicast destination-control enabled, after configuring the command, if IGMP-SPOOPING or IGMP is enabled, for adding the members to multicast group. If configuring multicast destination-control on specified net segment of transmitted igmp-report, and match configured access-list, such as matching permit, the interface can be added, otherwise do not be added. If relevant group or source in show ip igmp groups detail has been established before executing the command, it needs to execute clear ip igmp groups command to clear relevant groups in Admin mode.
Example	Switch#config Switch(config)#ip multicast destination-control 10.1.1.0/24 access-group 6000

## 12.1.5 ip multicast destination-control access-group (vmac)

Syntax	ip multicast destination-control <1-4094> <macaddr > access-group <6000-7999> no ip multicast destination-control <1-4094> <macaddr > access-group <6000-7999>						
Parameter	<table border="1"> <tr> <td>&lt;1-4094&gt;</td> <td>VLAN ID</td> </tr> <tr> <td>&lt;macaddr &gt;</td> <td>Transmitting source MAC address of IGMP-REPORT, the format is "xx-xx-xx-xx-xx";</td> </tr> <tr> <td>&lt;6000-7999&gt;</td> <td>Destination-control access-list number.</td> </tr> </table>	<1-4094>	VLAN ID	<macaddr >	Transmitting source MAC address of IGMP-REPORT, the format is "xx-xx-xx-xx-xx";	<6000-7999>	Destination-control access-list number.
<1-4094>	VLAN ID						
<macaddr >	Transmitting source MAC address of IGMP-REPORT, the format is "xx-xx-xx-xx-xx";						
<6000-7999>	Destination-control access-list number.						
Default	None						
Mode	Global Mode						
Usage	The command is only working under global multicast destination-control enabled, after configuring the command, if IGMP-SPOOPING is enabled, for adding the members to multicast group. If configuring multicast destination-control to source MAC address of transmitted igmp-report, and match configured access-list, such as matching: permit, the interface can be added, otherwise do not be added.						
Example	<pre>Switch#config Switch(config)#ip multicast destination-control 1 00-01-03-05-07-09 access-group 6000</pre>						



## 12.1.6 ip multicast policy

Syntax	ip multicast policy <IPADDRESS/M> <IPADDRESS/M> cos <priority> no ip multicast policy <IPADDRESS/M> <IPADDRESS/M> cos
Parameter	<IPADDRESS/M> are multicast source address, mask length, destination address, and mask length separately. <priority> specified priority, range from 0 to 7
Default	None
Mode	Global Mode
Usage	The command configuration modifies to a specified value through the switch matching priority of specified range multicast data packet, and the TOS is specified to the same value simultaneously. Carefully, the packet transmitted in UNTAG mode does not modify its priority.
Example	Switch(config)#ip multicast policy 10.1.1.0/24 225.1.1.0/24 cos 7

## 12.1.7 ip multicast source-control

Syntax	ip multicast source-control no ip multicast source-control
Parameter	None
Default	Disabled
Mode	Global Mode
Usage	The source control access-list applies to interface with only enabling global multicast source control, and configure to disabled global multicast source control without configuring source control access-list on every interface. After configuring the command, multicast data received from every interface does not have matching multicast source control list item, and then they will be thrown away by switches, namely only multicast data matching to PERMIT can be received and forwarded. °
Example	Switch(config)#ip multicast source-control

## 12.1.8 ip multicast source-control access-group

Syntax	<pre>ip multicast source-control access-group &lt;5000-5099&gt; no ip multicast source-control access-group &lt;5000-5099&gt;</pre>
Parameter	<5000-5099> Source control access-list number.
Default	None
Mode	Interface Configuration Mode
Usage	The command configures with only enabling global multicast source control. After that, it will match multicast data message imported from the interface according to configured access-list, such as matching: permit, the message will be received and forwarded; otherwise the message will be thrown away.
Example	<pre>Switch (config)#interface ethernet1/0/4 Switch (config-if-ethernet1/0/4)#ip multicast source-control access-group 5000 Switch (config-if-ethernet1/0/4)#</pre>

## 12.1.9 ip multicast destination-control

Syntax	ip multicast destination-control
Parameter	None
Default	Disabled
Mode	Global Mode
Usage	Only after globally enabling the multicast destination control, the other destination control configuration can take effect; the destination access list can be applied to ports, VLAN-MAC and SIP. After configuring this command, IGMP-SNOOPING and IGMP will match according to the rules mentioned above when they try to add ports after receiving IGMP-REPORT.
Example	Switch(config)#ip multicast destination-control

## 12.1.10 profile-id (Multicast Destination Control Rule List)

Syntax	profile-id <1-50> (deny   permit) ip ((<source> <wildcard-bit> )   (host-source <source-host-ip> [range <2-65535>])   any-source) ((<destination> <wildcard-bit>)   (host-destination <destination-host-ip> [range <2-255>])   any-destination) no profile-id <1-50>																		
Parameter	<table border="1"> <tr> <td>&lt;1-50&gt;</td> <td>profile-id</td> </tr> <tr> <td>deny   permit</td> <td>deny or permit.</td> </tr> <tr> <td>&lt;source&gt;</td> <td>multicast source address</td> </tr> <tr> <td>&lt;wildcard-bit&gt;</td> <td>address wildcard character.</td> </tr> <tr> <td>&lt;source-host-ip&gt;</td> <td>multicast source host address.</td> </tr> <tr> <td>&lt;2-65535&gt;</td> <td>range of multicast source host</td> </tr> <tr> <td>&lt;destination&gt;</td> <td>multicast destination address</td> </tr> <tr> <td>&lt;destination-host-ip&gt;</td> <td>multicast destination host address</td> </tr> <tr> <td>&lt;2-255&gt;</td> <td>range of multicast destination host.</td> </tr> </table>	<1-50>	profile-id	deny   permit	deny or permit.	<source>	multicast source address	<wildcard-bit>	address wildcard character.	<source-host-ip>	multicast source host address.	<2-65535>	range of multicast source host	<destination>	multicast destination address	<destination-host-ip>	multicast destination host address	<2-255>	range of multicast destination host.
<1-50>	profile-id																		
deny   permit	deny or permit.																		
<source>	multicast source address																		
<wildcard-bit>	address wildcard character.																		
<source-host-ip>	multicast source host address.																		
<2-65535>	range of multicast source host																		
<destination>	multicast destination address																		
<destination-host-ip>	multicast destination host address																		
<2-255>	range of multicast destination host.																		
Default	none																		
Mode	Global Mode																		
Usage	Profile-list of Multicast destination control list item is controlled by specifical profile-id number from 1 to 50, the command applies to configure this profile to add it into the ACL for using. Multicast destination control only needs to configure source IP address and destination IP address controlled (group IP address), the configuration mode is basically the same to ACLs, and use mask length to configure address range, and also specify a host address or all address. Remarkable, "all address" is 224.0.0.0/4 according to group IP address, not 0.0.0.0/0 in other access-list.																		
Example	switch(config)# profile-id 1 deny ip any-source host-destination 224.1.1.2																		

## 12.1.11 show ip multicast destination-control

Syntax	<pre>show ip multicast destination-control [detail] show ip multicast destination-control interface &lt;Interfacename&gt; [detail] show ip multicast destination-control host-address &lt;ipaddress&gt; [detail] show ip multicast destination-control &lt;vlan-id&gt; &lt;mac-address&gt; [detail]</pre>										
Parameter	<table border="1"> <tr> <td>detail</td> <td>expresses if it display information in detail or not</td> </tr> <tr> <td>&lt;Interfacename&gt;</td> <td>interface name or interface aggregation name, such as Ethernet1/0/1, port-channel 1 or ethernet1/0/1.</td> </tr> <tr> <td>&lt;ipaddress&gt;</td> <td>IP address</td> </tr> <tr> <td>&lt;vlan-id&gt;</td> <td>VLAN ID</td> </tr> <tr> <td>&lt;mac-address&gt;</td> <td>Mac address</td> </tr> </table>	detail	expresses if it display information in detail or not	<Interfacename>	interface name or interface aggregation name, such as Ethernet1/0/1, port-channel 1 or ethernet1/0/1.	<ipaddress>	IP address	<vlan-id>	VLAN ID	<mac-address>	Mac address
detail	expresses if it display information in detail or not										
<Interfacename>	interface name or interface aggregation name, such as Ethernet1/0/1, port-channel 1 or ethernet1/0/1.										
<ipaddress>	IP address										
<vlan-id>	VLAN ID										
<mac-address>	Mac address										
Default	None										
Mode	Admin Mode and Global Mode										
Usage	The command displays multicast destination control rules of configuration including detail option, and access-list information applied in detail.										
Example	<pre>Switch#show ip multicast destination-control ip multicast destination-control is enabled multicast destination-control access-group 6000 used on interface Ethernet1/0/4</pre>										

## 12.1.12 show ip multicast destination-control access-list

Syntax	<pre>show ip multicast destination-control access-list show ip multicast destination-control access-list &lt;6000-7999&gt;</pre>
Parameter	<pre>&lt;6000-7999&gt;          access-list number.</pre>
Default	None
Mode	Admin Mode and Global Mode
Usage	The command displays destination control multicast access-list of configuration.
Example	<pre>Switch#show ip multicast destination-control access-list access-list 6000 permit ip 10.1.1.1 0.0.0.255 232.0.0.0 0.0.0.255</pre>

### 12.1.13 show ip multicast destination-control filter-profile-list

Syntax	show ip multicast destination-control filter-profile-list show ip multicast destination-control filter-profile-list <1-50>										
Parameter	<1-50>                                  profile-id										
Default	None										
Mode	Admin Mode and Global Mode										
Usage	This command can show the configured destination control profile rule list.										
Example	Switch#show l2-address-table multicast vlan 1  <table border="1"> <thead> <tr> <th>Vlan Address</th> <th>Insert</th> <th>Type</th> <th>Creator</th> <th>Ports</th> </tr> </thead> <tbody> <tr> <td>-----</td> <td>-----</td> <td>-----</td> <td>-----</td> <td>-----</td> </tr> </tbody> </table>	Vlan Address	Insert	Type	Creator	Ports	-----	-----	-----	-----	-----
Vlan Address	Insert	Type	Creator	Ports							
-----	-----	-----	-----	-----							



## 12.1.14 show ip multicast policy

Syntax	<code>show ip multicast policy</code>
Parameter	None
Default	None
Mode	Admin Mode and Global Mode
Usage	The command displays multicast policy of configuration
Example	Switch#show ip multicast policy ip multicast-policy 10.1.1.0/24 225.0.0.0/8 cos 5

## 12.1.15 show ip multicast source-control

Syntax	<pre>show ip multicast source-control [detail] show ip multicast source-control interface &lt;Interfacename&gt; [detail]</pre>
Parameter	<pre>detail                expresses if it displays information in detail. &lt;Interfacename&gt;      interface name, such as ethernet 1/0/1 or ethernet1/0/1.</pre>
Default	None
Mode	Admin Mode and Global Mode
Usage	The command displays multicast source control rules of configuration, including detail option, and access-list information applied in detail.
Example	<pre>Switch#show ip multicast source-control detail ip multicast source-control is enabled Interface Ethernet1/0/13 use multicast source control access-list 5000 access-list 5000 permit ip 10.1.1.0 0.0.0.255 232.0.0.0 0.0.0.255 access-list 5000 deny ip 10.1.1.0 0.0.0.255 233.0.0.0 0.255.255.255</pre>

## 12.1.16 show ip multicast source-control access-list

Syntax	<pre>show ip multicast source-control access-list show ip multicast source-control access-list &lt;5000-5099&gt;</pre>
Parameter	<pre>&lt;5000-5099&gt;          access-list number</pre>
Default	None
Mode	Admin Mode and Global Mode
Usage	The command displays source control multicast access-list of configuration
Example	<pre>Switch#show ip multicast source-control access-list access-list 5000 permit ip 10.1.1.0 0.0.0.255 232.0.0.0 0.0.0.255 access-list 5000 deny ip 10.1.1.0 0.0.0.255 233.0.0.0 0.255.255.255</pre>

## 12.1.17 clear ip igmp snooping vlan

Syntax	clear ip igmp snooping vlan <1-4094> groups [A.B.C.D]
Parameter	<1-4094> VLAN ID [A.B.C.D] group address.
Default	None
Mode	Admin Configuration Mode
Usage	Use show command to check the deleted group record.
Example	Switch#clear ip igmp snooping vlan 1 groups

## 12.1.18 clear ip igmp snooping vlan

Syntax	clear ip igmp snooping vlan <1-4094> mrouter-port [ethernet] IFNAME
Parameter	<1-4094> VLAN ID IFNAME port name
Default	None
Mode	Admin Configuration Mode
Usage	use show command to check the deleted mrouter port of the specific VLAN. °
Example	Delete mrouter port in vlan 1. Switch#clear ip igmp snooping vlan 1 mrouter-port

## 12.1.19 ip igmp snooping

Syntax	ip igmp snooping no ip igmp snooping
Parameter	none
Default	IGMP Snooping is disabled by default.
Mode	Global Mode
Usage	Use this command to enable IGMP Snooping, that is permission every VLAN config the function of IGMP snooping. The "no ip igmp snooping" command disables this function.
Example	Enable IGMP Snooping Switch#config Switch(config)#ip igmp snooping Switch(config)#

## 12.1.20 ip igmp snooping proxy

Syntax	ip igmp snooping proxy no ip igmp snooping proxy
Parameter	none
Default	Enable
Mode	Global Mode
Usage	Enable IGMP Snooping proxy function, the no command disables the function.
Example	Switch#config Switch(config)#no ip igmp snooping proxy Switch(config)#

## 12.1.21 ip igmp snooping vlan

---

Syntax	<code>ip igmp snooping vlan &lt;vlan-id&gt;</code> <code>no ip igmp snooping vlan &lt;vlan-id&gt;</code>
Parameter	<vlan-id>                      VLAN ID
Default	IGMP Snooping is disabled by default.
Mode	Global Mode
Usage	To configure IGMP Snooping on specified VLAN, the global IGMP Snooping should be first enabled. <u>Disable IGMP Snooping on specified VLAN with the "no ip igmp snooping vlan &lt;vlan-id&gt;" command.</u>
Example	Enable IGMP Snooping for VLAN 100 in Global Mode. Switch#config <u>Switch(config)#ip igmp snooping vlan 100</u>

---



## 12.1.22 ip igmp snooping vlan immediate-leave

Syntax	<pre>ip igmp snooping vlan &lt;vlan-id&gt; immediate-leave no ip igmp snooping vlan &lt;vlan-id&gt; immediate-leave</pre>
Parameter	<pre>&lt;vlan-id&gt;          VLAN ID</pre>
Default	This function is disabled by default.
Mode	Global Mode
Usage	Enable immediate-leave function of the IGMP Snooping in specified VLAN; the "no" form of this command disables the immediate-leave function of the IGMP Snooping
Example	<pre>Enable the IGMP Snooping fast leave function for VLAN 100. Switch#config Switch(config)#ip igmp snooping vlan 100 immediate-leave</pre>

### 12.1.23 ip igmp snooping vlan

Syntax	ip igmp snooping vlan <vlan-id> immediately-leave mac-based no ip igmp snooping vlan <vlan-id> immediately-leave mac-based
Parameter	<vlan-id> VLAN ID
Default	This function is disabled by default.
Mode	Global Mode
Usage	Configure this command to delete the existed igmp snooping table entries according to the source mac in leave packet when the switch which is enabled the igmp snooping function receives the leave packet. Only when the received the port, source mac and multicast group of the leave packet are the same as the port, host mac and multicast group of the existed igmp snooping table entry, the snooping table entry can be deleted. If this command is not configured, delete the existed igmp snooping table entry according to the port and multicast group of the leave packet. Configure the immediately-leave under the same vlan at the same time to make this command effective. In this time, deal with it according to the host mac of the port.
Example	Use the following configuration when delete the table entry according to the host mac of the port. Switch#config Switch(config)#ip igmp snooping vlan 12 immediately-leave Switch(config)#ip igmp snooping vlan 12 immediately-leave mac-based

## 12.1.24 ip igmp snooping vlan l2-general-querier

Syntax	<pre>ip igmp snooping vlan &lt; vlan-id &gt; l2-general-querier no ip igmp snooping vlan &lt; vlan-id &gt; l2-general-querier</pre>
Parameter	<vlan-id> is ID number of the VLAN, ranging is <1-4094>
Default	VLAN is not as the IGMP Snooping layer 2 general querier.
Mode	Global Mode
Usage	<p>It is recommended to configure a layer 2 general querier on a segment. IGMP Snooping function will be enabled by this command if not enabled on this VLAN before configuring this command, IGMP Snooping function will not be disabled when disabling the layer 2 general querier function. This command is mainly for sending general queries regularly to help switches within this segment learn mrouter ports.</p> <p>Comment: There are three paths IGMP snooping learn mrouter</p> <ul style="list-style-type: none"> <li>1 Port receives the IGMP query messages</li> <li>2 Port receives multicast protocol packets, and supports DVMRP, PIM</li> <li>3 Static configured port</li> </ul>
Example	Switch(config)#ip igmp snooping vlan 1 l2-general-querier

## 12.1.25 ip igmp snooping vlan l2-general-querier-source

Syntax	<pre>ip igmp snooping vlan &lt;vlan-id&gt; l2-general-querier-source &lt;A.B.C.D&gt; no ip igmp snooping vlan &lt;vlanid&gt; l2-general-querier-source</pre>
Parameter	<pre>&lt;vlan-id&gt;          VLAN ID &lt;A.B.C.D&gt;         &lt;A.B.C.D&gt; is the source address of the query operation</pre>
Default	0.0.0.0
Mode	Global Mode
Usage	It is not supported on Windows 2000/XP to query with the source address as 0.0.0.0. So the layer 2 query source address configuration does not function. The client will stop sending requesting datagrams after one is sent. And after a while, it can not receive multicast datagrams.
Example	Switch(config)#ip igmp snooping vlan 2 l2-general-query-source 192.168.1.2

## 12.1.26 ip igmp snooping vlan l2-general-querier-version

Syntax	ip igmp snooping vlan <vlanid> l2-general-querier-version <version>	
Parameter	<vlan-id>	VLAN ID
	<version>	version number, limited to <1-3>.
Default	version 3	
Mode	Global Mode	
Usage	When the switch is connected to V1 and V2 capable environment, and for VLAN which has source of layer 2 query configuration, the VLAN can be queried only if the version number has been specified. This command is used to query the layer 2 version number.	
Example	Switch(config)#ip igmp snooping vlan 2 l2-general-querier-version 2	

## 12.1.27 ip igmp snooping vlan limit

Syntax	ip igmp snooping vlan <vlanid> limit {group <g_limit>   source <s_limit>} no ip igmp snooping vlan <vlan-id> limit						
Parameter	<table border="1"> <tr> <td>&lt;vlan-id&gt;</td> <td>VLAN ID</td> </tr> <tr> <td>&lt;g_limit&gt;</td> <td>&lt;1-65535&gt;, max number of groups joined</td> </tr> <tr> <td>&lt;s_limit&gt;</td> <td>&lt;1-65535&gt;, max number of source entries in each group, consisting of include source and exclude source.</td> </tr> </table>	<vlan-id>	VLAN ID	<g_limit>	<1-65535>, max number of groups joined	<s_limit>	<1-65535>, max number of source entries in each group, consisting of include source and exclude source.
<vlan-id>	VLAN ID						
<g_limit>	<1-65535>, max number of groups joined						
<s_limit>	<1-65535>, max number of source entries in each group, consisting of include source and exclude source.						
Default	Maximum 50 groups by default, with each group capable with 40 source entries.						
Mode	Global Mode						
Usage	When number of joined group reaches the limit, new group requesting for joining in will be rejected for preventing hostile attacks. To use this command, IGMP snooping must be enabled on VLAN. The "no" form of this command restores the default other than set to "no limit". For the safety considerations, this command will not be configured to "no limit". It is recommended to use default value and if layer 3 IGMP is in operation, please make this configuration in accordance with the IGMP configuration as possible.						
Example	Switch(config)#ip igmp snooping vlan 2 limit group 300						

## 12.1.28 ip igmp snooping vlan interface

Syntax	<pre>ip igmp snooping vlan &lt;vlanid&gt; interface (ethernet   port-channel) IFNAME limit {group &lt;g_limit&gt;   source &lt;s_limit&gt;} strategy (replace   drop)  no ip igmp snooping vlan &lt;1-4094&gt; interface (ethernet   port-channel) IFNAME limit group source strategy</pre>	
Parameter	<vlan-id>	VLAN ID
	IFNAME	Interface name
	<g_limit>	<1-65535>, The maximum number of groups allowed joining
	<s_limit>	<1-65535>, The maximum number of source table entries in each group, including include source and exclude source.
	replace	Replace the group and source information
	drop	Drop the new group and source information
Default	There is no limitation as default.	
Mode	Global Mode	
Usage	<p>When the number of the groups joined under the port or the number of sources in this group exceeds the limit, it will be dealt according to the configured strategy. If it is drop, drop the new group and source information; if it is replace, find a dynamic group and source from the port to conduct deleting and replacing, and then add the new group and source information. The premise of using this command is that this VLAN is enabled IGMP Snooping function. No command configures as “no limitation”.</p>	
Example	<pre>Switch(config)#ip igmp snooping vlan 2 interface ethernet 1/0/11 limit group 300 source 200 strategy replace</pre>	

## 12.1.29 ip igmp snooping vlan mrouter-port interface

Syntax	ip igmp snooping vlan <vlanid> mrouter-port interface [ehternet   port-channel] <ifname> no ip igmp snooping vlan <vlan-id> mrouter-port interface[<ehternet>   <port-channel>] <ifname>
Parameter	<vlan-id> VLAN ID IFNAME Name of interface
Default	No static mrouter port on VLAN by default.
Mode	Global Mode
Usage	When a port is a static mrouter port while also a dynamic mrouter port, it should be taken as a static mrouter port. Deleting static mrouter port can only be realized by the no command.
Example	Switch(config)#ip igmp snooping vlan 2 mrouter-port interface ethernet1/0/13



### 12.1.30 ip igmp snooping vlan mrouter-port learnpim

Syntax	ip igmp snooping vlan <vlanid> mrouter-port learnpim no ip igmp snooping vlan <vlan-id> mrouter-port learnpim
Parameter	<vlan-id> VLAN ID
Default	Enable
Mode	Global Mode
Usage	Enable the function that the specified VLAN learns mrouter-port (according to pim packets). After a port received pim packets, it will be set to mrouter port for implementing the automatic learning.
Example	Disable the function that vlan 100 learns mrouter-port (according to pim packets). Switch(config)#no ip igmp snooping vlan 100 mrouter-port learnpim

### 12.1.31 ip igmp snooping vlan mrpt

Syntax	<pre>ip igmp snooping vlan &lt;vlanid&gt; mrpt &lt;value&gt; no ip igmp snooping vlan &lt;vlan-id&gt; mrpt</pre>
Parameter	<pre>&lt;vlan-id&gt;          VLAN ID, ranging between &lt;1-4094&gt; &lt;value&gt;           mrouter port survive period, ranging between &lt;1-65535&gt;seconds</pre>
Default	255s
Mode	Global Mode
Usage	This command validates on dynamic mrouter ports but not on mrouter port. To use this command, IGMP Snooping of this VLAN should be enabled previously.
Example	Switch(config)#ip igmp snooping vlan 2 mrpt 100

### 12.1.32 ip igmp snooping vlan query-interval

Syntax	<pre>ip igmp snooping vlan &lt;vlanid&gt; query-interval &lt;value&gt; no ip igmp snooping vlan &lt;vlan-id&gt; query-interval</pre>
Parameter	<pre>&lt;vlan-id&gt;          VLAN ID, ranging between &lt;1-4094&gt; &lt;value&gt;           query interval, ranging between &lt;1-65535&gt;seconds</pre>
Default	125s
Mode	Global Mode
Usage	It is recommended to use the default settings. Please keep this configure in accordance with IGMP configuration as possible if layer 3 IGMP is running.
Example	Switch(config)#ip igmp snooping vlan 2 query-interval 130

### 12.1.33 ip igmp snooping vlan query-mrsp

Syntax	<pre>ip igmp snooping vlan &lt;vlanid&gt; query-mrsp &lt;value&gt; no ip igmp snooping vlan &lt;vlan-id&gt; query-mrspt</pre>
Parameter	<pre>&lt;vlan-id&gt;          VLAN ID, ranging between &lt;1-4094&gt; &lt;value&gt;           ranging between &lt;1-25&gt; seconds</pre>
Default	10s
Mode	Global Mode
Usage	It is recommended to use the default settings. Please keep this configure in accordance with IGMP configuration as possible if layer 3 IGMP is running.
Example	Switch(config)#ip igmp snooping vlan 2 query-mrsp 18

### 12.1.34 ip igmp snooping vlan query-robustness

Syntax	<pre>ip igmp snooping vlan &lt;vlanid&gt; query-robustness &lt;value&gt; no ip igmp snooping vlan &lt;vlan-id&gt; query-robustness</pre>
Parameter	<pre>&lt;vlan-id&gt;          VLAN ID &lt;value&gt;           ranging between &lt;2-10&gt;</pre>
Default	2s
Mode	Global Mode
Usage	It is recommended to use the default settings. Please keep this configure in accordance with IGMP configuration as possible if layer 3 IGMP is running.
Example	Switch(config)#ip igmp snooping vlan 2 query- robustness 3

### 12.1.35 ip igmp snooping vlan report source-address

Syntax	ip igmp snooping vlan <vlanid> report source-address <A.B.C.D> no ip igmp snooping vlan <vlan-id> report source-address
Parameter	<vlan-id> VLAN ID <A.B.C.D> IP address, can be 0.0.0.0
Default	Disabled
Mode	Global Mode
Usage	Default configuration is recommended here. If IGMP snooping needs to be configured, the source address for forwarded IGMP messages can be 0.0.0.0. If it is required by the upstream that IGMP messages should use the same network address, the source address of IGMP messages should be configured to be the same with upstream. °
Example	Switch(config)#ip igmp snooping vlan 2 report source-address 10.1.1.1

### 12.1.36 ip igmp snooping vlan specific-query-mrsp

Syntax	ip igmp snooping vlan <vlanid> specific-query-mrsp <value> no ip igmp snooping vlan <vlan-id> specific-query-mrspt
Parameter	<vlan-id> specific VLAN ID, the range from 1 to 4094 <value> the maximum query response time, unit is second, the range from 1 to 25, default value is 1
Default	Enable
Mode	Global Mode
Usage	After enable vlan snooping in global mode, input this command to configure the maximum query response time of the specific group.
Example	Configure/cancel the specific-query-mrsp of vlan3 as 2s. Switch(config)#ip igmp snooping vlan 3 specific-query-mrsp 2 Switch(config)#no ip igmp snooping vlan 3 specific-query-mrspt

## 12.1.37 ip igmp snooping vlan static-group

Syntax	<pre>ip igmp snooping vlan &lt;vlanid&gt; static-group &lt;A.B.C.D&gt; [source &lt;A.B.C.D&gt;] interface [ethernet   port-channel] &lt;IFNAME&gt;</pre> <pre>no ip igmp snooping vlan &lt;vlan-id&gt; static-group &lt;A.B.C.D&gt; [source &lt;A.B.C.D&gt;] interface [ethernet   port-channel] &lt;IFNAME&gt;</pre>						
Parameter	<table border="1"> <tr> <td>&lt;vlan-id&gt;</td> <td>VLAN ID, ranging between &lt;1-4094&gt;</td> </tr> <tr> <td>&lt;A.B.C.D&gt;</td> <td>address of group or source</td> </tr> <tr> <td>&lt;IFNAME&gt;</td> <td>Name of interface</td> </tr> </table>	<vlan-id>	VLAN ID, ranging between <1-4094>	<A.B.C.D>	address of group or source	<IFNAME>	Name of interface
<vlan-id>	VLAN ID, ranging between <1-4094>						
<A.B.C.D>	address of group or source						
<IFNAME>	Name of interface						
Default	None						
Mode	Global Mode						
Usage	<p>Configure static-group on specified port of the VLAN. The no form of the command cancels this configuration.</p> <p>When a group is a static while also a dynamic group, it should be taken as a static group. Deleting static group can only be realized by the no form of the command.</p>						
Example	<pre>Switch(config)#ip igmp snooping vlan 1 static-group 224.1.1.1 source 192.168.1.1 interface ethernet 1/0/1</pre>						



## 12.1.38 ip igmp snooping vlan suppression-query-time

Syntax	ip igmp snooping vlan <vlanid> suppression-query-time <value> no ip igmp snooping vlan <vlan-id> suppression-query-time
Parameter	<vlan-id> VLAN ID, ranging between <1-4094> <value> ranging between<1-65535> seconds
Default	255s
Mode	Global Mode
Usage	Configure the suppression query time. The “no ip igmp snooping vlan <vlan-id> suppression-query-time” command restores to the default value. This command can only be configured on L2 general querier. The Suppression-query-time refers to the period of suppression state in which the querier enters when receives query from the layer 3 IGMP in the segments.
Example	Switch(config)#ip igmp snooping vlan 2 suppression-query-time 270

## 12.1.39 show ip igmp snooping

Syntax	show ip igmp snooping [vlan <vlan-id>]	
Parameter	<vlan-id>	VLAN ID
Default	none	

Mode Admin Configuration Mode

Usage If no VLAN number is specified, it will show whether global IGMP Snooping switch is on, which VLAN is configured with I2-general-querier function, and if a VLAN number is specified, detailed IGMP messages for this VLAN will be shown.

Example Show IGMP Snooping summary messages of the switch

```
Switch(config)#show ip igmp snooping
```

```
Global igmp snooping status: Enabled
```

```
L3 multicasting: running
```

```
Igmp snooping is turned on for vlan 1(querier)
```

```
Igmp snooping is turned on for vlan 2
```

Displayed Information	Explanation
Global igmp snooping status	Whether the global igmp snooping switch on the switch is on
L3 multicasting	whether the layer 3 multicast protocol of the switch is running
Igmp snooping is turned on for vlan 1(querier)	which VLANs on the switch is enabled with igmp snooping function, whether they are I2-general-querier

2.Display the IGMP Snooping summary messages of vlan1.

```
Switch#show ip igmp snooping vlan 1
```

```
Igmp snooping information for vlan 1
```

```
Igmp snooping L2 general querier :Yes(COULD_QUERY)
```

```
Igmp snooping query-interval :125(s)
```

```
Igmp snooping max reponse time :10(s)
```

```
Igmp snooping robustness :2
```

```
Igmp snooping mrouter port keep-alive time :255(s)
```

```
Igmp snooping query-suppression time :255(s)
```

```
IGMP Snooping Connect Group Membership
```

```
Note: *-All Source, (S)- Include Source, [S]-Exclude Source
```

```
Groups Sources Ports Exptime System Level
```

```
238.1.1.1 (192.168.0.1) Ethernet1/0/8 00:04:14 V2
```

```
(192.168.0.2) Ethernet1/0/8 00:04:14 V2
```

```
Igmp snooping vlan 1 mrouter port
```

```
Note: "!"-static mrouter port
```

!Ethernet1/0/2

Displayed Information	Explanation
Igmp snooping L2 general querier	Whether the VLAN enables I2-general-querier function and show whether the querier state is could-query or suppressed
Igmp snooping query-interval	Query interval of the VLAN
Igmp snooping max reponse time	Max response time of the VLAN
Igmp snooping robustness	IGMP Snooping robustness configured on the VLAN
Igmp snooping mrouter port keep-alive time	keep-alive time of dynamic mrouter of the VLAN
Igmp snooping query-suppression time	Suppression timeout of VLAN when as I2-general-querier
IGMP Snooping Connect Group Membership	Group membership of this VLAN, namely the correspondence between ports and (S,G)
Igmp snooping vlan 1 mrouter port	mrouter port of the VLAN, including both static and dynamic

## 12.1.40 clear ipv6 mld snooping vlan

Syntax	clear ipv6 mld snooping vlan <1-4094> groups [X:X::X:X]
Parameter	<1-4094> VLAN ID [X:X::X:X] specific group address
Default	None
Mode	Admin Configuration Mode
Usage	Delete the group record of the specific VLAN. Use show command to check the deleted group record
Example	Delete all groups. Switch#clear ipv6 mld snooping vlan 1 groups

## 12.1.41 clear ipv6 mld snooping vlan <1-4094> mrouter-port

Syntax	clear ipv6 mld snooping vlan <1-4094> mrouter-port [ethernet] IFNAME
Parameter	<1-4094> VLAN ID IFNAME port name
Default	None
Mode	Admin Configuration Mode
Usage	Delete the mrouter port of the specific VLAN. Use show command to check the deleted group record.
Example	Delete the mrouter port in vlan 1. Switch#clear ipv6 mld snooping vlan 1 mrouter-port

## 12.1.42 ipv6 mld snooping

Syntax	ipv6 mld snooping no ipv6 mld snooping
Parameter	None
Default	MLD Snooping disabled on the switch by default
Mode	Global Mode
Usage	Enable global MLD Snooping on the switch, namely allow every VLAN to be configured with MLD Snooping; the “no” form of this command will disable MLD Snooping on all the VLANs as well as the global MLD snooping
Example	Enable MLD Snooping under global mode. Switch(config)#ipv6 mld snooping

## 12.1.43 ipv6 mld snooping vlan

Syntax	ipv6 mld snooping vlan <vlan-id> no ipv6 mld snooping vlan <vlan-id>
Parameter	<vlan-id> VLAN ID, with a valid range of <1-4094>.
Default	MLD Snooping disabled on VLAN by default
Mode	Global Mode
Usage	Enable MLD Snooping on specified VLAN; the "no" form of this command disables MLD Snooping on specified VLAN. To configure MLD snooping on certain VLAN, the global MLD snooping should be first enabled. Disable MLD snooping on specified VLAN with the no ipv6 mld snooping vlan vid command
Example	Enable MLD snooping on VLAN 100 under global mode. Switch(config)#ipv6 mld snooping vlan 100

## 12.1.44 ipv6 mld snooping vlan immediate-leave

Syntax	<pre>ipv6 mld snooping vlan &lt;vlan-id&gt; immediate-leave no ipv6 mld snooping vlan &lt;vlan-id&gt; immediate-leave</pre>
Parameter	<vlan-id> VLAN ID, with valid range of <1-4094>.
Default	Disabled by default
Mode	Global Mode
Usage	<p>Enable immediate-leave function of the MLD protocol in specified VLAN; the “no” form of this command disables the immediate-leave function of the MLD protocol</p> <p>Enabling the immediate-leave function of the MLD protocol will hasten the process the port leaves one multicast group, in which the specified group query of the group will not be sent and the port will be directly deleted.</p>
Example	<p>Enable the MLD immediate-leave function on VLAN 100.</p> <pre>Switch(config)#ipv6 mld snooping vlan 100 immediate-leave</pre>



## 12.1.45 ipv6 mld snooping vlan l2-general-querier

Syntax	<pre>ipv6 mld snooping vlan &lt;vlan-id&gt; l2-general-querier no ipv6 mld snooping vlan &lt; vlan-id &gt; l2-general-querier</pre>
Parameter	<vlan-id> VLAN ID, with a valid range of <1-4094>
Default	VLAN is not a MLD Snooping L2 general querier by default.
Mode	Global Mode
Usage	<p>It is recommended to configure an L2 general querier on a segment. If before configure with this command, MLD snooping is not enabled on this VLAN, this command will no be executed. When disabling the L2 general querier function, MLD snooping will not be disabled along with it. Main function of this command is sending general queries periodically to help the switches within this segment learn mrouter port.</p> <p>Comment: There are three ways to learn mrouter port in MLD Snooping:</p> <ol style="list-style-type: none"> <li>1. The port which receives MLD query messages</li> <li>2. The port which receives multicast protocol packets and support PIM</li> <li>3. The port statically configured.</li> </ol>
Example	<p>Set VLAN 100 to L2 general querier.</p> <pre>Switch(config)#ipv6 mld snooping vlan 100 l2-general-querier</pre>

## 12.1.46 ipv6 mld snooping vlan limit

Syntax	<pre>ipv6 mld snooping vlan &lt;vlan-id&gt; limit {group &lt;g_limit&gt;   source &lt;s_limit&gt;} no ipv6 mld snooping vlan &lt; vlan-id &gt; limit</pre>						
Parameter	<table border="1"> <tr> <td>&lt;vlan-id&gt;</td> <td>VLAN ID, the valid range is &lt;1-4094&gt;</td> </tr> <tr> <td>&lt;g_limit&gt;</td> <td>max number of groups joined, range: 1-65535</td> </tr> <tr> <td>&lt;s_limit&gt;</td> <td>max number of source entries in each group, consisting of include source and exclude source, range: 1-65535</td> </tr> </table>	<vlan-id>	VLAN ID, the valid range is <1-4094>	<g_limit>	max number of groups joined, range: 1-65535	<s_limit>	max number of source entries in each group, consisting of include source and exclude source, range: 1-65535
<vlan-id>	VLAN ID, the valid range is <1-4094>						
<g_limit>	max number of groups joined, range: 1-65535						
<s_limit>	max number of source entries in each group, consisting of include source and exclude source, range: 1-65535						
Default	Maximum 50 groups by default, with each group capable with 40 source entries.						
Mode	Global Mode						
Usage	<p>When number of joined group reaches the limit, new group requesting for joining in will be rejected for preventing hostile attacks. To use this command, MLD snooping must be enabled on VLAN. The “no” form of this command restores the default other than set to “no limit”. For the safety considerations, this command will not be configured to “no limit”. It is recommended to use default value and if layer 3 MLD is in operation, please make this configuration in accordance with the MLD configuration as possible.</p>						
Example	<pre>Switch(config)#ipv6 mld snooping vlan 2 limit group 300</pre>						

## 12.1.47 ipv6 mld snooping vlan mrouter-port interface

Syntax	<pre>ipv6 mld snooping vlan &lt;vlan-id&gt; mrouter-port interface [ethernet   port-channel] &lt;ifname&gt; no ipv6 mld snooping vlan &lt;vlan-id&gt; mrouter-port interface [ethernet   port-channel] &lt;ifname&gt;</pre>
Parameter	<pre>&lt;vlan-id&gt;          VLAN ID,the valid range is&lt;1-4094&gt; &lt;ifname&gt;          Name of interface</pre>
Default	When a port is made static and dynamic mrouter port at the same time, it's the static mrouter properties is preferred. Deleting the static mrouter port can only be done with the "no" form of this command
Mode	Global Mode
Usage	Set the static mrouter port of the VLAN; the "no" form of this command cancels the configuration.
Example	Switch(config)# <code>ipv6 mld snooping vlan 2 mrouter-port interface ethernet1/0/13</code>

## 12.1.48 ipv6 mld snooping vlan mrouter-port learnpim6

Syntax	ipv6 mld snooping vlan <vlan-id> mrouter-port learnpim6 no ipv6 mld snooping vlan <vlan-id> mrouter-port learnpim6
Parameter	<vlan-id> VLAN ID, ranging from 1 to 4094.
Default	Enable
Mode	Global Mode
Usage	Enable the function that the specified VLAN learns mrouter-port (according to pimv6 packets). After a port received pimv6 packets, it will be set to mrouter port for implementing the automatic learning.
Example	Disable the function that vlan 100 learns mrouter-port (according to pimv6 packets). Switch(config)#ipv6 mld snooping vlan 2 mrouter-port learnpim6

## 12.1.49 ipv6 mld snooping vlan mrpt

Syntax	<code>ipv6 mld snooping vlan &lt;vlan-id&gt; mrpt &lt;value&gt;</code> <code>no ipv6 mld snooping vlan &lt;vlan-id&gt; mrpt</code>
Parameter	<code>&lt;vlan-id&gt;</code> VLAN ID, the valid range is <1-4094> <code>&lt;value&gt;</code> mrouter port keep-alive time with a valid range of <1-65535> secs.
Default	255s
Mode	Global Mode
Usage	Configure the keep-alive time of the mrouter port. This configuration is applicable on dynamic mrouter port, but not on static mrouter port. To use this command, MLD snooping must be enabled on the VLAN.
Example	<code>Switch(config)#ipv6 mld snooping vlan 2 mrpt 100</code>

## 12.1.50 ipv6 mld snooping vlan query-interval

Syntax	<pre>ipv6 mld snooping vlan &lt;vlan-id&gt; query-interval &lt;value&gt; no ipv6 mld snooping vlan &lt;vlan-id&gt; query-interval</pre>
Parameter	<pre>&lt;vlan-id&gt;          VLAN ID, the valid range is &lt;1-4094&gt; &lt;value&gt;           query interval, valid range: &lt;1-65535&gt;secs.</pre>
Default	125s
Mode	Global Mode
Usage	Configure the query interval. It is recommended to use default value and if layer 3 MLD is in operation, please make this configuration in accordance with the MLD configuration as possible. °
Example	<pre>Switch(config)#ipv6 mld snooping vlan 2 query-interval 130</pre>

## 12.1.51 ipv6 mld snooping vlan query-mrsp

Syntax	<pre>ipv6 mld snooping vlan &lt;vlan-id&gt; query-mrsp &lt;value&gt; no ipv6 mld snooping vlan &lt;vlan-id&gt; query-mrsp</pre>
Parameter	<pre>&lt;vlan-id&gt;          VLAN ID,the valid range is&lt;1-4094&gt; &lt;value&gt;           the valid range is &lt;1-25&gt; secs .</pre>
Default	10s
Mode	Global Mode
Usage	<p>Configure the maximum query response period. The "no" form of this command restores the default value.</p> <p>It is recommended to use default value and if layer 3 MLD is in operation, please make this configuration in accordance with the MLD configuration as possible.</p>
Example	<pre>Switch(config)#ipv6 mld snooping vlan 2 query-mrsp 18</pre>

## 12.1.52 ipv6 mld snooping vlan query-robustness

Syntax	<pre>ipv6 mld snooping vlan &lt;vlan-id&gt; query-robustness &lt;value&gt; no ipv6 mld snooping vlan &lt;vlan-id&gt; query-robustness</pre>
Parameter	<pre>&lt;vlan-id&gt;          VLAN ID,the valid range is &lt;1-4094&gt; &lt;value&gt;           the valid range is &lt;2-10&gt;.</pre>
Default	2s
Mode	Global Mode
Usage	<p>Configure the query robustness; the “no” form of this command restores to the default value.</p> <p>It is recommended to use default value and if layer 3 MLD is in operation, please make this configuration in accordance with the MLD configuration as possible.</p>
Example	<pre>Switch(config)#ipv6 mld snooping vlan 2 query- robustness 3</pre>



## 12.1.53 ipv6 mld snooping vlan static-group

Syntax	<pre> ipv6 mld snooping vlan &lt;vlan-id&gt; static-group &lt;X::X:X&gt; [source&lt; X::X:X&gt;] interface [ethernet   port-channel] &lt;IFNAME&gt;  no ipv6 mld snooping vlan &lt;vlan-id&gt; static-group &lt;X::X:X&gt; [source&lt; X::X:X&gt;] interface [ethernet   port-channel] &lt;IFNAME&gt; </pre>						
Parameter	<table border="1"> <tr> <td>&lt;vlan-id&gt;</td> <td>VLAN ID, range : 1-4094</td> </tr> <tr> <td>&lt;X::X:X&gt;</td> <td>The address of group or source.</td> </tr> <tr> <td>&lt;IFNAME&gt;</td> <td>Name of interface</td> </tr> </table>	<vlan-id>	VLAN ID, range : 1-4094	<X::X:X>	The address of group or source.	<IFNAME>	Name of interface
<vlan-id>	VLAN ID, range : 1-4094						
<X::X:X>	The address of group or source.						
<IFNAME>	Name of interface						
Default	None						
Mode	Global Mode						
Usage	<p>Configure static-group on specified port of the VLAN. The no form of the command cancels this configuration.</p> <p>When a group is a static while also a dynamic group, it should be taken as a static group. Deleting static group can only be realized by the no form of the command.</p>						
Example	<pre> Switch(config)#ipv6 mld snooping vlan 2 static-group ff1e::15 source 2000::1 interface ethernet 1/0/1 </pre>						

## 12.1.54 ipv6 mld snooping vlan suppression-query-time

Syntax	<pre>ipv6 mld snooping vlan &lt;vlan-id&gt; suppression-query-time &lt;value&gt; no ipv6 mld snooping vlan &lt;vlan-id&gt; suppression-query-time</pre>
Parameter	<pre>&lt;vlan-id&gt;          VLAN ID, valid range: &lt;1-4094&gt; &lt;value&gt;           valid range: &lt;1-65535&gt;secs.</pre>
Default	255s
Mode	Global Mode
Usage	<p>Configure the suppression query time; the “no” form of this command restores the default value.</p> <p>This command can only be configured on L2 general querier. The Suppression-query-time represents the period the suppression state maintains when general querier receives queries from layer 3 MLD within the segment. To use this command, the query-intervals in different switches within the same segment must be in accordance. It is recommended to use the default value.</p>
Example	<pre>Switch(config)#ipv6 mld snooping vlan 2 suppression-query-time 270</pre>

## 12.1.55 show ipv6 mld snooping

Syntax	show ipv6 mld snooping [vlan <vlan-id>]
Parameter	<vlan-id> VLAN ID
Default	none
Mode	Admin Configuration Mode
Usage	If no VLAN number is specified, it will show whether the global MLD snooping is enabled and layer 3 multicast protocol is running, as well as on which VLAN the MLD Snooping is enabled and configured I2-general-querier. If a VLAN number is specified, the detailed MLD Snooping messages of this VLAN will be displayed.

Example

```

1.Summary of the switch MLD snooping
Switch(config)#show ipv6 mld snooping
Global mld snooping status: Enabled
L3 multicasting: running
Mld snooping is turned on for vlan 1(querier)
Mld snooping is turned on for vlan 2

```

Displayed Information	Explanation
Global mld snooping status	Whether or not the global MLD Snooping is enabled on the switch
L3 multicasting	Whether or not the layer 3 multicast protocol is running on the switch.
Mld snooping is turned on for vlan 1(querier)	On which VLAN of the switch is enabled MLD Snooping, if the VLAN are I2-general-querier.

2.Display the detailed MLD Snooping information of vlan1

```

Switch#show ipv6 mld snooping vlan 1
Mld snooping information for vlan 1

Mld snooping L2 general querier :Yes(COULD_QUERY)
Mld snooping query-interval :125(s)
Mld snooping max reponse time :10(s)
Mld snooping robustness :2
Mld snooping mrouter port keep-alive time :255(s)
Mld snooping query-suppression time :255(s)

```

MLD Snooping Connect Group Membership

Note: \*-All Source, (S)- Include Source, [S]-Exclude Source

Groups Sources Ports Exptime System Level

Ff1e::15 (2000::1) Ethernet1/0/8 00:04:14 V2

(2000::2) Ethernet1/0/8 00:04:14 V2

Mld snooping vlan 1 mrouter port

Note:"!"-static mrouter port

!Ethernet1/0/2

Displayed Information	Explanation
Mld snooping L2 general querier	whether or not I2-general-querier is enabled on VLAN, the querier display status is set to could-query or suppressed
Mld snooping query-interval	Query interval time of the VLAN
Mld snooping max reponse time	Max response time of this VLAN
Mld snooping robustness	Robustness configured on the VLAN
Mld snooping mrouter port keep-alive time	Keep-alive time of the dynamic mrouter on this VLAN
Mld snooping query-suppression time	timeout of the VLAN as I2-general-querier at suppressed status.
MLD Snooping Connect Group Membership	Group membership of the VLAN, namely the correspondence between the port and (S,G)
Mld snooping vlan 1 mrouter port	Mrouter port of the VLAN, including both static and dynamic.

## 12.1.56 multicast-vlan

---

Syntax	multicast-vlan no multicast-vlan
Parameter	none
Default	Multicast VLAN function not enabled by default.
Mode	VLAN Configuration Mode
Usage	Enable multicast VLAN function on a VLAN; the “no” form of this command disables the multicast VLAN function.  The multicast VLAN function can not be enabled on Private VLAN. To disabling the multicast VLAN function of the VLAN, configuration of VLANs associated with the multicast VLAN should be deleted. Note that the default VLAN can not be configured with this command and only one multicast VLAN is allowed on a switch.
Example	Switch(config)#vlan 2 Switch(config-vlan2)# multicast-vlan

---

## 12.1.57 multicast-vlan association

Syntax	multicast-vlan association <vlan-list>
	no multicast-vlan association <vlan-list>
Parameter	<vlan-list> <vlan-list> the VLAN ID list associated with multicast VLAN. Each VLAN can only be associated with one multicast VLAN and the association will only succeed when every VLAN listed in the VLAN ID table exists.
Default	The multicast VLAN is not associated with any VLAN by default.
Mode	VLAN Configuration Mode
Usage	<p>Associate several VLANs with a multicast VLAN; the “no” form of this command cancels the association relations.</p> <p>After a VLAN is associated with the multicast VLAN, when there comes the multicast order in the port of this VLAN, then the multicast data will be sent from the multicast VLAN to this port, so to reduce the data traffic. The VLAN associated with the multicast VLAN should not be a Private VLAN. A VLAN can only be associated with another VLAN after the multicast VLAN is enabled. Only one multicast VLAN can be enabled on a switch.</p>
Example	<pre>Switch(config)#vlan 2 Switch(config-vlan2)# multicast-vlan association 3, 4</pre>

## 12.1.58 multicast-vlan association interface

Syntax	<pre>multicast-vlan association interface (ethernet   port-channel) IFNAME out-tag &lt;tag-id&gt; no multicast-vlan association interface (ethernet   port-channel) IFNAME</pre>				
Parameter	<table border="1"> <tr> <td>IFNAME</td> <td>The name of the ethernet port or port-channel port</td> </tr> <tr> <td>&lt;tag-id&gt;</td> <td>Specify vlan tag of the multicast data forwarded by the associated port, only the tag of the associated port allows the multicast VLAN, the tag-id takes effect. Its range from 1 to 4094.</td> </tr> </table>	IFNAME	The name of the ethernet port or port-channel port	<tag-id>	Specify vlan tag of the multicast data forwarded by the associated port, only the tag of the associated port allows the multicast VLAN, the tag-id takes effect. Its range from 1 to 4094.
IFNAME	The name of the ethernet port or port-channel port				
<tag-id>	Specify vlan tag of the multicast data forwarded by the associated port, only the tag of the associated port allows the multicast VLAN, the tag-id takes effect. Its range from 1 to 4094.				
Default	None				
Mode	VLAN Configuration Mode				
Usage	<p>Associate the specified port with the multicast VLAN, so the associated ports are able to receive the multicast flow. The no command cancels the association between the ports and the multicast VLAN. 'associated VLAN' and 'associated port' of the multicast VLAN are absolute, they do not affect each other when happening the cross.</p> <p>The port of the aggregation member cannot be associated, but the associated port is able to be added to port-group and cancelling the association.</p> <p>The configured port type includes port-channel port or ethernet port and the port is only configured as ACCESS mode.</p> <p>The port (it will be associated) cannot belong to the multicast VLAN, in the same way, the associated port cannot be divided in multicast VLAN.</p> <p><u>5. When the associated port mode is set as non ACCESS mode, the mode cannot be changed.</u></p>				
Example	<pre>Switch(config)#vlan 2 Switch(config-vlan2)# multicast-vlan association interface ethernet 1/2 Switch(config-vlan2)#multicast-vlan association interface port-channel 2 Switch(config-vlan2)#no multicast-vlan association interface ethernet 1/2 Switch(config-vlan2)#no multicast-vlan association interface port-channel 2</pre>				

## 12.1.59 multicast-vlan mode

Syntax	multicast-vlan mode {dynamic   compatible} no multicast-vlan mode {dynamic   compatible}
Parameter	dynamic                      dynamic mode compatible                      compatible mode
Default	Neither of the two modes
Mode	VLAN Configuration Mode
Usage	<p>This command is used to configure the two modes of the multicast vlan; the no command cancels this configuration.</p> <p>When configured as dynamic mode, the mrouter port will not be added automatically any more when issuing the multicast entries; when configured as compatible mode, the report packet will be not transmitted to the mrouter port any more. When it is not configured as default, the mrouter port will be added when issuing the multicast entries and the report packet will be transmitted to the mrouter port when it is received.</p>
Example	<pre>Switch(config)#vlan 2 Switch(config-vlan2)# multicast vlan mode dynamic</pre>



## 12.1.60 switchport association multicast-vlan

Syntax	<pre>switchport association multicast-vlan &lt;vlan-id&gt; out-tag &lt;tag-id&gt; no switchport association multicast-vlan &lt;vlan-id&gt;</pre>
Parameter	<p>&lt;vlan-id&gt;                      The multicast VLAN associates with the port. Each port can only be associated with one multicast VLAN, and the association will be successful only when the multicast VLAN is existent.</p> <hr/> <p>&lt;tag-id&gt;                        Specify vlan tag of the multicast data forwarded by the associated port, only the tag of the associated port allows the multicast VLAN, the tag-id takes effect. Its range from 1 to 4094.</p>
Default	The port is not associated with any multicast VLAN by default.
Mode	Interface Configuration Mode
Usage	<p>Associate a port with the specified multicast VLAN; the no command cancels the association.</p> <p>After a port is associated with the multicast VLAN, when there comes the multicast order in the port, then the multicast data will be sent from the multicast VLAN to this port, so to reduce the data traffic.</p> <p>If the associated port is set as trunk port and allows the multicast VLAN, the multicast traffic with the specified vlan tag will be forwarded. The port can only be associated with the multicast VLAN after the multicast VLAN is enabled.</p>
Example	<pre>Switch(config)#vlan 2 Switch(config-vlan2)# multicast-vlan Switch(config)#interface ethernet 1/0/1 Switch(config-if-ethernet1/0/1)#switchport mode trunk Switch(config-if-ethernet1/0/1)#switchport association multicast-vlan 2 out-tag 5</pre>

# Chapter 13 Security Function

## 13.1 ACL

### 13.1.1 absolute-periodic/periodic

Command	<pre>[no] absolute-periodic {Monday Tuesday Wednesday Thursday Friday Saturday  Sunday}&lt;start_time&gt;to{Monday Tuesday Wednesday Thursday Friday Saturday  Sunday}&lt;end_time&gt;</pre> <pre>[no]periodic{{Monday+Tuesday+Wednesday+Thursday+Friday+Saturday+Sunday}  daily  weekdays   weekend} &lt;start_time&gt; to &lt;end_time&gt;</pre>																								
Parameter	<table border="1" style="width: 100%; border-collapse: collapse;"> <tr><td style="border: none;">Monday</td><td style="border: none;">Monday</td></tr> <tr><td style="border: none;">Tuesday</td><td style="border: none;">Tuesday</td></tr> <tr><td style="border: none;">Wednesday</td><td style="border: none;">Wednesday</td></tr> <tr><td style="border: none;">Thursday</td><td style="border: none;">Thursday</td></tr> <tr><td style="border: none;">Friday</td><td style="border: none;">Friday</td></tr> <tr><td style="border: none;">Saturday</td><td style="border: none;">Saturday</td></tr> <tr><td style="border: none;">Sunday</td><td style="border: none;">Sunday</td></tr> <tr><td style="border: none;">daily</td><td style="border: none;">Every day of the week</td></tr> <tr><td style="border: none;">weekdays</td><td style="border: none;">Monday thru Friday</td></tr> <tr><td style="border: none;">weekend</td><td style="border: none;">Saturday thru Sunday</td></tr> <tr><td style="border: none;">&lt;start_time&gt;</td><td style="border: none;">start time ,HH:MM:SS (hour: minute: second)</td></tr> <tr><td style="border: none;">&lt;end_time&gt;</td><td style="border: none;">end time,HH:MM:SS (hour: minute: second)</td></tr> </table>	Monday	Monday	Tuesday	Tuesday	Wednesday	Wednesday	Thursday	Thursday	Friday	Friday	Saturday	Saturday	Sunday	Sunday	daily	Every day of the week	weekdays	Monday thru Friday	weekend	Saturday thru Sunday	<start_time>	start time ,HH:MM:SS (hour: minute: second)	<end_time>	end time,HH:MM:SS (hour: minute: second)
Monday	Monday																								
Tuesday	Tuesday																								
Wednesday	Wednesday																								
Thursday	Thursday																								
Friday	Friday																								
Saturday	Saturday																								
Sunday	Sunday																								
daily	Every day of the week																								
weekdays	Monday thru Friday																								
weekend	Saturday thru Sunday																								
<start_time>	start time ,HH:MM:SS (hour: minute: second)																								
<end_time>	end time,HH:MM:SS (hour: minute: second)																								
Default	No time-range configuration.																								
Mode	time-range mode																								
Usage Guide	<p>This command is used for the switch configuration command effective time-range.</p> <p>By creating a time period and referencing it in a command, the user can make the command take effect within the time range defined that time period.</p> <p>When, for example, a ACL rule only needs to take effect within a specific time range, it can be configured first and then referenced when configuring the ACL rule, so that the ACL rule can only take effect within the time range defined for that time period.</p> <p>In a time period, the time range can be defined in two ways:</p> <p>Absolute cycle time a period of time that takes effect within a specified time range, such as Tuesday 8:00 to Saturday 8:00.</p> <p>Periodic period: a period of time in which a cycle (such as 14 to 16:00 a week) takes effect.</p>																								

---

The no command to delete the configured time-range.

---

Example

Make configurations effective within the period from 9:15:30 to 12:30:00 during Tuesday to Saturday.

```
Switch(config)#time-range admin_timer
```

```
Switch(config-time-range-admin_timer)#absolute-periodic Tuesday 9:15:30 to Saturday 12:30:00
```

Make configurations effective within the period from 14:30:00 to 16:45:00 on Monday, Wednesday, Friday and Sunday.

```
Switch(config-time-range-admin_timer)#periodic Monday Wednesday Friday Sunday  
14:30:00 to 16:45:00
```

---

### 13.1.2 absolute start

Command	[no] absolute start <start_time> <start_data> [end <end_time> <end_data>]								
Parameter	<table border="1"> <tr> <td>&lt;start_time&gt;</td> <td>start time ,HH:MM:SS (hour: minute: second)</td> </tr> <tr> <td>&lt;start_data&gt;</td> <td>start data ,YYYY.MM.DD ( year.month.day )</td> </tr> <tr> <td>&lt;end_time&gt;</td> <td>end time ,HH:MM:SS (hour: minute: second)</td> </tr> <tr> <td>&lt;end_data&gt;</td> <td>end data ,YYYY.MM.DD ( year.month.day )</td> </tr> </table>	<start_time>	start time ,HH:MM:SS (hour: minute: second)	<start_data>	start data ,YYYY.MM.DD ( year.month.day )	<end_time>	end time ,HH:MM:SS (hour: minute: second)	<end_data>	end data ,YYYY.MM.DD ( year.month.day )
<start_time>	start time ,HH:MM:SS (hour: minute: second)								
<start_data>	start data ,YYYY.MM.DD ( year.month.day )								
<end_time>	end time ,HH:MM:SS (hour: minute: second)								
<end_data>	end data ,YYYY.MM.DD ( year.month.day )								
Default	No time-range configuration by default.								
Mode	Time-range mode								
Usage Guide	<p>Define an absolute time-range, this time-range operates subject to the clock of this equipment. Absolute time and date, assign specific year, month, day, hour, minute of the start, shall not configure multiple absolute time and date, when in repeated configuration, the latter configuration covers the absolute time and date of the former configuration.</p> <p>The no command delete configuration.</p>								
Example	<p>Make configurations effective from 6:00:00 to 13:30:00 from Oct. 1, 2004 to Jan. 26, 2005.</p> <pre>Switch(config)#time-range admin_timer Switch(config-time-range-admin_timer)#absolute start 6:00:00 2004.10.1 end 13:30:00 2005.1.26</pre>								

### 13.1.3 access-list (ip extended)

---

Command                    access-list <num> {deny | permit} icmp {{<slpAddr> <sMask>} | any-source | {host-source <slpAddr>}} {{<dIpAddr> <dMask>} | any-destination | {host-destination <dIpAddr>}} [<icmp-type> [<icmp-code>]] [precedence <prec>] [tos <tos>] [time-range<time-range-name>]

access-list <num> {deny | permit} igmp {{<slpAddr> <sMask>} | any-source | {host-source <slpAddr>}} {{<dIpAddr> <dMask>} | any-destination | {host-destination <dIpAddr>}} [<igmp-type>] [precedence <prec>] [tos <tos>][time-range <time-range-name>]

access-list <num> {deny | permit} tcp {{ <slpAddr> <sMask> } | any-source | {host-source <slpAddr> } } [s-port { <sPort> | range <sPortMin> <sPortMax> } ] {{ <dIpAddr> <dMask> } | any-destination | {host-destination <dIpAddr> } } [d-port { <dPort> | range <dPortMin> <dPortMax> } ] [ack+ fin+ psh+ rst+ urg+ syn] [precedence <prec> ] [tos <tos> ] [time-range <time-range-name> ]

access-list <num> {deny | permit} udp {{ <slpAddr> <sMask> } | any-source | {host-source <slpAddr> } } [s-port { <sPort> | range <sPortMin> <sPortMax> } ] {{ <dIpAddr> <dMask> } | any-destination | {host-destination <dIpAddr> } } [d-port { <dPort> | range <dPortMin> <dPortMax> } ] [precedence <prec> ] [tos <tos> ] [time-range<time-range-name> ]

access-list <num> {deny | permit} {eigrp | gre | igmp | ipinip | ip | ospf |<protocol-num> } {{ <slpAddr> <sMask> } | any-source | {host-source <slpAddr> } } {{ <dIpAddr> <dMask> } | any-destination | {host-destination <dIpAddr> } } [precedence <prec> ] [tos <tos> ] [time-range <time-range-name> ]

no access-list <num>

---

Parameter	<num>	the No. of access-list, 100-299
	deny	deny packets
	permit	permit packets
	<slpAddr>	the source IP address, the format is dotted decimal notation
	<sMask>	the reverse mask of source IP, the format is dotted decimal notation
	<sPort>	source port No., 0-65535
	<sPortMin>	the down boundary of source port

---

<sPortMax>	the up boundary of source port
<protocol>	the No. of upper-layer protocol of ip, 0-255
<dIpAddr>	the destination IP address, the format is dotted decimal notation
<dMask>	the reverse mask of destination IP, the format is dotted decimal notation
<dPort>	destination port No. 0-65535
<dPortMin>	the down boundary of destination port
<dPortMax>	the up boundary of destination port
<igmp-type>	the type of igmp, 0-15
<icmp-type>	the type of icmp, 0-255
<icmp-code>	protocol No. of icmp, 0-255
<prec>	IP priority, 0-7
<tos>	to value, 0-15
<time-range-name>	the name of time-range

Default By default,no access-lists configured.

Mode Global mode

Usage Guide Create a numeric extended IP access rule to match specific IP protocol or all IP protocol;if access-list of this coded numeric extended does not exist,thus to create such a access-list.

When the user assign specific <num> for the first time,ACL of the serial number is created,then the lists are added into this ACL;the access list which marked 200-299 can configure not continual reverse mask of IP address.

<igmp-type>represent the type of IGMP packet, and usual values please refer to the following description:

- 17(0x11): IGMP QUERY packet
- 18(0x12): IGMP V1 REPORT packet
- 22(0x16): IGMP V2 REPORT packet
- 23(0x17): IGMP V2 LEAVE packet
- 34(0x22): IGMP V3 REPORT packet
- 19(0x13): DVMR packet
- 20(0x14): PIM V1 packet

Particular notice:The packet types included here are not the types excluding IP OPTION. Normally, IGMP packet contains OPTION fields, and such configuration is of no use for this type of packet. If you want to configure the packets containing OPTION, please directly use the manner where OFFSET is configured.

The no command delete configuration.

---

Example

---

Create the numeric extended access-list whose serial No. is 110. deny icmp packet to pass, and permit udp packet with destination address 192. 168. 0. 1 and destination port 32 to pass.

Switch(config)#access-list 110 deny icmp any any-destination

Switch(config)#access-list 110 permit udp any host-destination 192.168.0.1 d-port 32

---

### 13.1.4 access-list (ip standard)

Command	access-list <num> {deny   permit} {{<slpAddr> <sMask >}   any-source}{host-source <slpAddr>}} no access-list <num>										
Parameter	<table border="1"> <tr> <td>&lt;num&gt;</td> <td>the No. of access-list, 100-199</td> </tr> <tr> <td>deny</td> <td>deny packets</td> </tr> <tr> <td>permit</td> <td>permit packets</td> </tr> <tr> <td>&lt;slpAddr&gt;</td> <td>the source IP address, the format is dotted decimal notation</td> </tr> <tr> <td>&lt;sMask&gt;</td> <td>the reverse mask of source IP, the format is dotted decimal notation</td> </tr> </table>	<num>	the No. of access-list, 100-199	deny	deny packets	permit	permit packets	<slpAddr>	the source IP address, the format is dotted decimal notation	<sMask>	the reverse mask of source IP, the format is dotted decimal notation
<num>	the No. of access-list, 100-199										
deny	deny packets										
permit	permit packets										
<slpAddr>	the source IP address, the format is dotted decimal notation										
<sMask>	the reverse mask of source IP, the format is dotted decimal notation										
Default	By default,no access-lists configured.										
Mode	Global mode										
Usage Guide	<p>Create a numeric standard IP access-list. If this access-list exists, then add a rule list;When the user assign specific &lt;num&gt; for the first time, ACL of the serial number is created, then the lists are added into this ACL.</p> <p>The “no access-list &lt;num&gt;“ operation of this command is to delete a numeric standard IP access-list.</p>										
Example	<p>Create a numeric standard IP access-list whose serial No. is 20, and permit date packets with source address of 10.1.1.0/24 to pass, and deny other packets with source address of 10.1.1.0/16.</p> <pre>Switch(config)#access-list 20 permit 10.1.1.0 0.0.0.255 Switch(config)#access-list 20 deny 10.1.1.0 0.0.255.255</pre>										



### 13.1.5 access-list(mac extended)

Command	<pre>access-list &lt;num&gt; {deny   permit} {any-source-mac   {host-source-mac &lt;slpAddr&gt;}} &lt;host_smac&gt;}   {&lt;smac&gt; &lt;smac-mask&gt;}} {any-destination-mac   {host-destination-mac &lt;host_dmac&gt;}   {&lt;dmac&gt; &lt;dmac-mask&gt;}} [untagged-eth2   tagged-eth2   untagged-802-3   tagged-802-3] no access-list &lt;num&gt;</pre>																																				
Parameter	<table border="1"> <tr> <td>&lt;num&gt;</td> <td>the access-list No. which is a decimal's No. from 1100-1199</td> </tr> <tr> <td>deny</td> <td>deny packets</td> </tr> <tr> <td>permit</td> <td>permit packets</td> </tr> <tr> <td>any-source-mac</td> <td>any source address</td> </tr> <tr> <td>host-source-mac</td> <td>source mac address</td> </tr> <tr> <td>&lt;slpAddr&gt;</td> <td>the source IP address, the format is dotted decimal notation</td> </tr> <tr> <td>&lt;host_smac&gt;</td> <td>source mac address</td> </tr> <tr> <td>&lt;smac&gt;</td> <td>source mac address</td> </tr> <tr> <td>&lt;smac-mask&gt;</td> <td>mask (reverse mask) of source MAC address</td> </tr> <tr> <td>any-destination-mac</td> <td>any destination address</td> </tr> <tr> <td>host-destination-mac</td> <td>destination MAC address</td> </tr> <tr> <td>&lt;host_dmac&gt;</td> <td>destination MAC address</td> </tr> <tr> <td>&lt;dmac&gt;</td> <td>destination MAC address</td> </tr> <tr> <td>&lt;dmac-mask&gt;</td> <td>mask (reverse mask) of destination MAC address</td> </tr> <tr> <td>untagged-eth2</td> <td>format of untagged ethernet II packet</td> </tr> <tr> <td>tagged-eth2</td> <td>format of tagged ethernet II packet;</td> </tr> <tr> <td>untagged-802-3</td> <td>format of untagged ethernet 802.3 packet</td> </tr> <tr> <td>tagged-802-3</td> <td>format of tagged ethernet 802.3 packet</td> </tr> </table>	<num>	the access-list No. which is a decimal's No. from 1100-1199	deny	deny packets	permit	permit packets	any-source-mac	any source address	host-source-mac	source mac address	<slpAddr>	the source IP address, the format is dotted decimal notation	<host_smac>	source mac address	<smac>	source mac address	<smac-mask>	mask (reverse mask) of source MAC address	any-destination-mac	any destination address	host-destination-mac	destination MAC address	<host_dmac>	destination MAC address	<dmac>	destination MAC address	<dmac-mask>	mask (reverse mask) of destination MAC address	untagged-eth2	format of untagged ethernet II packet	tagged-eth2	format of tagged ethernet II packet;	untagged-802-3	format of untagged ethernet 802.3 packet	tagged-802-3	format of tagged ethernet 802.3 packet
<num>	the access-list No. which is a decimal's No. from 1100-1199																																				
deny	deny packets																																				
permit	permit packets																																				
any-source-mac	any source address																																				
host-source-mac	source mac address																																				
<slpAddr>	the source IP address, the format is dotted decimal notation																																				
<host_smac>	source mac address																																				
<smac>	source mac address																																				
<smac-mask>	mask (reverse mask) of source MAC address																																				
any-destination-mac	any destination address																																				
host-destination-mac	destination MAC address																																				
<host_dmac>	destination MAC address																																				
<dmac>	destination MAC address																																				
<dmac-mask>	mask (reverse mask) of destination MAC address																																				
untagged-eth2	format of untagged ethernet II packet																																				
tagged-eth2	format of tagged ethernet II packet;																																				
untagged-802-3	format of untagged ethernet 802.3 packet																																				
tagged-802-3	format of tagged ethernet 802.3 packet																																				
Default	By default, no access-lists configured.																																				
Mode	Global mode																																				
Usage Guide	<p>Define an extended numeric MAC ACL rule.</p> <p>When the user assign specific &lt;num&gt; for the first time, ACL of the serial number is created, then the lists are added into this ACL.</p> <p>“no access-list &lt;num&gt;” command deletes an extended numeric MAC access-list rule.</p>																																				
Example	<p>Permit tagged-eth2 with any source MAC addresses and any destination MAC addresses and the packets pass.</p> <pre>Switch(config)#access-list 1100 permit any-source-mac any-destination-mac tagged-eth2</pre>																																				

### 13.1.6 access-list(mac-ip extended)

Command

```
access-list<num>{deny|permit}{any-source-mac {host-source-mac<host_smac>}|
{<smac><smac-mask>}} {any-destination-mac{{host-destination-mac <host_dmac>}|
{<dmac><dmac-mask>}}icmp {{<source><source-wildcard>}}any-source|
{host-source<source-host-ip>}} {{<destination><destination-wildcard>}}
any-destination|{host-destination<destination-host-ip>}}[<icmp-type> [<icmp-code>]]
[precedence <precedence>] [tos <tos>][time-range<time-range-name>]
```

```
access-list<num>{deny|permit}{any-source-mac {host-source-mac<host_smac>}|
{<smac><smac-mask>}} {any-destination-mac{{host-destination-mac <host_dmac>}|
{<dmac><dmac-mask>}}igmp {{<source><source-wildcard>}}any-source|
{host-source<source-host-ip>}} {{<destination><destination-wildcard>}}
any-destination| {host-destination<destination-host-ip>}} [<igmp-type>] [precedence
<precedence>] [tos <tos>][time-range<time-range-name>]
```

```
access-list <num> {deny|permit}{any-source-mac {host-source-mac<host_smac> }
{ <smac> <smac-mask> }}{any-destination-mac {host-destination-mac <host_dmac> }
{ <dmac> <dmac-mask> }}tcp {{ <source> <source-wildcard> }}any-source|
{host-source <source-host-ip> }}[s-port{ <port1> | range <sPortMin> <sPortMax> }]
{{ <destination> <destination-wildcard> } | any-destination | {host-destination
<destination-host-ip> }} [d-port { <port3> | range <dPortMin> <dPortMax> }]
[ack+fin+psh+rst+urg+syn] [precedence<precedence> ] [tos <tos> ] [time-range
<time-range-name> ]
```

```
access-list <num> {deny|permit}{any-source-mac {host-source-mac<host_smac> }
{ <smac> <smac-mask> }}{any-destination-mac {host-destination-mac <host_dmac> }
{ <dmac> <dmac-mask> }}udp {{ <source> <source-wildcard> }}any-source|
{host-source <source-host-ip> }}[s-port{ <port1> | range <sPortMin> <sPortMax> }]
{{ <destination> <destination-wildcard> }}any-destination| {host-destination
<destination-host-ip> }}[d-port{ <port3> | range <dPortMin> <dPortMax> }]
[precedence <precedence> ] [tos <tos> ][time-range <time-range-name> ]
```

```
access-list <num> {deny|permit}{any-source-mac {host-source-mac <host_smac> }
{ <smac> <smac-mask> }} {any-destination-mac{{host-destination-mac <host_dmac> }
{ <dmac> <dmac-mask> }} {eigrp|gre|igrp|ip|ipinip|ospf{ <protocol-num> }}
{{ <source><source-wildcard> }}any-source|{host-source <source-host-ip> }}
{{ <destination><destination-wildcard> }}any-destination| {host-destination
<destination-host-ip> }}[precedence <precedence> ] [tos <tos> ][time-range
```

<time-range-name> ]

no access-list <num>

Parameter

<num>	access-list serial No. this is a decimal's No. from 3100-3299
deny	deny packets
permit	permit packets
any-source-mac	any source mac address
any-destination-mac	any destination mac address
host smac , smac	source mac address
smac-mask	(reverse mask) of source MAC address
host dmac , dmas	destination mac address
dmac-mask	(reverse mask) of destination MAC address
protocol	No. of name or IP protocol. It can be a key word: eigrp, gre, icmp, igmp, igmp, ip, ipinip, ospf, tcp, or udp, or an integer from 0-255 of list No. of IP address. Use key word 'ip' to match all Internet protocols (including ICMP, TCP, AND UDP) list
source-host-ip	No. of source network or source host of packet delivery. Numbers of 32-bit binary system with dotted decimal notation expression
source-wildcard	reverse of source IP. Numbers of 32-bit binary system expressed by decimal's numbers with four-point separated, reverse mask
destination-host-ip	No. of destination network or host to which packets are delivered. Numbers of 32-bit binary system with dotted decimal notation expression
destination-wildcard	mask of destination. I Numbers of 32-bit binary system expressed by decimal's numbers with four-point separated, reverse mask
s-port	means the need to match TCP/UDP source port
port1	value of TCP/UDP source interface No.,Interface No. is an integer from 0-65535
d-port	means need to match TCP/UDP destination interface
sPortMin	the down boundary of source port
sPortMax	the up boundary of source port
port3	value of TCP/UDP destination interface No., Interface No. is an integer from 0-65535
dPortMin	the down boundary of destination port
dPortMax	the up boundary of destination port
[ack] [fin] [psh]	only for TCP protocol, multi-choices of tag positions are available, and
[rst] [urg] [syn]	when TCP data reports the configuration of corresponding position, then

	initialization of TCP data report is enabled to form a match when in connection
precedence	packets can be filtered by priority which is a number from 0-7
tos	packets can be filtered by service type which ia number from 0-15
icmp-type	ICMP packets can be filtered by packet type which is a number from 0-255
icmp-code	ICMP packets can be filtered by packet code which is a number from 0-255
igmp-type	ICMP packets can be filtered by IGMP packet name or packet type which is a number from 0-255
time-range-name	name of time range

**Default** By default,no access-lists configured.

**Mode** Global mode

**Usage Guide** Define an extended numeric MAC-IP ACL rule.  
 When the user assign specific <num> for the first time, ACL of the serial number is created, then the lists are added into this ACL; the access list which marked 3200-3299 can configure not continual reverse mask of IP address.  
  
 The no command deletes a extended numeric MAC-IP ACL access-list rule.

**Example** Permit the passage of TCP packet with source MAC 00-12-34-45-XX-XX, any destination MAC address, source IP address 100.1.1.0 0.255.255.255, and source port 100.  
  
 Switch(config)#access-list 3199 permit 00-12-34-45-67-00 00-00-00-00-FF-FF any-destination-mac tcp 100.1.1.0 0.255.255.255 s-port 100 any-destination

### 13.1.7 access-list (mac standard)

Command	<pre>access-list &lt;num&gt; {deny   permit} {any-source-mac   {host-source-mac &lt;host_smac&gt; }   {&lt;smac&gt; &lt;smac-mask&gt;}} no access-list &lt;num&gt;</pre>										
Parameter	<table border="1"> <tr> <td>&lt;num&gt;</td> <td>the access-list No. which is a decimal's No. from 700-799</td> </tr> <tr> <td>deny</td> <td>deny packets</td> </tr> <tr> <td>permit</td> <td>permit packets</td> </tr> <tr> <td>host_smac · smac</td> <td>source mac address</td> </tr> <tr> <td>smac-mask</td> <td>(reverse mask) of source MAC address</td> </tr> </table>	<num>	the access-list No. which is a decimal's No. from 700-799	deny	deny packets	permit	permit packets	host_smac · smac	source mac address	smac-mask	(reverse mask) of source MAC address
<num>	the access-list No. which is a decimal's No. from 700-799										
deny	deny packets										
permit	permit packets										
host_smac · smac	source mac address										
smac-mask	(reverse mask) of source MAC address										
Default	By default, no access-lists configured.										
Mode	Global mode										
Usage Guide	<p>Define a standard numeric MAC ACL rule.</p> <p>When the user assign specific &lt;num&gt; for the first time, ACL of the serial number is created, then the lists are added into this ACL.</p> <p>The no command deletes a standard numeric MAC ACL access-list rule.</p>										
Example	<p>Permit the passage of packets with source MAC address 00-00-XX-XX-00-01, and deny passage of packets with source MAC address 00-00-00-XX-00-ab.</p> <pre>Switch(config)# access-list 700 permit 00-00-00-00-00-01 00-00-FF-FF-00-00 Switch(config)# access-list 700 deny 00-00-00-00-00-ab 00-00-00-FF-00-00</pre>										

### 13.1.8 clear access-group statistic

Command	clear access-group statistic [ethernet <interface-name> ]
Parameter	interface-name            interface-name
Default	None.
Mode	Admin Mode
Usage Guide	Empty packet statistics information of the specified interface.
Example	Empty packet statistics information of interface.  Switch#clear access-group statistic

### 13.1.9 firewall

Command	firewall {enable   disable}
Parameter	{enable   disable}      enable or disable
Default	None.
Mode	Global Mode
Usage Guide	Enable or disable firewall. Whether enabling or disabling firewall, access rules can be configured. But only when the firewall is enabled, the rules can be used in specific orientations of specific ports. When disabling the firewall, all ACL tied to ports will be deleted.
Example	Enable firewall.  Switch(config)#firewall enable

### 13.1.10 ip access extended

Command	[no] ip access extended <name>
Parameter	name the name of the access list. The name can be formed by non-all-digit characters of length of 1 to 32.
Default	By default, no access-lists configured.
Mode	Global mode
Usage Guide	Create a named extended IP access list. When this command is issued for the first time, an empty access list will be created.  The no prefix will remove the named extended IP access list including all the rules.
Example	To create a extended IP access list name tcpFlow.  Switch(config)#ip access-list extended tcpFlow



### 13.1.11 ip access standard

Command	[no] ip access standard<name>
Parameter	name the name of the access list. The name can be formed by non-all-digit characters of length of 1 to 32
Default	By default,no access-lists configured.
Mode	Global mode
Usage Guide	Create a named standard access list. When this command is issued for the first time, an empty access list will be created.  The no prefix will remove the named standard access list including all the rules in the list.
Example	To create a standard IP access list name ipFlow.  Switch(config)#ip access-list standard ipFlow

### 13.1.12 ipv6 access-list

Command	<pre> ipv6 access-list &lt;num-std&gt; {deny   permit} {&lt;sIPv6Prefix/sPrefixlen&gt;   any-source   {host-source &lt;sIPv6Addr&gt;}} no ipv6 access-list &lt;num-std&gt; </pre>												
Parameter	<table border="1"> <tr> <td>num-std</td> <td>the list number, list range is between 500 ~ 599</td> </tr> <tr> <td>deny</td> <td>deny packets</td> </tr> <tr> <td>permit</td> <td>permit packets</td> </tr> <tr> <td>sIPv6Prefix</td> <td>the prefix of the ipv6 source address</td> </tr> <tr> <td>sPrefixlen</td> <td>the length of prefix of the ipv6 source address, range is between 1 ~ 128</td> </tr> <tr> <td>sIPv6Addr</td> <td>the ipv6 source address</td> </tr> </table>	num-std	the list number, list range is between 500 ~ 599	deny	deny packets	permit	permit packets	sIPv6Prefix	the prefix of the ipv6 source address	sPrefixlen	the length of prefix of the ipv6 source address, range is between 1 ~ 128	sIPv6Addr	the ipv6 source address
num-std	the list number, list range is between 500 ~ 599												
deny	deny packets												
permit	permit packets												
sIPv6Prefix	the prefix of the ipv6 source address												
sPrefixlen	the length of prefix of the ipv6 source address, range is between 1 ~ 128												
sIPv6Addr	the ipv6 source address												
Default	By default, no access-lists configured.												
Mode	Global mode												
Usage Guide	<p>Creates a numbered standard IP access-list, if the access-list already exists, then a rule will add to the current access-list.</p> <p>The no command deletes a numbered standard IP access-list.</p>												
Example	<p>Creates a numbered 520 standard IP access-list, allow the source packet from 2003:1:2:3::1/64 pass through the net, and deny all the other packet from the source address 2003:1:2::1/48 pass through.</p> <pre> Switch (config)#ipv6 access-list 520 permit 2003:1:2:3::1/64 Switch (config)#ipv6 access-list 520 deny 2003:1:2::1/48 </pre>												



### 13.1.14 ipv6 access extended

Command	<code>ipv6 access-list extended &lt;name&gt;</code> <code>no ipv6 access-list extended &lt;name&gt;</code>
Parameter	<code>name</code> the name for access list, the character string length is from 1 to 32
Default	By default, no access-lists configured.
Mode	Global mode
Usage Guide	Create a name-based extended IPv6 access list. When this command is run for the first time, only an empty access list with no entry will be created.  The no command delete the name-based extended IPv6 access list.
Example	Create an extensive IPv6 access list named tcpFlow.  Switch(config)# <code>ipv6 access-list extended tcpFlow</code>

### 13.1.15 access-group

Command	<pre>{ip ipv6 mac mac-ip} access-group &lt;name&gt; {in} [traffic-statistic] no {ip ipv6 mac mac-ip} access-group &lt;name&gt; {in}</pre>				
Parameter	<table border="1"> <tr> <td>name</td> <td>the name for access list, the character string length is from 1 to 32</td> </tr> <tr> <td>traffic-statistic</td> <td>flow statistics</td> </tr> </table>	name	the name for access list, the character string length is from 1 to 32	traffic-statistic	flow statistics
name	the name for access list, the character string length is from 1 to 32				
traffic-statistic	flow statistics				
Default	By default,the entry of port is not bound ACL.				
Mode	Port Mode				
Usage Guide	<p>Apply an access-list on some direction of port, and determine if ACL rule is added statistic counter or not by options.</p> <p>Note:when a ACL has multiple rules, traffic-statistic can't configure.</p> <p>There are four kinds of packet head field based on concerned:MAC ACL,IP ACL,MAC-IP ACL and IPv6 ACL; to some extent,ACL filter behavior (permit,deny) has a conflict when a data packet matches multi types of four ACLs.The strict priorities are specified for each ACL based on outcome veracity.It can determine final behavior of packet filter through priority when the filter behavior has a conflict.</p> <p>When binding ACL to port, there are some limits as below:</p> <ol style="list-style-type: none"> <li>1. Each port can bind a MAC-IP ACL, a IP ACL, a MAC ACL and a IPv6 ACL.</li> <li>2. When binding four ACLs and data packet matching the multi ACLs simultaneity, the priority from high to low are shown as below,            Ingress IPv6 ACL            Ingress MAC-IP ACL            Ingress MAC ACL            Ingress IP ACL</li> </ol> <p>The no command deletes access-list binding on the port.</p>				
Example	<p>Binding AAA access-list to entry direction of port.</p> <pre>Switch(config)#interface ethernet 1/0/5 Switch(config-If-Ethernet1/0/5)#ip access-group aaa in</pre>				

### 13.1.16 mac access extended

Command	mac-access-list extended <name> no mac-access-list extended <name>
Parameter	name                      name of access-list excluding blank or quotation mark, and it must start with letter, and the length cannot exceed 32. (remark: sensitivity on capital or small letter.)
Default	By default · no access-lists configured.
Mode	Global mode
Usage Guide	Define a name-manner MAC ACL or enter access-list configuration mode. After assigning this command for the first time, only an empty name access-list is created and no list item included.  The no command deletes this ACL.
Example	Create an MAC ACL named mac_acl.  Switch(config)# mac-access-list extended mac_acl Switch(config-mac-ext-nacl-mac_acl)#

### 13.1.17 mac-ip access extended

Command	mac-ip-access-list extended <name> no mac-ip-access-list extended <name>
Parameter	name                      name of access-list excluding blank or quotation mark, and it must start with letter, and the length cannot exceed 32 (remark: sensitivity on capital or small letter).
Default	By default · no named MAC-IP access-list.
Mode	Global mode
Usage Guide	Define a name-manner MAC-IP ACL or enter access-list configuration mode. After assigning this command for the first time, only an empty name access-list is created and no list item included.  The no command deletes this ACL.
Example	Create an MAC-IP ACL named macip_acl.  Switch(config)# mac-ip-access-list extended macip_acl Switch(config-macip-ext-nacl-macip_acl)#

### 13.1.18 permit | deny (ip extended)

Command

```
[no] {deny | permit} icmp {{<slpAddr> <sMask>} | any-source | {host-source <slpAddr>}} {{<dIpAddr> <dMask>} | any-destination | {host-destination <dIpAddr>}} [<icmp-type> [<icmp-code>]] [precedence <prec>][tos <tos>] [time-range<time-range-name>]
```

```
[no] {deny | permit} igmp {{<slpAddr> <sMask>} | any-source | {host-source <slpAddr>}} {{<dIpAddr> <dMask>} | any-destination | {host-destination <dIpAddr>}} [<igmp-type>] [precedence <prec>] [tos <tos>] [time-range<time-range-name>]
```

```
[no] {deny | permit} tcp {{ <slpAddr> <sMask> } | any-source | {host-source <slpAddr> }} [s-port { <sPort> | range <sPortMin> <sPortMax> }] {{ <dIpAddr> <dMask> } | any-destination | {host-destination <dIpAddr> }} [d-port { <dPort> | range <dPortMin> <dPortMax> }] [ack+fin+psh+rst+urg+syn] [precedence <prec> ] [tos <tos> ] [time-range <time-range-name> ]
```

```
[no] {deny | permit} udp {{ <slpAddr> <sMask> } | any-source | {host-source <slpAddr> }} [s-port { <sPort> | range <sPortMin> <sPortMax> }] {{ <dIpAddr> <dMask> } | any-destination | {host-destination <dIpAddr> }} [d-port { <dPort> | range <dPortMin> <dPortMax> }] [precedence <prec> ] [tos <tos> ] [time-range<time-range-name> ]
```

```
[no] {deny | permit} {eigrp | gre | igmp | ipinip | ip | ospf | <protocol-num>} {{<slpAddr> <sMask>} | any-source | {host-source <slpAddr>}} {{<dIpAddr> <dMask>} | any-destination | {host-destination <dIpAddr>}} [precedence <prec>] [tos <tos>][time-range<time-range-name>]
```

Parameter

deny	deny packets
permit	permit packets
<slpAddr>	the source IP address, the format is dotted decimal notation
<sMask>	the reverse mask of source IP, the format is dotted decimal notation
<sPort>	source port No., 0-65535
<sPortMin>	the down boundary of source port
<sPortMax>	the up boundary of source port
<dIpAddr>	the destination IP address, the format is dotted decimal notation
<dMask>	the reverse mask of destination IP, the format is dotted decimal notation, attentive position 0, ignored position 1



---

<dPort>	destination port No. 0-65535
<dPortMin>	the down boundary of destination port
<dPortMax>	the up boundary of destination port
<igmp-type>	the type of igmp, 0-15
<icmp-type>	the type of icmp, 0-255
<icmp-code>	protocol No. of icmp, 0-255
<prec>	IP priority, 0-7
<tos>	to value, 0-15
<time-range-name>	time range name

---



---

Default                      By default · no access-list configured.

---

Mode                         Name extended IP access-list configuration mode

---

Usage Guide                Create a name extended IP access rule to match specific IP protocol or all IP protocol.

The no command will delete this access list.

---

Example                     Create the extended access-list, deny icmp packet to pass, and permit udp packet with destination address 192. 168. 0. 1 and destination port 32 to pass.

```
Switch(config)# access-list ip extended udpFlow
Switch(config-ip-ext-nacl-udpFlow)#deny igmp any any-destination
Switch(config-ip-ext-nacl-udpFlow)#permit udp any host-destination 192.168.0.1 d-port 32
```

---

### 13.1.19 permit | deny (ip standard)

Command	{deny   permit} {{<slpAddr> <sMask>}   any-source   {host-source <slpAddr>}} no {deny   permit} {{<slpAddr> <sMask>}   any-source   {host-source <slpAddr>}}								
Parameter	<table border="1"> <tr> <td>deny</td> <td>deny packets</td> </tr> <tr> <td>permit</td> <td>permit packets</td> </tr> <tr> <td>&lt;slpAddr&gt;</td> <td>the source IP address, the format is dotted decimal notation</td> </tr> <tr> <td>&lt;sMask&gt;</td> <td>the reverse mask of source IP, the format is dotted decimal notation</td> </tr> </table>	deny	deny packets	permit	permit packets	<slpAddr>	the source IP address, the format is dotted decimal notation	<sMask>	the reverse mask of source IP, the format is dotted decimal notation
deny	deny packets								
permit	permit packets								
<slpAddr>	the source IP address, the format is dotted decimal notation								
<sMask>	the reverse mask of source IP, the format is dotted decimal notation								
Default	By default · no access-list configured.								
Mode	Name standard IP access-list configuration mode								
Usage Guide	<p>Create a name standard IP access rule</p> <p>The no command deletes this name standard IP access rule.</p>								
Example	<p>Permit packets with source address 10.1.1.0/24 to pass, and deny other packets with source address 10.1.1.0/16.</p> <pre>Switch(config)# access-list ip standard ipFlow Switch(config-std-nacl-ipFlow)# permit 10.1.1.0 0.0.0.255 Switch(config-std-nacl-ipFlow)# deny 10.1.1.0 0.0.255.255</pre>								

### 13.1.20 permit | deny (ipv6 extended)

Command [no] {deny | permit} icmp {{<sIPv6Prefix/sPrefixlen>} | any-source | {host-source <sIPv6Addr>}} {<dIPv6Prefix/dPrefixlen> | any-destination | {host-destination <dIPv6Addr>}} [<icmp-type> [<icmp-code>]] [dscp <dscp>] [flow-label <fl>] [time-range <time-range-name>]

[no] {deny | permit} tcp { <sIPv6Prefix/sPrefixlen> | any-source | {host-source <sIPv6Addr> } } [s-port { <sPort> | range <sPortMin> <sPortMax> } ] { <dIPv6Prefix/dPrefixlen> | any-destination | {host-destination <dIPv6Addr> } } [d-port { <dPort> | range <dPortMin> <dPortMax> } ] [syn | ack | urg | rst | fin | psh] [dscp <dscp> ] [flow-label <fl> ] [time-range <time-range-name> ]

[no] {deny | permit} udp { <sIPv6Prefix/sPrefixlen> | any-source | {host-source <sIPv6Addr> } } [s-port { <sPort> | range <sPortMin> <sPortMax> } ] { <dIPv6Prefix/dPrefixlen> | any-destination | {host-destination <dIPv6Addr> } } [d-port { <dPort> | range <dPortMin> <dPortMax> } ] [dscp <dscp> ] [flow-label <fl> ] [time-range <time-range-name> ]

[no] {deny | permit} <next-header> {<sIPv6Prefix/sPrefixlen> | any-source | {host-source <sIPv6Addr>}} {<dIPv6Prefix/dPrefixlen> | any-destination | {host-destination <dIPv6Addr>}} [dscp <dscp>] [flow-label <fl>] [time-range <time-range-name>]

[no] {deny | permit} {<sIPv6Prefix/sPrefixlen> | any-source | {host-source <sIPv6Addr>}} {<dIPv6Prefix/dPrefixlen> | any-destination | {host-destination <dIPv6Addr>}} [dscp <dscp>] [flow-label <fl>] [time-range <time-range-name>]

Parameter	deny	deny packets
	permit	permit packets
	<sIPv6Addr>	the source IPv6 address
	<sPrefixlen>	the length of the IPv6 address prefix, the range is 1 ~ 128
	<sPort>	source port number, the range is 0 ~ 65535
	<sPortMin>	the down boundary of source port
	<sPortMax>	the up boundary of source port
	<dIPv6Addr>	the destination IPv6 address
	<dPrefixlen>	the length of the IPv6 address prefix, the range is 1 ~ 128

<dPort> destination port number, the range is 0 ~ 65535

<dPortMin> the down boundary of destination port

<dPortMax> the up boundary of destination port

<igmp-type> type of the IGMP

<icmp-type> icmp type

<icmp-code> icmp protocol number

<dscp> IPv6 priority ,the range is 0 ~ 63

<flowlabel> value of the flow label, the range is 0 ~ 1048575

syn,ack,urg,rst,fin,  
psh,tcp label position

<next-header> the IPv6 next-header

<time-range-name> time range name

**Default**

By default · No access control list configured.

**Mode**

IPv6 nomenclature extended access control list mode

**Usage Guide**

Create an extended nomenclature IPv6 access control rule for specific IPv6 protocol.

The no command will delete this access list.

**Example**

Create an extended access control list named udpFlow,denying the igmppackets while allowing udp packets with destination address 2001:1:2:3::1 and destination port 32.

```
Switch(config)#ipv6 access-list extended udpFlow
Switch(config-ipv6-ext-nacl-udpFlow)#deny igmp any any-destination
Switch(config-ipv6-ext-nacl-udpFlow)#permit udp any-source host-destination 2001:1:2:3::1
dPort 32
```

### 13.1.21 permit | deny (ipv6 standard)

Command	[no] {deny   permit} {{<sIPv6Prefix/sPrefixlen>}   any-source   {host-source <sIPv6Addr>}}								
Parameter	<table border="1"> <tr> <td>deny</td> <td>deny packets</td> </tr> <tr> <td>permit</td> <td>permit packets</td> </tr> <tr> <td>&lt;sPrefixlen&gt;</td> <td>the length of the IPv6 address prefix, the valid range is 1~128</td> </tr> <tr> <td>&lt;sIPv6Addr&gt;</td> <td>the source IPv6 address</td> </tr> </table>	deny	deny packets	permit	permit packets	<sPrefixlen>	the length of the IPv6 address prefix, the valid range is 1~128	<sIPv6Addr>	the source IPv6 address
deny	deny packets								
permit	permit packets								
<sPrefixlen>	the length of the IPv6 address prefix, the valid range is 1~128								
<sIPv6Addr>	the source IPv6 address								
Default	No access list configured by default.								
Mode	Standard IPv6 nomenclature access list mode								
Usage Guide	<p>Create a standard nomenclature IPv6 access control rule.</p> <p>The no form of this command deletes the nomenclature standard IPv6 access control rule.</p>								
Example	<p>Permit packets with source address of 2001:1:2:3::1/64 while denying those with source address of 2001:1:2:3::1/48.</p> <pre>Switch(config)#ipv6 access-list standard ipv6Flow Switch(config-ipv6-std-nacl-ipv6Flow)# permit 2001:1:2:3::1/64 Switch(config-ipv6-std-nacl-ipv6Flow)# deny 2001:1:2:3::1/48</pre>								

### 13.1.22 permit | deny (mac extended)

Command [no]{deny|permit} {any-source-mac}{host-source-mac <host\_smac> }{ <smac> <smac-mask> }} {any-destination-mac}{host-destination-mac <host\_dmac> }{ <dmac> <dmac-mask> }} [cos <cos-val> [ <cos-bitmask> ]] [vlanId <vid-value> [ <vid-mask> ]] [ethertype <protocol> [ <protocol-mask> ]]

[no]{deny|permit} {any-source-mac}{host-source-mac <host\_smac> }{ <smac> <smac-mask> }} {any-destination-mac}{host-destination-mac <host\_dmac> }{ <dmac> <dmac-mask> }} [untagged-eth2 [ethertype <protocol>[protocol-mask]]]

[no]{deny|permit}{any-source-mac}{host-source-mac <host\_smac> }{ <smac> <smac-mask> }} {any-destination-mac}{host-destination-mac <host\_dmac> }{ <dmac> <dmac-mask> }} [untagged-802-3]

[no]{deny|permit} {any-source-mac}{host-source-mac <host\_smac> }{ <smac> <smac-mask> }} {any-destination-mac}{host-destination-mac <host\_dmac> }{ <dmac> <dmac-mask> }} [tagged-eth2 [cos <cos-val>[ <cos-bitmask> ]] [vlanId <vid-value> [ <vid-mask> ]] [ethertype <protocol>[ <protocol-mask> ]]]

[no]{deny|permit}{any-source-mac}{host-source-mac <host\_smac> }{ <smac> <smac-mask> }} {any-destination-mac}{host-destination-mac <host\_dmac> }{ <dmac> <dmac-mask> }} [tagged-802-3 [cos <cos-val>[ <cos-bitmask> ]] [vlanId <vid-value> [ <vid-mask> ]]]

Parameter	deny	deny packets
	permit	permit packets
	any-source-mac	any source of MAC address
	any-destination-mac	any destination of MAC address
	host_smac, smac	source MAC address
	smac-mask	mask (reverse mask) of source MAC address
	host_dmac, dmas	destination MAC address
	dmac-mask	(reverse mask) of destination MAC address
	untagged-eth2	format of untagged ethernet II packet
	tagged-eth2	format of tagged ethernet II packet
	untagged-802-3	format of untagged ethernet 802.3 packet
	tagged-802-3	format of tagged ethernet 802.3 packet
	cos-val	cos value, 0-7
	cos-bitmask	cos mask, 0-7reverse mask and mask bit is consecutive
	vid-value	VLAN No, 1-4094

---

vid-bitmask	VLAN mask, 0-4095, reverse mask and mask bit is consecutive
protocol	specific Ethernet protocol No., 1536-65535
protocol-bitmask	protocol mask, 0-65535, reverse mask and mask bit is consecutive

---



---

**Default** By default · no access-list configured.

---

**Mode** Name extended MAC access-list configuration mode

---

**Usage Guide** Define an extended name MAC ACL rule.

Notice: mask bit is consecutive means the effective bit must be consecutively effective from the first bit on the left, no ineffective bit can be added through. For example: the reverse mask format of one byte is: 00001111b; mask format is 11110000; and this is not permitted: 00010011.

The no command deletes this extended name IP access rule.

---

**Example** The forward source MAC address is not permitted as 00-12-11-23-XX-XX of 802.3 data packet.

```
Switch(config)# mac-access-list extended macExt
Switch(config-mac-ext-nacl-macExt)#deny    00-12-11-23-00-00    00-00-00-00-ff-ff    any-
destination-mac untagged-802-3
Switch(config-mac-ext-nacl-macExt)#deny    00-12-11-23-00-00    00-00-00-00-ff-ff
any tagged-802
```

---

### 13.1.23 permit | deny (mac-ip extended)

Command

```
[no]{deny|permit} {any-source-mac}{host-source-mac<host_smac>}
{<smac><smac-mask>}} {any-destination-mac}{host-destination-mac<host_dmac>}
{<dmac><dmac-mask>}} icmp{{<source><source-wildcard>}}any-source|
{host-source<source-host-ip>}} {{<destination><destination-wildcard>}}
any-destination|{host-destination <destination-host-ip>}} [<icmp-type> [<icmp-code>]]
[precedence <precedence>] [tos <tos>][time-range<time-range-name>]
```

```
[no]{deny|permit} {any-source-mac}{host-source-mac<host_smac>}
{<smac><smac-mask>}} {any-destination-mac}{host-destination-mac<host_dmac>}
{<dmac><dmac-mask>}} igmp{{<source><source-wildcard>}}any-source|
{host-source<source-host-ip>}} {{<destination><destination-wildcard>}}
any-destination|{host-destination <destination-host-ip>}} [<igmp-type>]
[precedence <precedence>] [tos <tos>][time-range<time-range-name>]
```

```
[no]{deny|permit}{any-source-mac}{host-source-mac <host_smac > } { <smac>
<smac-mask > }}{any-destination-mac}{host-destination-mac<host_dmac > }|
{ <dmac> <dmac-mask > }}tcp{{ <source><source-wildcard > }}any-source| {host-source <source-
host-ip > }}[s-port { <port1> |range <sPortMin> <sPortMax > } ]
{{ <destination> <destination-wildcard > } | any-destination| {host-destination
<destination-host-ip > }} [d-port { <port3> | range<dPortMin> <dPortMax > } ]
[ack + fin + psh + rst + urg + syn] [precedence <precedence > ] [tos <tos > ]
[time-range <time-range-name > ]
```

```
[no]{deny|permit}{any-source-mac}{host-source-mac <host_smac > }{{ <smac>
<smac-mask > }}{any-destination-mac}{host-destination-mac <host_dmac > }|
{ <dmac> <dmac-mask > }}udp{{ <source> <source-wildcard > }}any-source|
{host-source <source-host-ip > }}[s-port{ <port1> | range <sPortMin> <sPortMax > } ]
{{ <destination> <destination-wildcard > }}any-destination| {host-destination
<destination-host-ip > }} [d-port { <port3> | range <dPortMin> <dPortMax > } ]
[precedence <precedence > ] [tos <tos > ] [time-range <time-range-name > ]
```

```
[no]{deny|permit}{any-source-mac}{host-source-mac<host_smac>}{<smac>
<smac-mask>}}{any-destination-mac}{host-destination-mac<host_dmac>}
{<dmac><dmac-mask>}}{eigrp|gre|igrp|ip|ipinip|ospf|{<protocol-num>}}
{{<source><source-wildcard>}}any-source|{host-source<source-host-ip>}}
{{<destination><destination-wildcard>}}any-destination|{host-destination
<destination-host-ip>}} [precedence <precedence>] [tos <tos>]
```



[time-range<time-range-name>]

Parameter

num	access-list serial No. this is a decimal's No. from 3100-3199
deny	deny packets
permit	permit packets
any-source-mac	any source MAC address
any-destination-mac	any destination MAC address
host smac, smac	source MAC address
smac-mask	(reverse mask) of source MAC address
host dmac, dmas	destination MAC address
dmac-mask	(reverse mask) of destination MAC address
protocol	No. of name or IP protocol. It can be a key word: eigrp, gre, icmp, igmp, igmp, ip, ipinip, ospf, tcp, or udp, or an integer from 0-255 of list No. of IP address. Use key word 'ip' to match all Internet protocols (including ICMP, TCP, AND UDP) list
source-host-ip, source	No. of source network or source host of packet delivery. Numbers of 32-bit binary system with dotted decimal notation expression
source-wildcard	reverse of source IP. Numbers of 32-bit binary system expressed by decimal's numbers with four-point separated, reverse mask
destination-host-ip destination	destination No. of destination network or host to which packets are delivered. Numbers of 32-bit binary system with dotted decimal notation expression
destination-wildcard	mask of destination. I Numbers of 32-bit binary system expressed by decimal's numbers with four-point separated, reverse mask
s-port	means the need to match TCP/UDP source port
port1	value of TCP/UDP source interface No., Interface No. is an integer from 0-65535
<sPortMin>	the down boundary of source port
<sPortMax>	the up boundary of source port
d-port	means need to match TCP/UDP destination interface
port3	value of TCP/UDP destination interface No., Interface No. is an integer from 0-65535
<dPortMin>	the down boundary of destination port
<dPortMax>	the up boundary of destination port
[ack] [fin] [psh] [rst] [urg] [syn]	(optional) only for TCP protocol, multi-choices of tag positions are available, and when TCP data reports the configuration of corresponding position, then initialization of TCP data report is enabled to form a match when in connection

precedence	packets can be filtered by priority which is a number from 0-7
tos	packets can be filtered by service type which ia number from 0-15
icmp-type	ICMP packets can be filtered by packet type which is a number from 0-255
icmp-code	ICMP packets can be filtered by packet code which is a number from 0-255
igmp-type	ICMP packets can be filtered by IGMP packet name or packet type which is a number from 0-255
time-range-name	name of time range

---

**Default**

By default · no access-list configured.

---

**Mode**

Name extended MAC-IP access-list configuration mode

---

**Usage Guide**

Define an extended name MAC-IP ACL rule.

No form deletes one extended numeric MAC-IP ACL access-list rule.

---

**Example**

Deny the passage of UDP packets with any source MAC address and destination MAC address, any source IP address and destination IP address, and source port 100.

```
Switch(config)# mac-ip-access-list extended maclpExt
Switch(config-macip-ext-nacl-maclpExt)# deny any-source-mac any-destination-mac
udp any-source s-port 100 any-destination
```

### 13.1.24 show access-lists

Command	show access-lists [<num> <acl-name>]
Parameter	<num> <acl-name>      specific ACL No specific ACL name character string
Default	None °
Mode	Admin Mode
Usage Guide	<p>Reveal ACL of configuration.</p> <p>When not assigning names of ACL, all ACL will be revealed, used x time ( s ) indicates the times of ACL to be used.</p>
Example	<p>Reveal ACL of configuration.</p> <pre>Switch#show access-lists access-list 10(used 0 time(s))     access-list 10 deny any-source access-list 100(used 1 time(s))     access-list 100 deny ip any any-destination     access-list 100 deny tcp any any-destination access-list 1100(used 0 time(s))     access-list 1100 permit any-source-mac any-destination-mac tagged-eth2 14 2 0800</pre>

### 13.1.25 show access-group

Command	show access-group in (interface {Ethernet   Ethernet IFNAME})
Parameter	IFNAME                      Port name
Default	None.
Mode	admin/ Global Mode
Usage Guide	Display the ACL binding status on the port. When not assigning interface names, all ACL tied to port will be revealed.
Example	Displays all ACL bound to the port.  Switch#show access-group interface name: Ethernet 1/0/1 IP Ingress access-list used is 100, traffic-statistics Disable. interface name: Ethernet1/0/2 IP Ingress access-list used is 1, packet(s) number is 11110.

### 13.1.26 show firewall

Command	show firewall
Parameter	none                      none
Default	None.
Mode	Admin/Global Mode
Usage Guide	Reveal configuration information of packet filtering functions.
Example	Display firewall status.  Switch#show firewall Firewall status: Enable.

### 13.1.27 show ipv6 access-lists

Command	show ipv6 access-lists [<num> <acl-name>]	
Parameter	<num>	the number of specific access control list, the valid range is 500 ~ 699, amongst 500 ~ 599 is digit standard IPv6 ACL number, 600 ~ 699 is the digit extended IPv6 ACL number
	<acl-name>	the nomenclature character string of a specific access control list, lengthening within 1 ~ 32
Default	None.	
Mode	Admin/Global Mode	
Usage Guide	<p>Show the configured IPv6 access control list.</p> <p>When no access control list is specified, all the access control lists will be displayed; in used x time ( s ) is shown the times the ACL had been quoted.</p>	
Example	<p>Show the configured IPv6 access control list.</p> <pre>Switch#show ipv6 access-lists ipv6 access-list 500(used 1 time(s))   ipv6 access-list 500 deny any-source ipv6 access-list 510(used 1 time(s))   ipv6 access-list 510 deny ip any-source any-destination   ipv6 access-list 510 deny tcp any-source any-destination ipv6 access-list 520(used 1 time(s))   ipv6 access-list 520 permit ip any-source any-destination</pre>	

### 13.1.28 show time-range

Command	show time-range <word>
Parameter	<word> assign name of time-range needed to be revealed
Default	None.
Mode	Admin/Global Mode
Usage Guide	<p>Reveal configuration information of time range functions.</p> <p>When not assigning time-range names, all time-range will be revealed.</p> <p>in used x time ( s ) is shown the times the ACL had been quoted.</p>
Example	<p>Reveal configuration information of time range functions.</p> <pre>Switch#show time-range time-range timer1 (inactive, used 0 times)   absolute-periodic Saturday 0:0:0 to Sunday 23:59:59 time-range timer2 (inactive, used 0 times)   absolute-periodic Monday 0:0:0 to Friday</pre>

## 13.1.29 time-range

Command	[no] time-range <time_range_name>
Parameter	<time_range_name>      time range name must start with letter or number, and the length cannot exceed 32 characters long
Default	By default · no time-range configuration.
Mode	Global Mode
Usage Guide	Create the name of time-range as time range name, enter the time-range mode at the same time.  The no command to delete this time range.
Example	Create a time-range named admin_timer.  Switch(config)#Time-range admin_timer



## 13.2 Self-defined ACL

### 13.2.1 userdefined-access-list standard offset

<p>Command</p>	<pre> userdefined-access-list standard offset [window1 { l3start   l4start } &lt;offset&gt;] [window2 { l3start   l4start } &lt;offset&gt;] [window3 { l3start   l4start } &lt;offset&gt;] [window4 { l3start   l4start } &lt;offset&gt;] [window5 { l3start   l4start } &lt;offset&gt;] [window6 { l3start   l4start } &lt;offset&gt;] [window7 { l3start   l4start } &lt;offset&gt;] [window8 { l3start   l4start } &lt;offset&gt;] [window9 { l3start   l4start } &lt;offset&gt;] [window10 { l3start   l4start } &lt;offset&gt;] [window11 { l3start   l4start } &lt;offset&gt;] [window12 { l3start   l4start } &lt;offset&gt;]  no userdefined-access-list standard offset [window1] [window2] [window3] [window4] [window5] [window6] [window7] [window8] [window9] [window10] [window11] [window12] </pre>								
<p>Parameter</p>	<table border="1"> <tr> <td data-bbox="419 920 687 958">window1-window12</td> <td data-bbox="708 920 1474 958">self-defined window 1 to 12</td> </tr> <tr> <td data-bbox="419 969 496 1003">l3start</td> <td data-bbox="708 969 1474 1055">The start offset position is start of layer3 (It can be effective only when the start of layer3 exists)</td> </tr> <tr> <td data-bbox="419 1066 496 1099">l4start</td> <td data-bbox="708 1066 1474 1151">The start offset position is start of layer4 (It can be effective only when the start of layer4 exists)</td> </tr> <tr> <td data-bbox="419 1162 488 1196">offset</td> <td data-bbox="708 1162 1474 1196">The configured offset is from 0 to 178 (unit is 2Bytes)</td> </tr> </table>	window1-window12	self-defined window 1 to 12	l3start	The start offset position is start of layer3 (It can be effective only when the start of layer3 exists)	l4start	The start offset position is start of layer4 (It can be effective only when the start of layer4 exists)	offset	The configured offset is from 0 to 178 (unit is 2Bytes)
window1-window12	self-defined window 1 to 12								
l3start	The start offset position is start of layer3 (It can be effective only when the start of layer3 exists)								
l4start	The start offset position is start of layer4 (It can be effective only when the start of layer4 exists)								
offset	The configured offset is from 0 to 178 (unit is 2Bytes)								
<p>Default</p>	<p>No Configuration Template.</p>								
<p>Mode</p>	<p>Global Mode</p>								
<p>Usage Guide</p>	<p>Create a standard self-defined ACL template. If the template exists, the corresponding window of the template can be modified.</p> <p>{l2endof tag   l3start   l4start}: used to configure the start offset position of a window, &lt;offset&gt;: used to the offset of a window, the range is &lt;0-178&gt;, unit is 2Bytes,namely, 0 means 0Bytes offset and 1 means 2Bytes offset. Standard self-defined ACL template can configure the start offset position and offset for 12 window at most. One standard self-defined ACL template can be shared in global mode. The window cannot be modified if the standard self-defined ACL rule is configured with this window. But if the standard self-defined ACL rule is not configured, the window configuration can be modified with this command.</p> <p>The no command can delete one or more offset configuration of the window in the template or delete the whole template. The window in the template can be deleted successfully when it is not used by the self-defined ACL rule.</p> <p>l3start only supports window1-6, the biggest offset of l3start includes the head of L2, the biggest</p>								

---

offset of I4start includes the head of L2 and L3.

The no command deletes the window of the standard self-defined ACL template. If the window is not specified, the standard self-defined ACL template will be deleted.

---

Example

Create a global template with 7 windows (3-9) to configure the start offset position and the offset:

```
Switch(config)#userdefined-access-list standard offset window3 I2 0 window4 I2 2 window5 I3 0  
window6 I3 1 window7 I3 2 window8 I4 1 window9 I4 2
```

## 13.2.2 userdefined-access-list standard

Command	<pre>userdefined-access-list standard &lt;1200-1299&gt; {permit deny} {window1 window2  window3 window4 window5 window6 window7 window8 window9 window10  window11 window12}  no userdefined-access-list standard &lt;1200-1299&gt; {permit deny} {window1 window2  window3 window4 window5 window6 window7 window8 window9 window10  window11 window12}</pre>								
Parameter	<table border="1"> <tr> <td>&lt;1200-1299&gt;</td> <td>the access-list No. from 1200 to 1299 in decimal notation</td> </tr> <tr> <td>permit</td> <td>permit access</td> </tr> <tr> <td>deny</td> <td>deny access</td> </tr> <tr> <td>window1-window12</td> <td>custom windows 1 to 12</td> </tr> </table>	<1200-1299>	the access-list No. from 1200 to 1299 in decimal notation	permit	permit access	deny	deny access	window1-window12	custom windows 1 to 12
<1200-1299>	the access-list No. from 1200 to 1299 in decimal notation								
permit	permit access								
deny	deny access								
window1-window12	custom windows 1 to 12								
Default	By default, no any access-list configured.								
Mode	Global Mode								
Usage Guide	<p>Create a numbered standard self-defined ACL. If the standard self-defined ACL exists, then a rule will be added to the ACL.</p> <p>When users specify the specified &lt;num&gt; for the first time, create the ACL with this serial number, then add the entry into this ACL.</p> <p>The no command deletes a numbered standard self-defined ACL.</p>								
Example	<pre>Permit the second bytes of the start of I3 is 0x4501. Permit the packets that the forth byte of the start of I4 is 0xFF.  Configure a rule in the same list to deny the packets that the fifth and the sixth bytes of the start of I3 is 0xFFAA.  Switch(config)#userdefined-access-list standard offset window1 I3 0 window2 I4 1 Switch(config)#userdefined-access-list standard 1200 permit window1 4501 FFFF window2 00FF 00FF Switch(config)#userdefined-access-list standard offset window3 I3 2 Switch(config)#userdefined-access-list standard 1200 deny any-source-mac any-destination-mac untagged-eth2 window3 FFAA FFFF</pre>								

### 13.2.3 userdefined access-group

Command	<pre>userdefined access-group &lt;name&gt; {in} [traffic-statistic]  no userdefined access-group &lt;name&gt; {in}</pre>
Parameter	<pre>&lt;name&gt;                the access-list name from 1200-1399 in decimal notation</pre>
Default	By default · userdefined-access-list is not bound to the port.
Mode	Physical Port Configuration Mode
Usage Guide	<p>Apply userdefined-access-list to one direction of the port. Decide whether the statistical counter should be added to the ACL according to the options.</p> <p>A self-defined access-list can be bound to the ingress of a port and can be configured at the ingress of the same port with other access-lists at the same time. The deny rule is precedent when different access-lists are matching, that means if there is a access-lists match the deny rule, the deny rule must be executed, the permit rule will be executed oppositely.</p> <p>The no command deletes the configuration bound to the port.</p>
Example	<p>The configured self-defined access-list is shown in the following:</p> <pre>Switch(config)#userdefined-access-list standard offset window1 I3 0 window2 I4 1 window3 I3 1  Switch(config)#userdefined-access-list standard 1300 permit window1 4501 FFFF window2 00FF 00FF  Switch(config)#userdefined-access-list standard 1300 deny window1 FFAA0000 FFFF0000</pre> <p>Bind the self-defined access-list to Ethernet1/1:</p> <pre>Switch(config)#interface ethernet1/1 Switch(config-if-ethernet1/1)#userdefined access-group 1300 in</pre>

## 13.2.4 vACL userdefined access-group

<p>Command</p>	<pre>vACL userdefined access-group &lt;name&gt; {in} vLAN &lt;vLANid&gt; [traffic-statistic]  no vACL userdefined access-group &lt;name&gt; {in} vLAN &lt;vLANid&gt;</pre>				
<p>Parameter</p>	<table border="1"> <tr> <td data-bbox="419 483 699 517">&lt;name&gt;</td> <td data-bbox="707 483 1471 517">the access-list name from 1200 to 1399 in decimal notation</td> </tr> <tr> <td data-bbox="419 528 699 562">vLANid</td> <td data-bbox="707 528 1471 562">the bound VLAN · the range is 1-4094</td> </tr> </table>	<name>	the access-list name from 1200 to 1399 in decimal notation	vLANid	the bound VLAN · the range is 1-4094
<name>	the access-list name from 1200 to 1399 in decimal notation				
vLANid	the bound VLAN · the range is 1-4094				
<p>Default</p>	<p>By default · userdefined-access-list is not bound to any VLAN.</p>				
<p>Mode</p>	<p>Global Mode</p>				
<p>Usage Guide</p>	<p>Apply userdefined-access-list to one direction of the specified VLAN, decide whether the statistical counter should be added to the ACL according to the options or.</p> <p>A self-defined access-list can be bound to the ingress of a VLAN and can be configured at the ingress of the same VLAN with other access-lists at the same time. The deny rule is precedent when different access-lists are matching, that means if there is a access-lists match the deny rule, the deny rule must be executed, the permit rule will be executed oppositely.</p> <p>The no command deletes the configuration bound to the specified VLAN.</p>				
<p>Example</p>	<p>The configured self-defined access-list is shown in the following:</p> <pre>Switch(config)#userdefined-access-list standard offset window1 I3 0 window2 I4 1 window3 I3 1  Switch(config)#userdefined-access-list standard 1300 permit window1 4501 FFFF window2 00FF 00FF  Switch(config)#userdefined-access-list standard 1300 deny window1 FFAA0000 FFFF0000</pre> <p>Bind the self-defined access-list to VLAN1:</p> <pre>Switch(config)#vACL userdefined access-group 1300 in vLAN 1</pre>				

## 13.3 802.1x

### 13.3.1 dot1x accept-mac

Command	[no] dot1x accept-mac <mac-address> [interface <interface-name>]				
Parameter	<table border="1"> <tr> <td>mac-address</td> <td>stands for MAC address</td> </tr> <tr> <td>interface-name</td> <td>for interface name and port number</td> </tr> </table>	mac-address	stands for MAC address	interface-name	for interface name and port number
mac-address	stands for MAC address				
interface-name	for interface name and port number				
Default	None.				
Mode	Global Mode				
Usage Guide	<p>Add a MAC address entry to the dot1x address filter table. If a port is specified, the entry added applies to the specified port only. If no port is specified, the entry added applies to all the ports.</p> <p>The dot1x address filter function is implemented according to the MAC address filter table, dot1x address filter table is manually added or deleted by the user.</p> <p>When a port is specified in adding a dot1x address filter table entry, that entry applies to the port only; when no port is specified, the entry applies to all ports in the switch. When dot1x address filter function is enabled, the switch will filter the authentication user by the MAC address. Only the authentication request initiated by the users in the dot1x address filter table will be accepted, the rest will be rejected.</p> <p>The no command deletes the entry from dot1x address filter table.</p>				
Example	<p>Adding MAC address 00-01-34-34-2e-0a to the filter table of Ethernet 1/0/5.</p> <pre>Switch(config)#dot1x accept-mac 00-01-34-34-2e-0a interface ethernet 1/0/5</pre>				

### 13.3.2 dot1x eapor enable

Command	[no] dot1x eapor enable
Parameter	none                      none
Default	EAP relay authentication is used by default.
Mode	Global Mode
Usage Guide	<p>Enables the EAP relay authentication function in the switch.</p> <p>The switch and RADIUS may be connected via Ethernet or PPP. If an Ethernet connection exists between the switch and RADIUS server, the switch needs to authenticate the user by EAP relay (EAPoR authentication); if the switch connects to the RADIUS server by PPP, the switch will use EAP local end authentication (CHAP authentication). The switch should use different authentication methods according to the connection between the switch and the authentication server.</p> <p>The no command sets EAP local end authentication.</p>
Example	<p>Setting EAP local end authentication for the switch.</p> <p>Switch(config)#no dot1x eapor enable</p>

### 13.3.3 dot1x enable

Command	[no] dot1x enable
Parameter	none                      none
Default	802.1x function is not enabled in global mode by default; if 802.1x is enabled under Global Mode, 802.1x will not be enabled for the ports by default.
Mode	Global Mode and Port Mode
Usage Guide	<p>Enables the 802.1x function in the switch and ports.</p> <p>The 802.1x authentication for the switch must be enabled first to enable 802.1x authentication for the respective ports. If Spanning Tree or MAC binding is enabled on the port, or the port is a Trunk port or member of port aggregation group, 802.1x function cannot be enabled for that port unless such conditions are removed.</p> <p>The no command disables the 802.1x function.</p>
Example	<p>Enabling the 802.1x function of the switch and enable 802.1x for port1/0/12.</p> <pre>Switch(config)#dot1x enable Switch(config)#interface ethernet 1/0/12 Switch(config-if-ethernet1/0/12)#dot1x enable</pre>



### 13.3.4 dot1x ipv6 passthrough

Command	[no] dot1x ipv6 passthrough
Parameter	none                      none
Default	IPv6 passthrough function is disabled on the switch by default.
Mode	Port Mode
Usage Guide	<p>Enable IPv6 passthrough function on a switch port, only applicable when access control mode is userbased.</p> <p>The function can only be enabled when 802.1x function is enabled both globally and on the port,with userbased being the control access mode. After it is enabled,users can send IPv6 messages without authentication.</p> <p>The no operation of this command will disable the function.</p>
Example	<p>Enable IPv6 passthrough function on port Ethernet1/0/12.</p> <pre>Switch(config)#dot1x enable Switch(config)#interface ethernet 1/0/12 Switch(config-if-ethernet1/0/12)#dot1x enable Switch(config-if-ethernet1/0/12)#dot1x ipv6 passthrough</pre>



### 13.3.6 dot1x macfilter enable

Command	[no] dot1x macfilter enable
Parameter	none                      none
Default	dot1x address filter is disabled by default.
Mode	Global Mode
Usage Guide	<p>Enables the dot1x address filter function in the switch.</p> <p>When dot1x address filter function is enabled, the switch will filter the authentication user by the MAC address. Only the authentication request initialed by the users in the dot1x address filter table will be accepted.</p> <p>The no command disables the dot1x address filter function.</p>
Example	<p>Enabling dot1x address filter function for the switch.</p> <pre>Switch(config)#dot1x macfilter enable</pre>

### 13.3.7 dot1x macbased guest-vlan

Command	<code>dot1x macbased guest-vlan &lt;vlanid&gt;</code> <code>no dot1x macbased guest-vlan</code>
Parameter	<code>vlanid</code> the configured vlan id, the range is from 1 to 4094
Default	Do not configure 802.1x macbased guest-vlan by default.
Mode	Port Mode
Usage Guide	<p>Configure to appoint the port's guest-vlan based on the mac authentication.</p> <p>If there is no dedicated authentication client or the client version was too low, and it makes no clients authenticate successfully on the port in some time, then the access device will make this user join to the guest VLAN. User can get the 802.1x client software in guest VLAN, update the client or do other updating things (such as anti-virus software, system patches and etc.) When the user under the port in Guest VLAN issues the authentication, this port will be stay in guest VLAN if the authentication failed;</p> <p>if it was successful, there are two situations as below:</p> <p>The authentication server issues an auto VLAN, in this time, the user left the guest VLAN and joined to the auto VLAN. After the user was downline, this user will be assigned to the configured guest VLAN again.</p> <p>The authentication server did not issue the VLAN, in this time, the user left the guest VLAN and joined to the configured native VLAN. After the user was downline, this user will be assigned to the configured guest VLAN again.</p> <p>Notice :</p> <p>dot1x macbased guest-vlan can be configured only on the port based on mac authentication and in HYBRID mode.</p> <p>Different macbased guestVLAN can be configured on different ports, but only one macbased guestVLAN can be configured on one port.</p> <p>The no command deletes this guest-vlan.</p>
Example	<p>Configure the guest-vlan of Ethernet1/0/3 as Vlan 10.</p> <pre>Switch(config-if-ethernet1/0/3)#dot1x macbased guest-vlan 10</pre>

### 13.3.8 dot1x macbased port-down-flush

Command	[no] dot1x macbased port-down-flush
Parameter	none                                  none
Default	The command is not enabled by default.
Mode	Global Mode
Usage Guide	<p>Enables this command, when the dot1x certification according to mac is down, delete the user who passed the certification of the port</p> <p>When users who passed the certification according to mac changed among different ports, delete the user for the new certification. The command should be enable to delete the user.</p> <p>The no command does not make the down operation.</p>
Example	<p>When the dot1x certification according to mac is down, delete the user who passed the certification of the port.</p> <p>Switch(config)#dot1x macbased port-down-flush</p>

### 13.3.9 dot1x max-req

Command	dot1x max-req <count> no dot1x max-req
Parameter	count                      the times to re-transfer EAP request/ MD5 frames, the valid range is 1 to 10
Default	The default maximum for retransmission is 2.
Mode	Global Mode
Usage Guide	Sets the number of EAP request/MD5 frame to be sent before the switch re-initials authentication on no supplicant response. The default value is recommended in setting the EAP request/ MD5 retransmission times.  The no command restores the default setting.
Example	Changing the maximum retransmission times for EAP request/ MD5 frames to 5 times.  Switch(config)#dot1x max-req 5

### 13.3.10 dot1x user allow-movement

Command	[no] dot1x user allow-movement
Parameter	none                      none
Default	Disable the authentication function after the user moves the port.
Mode	Global Mode
Usage Guide	<p>Enable the authentication function after the user moves the port, so the switch allows user to process this authentication. In the condition that the switch connects with hub, when the user will be moved to other port, dot1x user allow-movement command should be enabled.</p> <p>The no command disables the function.</p>
Example	<p>Enable the authentication function after the user moves the port.</p> <pre>Switch(config)#dot1x user allow-movement</pre>

### 13.3.11 dot1x user free-resource

Command	dot1x user free-resource <prefix> <mask> no dot1x user free-resource				
Parameter	<table border="1"> <tr> <td>prefix</td> <td>the segment for limited resource, in dotted decimal format</td> </tr> <tr> <td>mask</td> <td>the mask for limited resource, in dotted decimal format</td> </tr> </table>	prefix	the segment for limited resource, in dotted decimal format	mask	the mask for limited resource, in dotted decimal format
prefix	the segment for limited resource, in dotted decimal format				
mask	the mask for limited resource, in dotted decimal format				
Default	There is no free resource by default.				
Mode	Global Mode				
Usage Guide	<p>To configure 802.1x free resource.</p> <p>This command is available only if user based access control is applied. If user based access control has been applied, this command configures the limited resources which can be accessed by the un-authenticated users. For port based and MAC based access control, users could access no network resources before authentication.</p> <p>If TrustView management system is available, the free resource can be configured in TrustView server, and the TrustView server will distribute the configuration to the switches.</p> <p>To be noticed, only one free resource can be configured for the overall network.</p> <p>The no form command closes this function.</p>				
Example	<p>To configure the free resource segment as 1.1.1.0, the mask is 255.255.255.0.</p> <pre>Switch(config)#dot1x user free-resource 1.1.1.0 255.255.255.0</pre>				



### 13.3.12 dot1x max-user macbased

Command	dot1x max-user macbased <number> no dot1x max-user macbased
Parameter	number                      the maximum users allowed, the valid range is 1 to 256
Default	The default maximum user allowed is 1.
Mode	Port Mode
Usage Guide	Sets the maximum users allowed connect to the port.  This command is available for ports using MAC-based access management, if MAC address authenticated exceeds the number of allowed user, additional users will not be able to access the network.  The no command restores the default setting.
Example	Setting port 1/0/3 to allow 5 users.  Switch(config-if-ethernet1/0/3)#dot1x max-user macbased 5

### 13.3.13 dot1x max-user userbased

Command	dot1x max-user userbased <number> no dot1x max-user userbased
Parameter	number                      the maximum number of users allowed to access the network, ranging from 1 to 1~256
Default	The maximum number of users allowed to access each port is 10 by default.
Mode	Port Mode
Usage Guide	<p>Set the upper limit of the number of users allowed access the specified port when using user-based access control mode.</p> <p>This command can only take effect when the port adopts user-based access control mode. If the number of authenticated users exceeds the upper limit of the number of users allowed access the network, those extra users can not access the network.</p> <p>the no command is used to reset the default value.</p>
Example	<p>Setting port 1/0/3 to allow 5 users.</p> <pre>Switch(config-if-ethernet1/0/3)#dot1x max-user userbased 5</pre>

### 13.3.14 dot1x portbased mode single-mode

Command	[no] dot1x portbased mode single-mode
Parameter	none                      none
Default	Disable the single-mode by default.
Mode	Port Mode
Usage Guide	<p>Set the single-mode based on portbase authentication mode.</p> <p>This command takes effect when the access mode of the port is set as portbase only. Before configuring the single-mode, if the port has enabled dot1x port-method portbased command and exist online users, the switch will enforce all users of this port are offline. After that, this port only allows a user to pass the authentication, the user can access the specified network resource, but other authentication users of this port will be denied and can not access the network. After disabling the single-mode, the switch also enforce the authenticated user is offline.</p> <p>The no command disables this function.</p>
Example	<p>Set port 1/0/1 based on port authentication mode to single mode.</p> <pre>Switch(config-if-ethernet1/0/1)#dot1x portbased mode single-mode</pre>

### 13.3.15 dot1x port-control

Command	dot1x port-control {auto   force-authorized   force-unauthorized} no dot1x port-control						
Parameter	<table border="1"> <tr> <td>auto</td> <td>enable 802.1x authentication, the port authorization status is determined by the authentication information between the switch and the supplicant</td> </tr> <tr> <td>force-authorized</td> <td>sets port to authorized status, unauthenticated data is allowed to pass through the port</td> </tr> <tr> <td>force-unauthorized</td> <td>will set the port to non-authorized mode, the switch will not provide authentication for the supplicant and prohibit data from passing through the port</td> </tr> </table>	auto	enable 802.1x authentication, the port authorization status is determined by the authentication information between the switch and the supplicant	force-authorized	sets port to authorized status, unauthenticated data is allowed to pass through the port	force-unauthorized	will set the port to non-authorized mode, the switch will not provide authentication for the supplicant and prohibit data from passing through the port
auto	enable 802.1x authentication, the port authorization status is determined by the authentication information between the switch and the supplicant						
force-authorized	sets port to authorized status, unauthenticated data is allowed to pass through the port						
force-unauthorized	will set the port to non-authorized mode, the switch will not provide authentication for the supplicant and prohibit data from passing through the port						
Default	When 802.1x is enabled for the port, auto is set by default.						
Mode	Port Mode						
Usage Guide	<p>Sets the 802.1x authentication status.</p> <p>If the port needs to provide 802.1x authentication for the user, the port authentication mode should be set to auto.</p> <p>The no command restores the default setting.</p>						
Example	<p>Setting port1/0/1 to require 802.1x authentication mode.</p> <pre>Switch(config-if-ethernet1/0/1)#dot1x port-control auto</pre>						

### 13.3.16 dot1x port-method

Command	dot1x port-method {macbased   portbased   userbased {standard   advanced}} no dot1x port-method										
Parameter	<table border="1"> <tr> <td>macbased</td> <td>means the access control method based on MAC address</td> </tr> <tr> <td>portbased</td> <td>means the access control method based on port</td> </tr> <tr> <td>userbased</td> <td>means the access control method based on user, it can be divided into two types, one is standard access control method, and the other is advanced access control method</td> </tr> <tr> <td>standard</td> <td>Standard Access Control Method Based on User</td> </tr> <tr> <td>advanced</td> <td>Advanced User-Based Access Control</td> </tr> </table>	macbased	means the access control method based on MAC address	portbased	means the access control method based on port	userbased	means the access control method based on user, it can be divided into two types, one is standard access control method, and the other is advanced access control method	standard	Standard Access Control Method Based on User	advanced	Advanced User-Based Access Control
macbased	means the access control method based on MAC address										
portbased	means the access control method based on port										
userbased	means the access control method based on user, it can be divided into two types, one is standard access control method, and the other is advanced access control method										
standard	Standard Access Control Method Based on User										
advanced	Advanced User-Based Access Control										
Default	Advanced access control method based on user is used by default.										
Mode	Port Mode										
Usage Guide	<p>This command is used to configure the dot1x authentication method for the specified port. When port based authentication is applied, only one host can authenticate itself through one port. And after authentication, the host will be able to access all the resources. When MAC based authentication is applied, multiple host which are connected to one port can access all the network resources after authentication. When either of the above two kinds of access control is applied, un-authenticated host cannot access any resources in the network.</p> <p>When user based access control is applied, un-authenticated users can only access limited resources of the network. The user based access control falls into two kinds – the standard access control and the advanced access control. The standard user based access control does not limit the access to the limited resources when the host is not authenticated yet. While the user based advanced access control can control the access to the limited resources before authentication is done.</p> <p>Notes :</p> <p>For standard control method based on user, the 802.1x free resource must be configured first, and it needs to be used with dot1x privateclient enable.</p> <p>The no form command restores the default access control method.</p>										
Example	<p>To configure the access control method based on port for Ethernet1/0/4.</p> <pre>Switch(config-if-ethernet1/0/4)#dot1x port-method portbased</pre>										

### 13.3.17 dot1x privateclient enable

Command	[no] dot1x privateclient enable
Parameter	none                      none
Default	Private 802.1x authentication packet format is disabled by default.
Mode	Global Mode
Usage Guide	<p>To configure the switch to force the authentication client to use private 802.1x authentication protocol.</p> <p>To implement integrated solution, the switch must be enabled to use private 802.1x protocol, or many applications will not be able to function. For detailed information, please refer to DCBI integrated solution. If the switch forces the authentication client to use private 802.1x protocol, the standard client will not be able to work.</p> <p>The no prefix will disable the command and allow the authentication client to use the standard 802.1x authentication protocol.</p>
Example	<p>To force the authentication client to use private 802.1x authentication protocol.</p> <p>Switch(config)#dot1x privateclient enable</p>

### 13.3.18 dot1x privateclient protect enable

Command	[no] dot1x privateclient protect enable
Parameter	none                      none
Default	Disable the privateclient protect function by default.
Mode	Global Mode
Usage Guide	<p>Enable the privateclient protect function of the switch.</p> <p>Support the partial encryption of the privateclient protocol to advance the security of the privateclient.</p> <p>The no command disables the protect function.</p>
Example	<p>Enable the privateclient protect function of the switch.</p> <pre>Switch(config)#dot1x privateclient protect enable</pre>

### 13.3.19 dot1x re-authenticate

Command	dot1x re-authenticate [interface <interface-name>]
Parameter	interface-name stands for port number, omitting the parameter for all ports
Default	None
Mode	Global Mode
Usage Guide	<p>Enables real-time 802.1x re-authentication (no wait timeout requires) for all ports or a specified port.</p> <p>It makes the switch to re-authenticate the client at once without waiting for re-authentication timer timeout. This command is no longer valid after authentication.</p>
Example	<p>Enabling real-time re-authentication on port1/0/8.</p> <pre>Switch(config)#dot1x re-authenticate interface ethernet 1/0/8</pre>



### 13.3.20 dot1x re-authentication

Command	[no] dot1x re-authentication
Parameter	none                      none
Default	Periodical re-authentication is disabled by default.
Mode	Global Mode
Usage Guide	<p>Enables periodical supplicant authentication.</p> <p>When periodical re-authentication for supplicant is enabled, the switch will re-authenticate the supplicant at regular interval. This function is not recommended for common use.</p> <p>The no command disables this function.</p>
Example	<p>Enabling the periodical re-authentication for authenticated users.</p> <p>Switch(config)#dot1x re-authentication</p>

### 13.3.21 dot1x timeout quiet-period

Command	<code>dot1x timeout quiet-period &lt;seconds&gt;</code> <code>no dot1x timeout quiet-period</code>
Parameter	<code>seconds</code> the silent time for the port in seconds, the valid range is 1 to 65535
Default	The default value is 10 seconds.
Mode	Global Mode
Usage Guide	Sets time to keep silent on supplicant authentication failure. Default value is recommended.  The no command restores the default value.
Example	Setting the silent time to 120 seconds.  <code>Switch(config)#dot1x timeout quiet-period 120</code>

### 13.3.22 dot1x timeout re-authperiod

Command	dot1x timeout re-authperiod <seconds> no dot1x timeout re-authperiod
Parameter	seconds                      the interval for re-authentication, in seconds, the valid range is 1 to 65535
Default	The default value is 3600 seconds.
Mode	Global Mode
Usage Guide	<p>Sets the supplicant re-authentication interval.</p> <p>dot1x re-authentication must be enabled first before supplicant re-authentication interval can be modified. If authentication is not enabled for the switch, the supplicant re-authentication interval set will not take effect.</p> <p>The no command restores the default setting.</p>
Example	<p>Setting the re-authentication time to 1200 seconds.</p> <pre>Switch(config)#dot1x timeout re-authperiod 1200</pre>

### 13.3.23 dot1x timeout tx-period

Command	<code>dot1x timeout tx-period &lt;seconds&gt;</code> <code>no dot1x timeout tx-period</code>
Parameter	<code>seconds</code> the interval for re-transmission of EAP request frames, in seconds; the valid range is 1 to 65535
Default	The default value is 30 seconds.
Mode	Global Mode
Usage Guide	Sets the interval for the supplicant to re-transmit EAP request/identity frame. Default value is recommended.  The no command restores the default setting.
Example	Setting the EAP request frame re-transmission interval to 1200 seconds.  <code>Switch(config)#dot1x timeout tx-period 1200</code>

### 13.3.24 dot1x unicast enable

Command	[no] dot1x unicast enable
Parameter	none                      none
Default	The 802.1x unicast passthrough function is not enabled in global mode.
Mode	Global Mode
Usage Guide	<p>Enable the 802.1x unicast passthrough function of switch.</p> <p>The 802.1x unicast passthrough authentication for the switch must be enabled first to enable the 802.1x unicast passthrough function, then the 802.1x function is configured.</p> <p>The no operation of this command will disable this function.</p>
Example	<p>Enabling the 802.1x unicast passthrough function of the switch and enable the 802.1x for port 1/0/1.</p> <pre>Switch(config)#dot1x enable Switch(config)# dot1x unicast enable Switch(config)#interface ethernet1/0/1 Switch(Config-If-Ethernet1/0/1)#dot1x enable</pre>

### 13.3.25 show dot1x

Command	show dot1x [interface <interface-list>]	
Parameter	interface-list	the port list, If no parameter is specified, information for all ports is displayed.
Default	None.	
Mode	Admin/Global Mode	
Usage Guide	Displays dot1x parameter related information, if parameter information is added, corresponding dot1x status for corresponding port is displayed.	
Example	<p>Display information about dot1x global parameter for the switch.</p> <pre> Switch#show dot1x Global 802.1x Parameters reauth-enabled      no reauth-period       3600 quiet-period        10 tx-period           30 max-req             2 authenticator mode  passive  Mac Filter Disable MacAccessList : dot1x-EAPoR Enable dot1x-privateclient Disable dot1x-unicast Disable  802.1x is enabled on ethernet Ethernet1/0/1 Authentication Method:Port based Max User Number:1 Status              Authorized Port-control        Auto Supplicant           00-03-0F-FE-2E-D3  Authenticator State Machine </pre>	

---

State	Authenticated
Backend State Machine	
State	Idle
Reauthentication State Machine	
State	Stop

---

## 13.4 The Number Limitation Function of MAC and IP in Port, VLAN

### 13.4.1 ip arp dynamic maximum

Command	ip arp dynamic maximum <value> no ip arp dynamic maximum
Parameter	value                      upper limit of the number of dynamic ARP in the VLAN, ranging from 1 to 4096
Default	The number limitation function of dynamic ARP in the VLAN is disabled.
Mode	VLAN Configuration Mode
Usage Guide	<p>Set the max number of dynamic ARP allowed in the VLAN, and, at the same time, enable the number limitation function of dynamic ARP in the VLAN.</p> <p>When configuring the max number of dynamic ARP allowed in the VLAN, if the number of dynamically learnt ARP in the VLAN is already larger than the max number to be set, the extra dynamic ARP will be deleted.</p> <p>The no command is used to disable the number limitation function of dynamic ARP in the VLAN.</p>
Example	<p>Enable the number limitation function of dynamic ARP in VLAN 1, the max number to be set is 50.</p> <pre>Switch(config)#interface vlan1 Switch(config-if-vlan1)# ip arp dynamic maximum 50</pre>



## 13.4.2 ipv6 nd dynamic maximum

Command	<pre>ipv6 nd dynamic maximum &lt;value&gt; no ipv6 nd dynamic maximum</pre>		
Parameter	<table border="1"> <tr> <td>value</td> <td>upper limit of the number of dynamic NEIGHBOR in the VLAN, ranging from 1 to 4096</td> </tr> </table>	value	upper limit of the number of dynamic NEIGHBOR in the VLAN, ranging from 1 to 4096
value	upper limit of the number of dynamic NEIGHBOR in the VLAN, ranging from 1 to 4096		
Default	The number limitation function of dynamic NEIGHBOR in the VLAN is disabled.		
Mode	VLAN Configuration Mode		
Usage Guide	<p>Set the max number of dynamic NEIGHBOR allowed in the VLAN, and, at the same time, enable the number limitation function of dynamic NEIGHBOR in the VLAN.</p> <p>When configuring the max number of dynamic NEIGHBOR allowed in the VLAN, if the number of dynamically learnt NEIGHBOR in the VLAN is already larger than the max number to be set, the extra dynamic NEIGHBOR will be deleted.</p> <p>The no command is used to disable the number limitation function of dynamic NEIGHBOR in the VLAN.</p>		
Example	<p>Enable the number limitation function of dynamic NEIGHBOR in VLAN 1, the max number to be set is 50.</p> <pre>Switch(config)#interface vlan1 Switch(config-if-vlan1)# ipv6 nd dynamic maximum 50</pre>		

### 13.4.3 show arp-dynamic count

Command	show arp-dynamic count {vlan   interface ethernet <portName>}												
Parameter	<table border="1"> <tr> <td>vlan</td> <td>the specified vlan ID</td> </tr> <tr> <td>portName</td> <td>the name of layer-2 port</td> </tr> </table>	vlan	the specified vlan ID	portName	the name of layer-2 port								
vlan	the specified vlan ID												
portName	the name of layer-2 port												
Default	None.												
Mode	Admin/Global Mode												
Usage Guide	Display the number of dynamic ARP of corresponding port and VLAN.												
Example	<p>Display the number of dynamic ARP of the port and VLAN which are configured with number limitation function of ARP.</p> <pre>Switch(config)# show arp-dynamic count interface ethernet 1/0/3</pre> <table border="1"> <thead> <tr> <th>Port</th> <th>MaxCount</th> <th>CurrentCount</th> </tr> </thead> <tbody> <tr> <td>Ethernet1/0/3</td> <td>5</td> <td>1</td> </tr> </tbody> </table> <pre>Switch(config)# show arp-dynamic count vlan 1</pre> <table border="1"> <thead> <tr> <th>Vlan</th> <th>MaxCount</th> <th>CurrentCount</th> </tr> </thead> <tbody> <tr> <td>1</td> <td>55</td> <td>15</td> </tr> </tbody> </table>	Port	MaxCount	CurrentCount	Ethernet1/0/3	5	1	Vlan	MaxCount	CurrentCount	1	55	15
Port	MaxCount	CurrentCount											
Ethernet1/0/3	5	1											
Vlan	MaxCount	CurrentCount											
1	55	15											

### 13.4.4 show mac-address dynamic count

Command	show mac-address dynamic count { vlan   interface ethernet <portName>}											
Parameter	vlan                                    display the specified VLAN ID											
	portName                                the name of layer-2 port											
Default	None.											
Mode	Admin/Global Mode											
Usage Guide	Display the number of dynamic MAC of corresponding port and VLAN.											
Example	Display the number of dynamic MAC of the port and VLAN which are configured with number limitation function of MAC.											
	<pre>Switch(config)# show mac-address dynamic count interface ethernet 1/0/3</pre> <table border="1"> <thead> <tr> <th>Port</th> <th>MaxCount</th> <th>CurrentCount</th> </tr> </thead> <tbody> <tr> <td>Ethernet1/0/3</td> <td>5</td> <td>1</td> </tr> </tbody> </table> <pre>Switch(config)# show mac-address dynamic count vlan 1</pre> <table border="1"> <thead> <tr> <th>Vlan</th> <th>MaxCount</th> <th>CurrentCount</th> </tr> </thead> <tbody> <tr> <td>1</td> <td>55</td> <td>15</td> </tr> </tbody> </table>	Port	MaxCount	CurrentCount	Ethernet1/0/3	5	1	Vlan	MaxCount	CurrentCount	1	55
Port	MaxCount	CurrentCount										
Ethernet1/0/3	5	1										
Vlan	MaxCount	CurrentCount										
1	55	15										

### 13.4.5 show nd-dynamic count

Command	show nd-dynamic count { vlan   interface ethernet <portName>}											
Parameter	vlan                                    display the specified VLAN ID											
	portName                                the name of layer-2 port											
Default	None.											
Mode	Admin/Global Mode											
Usage Guide	Display the number of dynamic ND of corresponding port and VLAN.											
Example	Display the number of dynamic ND of the port and VLAN which are configured with number limitation function of ND.											
	<pre>Switch(config)# show nd-dynamic dynamic count interface ethernet 1/0/3</pre> <table border="1"> <thead> <tr> <th>Port</th> <th>MaxCount</th> <th>CurrentCount</th> </tr> </thead> <tbody> <tr> <td>Ethernet1/0/3</td> <td>5</td> <td>1</td> </tr> </tbody> </table> <pre>Switch(config)# show nd-dynamic dynamic count vlan 1</pre> <table border="1"> <thead> <tr> <th>Vlan</th> <th>MaxCount</th> <th>CurrentCount</th> </tr> </thead> <tbody> <tr> <td>1</td> <td>55</td> <td>15</td> </tr> </tbody> </table>	Port	MaxCount	CurrentCount	Ethernet1/0/3	5	1	Vlan	MaxCount	CurrentCount	1	55
Port	MaxCount	CurrentCount										
Ethernet1/0/3	5	1										
Vlan	MaxCount	CurrentCount										
1	55	15										

## 13.4.6 switchport arp dynamic maximum

Command	switchport arp dynamic maximum <value> no switchport arp dynamic maximum
Parameter	value                      upper limit of the number of dynamic ARP of the port, ranging from 1 to 4096
Default	The number limitation function of dynamic ARP on the port is disabled.
Mode	Port Mode
Usage Guide	<p>Set the max number of dynamic ARP allowed by the port, and, at the same time, enable the number limitation function of dynamic ARP on the port.</p> <p>When configuring the max number of dynamic ARP allowed by the port, if the number of dynamically learnt ARP on the port is already larger than the max number to be set, the extra dynamic ARP will be deleted. TRUNK ports do not supports this function.</p> <p>The no command is used to disable the number limitation function of dynamic ARP on the port.</p>
Example	<p>Enable the number limitation function of dynamic ARP in port 1/0/2 mode, the max number to be set is 20.</p> <pre>Switch(config)#interface ethernet 1/0/2 Switch(config-if-ethernet1/0/2)# switchport arp dynamic maximum 20</pre>

### 13.4.7 switchport mac-address dynamic maximum

Command	<p>switchport mac-address dynamic maximum &lt;value&gt;</p> <p>no switchport mac-address dynamic maximum</p>
Parameter	<p>value                                    upper limit of the number of dynamic MAC address of the port, ranging from 1 to 4096</p>
Default	The number limitation function of dynamic MAC address on the port is disabled.
Mode	Port Mode
Usage Guide	<p>Set the max number of dynamic MAC address allowed by the port, and at the same time, enable the number limitation function of dynamic MAC address on the port.</p> <p>When configuring the max number of dynamic MAC address allowed by the port, if the number of dynamically learnt MAC address on the port is already larger than the max number of dynamic MAC address to be set, the extra dynamic MAC addresses will be deleted. This function is mutually exclusive to functions such as dot1x, MAC binding, if the functions of dot1x, MAC binding or TRUNK are enabled on the port, this function will not be allowed.</p> <p>The no command is used to disable the number limitation function of dynamic MAC address on the port.</p>
Example	<p>Enable the number limitation function of dynamic MAC address in port 1/0/2 mode, the max number to be set is 20.</p> <pre>Switch(config)#interface ethernet 1/0/2 Switch(config-if-ethernet1/0/2)# switchport mac-address dynamic maximum 20</pre>

### 13.4.8 switchport mac-address violation

Command	switchport mac-address violation {protect   shutdown} [recovery <5-3600>] no switchport mac-address violation								
Parameter	<table border="1"> <tr> <td>protect</td> <td>protect mode</td> </tr> <tr> <td>shutdown</td> <td>shutdown mode</td> </tr> <tr> <td>recovery</td> <td>Configure the border port to automatically restore after execute shutdown violation mode</td> </tr> <tr> <td>&lt;5-3600&gt;</td> <td>Recovery time, do not restore by default</td> </tr> </table>	protect	protect mode	shutdown	shutdown mode	recovery	Configure the border port to automatically restore after execute shutdown violation mode	<5-3600>	Recovery time, do not restore by default
protect	protect mode								
shutdown	shutdown mode								
recovery	Configure the border port to automatically restore after execute shutdown violation mode								
<5-3600>	Recovery time, do not restore by default								
Default	By default, the port is protected mode.								
Mode	Port Mode								
Usage Guide	<p>Set the violation mode of the port.</p> <p>The port sets the violation mode after enable the number limit function of MAC only. If the violation mode is protect, the port only disable the dynamic MAC address learning function when the MAC address number of the port exceeds the upper limit of secure MAC. If the violation mode is shutdown, the port will be disabled when the MAC address number exceeds the upper limit of secure MAC, and the user can enable the port by configuring no shutdown command manually or the automatic recovery timeout.</p> <p>The no command restores the violation mode to protect.</p>								
Example	<p>Set the violation mode as shutdown, the recovery time as 60s for port1.</p> <pre>Switch(config)#interface ethernet 1/0/1 Switch(config-if-ethernet1/0/1)# switchport mac-address violation shutdown recovery 60</pre>								

### 13.4.9 switchport nd dynamic maximum

Command	<p>switchport nd dynamic maximum &lt;value&gt;</p> <p>no switchport nd dynamic maximum</p>
Parameter	<p>value                            upper limit of the number of dynamic NEIGHBOR of the port, ranging from 1 to 4096</p>
Default	The number limitation function of dynamic ARP on the port is disabled.
Mode	Port Mode
Usage Guide	<p>Set the max number of dynamic NEIGHBOR allowed by the port, and, at the same time, enable the number limitation function of dynamic NEIGHBOR on the port.</p> <p>When configuring the max number of dynamic NEIGHBOR allowed by the port, if the number of dynamically learnt NEIGHBOR on the port is already larger than the max number to be set, the extra dynamic NEIGHBOR will be deleted. TRUNK ports do not supports this function.</p> <p>The no command is used to disable the number limitation function of dynamic NEIGHBOR on the port.</p>
Example	<p>Enable the number limitation function of dynamic NEIGHBOR in port 1/0/2 mode, the max number to be 20.</p> <pre>Switch(config)#interface ethernet 1/0/2 Switch(config-if-ethernet1/0/2)# switchport nd dynamic maximum 20</pre>



### 13.4.10 vlan mac-address dynamic maximum

Command	<p>vlan mac-address dynamic maximum &lt;value&gt;</p> <p>no vlan mac-address dynamic maximum</p>
Parameter	<p>value                                    upper limit of the number of MAC address in the VLAN, ranging from 1 to 4096</p>
Default	The number limitation function of dynamic MAC address in the VLAN is disabled.
Mode	VLAN Configuration Mode
Usage Guide	<p>Set the max number of dynamic MAC address allowed in the VLAN, and, at the same time, enable the number limitation function of dynamic MAC address in the VLAN.</p> <p>When configuring the max number of dynamic MAC allowed in the VLAN, if the number of dynamically learnt MAC address in the VLAN is already larger than the max number to be set, the extra dynamic MAC addresses will be deleted. After enabling number limitation function of dynamic MAC in the VLAN, the number limitation of MAC is only applied to general access port, the number of MAC on TURNK ports and special ports which has enabled dot1x, MAC binding function will not be limited or counted.</p> <p>The no command is used to disable the number limitation function of dynamic MAC address in the VLAN.</p>
Example	<p>Enable the number limitation function of dynamic MAC address in VLAN 1, the max number to be set is 50.</p> <pre>Switch(config)#vlan1 Switch(config-if-vlan1)#vlan mac-address dynamic maximum 50</pre>

## 13.5 AM Configuration

### 13.5.1 am enable

Command	[no] am enable
Parameter	none                      none
Default	AM function is disabled by default.
Mode	Global Mode
Usage Guide	Globally enable/disable AM function.  The no command disables AM function.
Example	Enable AM function on the switch.  Switch(config)#am enable

## 13.5.2 am port

Command	[no] am port
Parameter	none                      none
Default	AM function is disabled on all port.
Mode	Port Mode
Usage Guide	Enable/disable AM function on port.  The no command disables AM function on the port.
Example	Enable AM function on interface 1/0/3 of the switch.  Switch(config-if-ethernet 1/0/3)#am port

### 13.5.3 am ip-pool

Command	[no] am ip-pool <ip-address> <num>
Parameter	ip-address                      the starting address of an address segment in the IP address pool
	num                                the number of consecutive addresses following ip-address, less than or equal with 32
Default	By default · IP address pool is empty.
Mode	Port Mode
Usage Guide	Set the AM IP segment of the interface, allow/deny the IP messages or APRmessages from a source IP within that segment to be forwarded via the interface.  The no command delete configuration.
Example	Configure that interface 1/0/3 of the switch will forward data packets from an IP address which is one of 10 consecutive IP addresses starting from 10.10.10.1.  Switch(config-if-ethernet 1/0/3)#am ip-pool 10.10.10.1 10

## 13.5.4 am mac-ip-pool

Command	[no] am mac-ip-pool <mac-address> <ip-address>
Parameter	mac-address                      the source MAC address
	ip-address                        the source IP address of the packets, which is a 32 bit binary number represented in four decimal numbers
Default	By default · MAC-IP address pool is empty.
Mode	Port Mode
Usage Guide	Set the AM MAC-IP address of the interface, allow/deny the IP messages or APR messages from a source IP within that segment to be forwarded via the interface.  The no command delete configuration.
Example	Configure that the interface 1/0/3 of the switch will allow data packets with a source MAC address of 11-22-22-11-11-11 and a source IP address of 10.10.10.1 to be forwarded.  Switch(config-if-ethernet 1/0/3)#am mac-ip-pool 11-22-22-11-11-11 10.10.10.1

### 13.5.5 no am all

Command	no am all [ip-pool   mac-ip-pool]
Parameter	ip-pool                      the IP address pool
	mac-ip-pool                the MAC-IP address pool
Default	By default · both address pools are empty at the beginning.
Mode	Global Mode
Usage Guide	Delete MAC-IP address pool or IP address pool or both pools configured by all users.
Example	Delete all configured IP address pools.
	Switch(config)#no am all ip-pool

### 13.5.6 show am

Command	show am [interface <interface-name>]
Parameter	interface-name            the name of the interface of which the configuration information will be displayed
Default	None.
Mode	Admin/Global Mode
Usage Guide	Display the configured AM entries. No parameter means to display the AM configuration information of all interfaces.
Example	Display all configured AM entries.  Switch#show am interface ethernet 1/0/5 AM is enabled Interface Etherne1/0/5 am interface am ip-pool 50.10.10.1 30 am mac-ip-pool 00-02-04-06-08-09 20.10.10.5 am ip-pool 50.20.10.1 20

## 13.6 Security Feature

### 13.6.1 dosattack-check srcip-equal-dstip enable

Command	[no] dosattack-check srcip-equal-dstip enable
Parameter	none                      none
Default	Disable the function by which the switch checks if the source IP address is equal to the destination IP address.
Mode	Global Mode
Usage Guide	<p>Enable the function by which the switch checks if the source IP address is equal to the destination IP address.</p> <p>By enabling this function, data packet whose source IP address is equal to its destination address will be dropped.</p> <p>The "no" form of this command disables this function.</p>
Example	<p>Drop the data packet whose source IP address is equal to its destination address.</p> <pre>Switch(config)# dosattack-check srcip-equal-dstip enable</pre>



## 13.6.2 dosattack-check tcp-flags enable

Command	[no] dosattack-check srcip-equal-dstip enable
Parameter	none                      none
Default	This function disable on the switch by default.
Mode	Global Mode
Usage Guide	<p>Enable the function by which the switch will check the unauthorized TCP label function.</p> <p>With this function enabled, the switch will be able to drop follow four data packets containing unauthorized TCP label: SYN=1 while source port is smaller than 1024;TCP label positions are all 0 while its serial No. =0;FIN=1,URG=1,PSH=1 and the TCP serial No.=0;SYN=1 and FIN=1. This function can be used associating the "dosattack-check ipv4-first-fragment enable" command.</p> <p>The "no" form of this command will disable this function.</p>
Example	<p>Drop one or more types of above four packet types.</p> <p>Switch(config)# dosattack-check tcp-flags enable</p>

### 13.6.3 dosattack-check srcport-equal-dstport enable

Command	[no] dosattack-check srcport-equal-dstport enable
Parameter	none                      none
Default	Disable the function by which the switch will check if the source port is equal to the destination port.
Mode	Global Mode
Usage Guide	<p>Enable the function by which the switch will check if the source port is equal to the destination port.</p> <p>With this function enabled, the switch will be able to drop TCP and UDP data packet whose destination port is equal to the source port. This function can be used associating the “dosattack-check ipv4-first-fragment enable” function so to block the IPv4 fragment TCP and UDP data packet whose destination port is equal to the source port.</p> <p>The no command disables this function.</p>
Example	<p>Drop the non-fragment TCP and UDP data packet whose destination port is equal to the source port.</p> <pre>Switch(config)#dosattack-check srcport-equal-dstport enable</pre>

### 13.6.4 dosattack-check icmp-attacking enable

Command	[no] dosattack-check icmp-attacking enable
Parameter	none                      none
Default	By default · disable the ICMP fragment attack checking function on the switch.
Mode	Global Mode
Usage Guide	<p>Enable the ICMP fragment attack checking function on the switch.</p> <p>With this function enabled the switch will be protected from the ICMP fragment attacks, dropping the fragment ICMPv4/v6 data packets whose net length is smaller than the specified value.</p> <p>The “no” form of this command disables this function.</p>
Example	<p>Enable the ICMP fragment attack checking function.</p> <p>Switch(config)#dosattack-check icmp-attacking enable</p>

### 13.6.5 dosattack-check icmpV4-size

Command	dosattack-check icmpV4-size <64-1023>
Parameter	<64-1023> the max net length of the ICMPv4 data packet permitted by the switch
Default	The value is 0x200 by default.
Mode	Global Mode
Usage Guide	Configure the max net length of the ICMPv4 data packet permitted by the switch. To use this function you have to enable "dosattack-check icmp-attacking enable" first.
Example	Set the max net length of the ICMPv4 data packet permitted by the switch to 100.  Switch(config)#dosattack-check icmp-attacking enable Switch(config)#dosattack-check icmpV4-size 100

## 13.7 ACACS+

### 13.7.1 tacacs-server authentication host

Command	<p>tacacs-server authentication host &lt;ip-address&gt; [port &lt;port-number&gt;][timeout &lt;seconds&gt;] [key {0   7} &lt;string&gt;] [primary]</p> <p>no tacacs-server authentication host &lt;ip-address&gt;</p>	
Parameter	ip-address	the IP address of the server
	port-number	the listening port number of the server, the valid range is 0~65535, amongst 0 indicates it will not be an authentication server
	seconds	the value of TACACS+ authentication timeout timer, shown in seconds and the valid range is 1~60
	string	the key string, If key option is set as 0, the key is not encrypted and its range should not exceed 64 characters, if key option is set as 7, the key is encrypted and its range should not exceed 64 characters
	primary	indicates it's a primary server
Default	No TACACS+ authentication configured on the system by default.	
Mode	Global Mode	
Usage Guide	<p>This command is for specifying the IP address, port number, timeout timer value and the key string of the TACACS+ server used on authenticating with the switch.</p> <p>The parameter port is for define an authentication port number which must be in accordance with the authentication port number of specified TACACS+ server which is 49 by default. The parameters key and timeout is used to configure the self-key and self-timeout, if the switch is not configure the timeout&lt;seconds&gt; and key&lt;string&gt;, it will use the global value and key by command tacacs-server timeout&lt;seconds&gt; and tacacs-server key &lt;string&gt;. This command can configure several TACACS+ servers communicate with the switch. The configuration sequence will be used as authentication server sequence. And in case primary is configured on one TACACS+ server, the server will be the primary server.</p> <p>The no form of this command deletes TACACS+ authentication server.</p>	
Example	<p>Configure the TACACS+ authentication server address to 192.168.1.2, and use the global configured key.</p> <pre>Switch(config)#tacacs-server authentication host 192.168.1.2</pre>	

## 13.7.2 tacacs-server key

Command	<p>tacacs-server key {0   7} &lt;string&gt;</p> <p>no tacacs-server key</p>
Parameter	<p>string                      the key string of the TACACS+ server. If key option is set as 0, the key is not encrypted and its range should not exceed 64 characters, if key option is set as 7, the key is encrypted and its range should not exceed 64 characters.</p>
Default	None.
Mode	Global Mode
Usage Guide	<p>Configure the key of TACACS+ authentication server.</p> <p>The key is used on encrypted packet communication between the switch and the TACACS+ server. The configured key must be in accordance with the one on the TACACS+ server or else no correct TACACS+ authentication will be performed. It is recommended to configure the authentication server key to ensure the data security.</p> <p>The no command deletes the TACACS+ server key.</p>
Example	<p>Configure test as the TACACS+ server authentication key.</p> <p>Switch(config)#tacacs-server key 0 test</p>

### 13.7.3 tacacs-server nas-ipv4

Command	<pre>tacacs-server nas-ipv4 &lt;ip-address&gt; no tacacs-server nas-ipv4</pre>
Parameter	<pre>ip-address</pre> the source IP address of TACACS+ packet, in dotted decimal notation, it must be a valid unicast IP address
Default	By default · no specific source IP address for TACACS+ packet is configured, the IP address of the interface from which the TACACS+ packets are sent is used as source IP address of TACACS+ packet.
Mode	Global Mode
Usage Guide	<p>Configure the source IP address of TACACS+ packet sent by the switch.</p> <p>The source IP address must belongs to one of the IP interface of the switch, otherwise an failure message of binding IP address will be returned when the switch send TACACS+ packet. We suggest using the IP address of loopback interface as source IP address, it avoids that the packets from TACACS+ server are dropped when the interface link-down.</p> <p>The no command deletes the configuration.</p>
Example	<p>Configure the source ip address of TACACS+ packet as 192.168.2.254.</p> <pre>Switch(config)#tacacs-server nas-ipv4 192.168.2.254</pre>

## 13.7.4 tacacs-server timeout

Command	<p>tacacs-server timeout &lt;seconds&gt;</p> <p>no tacacs-server timeout</p>
Parameter	<p>seconds                      the value of TACACS+ authentication timeout timer, shown in seconds and the valid range is 1~60</p>
Default	<p>3 seconds by default.</p>
Mode	<p>Global Mode</p>
Usage Guide	<p>Configure a TACACS+ server authentication timeout timer.</p> <p>The command specifies the period the switch wait for the authentication through TACACS+ server. When connected to the TACACS+, and after sent the authentication query data packet to the TACACS+ server, the switch waits for the response. If no replay is received during specified period, the authentication is considered failed.</p> <p>The no command restores the default configuration.</p>
Example	<p>Configure the timeout timer of the tacacs+ server to 30 seconds.</p> <p>Switch(config)#tacacs-server timeout 30</p>



## 13.8 RADIUS

### 13.8.1 aaa enable

Command	[no] aaa enable
Parameter	none                      none
Default	AAA authentication is not enabled by default.
Mode	Global Mode
Usage Guide	<p>Enables the AAA authentication function in the switch.</p> <p>The AAA authentication for the switch must be enabled first to enable IEEE 802.1x authentication for the switch.</p> <p>The no command disables the AAA authentication function.</p>
Example	<p>Enabling AAA function for the switch.</p> <p>Switch(config)#aaa enable</p>

## 13.8.2 aaa-accounting enable

Command	[no] aaa-accounting enable
Parameter	none                      none
Default	AAA accounting is not enabled by default.
Mode	Global Mode
Usage Guide	<p>Enables the AAA accounting function in the switch.</p> <p>When accounting is enabled in the switch, accounting will be performed according to the traffic or online time for port the authenticated user is using. The switch will send an "accounting started" message to the RADIUS accounting server on starting the accounting, and an accounting packet for the online user to the RADIUS accounting server every five seconds, and an "accounting stopped" message is sent to the RADIUS accounting server on accounting end.</p> <p>Note: The switch send the "user offline" message to the RADIUS accounting server only when accounting is enabled, the "user offline" message will not be sent to the RADIUS authentication server.</p> <p>The no command disables the AAA accounting function.</p>
Example	<p>Enabling AAA accounting for the switch.</p> <p>Switch(config)#aaa-accounting enable</p>

### 13.8.3 aaa-accounting update

Command	aaa-accounting update {enable   disable}
Parameter	none                      none
Default	By default · Enable the AAA update accounting function.
Mode	Global Mode
Usage Guide	Enable or disable the AAA update accounting function. After the update accounting function is enabled, the switch will sending accounting message to each online user on time.
Example	Disable the AAA update accounting function for switch.  Switch(config)#aaa-accounting update disable

### 13.8.4 radius nas-ipv4

Command	radius nas-ipv4 <ip-address> no radius nas-ipv4
Parameter	ip-address                      the source IP address of the RADIUS packet, in dotted decimal notation, it must be a valid unicast IP address
Default	By default · No specific source IP address for RADIUS packet is configured, the IP address of the interface from which the RADIUS packets are sent is used as source IP address of RADIUS packet.
Mode	Global Mode
Usage Guide	Configure the source IP address for RADIUS packet sent by the switch. The source IP address must belongs to one of the IP interface of the switch, otherwise an failure message of binding IP address will be returned when the switch send RADIUS packet. We suggest using the IP address of loopback interface as source IP address, it avoids that the packets from RADIUS server are dropped when the interface link-down.  The no command deletes the configuration.
Example	Configure the source ip address of RADIUS packet as 192.168.2.254.  Switch(config)#radius nas-ipv4 192.168.2.254

## 13.8.5 radius nas-ipv6

Command	radius nas-ipv6 <ipv6-address> no radius nas-ipv6
Parameter	ipv6-address            the source IPv6 address of the RADIUS packet, it must be a valid unicast IPv6 address
Default	By default, No specific source IPv6 address for RADIUS packet is configured, the IPv6 address of the interface from which the RADIUS packets are sent is used as source IPv6 address of RADIUS packet.
Mode	Global Mode
Usage Guide	<p>Configure the source IPv6 address for RADIUS packet sent by the switch.</p> <p>The source IPv6 address must belongs to one of the IPv6 interface of the switch, otherwise a failure message of binding IPv6 address will be returned when the switch send RADIUS packet.</p> <p>We suggest using the IPv6 address of loopback interface as source IPv6 address, it avoids that the packets from RADIUS server are dropped when the interface link-down.</p> <p>The no command deletes the configuration.</p>
Example	<p>Configure the source ipv6 address of RADIUS packet as 2001:da8:456::1.</p> <p>Switch(config)#radius nas-ipv6 2001:da8:456::1</p>

### 13.8.6 radius-server accounting host

Command	radius-server accounting host {<ipv4-address>   <ipv6-address>} [port <port-number>] [key {0   7} <string>] [primary] no radius-server accounting host {<ipv4-address>   <ipv6-address>}										
Parameter	<table border="1"> <tr> <td>ipv4-address</td> <td>stands for the server IPv4 address</td> </tr> <tr> <td>ipv6-address</td> <td>stands for the server IPv6 address</td> </tr> <tr> <td>port-number</td> <td>server listening port number from 0 to 65535</td> </tr> <tr> <td>string</td> <td>the key string. If key option is set as 0, the key is not encrypted and its range should not exceed 64 characters, if key option is set as 7, the key is encrypted and its range should not exceed 64 characters</td> </tr> <tr> <td>primary</td> <td>for primary server. Multiple RADIUS sever can be configured and would be available. RADIUS server will be searched by the configured order if primary is not configured, otherwise, the specified RADIUS server will be used first</td> </tr> </table>	ipv4-address	stands for the server IPv4 address	ipv6-address	stands for the server IPv6 address	port-number	server listening port number from 0 to 65535	string	the key string. If key option is set as 0, the key is not encrypted and its range should not exceed 64 characters, if key option is set as 7, the key is encrypted and its range should not exceed 64 characters	primary	for primary server. Multiple RADIUS sever can be configured and would be available. RADIUS server will be searched by the configured order if primary is not configured, otherwise, the specified RADIUS server will be used first
ipv4-address	stands for the server IPv4 address										
ipv6-address	stands for the server IPv6 address										
port-number	server listening port number from 0 to 65535										
string	the key string. If key option is set as 0, the key is not encrypted and its range should not exceed 64 characters, if key option is set as 7, the key is encrypted and its range should not exceed 64 characters										
primary	for primary server. Multiple RADIUS sever can be configured and would be available. RADIUS server will be searched by the configured order if primary is not configured, otherwise, the specified RADIUS server will be used first										
Default	No RADIUS accounting server is configured by default.										
Mode	Global Mode										
Usage Guide	<p>Specifies the IPv4/IPv6 address and the port number, whether be primary server for RADIUS accounting server.</p> <p>This command is used to specify the IPv4/IPv6 address and port number of the specified RADIUS server for switch accounting, multiple command instances can be configured. The &lt;port-number&gt; parameter is used to specify accounting port number, which must be the same as the specified accounting port in the RADIUS server; the default port number is 1813. If this port number is set to 0, accounting port number will be generated at random and can result in invalid configuration. This command can be used repeatedly to configure multiple RADIUS servers communicating with the switch, the switch will send accounting packets to all the configured accounting servers, and all the accounting servers can be backup servers for each other. If primary is specified, then the specified RADIUS server will be the primary server. It only configures a RADIUS primary server whether the server use IPv4 address or IPv6 address.</p> <p>The no command deletes the RADIUS accounting server.</p>										
Example	<p>Sets the RADIUS accounting server of IPv6 address to 2004:1:2:3::2, as the primary server, with the accounting port number as 3000.</p> <pre>Switch(config)#radius-server accounting host 2004:1:2:3::2 port 3000 primary</pre>										

## 13.8.7 radius-server authentication host

Command	radius-server authentication host {<ipv4-address>   <ipv6-address>}[port <port-number>] [key {0   7} <string>] [primary] [access-mode {dot1x   telnet}] no radius-server authentication host {<ipv4-address>   <ipv6-address>}												
Parameter	<table border="1"> <tr> <td>ipv4-address</td> <td>stands for the server IPv4 address</td> </tr> <tr> <td>ipv6-address</td> <td>stands for the server IPv6 address</td> </tr> <tr> <td>port-number</td> <td>server listening port number from 0 to 65535</td> </tr> <tr> <td>string</td> <td>the key string. If key option is set as 0, the key is not encrypted and its range should not exceed 64 characters, if key option is set as 7, the key is encrypted and its range should not exceed 64 characters</td> </tr> <tr> <td>primary</td> <td>for primary server. Multiple RADIUS sever can be configured and would be available. RADIUS server will be searched by the configured order if primary is not configured, otherwise, the specified RADIUS server will be used first</td> </tr> <tr> <td>dot1x   telnet</td> <td>designates the current RADIUS server only use 802.1x authentication or telnet authentication, all services can use current RADIUS server by default</td> </tr> </table>	ipv4-address	stands for the server IPv4 address	ipv6-address	stands for the server IPv6 address	port-number	server listening port number from 0 to 65535	string	the key string. If key option is set as 0, the key is not encrypted and its range should not exceed 64 characters, if key option is set as 7, the key is encrypted and its range should not exceed 64 characters	primary	for primary server. Multiple RADIUS sever can be configured and would be available. RADIUS server will be searched by the configured order if primary is not configured, otherwise, the specified RADIUS server will be used first	dot1x   telnet	designates the current RADIUS server only use 802.1x authentication or telnet authentication, all services can use current RADIUS server by default
ipv4-address	stands for the server IPv4 address												
ipv6-address	stands for the server IPv6 address												
port-number	server listening port number from 0 to 65535												
string	the key string. If key option is set as 0, the key is not encrypted and its range should not exceed 64 characters, if key option is set as 7, the key is encrypted and its range should not exceed 64 characters												
primary	for primary server. Multiple RADIUS sever can be configured and would be available. RADIUS server will be searched by the configured order if primary is not configured, otherwise, the specified RADIUS server will be used first												
dot1x   telnet	designates the current RADIUS server only use 802.1x authentication or telnet authentication, all services can use current RADIUS server by default												
Default	No RADIUS authentication server is configured by default.												
Mode	Global Mode												
Usage Guide	<p>Specifies the IPv4 address or IPv6 address and listening port number, cipher key, whether be primary server or not and access mode for the RADIUS server.</p> <p>This command is used to specify the IPv4 address or IPv6 address and port number, cipher key string and access mode of the specified RADIUS server for switch authentication, multiple command instances can be configured. The port parameter is used to specify authentication port number, which must be the same as the specified authentication port in the RADIUS server, the default port number is 1812. If this port number is set to 0, the specified server is regard as non-authenticating. This command can be used repeatedly to configure multiple RADIUS servers communicating with the switch, the configured order is used as the priority for the switch authentication server. When the first server has responded (whether the authentication is succeeded or failed), switch does not send the authentication request to the next. If primary is specified, then the specified RADIUS server will be the primary server. It will use the cipher key which be configured by radius-server key &lt;string&gt; global command if the current RADIUS server not configure key&lt;string&gt;. Besides, it can designate the current RADIUS server only use 802.1x authentication or telnet authentication via access-mode option. It is not configure access-mode</p>												

---

option and all services can use current RADIUS server by default.

The no command deletes the RADIUS authentication server.

---

Example

---

Setting the RADIUS authentication server address as 2004:1:2:3::2.

Switch(config)#radius-server authentication host 2004:1:2:3::2

---



### 13.8.8 radius-server dead-time

Command	radius-server dead-time <minutes> no radius-server dead-time
Parameter	minutes                      the down -restore time for RADIUS server in minutes, the valid range is 1 to 255
Default	The default value is 5 minutes.
Mode	Global Mode
Usage Guide	<p>This command specifies the time to wait for the RADIUS server to recover from inaccessible to accessible. When the switch acknowledges a server to be inaccessible, it marks that server as having invalid status, after the interval specified by this command; the system resets the status for that server to valid.</p> <p>The no command restores the default setting.</p>
Example	<p>Setting the down-restore time for RADIUS server to 3 minutes.</p> <pre>Switch(config)#radius-server dead-time 3</pre>

### 13.8.9 radius-server key

Command	radius-server key {0   7} <string> no radius-server key
Parameter	string a key string for RADIUS server, If key option is set as 0, the key is not encrypted and its range should not exceed 64 characters, if key option is set as 7, the key is encrypted and its range should not exceed 64 characters
Default	None.
Mode	Global Mode
Usage Guide	<p>Specifies the key for the RADIUS server (authentication and accounting).</p> <p>The key is used in the encrypted communication between the switch and the specified RADIUS server. The key set must be the same as the RADIUS server set, otherwise, proper RADIUS authentication and accounting will not perform properly.</p> <p>The no command deletes the key for RADIUS server.</p>
Example	<p>Setting the RADIUS authentication key to be "test".</p> <pre>Switch(config)#radius-server key 0 test</pre>

### 13.8.10 radius-server retransmit

Command	radius-server retransmit <retries> no radius-server retransmit
Parameter	retries a retransmission times for RADIUS server, the valid range is 0 to 100
Default	The default value is 3 times.
Mode	Global Mode
Usage Guide	<p>This command specifies the retransmission time for a packet without a RADIUS server response after the switch sends the packet to the RADIUS server. If authentication information is missing from the authentication server, AAA authentication request will need to be re-transmitted to the authentication server. If AAA request retransmission count reaches the retransmission time threshold without the server responding, the server will be considered to as not work, the switch sets the server as invalid.</p> <p>The no command restores the default setting.</p>
Example	<p>Setting the RADIUS authentication packet retransmission time to five times.</p> <pre>Switch(config)#radius-server retransmit 5</pre>

### 13.8.11 radius-server timeout

Command	radius-server timeout <seconds> no radius-server timeout
Parameter	seconds                      the timer value (second) for RADIUS server timeout, the valid range is 1 to 1000
Default	The default value is 3 seconds.
Mode	Global Mode
Usage Guide	<p>This command specifies the interval for the switch to wait RADIUS server response. The switch waits for corresponding response packets after sending RADIUS Server request packets. If RADIUS server response is not received in the specified waiting time, the switch resends the request packet or sets the server as invalid according to the current conditions.</p> <p>The no command restores the default setting.</p>
Example	<p>Setting the RADIUS authentication timeout timer value to 30 seconds.</p> <pre>Switch(config)#radius-server timeout 30</pre>

### 13.8.12 radius-server accounting-interim-update timeout

Command	radius-server accounting-interim-update timeout <seconds> no radius-server accounting-interim-update timeout												
Parameter	seconds                      the interval of sending fee-counting update messages, in seconds, ranging from 60 to 3600												
Default	The default interval of sending fee-counting update messages is 300 seconds.												
Mode	Global Mode												
Usage Guide	<p>This command set the interval at which NAS sends fee-counting update messages. In order to realize the real time fee-counting of users, from the moment the user becomes online, NAS will send a fee-counting update message of this user to the RADIUS server at the configured interval.</p> <p>The interval of sending fee-counting update messages is relative to the maximum number of users supported by NAS. The smaller the interval, the less the maximum number of the users supported by NAS; the bigger the interval, the more the maximum number of the users supported by NAS. The following is the recommended ratio of interval of sending fee-counting update messages to the maximum number of the users supported by NAS:</p> <table border="1"> <thead> <tr> <th>The maximum number of users</th> <th>The interval of sending fee-counting update messages(in seconds)</th> </tr> </thead> <tbody> <tr> <td>1-299</td> <td>300 ( default )</td> </tr> <tr> <td>300-599</td> <td>600</td> </tr> <tr> <td>600-1199</td> <td>1200</td> </tr> <tr> <td>1200-1799</td> <td>1800</td> </tr> <tr> <td>≥1800</td> <td>3600</td> </tr> </tbody> </table> <p>The no operation of this command will reset to the default configuration.</p>	The maximum number of users	The interval of sending fee-counting update messages(in seconds)	1-299	300 ( default )	300-599	600	600-1199	1200	1200-1799	1800	≥1800	3600
The maximum number of users	The interval of sending fee-counting update messages(in seconds)												
1-299	300 ( default )												
300-599	600												
600-1199	1200												
1200-1799	1800												
≥1800	3600												
Example	<p>The maximum number of users supported by NAS is 700, the interval of sending fee-counting update messages 1200 seconds.</p> <pre>Switch(config)#radius-server accounting-interim-update timeout 1200</pre>												

### 13.8.13 show aaa authenticated-user

Command	show aaa authenticated-user
Parameter	none                      none
Default	None.
Mode	Admin/Global Mode
Usage Guide	<p>Displays the authenticated users online.</p> <p>Usually the administrator concerns only information about the online user, the other information displayed is used for troubleshooting by technical support.</p>
Example	<p>Displays the authenticated users online.</p> <pre> Switch(config)#show aaa authenticated-user ----- authenticated users ----- UserName  Retry RadID  Port  EapID  ChapID  OnTime  UserIP  MAC ----- ----- total: 0 ----- </pre>

### 13.8.14 show aaa authenticating-user

Command	show aaa authenticating-user
Parameter	none                      none
Default	None.
Mode	Admin/Global Mode
Usage Guide	<p>Display the authenticating users.</p> <p>Usually the administrator concerns only information about the authenticating user, the other information displays is used for troubleshooting by the technical support.</p>
Example	<p>Display the authenticating users.</p> <pre> Switch(config)#show aaa authenticating-user ----- authenticating users ----- User-name  Retry-time  Radius-ID  Port  Eap-ID  Chap-ID  Mem-Addr  State ----- ----- total: 0 ----- </pre>

### 13.8.15 show aaa config

Command	show aaa config
Parameter	none                      none
Default	None.
Mode	Admin/Global Mode
Usage Guide	Displays whether aaa authentication, accounting are enabled and information for key, authentication and accounting server specified.
Example	<p>Display aaa configuration information.</p> <pre> Switch(config)#show aaa config ----- AAA config data ----- Is Aaa Enabled = 1                      :1 means AAA authentication is enabled, 0 means is not enabled Is Account Enabled= 1                    :1 means AAA account is enabled, 0 means is not enabled MD5 Server Key = yangshifeng         : Authentication key authentication server sum = 2         :Configure the number of authentication server ..... </pre>



### 13.8.16 show radius authenticated-user count

Command	show radius authenticated-user count
Parameter	none                      none
Default	None.
Mode	Admin/Global Mode
Usage Guide	Show the number of on-line users who have already passed the authentication.
Example	Show the number of on-line users who have already passed the authentication.  Switch(config)#show radius authenticated-user count The authenticated online user num is: 105

### 13.8.17 show radius authenticating-user count

Command	show radius authenticating-user count
Parameter	none                      none
Default	None.
Mode	Admin/Global Mode
Usage Guide	Show the number of the authenticating-user.
Example	Show the number of the authenticating-user.  Switch(config)#show radius authenticating-user count The authenticating user num is: 10

### 13.8.18 show radius count

Command	show radius count {authenticated-user authenticating-user} count
Parameter	authenticated-user      displays the authenticated users online authenticating-user      displays the authenticating users
Default	None.
Mode	Admin/Global Mode
Usage Guide	Displays the statistics for users of RADIUS authentication.
Example	Displays the statistics for users of RADIUS authentication.  Switch#show radius authenticated-user count The authenticated online user num is: 0

## 13.9 IPv6 Security RA

### 13.9.1 ipv6 security-ra enable

Command	[no] ipv6 security-ra enable
Parameter	none                                  none
Default	The IPv6 security RA function is disabled by default.
Mode	Global Mode
Usage Guide	<p>Globally enable IPv6 security RA function, all the RA advertisement messages will not be forwarded through hardware, but only sent to CPU to handle.</p> <p>Only after enabling the global security RA function, the security RA on a port can be enabled. Globally disabling security RA will clear all the configured security RA ports. The global security RA function and the global IPv6 SAVI function are mutually exclusive, so they can not be enabled at the same time.</p> <p>The no operation of this command will globally disable IPv6 security RA function.</p>
Example	<p>Globally enable IPv6 security RA.</p> <pre>Switch(config)#ipv6 security-ra enable</pre>

## 13.9.2 ipv6 security-ra enable

Command	[no] ipv6 security-ra enable
Parameter	none                      none
Default	The IPv6 security RA function is disabled by default.
Mode	Port Configuration Mode
Usage Guide	<p>Enable IPv6 security RA on a port, causing this port not to forward the received RA message.</p> <p>Only after globally enabling the security RA function, can the security RA on a port be enabled. Globally disabling security RA will clear all the configured security RA ports.</p> <p>The no ipv6 security-ra enable will disable the IPv6 security RA on a port.</p>
Example	<p>Enable IPv6 security RA on a port.</p> <pre>Switch(config-if-ethernet1/0/2)#ipv6 security-ra enable</pre>

### 13.9.3 show ipv6 security-ra

Command	show ipv6 security-ra [interface <interface-list>]
Parameter	interface-list                      Specifies the port number. No parameter will display all distrust ports, entering a parameter will display the corresponding distrust port.
Default	None.
Mode	Admin/Global Mode
Usage Guide	Display all the interfaces with IPv6 RA function enabled.
Example	<p>Display all the interfaces with IPv6 RA function enabled.</p> <pre> Switch# show ipv6 security-ra IPv6 security ra config and state information in the switch Global IPv6 Security RA State: Enable Ethernet1/0/1 IPv6 Security RA State: Yes Ethernet1/0/3 IPv6 Security RA State: Yes </pre>

## 13.10 MAB

### 13.10.1 authentication mab

Command	authentication mab {radius local} (none) no authentication mab
Parameter	radius means RADIUS authentication mode local means the local authentication none means the authentication is needless
Default	By default · using RADIUS authentication mode.
Mode	Global Mode
Usage Guide	<p>Configure the authentication mode and priority of MAC address authentication.</p> <p>none option is used to the fleeing function of MAC address authentication.</p> <p>If all configured RADIUS servers don't respond, switch will adopt none authentication mode to allow that MAC address authentication users access the network directly. The option of local is used for the local authentication of MAC address, it authenticates through the local user name and password. If configured as the method of authentication mab radius local none, judge if configured the user name and password used in mab authentication in local when the radius server has no response. If it has been configured, use the local authentication, if not, use the backup none authentication.</p> <p>The no command restores the default authentication mode.</p>
Example	<p>Configure the local authentication and the fleeing function of MAC address authentication.</p> <p>Switch(config)#authentication mab radius local none</p>

## 13.10.2 clear mac-authentication-bypass binding

Command	clear mac-authentication-bypass binding {mac WORD   interface (ethernet IFNAME   IFNAME)   all}						
Parameter	<table border="1"> <tr> <td>mac</td> <td>Delete MAB binding of the specified MAC address</td> </tr> <tr> <td>IFNAME</td> <td>Delete MAB binding of the specified port</td> </tr> <tr> <td>all</td> <td>Delete all MAB binding</td> </tr> </table>	mac	Delete MAB binding of the specified MAC address	IFNAME	Delete MAB binding of the specified port	all	Delete all MAB binding
mac	Delete MAB binding of the specified MAC address						
IFNAME	Delete MAB binding of the specified port						
all	Delete all MAB binding						
Default	None.						
Mode	Admin Mode						
Usage Guide	Clear MAB binding information.						
Example	<p>Delete all MAB binding.</p> <pre>Switch#clear mac-authentication-bypass binding all</pre>						



### 13.10.3 mac-authentication-bypass binding-limit

Command	mac-authentication-bypass binding-limit <1-100> no mac-authentication-bypass binding-limit
Parameter	1-100 the max binding number of MAB, ranging from 1 to 100
Default	By default · the max binding number of MAB is 3.
Mode	Port Configuration Mode
Usage Guide	<p>Set the max binding number of MAB.</p> <p>Set the max binding number of MAB. When the binding number reaches to the max value, the port will stop binding, if the max binding number is less than the current binding number of the port, the setting will be unsuccessful.</p> <p>The no command will restore the default binding number as 3.</p>
Example	<p>Configure the max binding number as 10.</p> <pre>Switch(config)#interface ethernet 1/0/1 Switch(config-if-ethernet1/0/1)#mac-authentication-bypass binding-limit 10</pre>

### 13.10.4 mac-authentication-bypass enable

Command	[no] mac-authentication-bypass enable
Parameter	none                      none
Default	By default · disable the global and port MAB function.
Mode	Port Configuration Mode
Usage Guide	<p>Enable the global and port MAB function.</p> <p>To process MAB authentication of a port, enable the global MAB function first, and then, enable the MAB function of the corresponding port.</p> <p>The no command disables MAB function.</p>
Example	<p>Enable the global and port Eth1/0/1 MAB function.</p> <pre>Switch(config)#mac-authentication-bypass enable Switch(config)#interface ethernet 1/0/1 Switch(config-if-ethernet1/0/1)#mac-authentication-bypass enable</pre>

### 13.10.5 mac-authentication-bypass guest-vlan

Command	<pre>mac-authentication-bypass guest-vlan &lt;1-4094&gt; no mac-authentication-bypass guest-vlan</pre>
Parameter	<pre>1-4094</pre> <p>guest vlan ID, ranging from 1 to 4094</p>
Default	None.
Mode	Port Configuration Mode
Usage Guide	<p>Set guest vlan of MAB authentication.</p> <p>Set guest vlan of MAB authentication, only Hybrid port use this command, it is not take effect on access port. After MAB authentication is failing, if the existent guest vlan is configured by the port connecting to the MAB user, the MAB user can join and access guest vlan.</p> <p>The no command deletes guest vlan.</p>
Example	<p>Configure guest vlan of MAB authentication for port 1/0/1.</p> <pre>Switch(config)#interface ethernet 1/0/1 Switch(config-if-ethernet1/0/1)#mac-authentication-bypass guest-vlan 10</pre>

## 13.10.6 mac-authentication-bypass spoofing-garp-check

Command	[no] mac-authentication-bypass spoofing-garp-check
Parameter	none                      none
Default	By default · disable spoofing-garp-check function.
Mode	Global Mode
Usage Guide	<p>Enable the spoofing-garp-check function, MAB function will not deal with spoofing-garp any more. When the terminal of Windows operating system detects the address conflict, it will send a gratuitous ARP to correct the error ARP entries generated by gratuitous ARP of the conflict detection. This command is used to detect the spoofing-garp when occurring the address conflict, MAB function is not deal with the packet any more.</p> <p>Notice: when enabling the check function, all ARP will be processed the software check, it will add switch's load.</p> <p>The no command disables the function.</p>
Example	<p>Enable spoofing-garp-check function.</p> <pre>Switch(config)#mac-authentication-bypass spoofing-garp-check enable</pre>

### 13.10.7 mac-authentication-bypass timeout linkup-period

Command	mac-authentication-bypass timeout linkup-period <0-30> no mac-authentication-bypass timeout linkup-period
Parameter	0-30 After the port is shutdown automatically, the interval before it up again, the unit is second, 0 means there is no down/up operation
Default	By default · the interval is 0.
Mode	Global Mode
Usage Guide	<p>Set the interval between down and up when VLAN binding in a port is changing to assure the user can obtain IP again.</p> <p>When MAB authentication is successful, belong to vlan according to auto-vlan setting, when MAB authentication is failing, belong to vlan according to guest-vlan setting. After linkup-period is set, when VLAN binding of a port is changing, the port will be shutdown automatically, and will be up again after linkup-period to assure the client obtain IP.</p> <p>The no command to restore default values.</p>
Example	<p>Configure down/up time as 12s.</p> <pre>Switch(config)#mac-authentication-bypass timeout linkup-period 12</pre>

### 13.10.8 mac-authentication-bypass timeout offline-detect

Command	mac-authentication-bypass timeout offline-detect (0   <60-7200>) no mac-authentication-bypass timeout offline-detect
Parameter	0   <60-7200>                      offline-detect time, the range is 0 or 60 to 7200s
Default	By default · offline-detect time is 180s.
Mode	Global Mode
Usage Guide	Configure offline-detect time. When offline-detect time is 0, the switch does not detect MAB binding, when offline-detect time is 60s to 7200s, the switch timely detects the flow corresponding to the MAB binding. If there is no flow in the period of offline-detect time, it will delete this binding and forbid the flow to pass.  The no command restores the default value.
Example	Configure offline-detect time as 200s.  Switch(config)#mac-authentication-bypass timeout offline-detect 200

### 13.10.9 mac-authentication-bypass timeout quiet-period

Command	mac-authentication-bypass timeout quiet-period <1-60> no mac-authentication-bypass timeout quiet-period
Parameter	1-60 quiet-period, ranging from 1 to 60s
Default	By default quiet-period is 30s.
Mode	Global Mode
Usage Guide	Set quiet-period of MAB authentication. If MAB authentication is failing, within the quiet-period the switch will not respond the authentication request of this MAC, after quiet-period, it will respond the request again.  The no command restores quiet-period as the default value.
Example	Configure quiet-period of MAB authentication as 60s.  Switch(config)#mac-authentication-bypass timeout quiet-period 60

## 13.10.10 mac-authentication-bypass timeout reauth-period

Command	mac-authentication-bypass timeout reauth-period <1-3600> no mac-authentication-bypass timeout reauth-period
Parameter	1-3600 reauthentication interval, ranging from 1 to 3600s
Default	By default · reauthentication interval is 30s.
Mode	Global Mode
Usage Guide	<p>Set the reauthentication interval at failing authentication state.</p> <p>At failing authentication state, the user processes the reauthentication timely until the authentication is successful; at the successful state, the user can access the network resources.</p> <p>The no command restores the default value.</p>
Example	<p>Configure reauthentication time as 20s.</p> <pre>Switch(config)#mac-authentication-bypass timeout reauth-period 20</pre>



### 13.10.11 mac-authentication-bypass timeout stale-period

Command	mac-authentication-bypass timeout stale-period <0-60> no mac-authentication-bypass timeout stale-period
Parameter	0-60                                      The time that delete the binding, ranging from 0 to 60s
Default	By default, it takes 30 s. to delete the binding.
Mode	Global Mode
Usage Guide	Set the time that delete the binding user after MAB port is down. If the time that delete the binding as 0, delete all user binding of this port as soon as the MAB port is down, if the time is bigger than 0, delete the user binding with a delay after the MAB port is down.  The no command restores the default value.
Example	Configure the deletion time as 40s.  Switch(config)#mac-authentication-bypass timeout stale-period 40

### 13.10.12 mac-authentication-bypass username-format

Command	[no] mac-authentication-bypass username-format {mac-address   {fixed username WORD password WORD}}
Parameter	mac-address                      Use MAC address of MAB user as username and password to authenticate
	fixed username WORD              Use the specified username and password to authenticate, the length password WORD                      of username and password ranges between 1 and 32 characters
Default	By default · use MAC address of MAB user as username and password to authenticate.
Mode	Global Mode
Usage Guide	<p>Set the authenticate method of MAB authentication.</p> <p>There are two methods for MAB authentication: use MAC address of MAB user as username and password to authenticate or use the specified username and password to authenticate. If there is no specified username and password, the device uses the first method to authenticate by default.</p> <p>The no command to restore default values.</p>
Example	<p>All MAB users use the same username and password to authenticate, the username is mab-user, the password is mab-pwd.</p> <pre>Switch(config)#mac-authentication-bypass username-format fixed username mab-user password mab-pwd</pre>

### 13.10.13 show mac-authentication-bypass

Command	show mac-authentication-bypass {interface {ethernet IFNAME   IFNAME}}		
Parameter	IFNAME	Port name	
Default	None.		
Mode	Admin/Global Mode		
Usage Guide	Show the binding information of MAB authentication.		
Example	<p>Show the binding information of MAB authentication.</p> <pre> Switch#show mac-authentication-bypass The Number of all binding is 5 MAC                Interface    Vlan ID          State ----- 04-0a-eb-6a-7f-88  Ethernet1/0/1  1                MAB_QUIET 03-0a-eb-6a-7f-88  Ethernet1/0/1  1                MAB_QUIET 02-0a-eb-6a-7f-88  Ethernet1/0/1  1                MAB_AUTHENTICATED 00-0a-eb-6a-7f-8e  Ethernet1/0/1  1                MAB_AUTHENTICATED  Switch(config)#show mac-authentication-bypass int e1/0/1 Interface Ethernet1/0/1 user config: MAB enable: Enable Binding info: 1  -----  MAB Binding built at SUN JAN 01 01:14:48 2006 VID 1, Port: Ethernet1/1 Client MAC: 00-0a-eb-6a-7f-8e Binding State: MAB_AUTHENTICATED Binding State Lease: 164 seconds left </pre>		

## 13.11 MAB PPPoE Intermediate Agent

### 13.11.1 pppoe intermediate-agent

Command	[no] pppoe intermediate-agent
Parameter	none none
Default	By default, disable global PPPoE intermediate agent function.
Mode	Global Mode
Usage Guide	<p>Enable global PPPoE intermediate agent function.</p> <p>After enable global PPPoE IA function, process the packet of PPPoE discovery stage according to the related configuration.</p> <p>The no command disables global PPPoE intermediate agent function.</p>
Example	<p>Enable global PPPoE intermediate agent function.</p> <p>Switch(config)#pppoe intermediate agent</p>

### 13.11.2 pppoe intermediate-agent (Port)

Command	[no] pppoe intermediate-agent
Parameter	none                      none
Default	By default · disable PPPoE intermediate agent function of the port.
Mode	Port Configuration Mode
Usage Guide	<p>Enable PPPoE intermediate agent function of the port.</p> <p>After enable PPPoE IA function of the port, add vendor tag for PPPoE packet of the port.</p> <p>Note:</p> <ol style="list-style-type: none"> <li>1. It must enable global pppoe intermediate-agent function.</li> <li>2. At least one port is connected to PPPoE server, and the port mode is trust.</li> </ol> <p>The no command disables PPPoE intermediate agent function of the port.</p>
Example	<p>Enable PPPoE intermediate agent function of the port ethernet 1/0/2.</p> <pre>Switch(config-if-ethernet1/0/2)#pppoe intermediate agent</pre>

### 13.11.3 pppoe intermediate-agent circuit-id

Command	[no] pppoe intermediate-agent circuit-id <string>
Parameter	string circuit-id, the max character number is 63 bytes
Default	This function is not configured by default.
Mode	Port Configuration Mode
Usage Guide	<p>Configure circuit ID of the port.</p> <p>This command configures circuit-id alone for each port, the priority is higher than pppoe intermediate-agent identifier-string command.</p> <p>The no command cancels this configuration.</p>
Example	<p>Configure circuit-id as abcd/efgh on port ethernet1/0/3 of vlan3.</p> <pre>Switch(config-if-ethernet1/0/3)#pppoe intermediate-agent circuit-id abcd/efgh</pre>

### 13.11.4 pppoe intermediate-agent delimiter

Command	pppoe intermediate-agent delimiter <WORD> no pppoe intermediate-agent delimiter
Parameter	WORD                      the delimiter, its range is (# . . . : / space)
Default	By default · the fields is comparted with '\0'.
Mode	Global Mode
Usage Guide	Configure the delimiter among the fields in circuit-id and remote-id. After configuring the delimiter, the added fields of circuit-id and remote-id use the configured delimiter to compart. Notice: The global pppoe intermediate-agent function must be enabled.  The no command cancels the configuration.
Example	Configuration delimiter is space.  Switch(config)#pppoe intermediate-agent delimiter space

### 13.11.5 pppoe intermediate-agent format

Command	pppoe intermediate-agent format (circuit-id   remote-id) (hex   ascii) no pppoe intermediate-agent format (circuit-id   remote-id)
Parameter	hex                      hexadecimal ascii                      ASCII code
Default	This function is not configured by default.
Mode	Global Mode
Usage Guide	Configure the format with hex or ASCII for circuit-id and remote-id. Encapsulation circuit-id and remote-id with hex ASCII format to vendor tag. Notice: The global pppoe intermediate-agent function must be enabled.  The no command cancels the configuration.
Example	Configure the trust port 1/0/1 to enable vendor-tag strip function.  Switch(config)#pppoe intermediate-agent format remote-id ascii



### 13.11.6 pppoe intermediate-agent remote-id

Command	[no] pppoe intermediate-agent remote-id <string>
Parameter	string remote-id, the max character number is 63 bytes
Default	This function is not configured by default.
Mode	Port Configuration Mode
Usage Guide	<p>Configure remote-id of the port.</p> <p>Configure remote-id for each port, if there is no configuration, use switch's MAC as remote-id value.</p> <p>The no command cancels this configuration.</p>
Example	<p>Configure remote-id as abcd on port ethernet1/0/2.</p> <pre>Switch(config-if-ethernet1/0/2)# pppoe intermediate-agent remote-id abcd</pre>

### 13.11.7 pppoe intermediate-agent trust

Command	[no] pppoe intermediate-agent trust
Parameter	none                      none
Default	By default, the port is a untrust port.
Mode	Port Configuration Mode
Usage Guide	Configure the port as trust port. The port which connect to server must be configured as trust port. Note: At least one trust port is connected to PPPoE server.  The no command configures the port as untrust port.
Example	Configure port ethernet1/0/1 as trust port.  Switch(config-if-ethernet1/0/1)#pppoe intermediate-agent trust

### 13.11.8 pppoe intermediate-agent type self-defined circuit-id

Command	<pre>pppoe intermediate-agent type self-defined circuit-id {vlan   port   id (switch-id (mac   hostname)   remote-mac)   string WORD} no pppoe intermediate-agent type self-defined circuit-id</pre>												
Parameter	<table border="1"> <tr> <td>vlan</td> <td>VLAN ID</td> </tr> <tr> <td>port</td> <td>port number</td> </tr> <tr> <td>id switch-id mac</td> <td>the local MAC address</td> </tr> <tr> <td>id switch-id hostname</td> <td>the local host name</td> </tr> <tr> <td>remote-mac</td> <td>the remote MAC address</td> </tr> <tr> <td>string WORD</td> <td>the specified keyword</td> </tr> </table>	vlan	VLAN ID	port	port number	id switch-id mac	the local MAC address	id switch-id hostname	the local host name	remote-mac	the remote MAC address	string WORD	the specified keyword
vlan	VLAN ID												
port	port number												
id switch-id mac	the local MAC address												
id switch-id hostname	the local host name												
remote-mac	the remote MAC address												
string WORD	the specified keyword												
Default	By default · this configuration is null.												
Mode	Global Mode												
Usage Guide	<p>Configure the self-defined circuit-id.</p> <p>This configuration and type tr-101 circuit-id are mutually exclusive, it will clear the corresponding configuration of type tr-101 circuit-id.</p> <p>The no command cancels the configuration.</p>												
Example	<p>Configure the self-defined circuit-id as vlan port id switch-id hostname.</p> <pre>Switch(config)#pppoe intermediate-agent type self-defined circuit-id vlan port id switch-id hostname</pre>												

### 13.11.9 pppoe intermediate-agent type self-defined remoteid

Command	pppoe intermediate-agent type self-defined remoteid {mac   vlan-mac   hostname   string WORD} no pppoe intermediate-agent type self-defined remote-id								
Parameter	<table border="1"> <tr> <td>mac</td> <td>Ethernet port MAC address</td> </tr> <tr> <td>vlan-mac</td> <td>IP interface MAC address</td> </tr> <tr> <td>hostname</td> <td>the local host name</td> </tr> <tr> <td>string WORD</td> <td>the specified keyword</td> </tr> </table>	mac	Ethernet port MAC address	vlan-mac	IP interface MAC address	hostname	the local host name	string WORD	the specified keyword
mac	Ethernet port MAC address								
vlan-mac	IP interface MAC address								
hostname	the local host name								
string WORD	the specified keyword								
Default	By default, this configuration is empty.								
Mode	Global Mode								
Usage Guide	<p>Configure the self-defined remote-id.</p> <p>Configuration order of this command according to the fields order in remote-id.</p> <p>The no command cancels the configuration.</p>								
Example	<p>Configure the self-defined remote-id as string abcd mac hostname.</p> <pre>Switch(config)#pppoe intermediate-agent type self-defined remoteid string abcd mac hostname</pre>								

### 13.11.10 pppoe intermediate-agent type tr-101 circuit-id access-node-id

Command	pppoe intermediate-agent type tr-101 circuit-id access-node-id <string> no pppoe intermediate-agent type tr-101 circuit-id access-node-id
Parameter	string access-node-id, the max character number is 47 bytes.
Default	By default · MAC address of the switch.
Mode	Global Mode
Usage Guide	<p>Configure access-node-id field value of circuit ID in the added vendor tag with tr-101 standard.</p> <p>Use this configuration to create access-node-id of circuit ID in vendor tag.circuit-id value is access-node-id + " eth "+ Slot ID + delimiter + Port Index + delimiter + Vlan ID, access-node-id occupies n bytes (n&lt;48), " eth " is space + e + t + h + space, it occupies 5 bytes, Slot ID occupies 2 bytes, Port Index occupies 3 bytes, Vlan ID occupies 4 bytes, delimiter occupies 1 byte. In default state, access-node-id value of circuit-id is switch's MAC, it occupies 6 bytes. For example: MAC address is "0a0b0c0d0e0f", Slot ID is 12, Port Index is 34, Vlan ID is 567, the default circuit-id value is "0a0b0c0d0e0f eth 12/034:0567".</p> <p>The no command unconfigured.</p>
Example	<p>Configure access-node-id value of circuit ID as abcd in vendor tag.</p> <p>Switch(config)#pppoe intermediate-agent access-node-id abcd</p> <p>After port ethernet1/0/3 of vlan3 receives PPPoE packets, circuit-id value of the added vendor tag is "abcd eth 01/003:0003".</p>

### 13.11.11 pppoe intermediate-agent type tr-101 circuit-id identifier-string option delimiter

Command	pppoe intermediate-agent type tr-101 circuit-id identifier-string <string> option {sp   sv   pv   spv} delimiter <WORD> [delimiter <WORD>] no pppoe intermediate-agent type tr-101 circuit-id identifier-string option delimiter						
Parameter	<table border="1"> <tr> <td>string</td> <td>identifier-string, the max character number is 47 bytes</td> </tr> <tr> <td>{sp   sv   pv   spv}</td> <td>This option can select the combination format for slot, port, vlan, sp means slot and port, sv means slot and vlan, pv means port and vlan, spv means slot, port and vlan</td> </tr> <tr> <td>WORD</td> <td>The delimiter between slot, port and vlan, the range is (#   .   ,   ;   :   /   space). Note: There are two delimiter WORDs in spv combo mode, the first between slot and port, the second between port and vlan</td> </tr> </table>	string	identifier-string, the max character number is 47 bytes	{sp   sv   pv   spv}	This option can select the combination format for slot, port, vlan, sp means slot and port, sv means slot and vlan, pv means port and vlan, spv means slot, port and vlan	WORD	The delimiter between slot, port and vlan, the range is (#   .   ,   ;   :   /   space). Note: There are two delimiter WORDs in spv combo mode, the first between slot and port, the second between port and vlan
string	identifier-string, the max character number is 47 bytes						
{sp   sv   pv   spv}	This option can select the combination format for slot, port, vlan, sp means slot and port, sv means slot and vlan, pv means port and vlan, spv means slot, port and vlan						
WORD	The delimiter between slot, port and vlan, the range is (#   .   ,   ;   :   /   space). Note: There are two delimiter WORDs in spv combo mode, the first between slot and port, the second between port and vlan						
Default	By default, this configuration is empty.						
Mode	Global Mode						
Usage Guide	<p>Configure circuit-id of the added vendor tag with tr-101 standard.</p> <p>This command is used to configure global circuit id, the priority is higher than pppoe intermediate-agent access-node-id command. circuit-id value is access-node-id + " eth " + Slot ID + delimiter + Port Index + delimiter + Vlan ID,</p> <p>access-node-id occupies n bytes (n&lt;48), " eth " is space + e + t + h + space, it occupies 5 bytes, Slot ID occupies 2 bytes, Port Index occupies 3 bytes, Vlan ID occupies 4 bytes, delimiter occupies 1 byte.</p> <p>The no command deletes this configuration.</p>						
Example	<p>Configure access-node-id as xyz, use spv combination mode, delimiter with "#"between Slot ID and Port ID, delimiter with "/"between Port ID and Vlan ID.</p> <pre>Switch(config)#pppoe intermediate-agent identifier-string xyz option spv delimiter # delimiter / Switch# show pppoe intermediate-agent identifier-string option delimiter config identifier string is : xyz config option is : slot , port and vlan the first delimiter is : "# " the second delimiter is : "/" "</pre> <p>After port ethernet1/0/3 of vlan3 receives PPPoE packets, circuit-id value of the added vendor tag is "xyz eth 01#003/0003".</p>						

### 13.11.12 pppoe intermediate-agent vendor-tag strip

Command	[no] pppoe intermediate-agent vendor-tag strip
Parameter	none                      none
Default	By default , disable vendor-tag strip function of the port.
Mode	Port Configuration Mode
Usage Guide	<p>Enable vendor-tag strip function of the port.</p> <p>If the received packet includes vendor tag from server to client, strip this vendor tag.</p> <p>Note:</p> <ol style="list-style-type: none"> <li>1. Must enable global pppoe intermediate-agent function.</li> <li>2. It must be configured on trust port.</li> </ol> <p>The no command cancels this function.</p>
Example	<p>Trust port ethernet1/0/1 enables vendor tag strip function.</p> <pre>Switch(config-if-ethernet1/0/1)#pppoe intermediate-agent trust Switch(config-if-ethernet1/0/1)#pppoe intermediate-agent vendor-tag strip</pre>

#### show pppoe intermediate-agent access-node-id

Command	show pppoe intermediate-agent access-node-id
Parameter	none                      none
Default	By default,the configuration information is null.
Mode	Admin mode
Usage Guide	This command is used to show access-node-id configured by user.

---

Example

Show access-node-id configuration information.

```
Switch#pppoe intermediate-agent access-node-id abcd  
Switch#show pppoe intermediate-agent access-node-id  
pppoe intermediate-agent access-node-id is : abcd
```

---



### 13.11.13 show pppoe intermediate-agent identifier-string option delimiter

Command	show pppoe intermediate-agent identifier-string option delimiter
Parameter	none                      none
Default	By default,the configuration information is null.
Mode	Admin mode
Usage Guide	Show the configured identifier-string, the combo format and delimiter of slot, port and vlan.
Example	<p>Show the configuration information for pppoe intermediate-agent identifier-string.</p> <pre> Switch#pppoe intermediate-agent identifier-string abcd option spv delimiter # delimiter / Switch# show pppoe intermediate-agent identifier-string option delimiter config identifier string is : abcd config option is : slot , port and vlan the first delimiter is : "# " the second delimiter is : "/" </pre>

### 13.11.14 show pppoe intermediate-agent info

Command	show pppoe intermediate-agent info [interface ethernet <interface-name>]
Parameter	interface-name                      port name
Default	By default,the configuration information is null.
Mode	Admin mode
Usage Guide	Show the related PPPoE IA configuration information of all ports or the specified port. Check the configuration information of the corresponding port, show whether the port is trust port, strip function is enabled, rate limit is enabled, show the configured circuit ID and remote ID.
Example	Show pppoe intermediate-agent configuration information of port ethernet1/0/2.  Switch# show pppoe intermediate-agent info interface ethernet 1/0/2 Interface    IA    Trusted    vendor Strip    Rate limit    circuit id    remote id -----    ----    -----    -----    -----    -----    ----- Ethernet1/0/2    yes    no            no            no            test1/port1    host1

## 13.12 VLAN-ACL

### 13.12.1 clear vacl statistic vlan

Command	clear vacl [in   out] statistic vlan [<1-4094>]	
Parameter	in   out	Clear the traffic statistic of the ingress/egress
	1-4094	The VLAN which needs to clear the VACL statistic information. If do not input VLAN ID, then clear all VLAN statistic information
Default	None.	
Mode	Admin mode	
Usage Guide	This command can clear the statistic information of VACL.	
Example	Clear VACL statistic information of Vlan1.	
	Switch#clear vacl statistic vlan 1	

## 13.12.2 show vacl vlan

Command	show vacl [in   out] vlan [<1-4094>]   [begin   include   exclude <regular-expression>]	
Parameter	in   out	Show ingress/egress configuration and statistic
	1-4094	The VLAN which needs to show the configuration and the statistic information of VACL. If do not input VLAN ID, then show VACL configuration and statistic information of all VLANs.
	begin   include   exclude	the regular expression
	<regular-expression>	<p>. match any characters except the line feed character</p> <p>^ match the beginning of the row</p> <p>\$ match the end of the row</p> <p>  match the character string at the left or right of upright line</p> <p>[0-9] match the number 0 to the number 9</p> <p>z] match the lowercase a to z</p> <p>[aeiou] match any letter in "aeiou"</p> <p>\ Escape Character is used to match the intervocalic character, for example, \\$ will match the \$ character, but it is not match the end of the character string</p> <p>\w match the letter, the number or the underline</p> <p>\b match the beginning or the end of the words</p> <p>\W match any characters which are not alphabet letter, number and underline</p> <p>\B match the locations which are not the begin or end of the word</p> <p>[^x] match any characters except x</p> <p>[^aeiou] match any characters except including aeiou letters</p> <p>* repeat zero time or many times</p> <p>+ repeat one time or many times</p> <p>(n) repeat n times</p> <p>(n · ) repeat n or more times</p> <p>(n · m) repeat n to m times</p> <p>At present, the regular expression used does not support the following syntaxes:</p> <p>\s match the blank character</p> <p>\d match the number</p> <p>\S match any characters except blank character</p> <p>\D match non-number character</p>

---

? repeat zero time or one time

---

---

Default

None.

---

Mode

Admin Mode

---

Usage Guide

This command shows the configuration and the statistic information of VACL.

---

Example

Show vlan2 VACL statistics.

Switch (config)#show vacl vlan 2

Vlan 2:

IP Ingress access-list used is 100, traffic-statistics Disable.

---

### 13.12.3 vACL ip access-group

Command	<pre> vacl ip access-group {&lt;1-299&gt;   WORD} {in   out} [traffic-statistic] vlan WORD no vACL ip access-group {&lt;1-299&gt;   WORD} {in   out} vlan WORD </pre>	
Parameter	<1-299>   WORD	Configure the numeric IP ACL (include: standard ACL rule <1-99>, extended ACL rule <100-299>) or the named ACL.
	in   out	Filter the ingress/egress traffic
	traffic-statistic	Enable the statistic of matched packets number
	vlan WORD	The VLAN will be bound to VACL
Default	None	
Mode	Global Mode	
Usage Guide	<p>This command configure VACL of IP type on the specific VLAN.</p> <p>Use “;” or “-” to input the VLAN or multi-VLANs, but do not exceed 128, and CLI length cannot exceed 80 characters. Egress direction filtering is not supported by switch.</p> <p>The no command unconfigured.</p>	
Example	<p>Configure the numeric IP ACL and enable the statistic function for Vlan 1-5,6,7-9.</p> <pre> Switch(config)#vacl ip access-group 1 in traffic-statistic vlan 1-5; 6; 7-9 </pre>	

### 13.12.4 vACL ipv6 access-group

Command	<pre> vacl ipv6 access-group (&lt;500-699&gt;   WORD) {in } (traffic-statistic) vlan WORD no ipv6 access-group {&lt;500-699&gt;   WORD} {in } vlan WORD </pre>								
Parameter	<table border="1"> <tr> <td>&lt;500-699&gt;   WORD</td> <td>Configure the IPv6 numeric standard ACL or IPV6 standard ACL rule.</td> </tr> <tr> <td>in   out</td> <td>Filter inlet/ outlet flow</td> </tr> <tr> <td>traffic-statistic</td> <td>Enable the statistic of matched packets number</td> </tr> <tr> <td>vlan WORD</td> <td>The VLAN will be bound to VACL.</td> </tr> </table>	<500-699>   WORD	Configure the IPv6 numeric standard ACL or IPV6 standard ACL rule.	in   out	Filter inlet/ outlet flow	traffic-statistic	Enable the statistic of matched packets number	vlan WORD	The VLAN will be bound to VACL.
<500-699>   WORD	Configure the IPv6 numeric standard ACL or IPV6 standard ACL rule.								
in   out	Filter inlet/ outlet flow								
traffic-statistic	Enable the statistic of matched packets number								
vlan WORD	The VLAN will be bound to VACL.								
Default	None.								
Mode	Global Mode								
Usage Guide	<p>This command configure VACL of IPv6 on the specific VLAN.</p> <p>Use “;” or “-” to input the VLAN or multi-VLANs, but do not exceed 128, and CLI length cannot exceed 80 characters. Egress direction filtering and extended IPv6 is not supported by switch.</p> <p>The no command unconfigured.</p>								
Example	<p>Configure the numeric IPv6 ACL for Vlan 5.</p> <pre> Switch(config)#vacl ipv6 access-group 600 in traffic-statistic vlan 5 </pre>								

## 13.12.5 vACL mac access-group

Command	<pre> vacl mac access-group {&lt;700-1199&gt;   WORD} {in } [traffic-statistic] vlan WORD no vACL mac access-group {&lt;700-1199&gt;   WORD} {in } vlan WORD </pre>								
Parameter	<table border="1"> <tr> <td>&lt;700-1199&gt;   WORD</td> <td>Configure the numeric IP ACL (include: &lt;700-799&gt; MAC standard access list, &lt;1100-1199&gt; MAC extended access list) or the named ACL</td> </tr> <tr> <td>in</td> <td>Filter the ingress traffic</td> </tr> <tr> <td>traffic-statistic</td> <td>Enable the statistic of matched packets number</td> </tr> <tr> <td>vlan WORD</td> <td>The VLAN will be bound to VACL</td> </tr> </table>	<700-1199>   WORD	Configure the numeric IP ACL (include: <700-799> MAC standard access list, <1100-1199> MAC extended access list) or the named ACL	in	Filter the ingress traffic	traffic-statistic	Enable the statistic of matched packets number	vlan WORD	The VLAN will be bound to VACL
<700-1199>   WORD	Configure the numeric IP ACL (include: <700-799> MAC standard access list, <1100-1199> MAC extended access list) or the named ACL								
in	Filter the ingress traffic								
traffic-statistic	Enable the statistic of matched packets number								
vlan WORD	The VLAN will be bound to VACL								
Default	None.								
Mode	Global Mode								
Usage Guide	<p>This command configure VACL of MAC type on the specific VLAN.</p> <p>Use “;” or “-” to input the VLAN or multi-VLANs, but do not exceed 128, and CLI length cannot exceed 80 characters. Egress direction filtering is not supported by switch.</p> <p>The no command unconfigured.</p>								
Example	<p>Configure the numeric MAC ACL for Vlan 1-5</p> <pre> Switch(config)#vacl mac access-group 700 in traffic-statistic vlan 1-5 </pre>								



## 13.12.6 vACL mac-ip access-group

Command	<pre> vacl mac-ip access-group {&lt;3100-3299&gt;   WORD} {in } [traffic-statistic] vlan WORD no vACL mac-ip access-group {&lt;3100-3299&gt;   WORD} {in } vlan WORD </pre>								
Parameter	<table border="1"> <tr> <td>&lt;3100-3299&gt;   WORD</td> <td>Configure the numeric MAC-IP ACL or the named ACL</td> </tr> <tr> <td>in</td> <td>Filter the ingress traffic</td> </tr> <tr> <td>traffic-statistic</td> <td>Enable the statistic of matched packets number</td> </tr> <tr> <td>vlan WORD</td> <td>The VLAN will be bound to VACL.</td> </tr> </table>	<3100-3299>   WORD	Configure the numeric MAC-IP ACL or the named ACL	in	Filter the ingress traffic	traffic-statistic	Enable the statistic of matched packets number	vlan WORD	The VLAN will be bound to VACL.
<3100-3299>   WORD	Configure the numeric MAC-IP ACL or the named ACL								
in	Filter the ingress traffic								
traffic-statistic	Enable the statistic of matched packets number								
vlan WORD	The VLAN will be bound to VACL.								
Default	None.								
Mode	Global mode								
Usage Guide	<p>This command configure VACL of MAC-IP type on the specific VLAN.</p> <p>Use “;” or “-” to input the VLAN or multi-VLANs, but do not exceed 128, and CLI length cannot exceed 80 characters. Egress direction filtering is not supported by switch.</p> <p>The no command unconfigured.</p>								
Example	<p>Configure the numeric MAC-IP ACL for Vlan 1, 2, 5.</p> <pre> Switch(config)#vacl mac-ip access-group 3100 in traffic-statistic vlan 1;2;5 </pre>								

## 13.13 SAVI

### 13.13.1 ipv6 cps prefix

Command	<pre>ipv6 cps prefix &lt;ipv6-address&gt; vlan &lt;vid&gt; no ipv6 cps prefix&lt;ipv6-address&gt;</pre>				
Parameter	<table border="1"> <tr> <td>ipv6-address</td> <td>the address prefix of link, like 2001::/64</td> </tr> <tr> <td>vid</td> <td>vlan ID of the current link</td> </tr> </table>	ipv6-address	the address prefix of link, like 2001::/64	vid	vlan ID of the current link
ipv6-address	the address prefix of link, like 2001::/64				
vid	vlan ID of the current link				
Default	None.				
Mode	Global Mode				
Usage Guide	<p>Configure IPv6 address prefix of the link manually.</p> <p>Users should configure local address prefix: fe80::/64 of the link before enable the function of matching address prefix of the link, it accepts the packets of which source addresses are the local addresses of the link.</p> <p>The no command deletes IPv6 address prefix.</p>				
Example	<p>Configure IPv6 address prefix of the link manually is 2001::/64 °</p> <pre>Switch(config)#ipv6 cps prefix 2001::/64</pre>				

### 13.13.2 ipv6 cps prefix check enable

Command	[no] ipv6 cps prefix check enable
Parameter	none                      none
Default	By default,disable SAVI address prefix check function.
Mode	Global Mode
Usage Guide	<p>Enable SAVI address prefix check function.</p> <p>After enable the prefix check function, if the IPv6 address prefix of the packets does not accord with the link prefix, then do not establish the corresponding IPv6 address binding. If users enable the matched address prefix of the link, configure the local address prefix of fe80::/64 first to accept the packets with the source address as local link address. Disable address prefix check function by default.</p> <p>The no command will disable this function.</p>
Example	<p>Enable SAVI address prefix check function.</p> <p>Switch(config)#ipv6 cps prefix check enable</p>

### 13.13.3 ipv6 dhcp snooping trust

Command	[no] ipv6 dhcp snooping trust
Parameter	none                      none
Default	By default, this function is disabled.
Mode	Port Mode
Usage Guide	<p>Configure the port as dhcpv6 trust port, it does not establish dynamic DHCPv6 binding again and allows all DHCPv6 protocol packets to pass.</p> <p>Set the port as dhcpv6 trust attribute, enable uplink port of the switch with SAVI function for connecting dhcpv6 server or dhcpv6 relay generally.</p> <p>no command deletes the port trust function.</p>
Example	<p>Set ethernet1/0/1 to be DHCP trust port.</p> <pre>Switch(config)#interface ethernet1/0/1 Switch(config-if-ethernet1/0/1)#ipv6 dhcp snooping trust</pre>

### 13.13.4 ipv6 nd snooping trust

Command	[no] ipv6 nd snooping trust
Parameter	none                      none
Default	By default, this function is disabled.
Mode	Port Mode
Usage Guide	<p>Configure the port as slaac trust and RA trust port, this port will not establish dynamic slaac binding anymore and forwards RA packets.</p> <p>If the port disables ipv6 nd snooping trust function, it is considered to untrust RA packets port and discards all RA packets. Setting the port as trust attribute, enable the uplink port of the switch with SAVI or the conjoint port between switches with SAVI generally.</p> <p>The no command deletes the port trust function.</p>
Example	<p>Set the port ethernet1/0/1 to be nd trust port.</p> <pre>Switch(config)#interface ethernet1/0/1 Switch(config-if-ethernet1/0/1)#ipv6 nd snooping trust</pre>

#### savi check binding

Command	savi check binding <simple   probe> mode no savi check binding mode
Parameter	<p>simple                      only check the port state for conflict binding, if the state is up,keep the conflict binding and do not set new binding. If the state is down, delete the conflict binding to set a new one</p> <p>probe                      besides checking the port state for conflict binding, it will send NS packets to probe the usability of the corresponding user when the port state is up. If receiving the responded NA packets from users, it will keep the current conflict binding and does not set new binding, otherwise delete the conflict binding to set new one</p>

---

Default	Disable the conflict binding check mode by default. It will adopt the mode that delete the conflict binding directly to set new one.
Mode	Global Mode
Usage Guide	<p>Configure the check mode for conflict binding.</p> <p>It is recommended to configure probe mode to prevent the attack that the spurious address conflict binding deletes the legal user binding.</p> <p>The no command deletes the check mode.</p>
Example	<p>Configure the conflict binding check mode to probe mode.</p> <pre>Switch(config)#savi check binding probe mode</pre>

---

### 13.13.5 savi enable

Command	[no] savi enable
Parameter	none                      none
Default	By default,disable the global SAVI function.
Mode	Global Mode
Usage Guide	<p>Enable the global SAVI function.</p> <p>Command configuration can be processed for SAVI function after enabling the global SAVI function. Because SAVI function has already contained security RA function, global SAVI function and security RA function are mutually exclusive in the global mode.</p> <p>The no command disables this global function.</p>
Example	<p>Enable SAVI function.</p> <p>Switch(config)#savi enable</p>

### 13.13.6 savi ipv6 binding num

Command	savi ipv6 binding num <limit-num> no savi ipv6 binding num
Parameter	limit-num                      set the range from 0 to 65535
Default	The default value of the port binding number is 65535.
Mode	Port Mode
Usage Guide	Configure the number of the corresponding binding with the port. The configured binding number only include the dynamic binding type of slaac, dhcp. If the binding sum exceeds the configured number, this port does not create new dynamic binding any more, if the configured number is 0, this port does not create any dynamic binding.  The no command restores the default value.
Example	Configure the binding number to be 100 for port ethernet1/0/1.  Switch(config)#interface ethernet1/0/1 Switch(config-if-ethernet1/0/1)# savi ipv6 binding num 100



### 13.13.7 savi ipv6 check source binding

Command	<pre>savi ipv6 check source binding ip &lt;ip-address&gt; mac &lt;mac-address&gt; interface &lt;if-name&gt; {type [slaac   dhcp] lifetime &lt;lifetime&gt;   type static} no savi ipv6 check source binding ip &lt;ip-address&gt; interface &lt;if-name&gt;</pre>												
Parameter	<table border="1"> <tr> <td>ip-address</td> <td>the unicast IPv6 address, including local link and global unicast address</td> </tr> <tr> <td>mac-address</td> <td>the mac address of Ethernet</td> </tr> <tr> <td>if-name</td> <td>the port name, like interface ethernet 1/0/1</td> </tr> <tr> <td>slaac   dhcp</td> <td>slaac means create the dynamic binding for slaac type, dhcp means create the dynamic binding for dhcp type</td> </tr> <tr> <td>lifetime</td> <td>configure the lifetime period for the dynamic binding, the unit is second</td> </tr> <tr> <td>static</td> <td>create the binding of the static type</td> </tr> </table>	ip-address	the unicast IPv6 address, including local link and global unicast address	mac-address	the mac address of Ethernet	if-name	the port name, like interface ethernet 1/0/1	slaac   dhcp	slaac means create the dynamic binding for slaac type, dhcp means create the dynamic binding for dhcp type	lifetime	configure the lifetime period for the dynamic binding, the unit is second	static	create the binding of the static type
ip-address	the unicast IPv6 address, including local link and global unicast address												
mac-address	the mac address of Ethernet												
if-name	the port name, like interface ethernet 1/0/1												
slaac   dhcp	slaac means create the dynamic binding for slaac type, dhcp means create the dynamic binding for dhcp type												
lifetime	configure the lifetime period for the dynamic binding, the unit is second												
static	create the binding of the static type												
Default	None.												
Mode	Global Mode												
Usage Guide	<p>Configure the static or dynamic binding function manually °</p> <p>After the dynamic binding configured by handwork is overtime, the corresponding binding will be deleted but the configuration is still be kept, so the binding still be shown. If the binding needs to take effect again, it should delete it first and configure a new binding again.</p> <p>When the binding type is static type, do not configure lifetime period, the lifetime period is infinite.</p> <p>The no command deletes the configured binding.</p>												
Example	<p>Configure the dynamic binding of slaac type for SAVI manually.</p> <pre>Switch(config)#savi ipv6 check source binding ip 2001::10 mac 00-25-64-BB-8F-04 Interface ethernet1/0/1 type slaac lifetime 2010</pre> <p>Configure the static binding for SAVI manually.</p> <pre>Switch(config)#savi ipv6 check source binding ip 2001::20 mac 00-25-64-BB-8F-04 Interface ethernet1/0/1 type static</pre>												

### 13.13.8 savi ipv6 check source ip-address mac-address

Command	savi ipv6 check source [ip-address mac-address   ip-address   mac-address] no savi ipv6 check source
Parameter	none                      none
Default	By default,disable the control filtering function of the port.
Mode	Port Mode
Usage Guide	Enable the control authentication function for the packets of the port. The global SAVI function must be enabled before configuring this command.  The no command disables this function.
Example	Enable the control filtering function of the packets on port ethernet1/0/1.  Switch(config)#interface ethernet1/0/1 Switch(config-if-ethernet1/0/1)# savi ipv6 check source ip-address mac-address

### 13.13.9 savi ipv6 {dhcp-only | slaac-only | dhcp-slaac} enable

Command	[no] savi ipv6 {dhcp-only   slaac-only   dhcp-slaac} enable						
Parameter	<table border="1"> <tr> <td>dhcp-only</td> <td>dhcp-only application scene</td> </tr> <tr> <td>slaac-only</td> <td>slaac-only application scene</td> </tr> <tr> <td>dhcp-slaac</td> <td>combination application scene of dhcp-only and slaac-only</td> </tr> </table>	dhcp-only	dhcp-only application scene	slaac-only	slaac-only application scene	dhcp-slaac	combination application scene of dhcp-only and slaac-only
dhcp-only	dhcp-only application scene						
slaac-only	slaac-only application scene						
dhcp-slaac	combination application scene of dhcp-only and slaac-only						
Default	By default,disable SAVI application scene.						
Mode	Global Mode						
Usage Guide	<p>Enable SAVI application scene function.</p> <p>dhcp-only application scene only detects DHCPv6 packets and DAD NS packets of link-local ipv6 address to be IPv6 address with target field, it does not detect DAD NS packets of non-link-local address. slaac-only application scene detects DAD NS packets of all types. dhcp-slaac combination application scene detects all DHCPv6 and DAD NS packets. Disable all kinds of application scene detection function for SAVI by default.</p> <p>The no command disables the function.</p>						
Example	<p>Enable the specified dhcp-only application scene for SAVI.</p> <pre>Switch(config)#savi ipv6 dhcp-only enable</pre>						

### 13.13.10 savi ipv6 mac-binding-limit

Command	savi ipv6 mac-binding-limit <limit-num> no savi ipv6 mac-binding-limit
Parameter	limit-num                      set the ranging from 1 to 10, the default dynamic binding number is 32 for the same MAC address
Default	The default dynamic binding number is 32 for the same MAC address.
Mode	Global Mode
Usage Guide	Configure the dynamic binding number of the same MAC address. This command is used to prevent the exhaust attack of the dynamic binding entry for SAVI.  The no command restores the default value.
Example	Set the dynamic binding number to be 5 for the same MAC address.  Switch(config)#savi ipv6 mac-binding-limit 5

### 13.13.11 savi max-dad-delay

Command	savi max-dad-delay <max-dad-delay> no savi max-dad-delay
Parameter	max-dad-delay            set the ranging between 1 and 65535 seconds, its default value is 1 second
Default	Its default value is 1 second.
Mode	Global Mode
Usage Guide	Configure the dynamic binding at DETECTION state and send lifetime period of DAD NS packet detection. It is recommended to use the default value.  The no command restores the default value.
Example	Set the detection lifetime as 2 seconds.  Switch(config)#savi max-dad-delay 2

### 13.13.12 savi max-dad-prepare-delay

Command	savi max-dad-prepare-delay <max-dad-prepare-delay> no savi max-dad-prepare-delay
Parameter	max-dad-prepare-delay      set the ranging between 1 and 65535 seconds, its default value is 1 second
Default	Its default value is 1 second.
Mode	Global Mode
Usage Guide	Configure lifetime period of redetection for the dynamic binding. It is recommended to user the default value.  The no command restores the default value.
Example	Set the redetection lifetime as 2 seconds.  Switch(config)#savi max-dad-prepare-delay 2

### 13.13.13 savi max-slaac-life

Command	savi max-slaac-life <max-slaac-life> no savi max-slaac-life
Parameter	max-slaac-life            set the ranging between 1 and 31536000 seconds, its default value is 4 hours
Default	Its default value is 4 hours.
Mode	Global Mode
Usage Guide	Configure lifetime period of slaac dynamic binding at BOUND state.  The no command restores the default value.
Example	Configure lifetime period of slaac binding type as 2010 seconds at BOUND state.  Switch(config)#savi max-slaac-life 2000

### 13.13.14 savi timeout bind-protect

Command	savi timeout bind-protect <protect-time> no savi timeout bind-protect
Parameter	protect-time                    set the ranging between 1 and 300 seconds, its default value is 30 seconds
Default	Its default value is 30 seconds.
Mode	Global Mode
Usage Guide	<p>Configure the bind-protect lifetime period for a port after its state from up to down.</p> <p>After the configured lifetime period is overtime, the port is still at down state, the binding of this port will be deleted. If the port state is changed from down to up state during the configured lifetime period, the binding of the port will reset it as lifetime period of BOUND state. If the configured parameter is 0 second, all binding of the port will be deleted immediately.</p> <p>The no command restores the default value.</p>
Example	<p>Set bind-protect lifetime period to be 20 seconds.</p> <p>Switch(config)#savi timeout bind-protect 20</p>



### 13.13.15 show savi ipv6 check source binding

Command	show savi ipv6 check source binding [interface<if-name>]																												
Parameter	if-name                      port name such as interface ethernet 1/0/1																												
Default	None.																												
Mode	Admin Mode																												
Usage Guide	Show the global SAVI binding entry list.																												
Example	<p>Show the global binding state of SAVI.</p> <pre>Switch(config)#show savi ipv6 check source binding Static binding count: 0 Dynamic binding count: 3 Binding count: 3</pre> <table border="1"> <thead> <tr> <th>MAC</th> <th>IP</th> <th>VLAN</th> <th>Port</th> <th>Type</th> <th>State</th> <th>Expires</th> </tr> </thead> <tbody> <tr> <td>00-25-64-bb-8f-04</td> <td>fe80::225:64ff:febb:8f04</td> <td></td> <td>1</td> <td>Ethernet1/0/5</td> <td>slaac</td> <td>BOUND 14370</td> </tr> <tr> <td>00-25-64-bb-8f-04</td> <td>2001::13:1</td> <td></td> <td>1</td> <td>Ethernet1/0/5</td> <td>slaac</td> <td>BOUND 14370</td> </tr> <tr> <td>00-25-64-bb-8f-04</td> <td>2001::10:1</td> <td></td> <td>1</td> <td>Ethernet1/0/5</td> <td>slaac</td> <td>BOUND 14370</td> </tr> </tbody> </table>	MAC	IP	VLAN	Port	Type	State	Expires	00-25-64-bb-8f-04	fe80::225:64ff:febb:8f04		1	Ethernet1/0/5	slaac	BOUND 14370	00-25-64-bb-8f-04	2001::13:1		1	Ethernet1/0/5	slaac	BOUND 14370	00-25-64-bb-8f-04	2001::10:1		1	Ethernet1/0/5	slaac	BOUND 14370
MAC	IP	VLAN	Port	Type	State	Expires																							
00-25-64-bb-8f-04	fe80::225:64ff:febb:8f04		1	Ethernet1/0/5	slaac	BOUND 14370																							
00-25-64-bb-8f-04	2001::13:1		1	Ethernet1/0/5	slaac	BOUND 14370																							
00-25-64-bb-8f-04	2001::10:1		1	Ethernet1/0/5	slaac	BOUND 14370																							

# Chapter 14 Reliability

## 14.1 MRPP

### 14.1.1 control-vlan

<b>Command</b>	<code>control-vlan &lt;vid&gt;</code> <code>no control-vlan</code>
<b>parameter</b>	<b>vid</b> expresses control VLAN ID, the valid range is from 1 to 4094
<b>default</b>	-
<b>Mode</b>	MRPP ring mode
<b>Usage Guide</b>	<p>The command specifies Virtual VLAN ID of MRPP ring, currently it can be any value in 1-4094. To avoid confusion, it is recommended that the ID is non-configured VLAN ID, and the same to MRPP ring ID. In configuration of MRPP ring of the same MRPP loop switches, the control VLAN ID must be the same, otherwise the whole MRPP loop may not be able to work normally or form broadcast.</p> <p>The mrpp enable command must be start before the control-vlan command be used. If primary port, secondary port, node-mode and enable commands all be configured after control-vlan, the mrpp-ring function is enabled.</p>
<b>Example</b>	<p>Configure control VLAN of mrpp ring 4000 is 4000.</p> <pre>Switch(config)#mrpp ring 4000 Switch(mrpp-ring-4000)#control-vlan 4000</pre>

## 14.1.2 clear mrpp statistics

<b>Command</b>	<code>clear mrpp statistics [&lt;ring-id&gt;]</code>
<b>parameter</b>	<i>ring-id</i> is MRPP ring ID, the valid range is from 1 to 4096, if not specified ID, it clears all of MRPP ring statistic information.
<b>default</b>	-
<b>Mode</b>	Admin Mode.
<b>Usage Guide</b>	Clears statistics for MRPP packets received and transmitted by the MRPP loop.
<b>Example</b>	Clear switch MR P ring 4000 statistics. Switch#clear mrpp statistics 4000

### 14.1.3 enable

<b>Command</b>	<b>enable</b> <b>no enable</b>
<b>parameter</b>	-
<b>default</b>	Default disable MRPP ring
<b>Mode</b>	MRPP ring mode
<b>Usage Guide</b>	This command is used to enable the configured MRPP ring , " no enable" command disables this enabled MRPP ring.
<b>Example</b>	<pre> Configure MRPP ring 4000 of switch to primary node, and enable the MRPP ring. Switch(config)#mrpp enable Switch(config)#mrpp ring 4000 Switch(mrpp-ring-4000)#control-vlan 4000 Switch(mrpp-ring-4000)# node-mode master Switch(mrpp-ring-4000)#fail-timer 18 Switch(mrpp-ring-4000)#hello-timer 6 Switch(mrpp-ring-4000)#enable Switch(mrpp-ring-4000)#exit Switch(config)#in ethernet1/0/1 Switch(config-If-Ethernet1/0/1)#mrpp ring 4000 primary-port Switch(config)#in ethernet 1/0/3 Switch(config-If-Ethernet1/0/3)#mrpp ring 4000 secondary-port </pre>

## 14.1.4 errp domain

<b>Command</b>	<code>errp domain &lt;domain-id&gt;</code> <code>no errp domain &lt;domain-id&gt;</code>
<b>parameter</b>	<b><i>domain-id</i></b> domain ID of ERRP, the range between 1 and 15.
<b>default</b>	Default Unconfigured ID
<b>Mode</b>	Global mode
<b>Usage Guide</b>	If domain ID of ERRP needs to be configured, the compatible mode of ERRP should be enabled firstly. When executing this command, it should create a new ERRP domain if there is no ERRP domain. However, the no command is used to delete the corresponding domain ID of ERRP.
<b>Example</b>	Configure domain ID for ERRP globally. Switch(Config)#errp domain 1

### 14.1.5 fail-timer

<b>Command</b>	<b>fail-timer &lt;timer&gt;</b> <b>no fail-timer</b>
<b>parameter</b>	<b>timer</b> valid range is from 1 to 300s.
<b>default</b>	Default configure timer interval 3s
<b>Mode</b>	MRPP ring mode
<b>Usage Guide</b>	If primary node of MRPP ring doesn't receives Hello packet from primary port of primary node on configured fail timer, the whole loop is fail. Transfer node of MRPP doesn't need this timer and configure. To avoid time delay by transfer node forwards Hello packet, the value of fail timer must be more than or equal to 3 times of Hello timer. On time delay loop, it needs to modify the default and increase the value to avoid primary node doesn't receive Hello packet on fail timer due to time delay.
<b>Example</b>	Configure fail timer of MRPP ring 4000 to 10s. Switch(config)# mrpp ring 4000 Switch(mrpp-ring-4000)#fail-timer 10

## 14.1.6 hello-timer

<b>Command</b>	<b>hello-timer &lt;timer&gt;</b> <b>no hello-timer</b>
<b>parameter</b>	<b>timer</b> valid range is from 1 to 100s.
<b>default</b>	Default configuration timer interval is 1s.
<b>Mode</b>	MRPP ring mode
<b>Usage Guide</b>	The primary node of MRPP ring continuously sends Hello packet on configured Hello timer interval, if secondary port of primary node can receive this packet in configured period; the whole loop is normal, otherwise fail. Transfer node of MRPP ring doesn't need this timer and configure.
<b>Example</b>	Configure hello-timer of MRPP ring 4000 to 3 seconds. Switch(config)# mrpp ring 4000 Switch(mrpp-ring-4000)#hello-timer 3

## 14.1.7 mrpp eaps compatible

---

<b>Command</b>	<b>mrpp eaps compatible</b> <b>no mrpp eaps compatible</b>
<b>parameter</b>	-
<b>default</b>	Disable the compatible function of EAPS
<b>Mode</b>	Global mode
<b>Usage Guide</b>	If the compatible function of EAPS needs to be configured, MRPP protocol should be enabled firstly. When executing no mrpp eaps compatible command, it should ensure that the switch has enabled MRPP protocol.
<b>Example</b>	Enable the compatible function of EAPS globally Switch(Config)#mrpp enable Switch(Config)#mrpp eaps compatible



## 14.1.8 mrpp enable

<b>Command</b>	<b>mrpp enable</b> <b>no mrpp enable</b>
<b>parameter</b>	-
<b>default</b>	The system doesn't enable MRPP protocol module
<b>Mode</b>	Global Mode
<b>Usage Guide</b>	If it needs to configure MRPP ring, it enables MRPP protocol. Executing "no mrpp enable" command, it ensures to disable the switch enabled MRPP ring.
<b>Example</b>	Globally enable MRPP. Switch(config)#mrpp enable

## 14.1.9 mrpp errp compatible

<b>Command</b>	<b>mrpp errp compatible</b> <b>no mrpp errp compatible</b>
<b>parameter</b>	-
<b>default</b>	Disable the compatible function of ERRP.
<b>Mode</b>	Global mode
<b>Usage Guide</b>	If the compatible function of ERRP needs to be configured, MRPP protocol should be enabled firstly. Furthermore, the port with ERRP compatible mode should be configured as hybrid or trunk mode and allow the packets with Control Vlan information.
<b>Example</b>	Enable the compatible function of ERRP globally. Switch(Config)#mrpp enable Switch(Config)#mrpp errp compatible Switch(Config)#mrpp ring 2 Switch(mrpp-ring-2)#control-vlan 4000 Switch(config-if-ethernet1/51)#switchport mode hybrid Switch(config-if-ethernet1/51)#switchport hybrid allowed vlan 4000 tag Switch(config-if-ethernet1/52)#switchport mode hybrid Switch(config-if-ethernet1/52)#switchport hybrid allowed vlan 4000 tag

### 14.1.10 mrpp poll-time

<b>Command</b>	mrpp poll-time <20-2000>
<b>parameter</b>	<20-2000> Enquiry Time, Unit: ms
<b>default</b>	Default configuration ms 100
<b>Mode</b>	Global mode.
<b>Usage Guide</b>	Configure the query time to adjust the query interval of MRPP, the default interval is 100ms.
<b>Example</b>	Set the query time as 200ms. Switch(Config)# mrpp poll-time 200

### 14.1.11 mrpp ring

<b>Command</b>	<code>mrpp ring &lt;ring-id&gt;</code> <code>no mrpp ring &lt;ring-id&gt;</code>
<b>parameter</b>	<i>ring-id</i> is MRPP ring ID, the valid range is from 1 to 4096
<b>default</b>	Default does not configure ring id
<b>Mode</b>	Global mode
<b>Usage Guide</b>	If this MRPP ring doesn't exist it create new MRPP ring when executing the command, and then it enter MRPP ring mode. It needs to ensure disable this MRPP ring when executing the "no mrpp ring" command.
<b>Example</b>	Create a mrpp ring 100. Switch(config)#mrpp ring 100

### 14.1.12 mrpp ring primary-port

<b>Command</b>	<pre>mrpp ring &lt;ring-id&gt; primary-port {cos &lt;cos&gt;}</pre> <pre>no mrpp ring &lt;ring-id&gt; primary-port</pre>
<b>parameter</b>	<p><b>ring-id</b> is the ID of MRPP ring; range is &lt;1-4096&gt;.</p> <p><b>cos &lt;cos&gt;</b> is the cos value in the packet head; range is &lt;0-7&gt;</p>
<b>default</b>	There is no configuration and the cos value is 0 as default.
<b>Mode</b>	Port mode
<b>Usage Guide</b>	<p>The command specifies MRPP ring primary port. Primary node uses primary port to send Hello packet, secondary port is used to receive Hello packet from primary node. There are no difference on function between primary port and secondary of secondary node.</p>
<b>Example</b>	<pre>Configure the primary of MRPP ring 4000 to Ethernet 1/0/1</pre> <pre>Switch(Config)#interface ethernet 1/0/1</pre> <pre>Switch(config-If-Ethernet1/0/1)#mrpp ring 4000 primary-port</pre>

### 14.1.13 mrpp ring secondary-port

<b>Command</b>	<pre>mrpp ring &lt; ring-id &gt; secondary-port {cos &lt;cos&gt; } no mrpp ring &lt; ring-id &gt; secondary-port</pre>
<b>parameter</b>	<p><i>ring-id</i> is the ID of MRPP ring; range is &lt;1-4096&gt;.</p> <hr/> <p><b>cos &lt;cos&gt;</b> is the cos value in the packet head; range is &lt;0-7&gt;.</p> <hr/>
<b>default</b>	There is no configuration and the cos value is 0 as default
<b>Mode</b>	Port mode
<b>Usage Guide</b>	<p>The command specifies secondary port of MRPP ring. The primary node uses secondary port to receive Hello packet from primary node. There are no difference on function between primary port and secondary of secondary node.</p> <p>The mrpp enable command must be enabled before the control-vlan command be used. If primary port, secondary port, node-mode and enable commands all be configured after control-vlan, then the mrpp-ring function is enabled.</p>
<b>Example</b>	<pre>Configure secondary port of MRPP ring to 1/0/3. Switch(config)#interface ethernet1/0/3 Switch(Config-If-Ethernet1/0/3)#mrpp ring 4000 secondary-port</pre>

### 14.1.14 node-mode

<b>Command</b>	<code>node-mode {maser   transit}</code>
<b>parameter</b>	-
<b>default</b>	Default the node mode is secondary node.
<b>Mode</b>	MRPP ring mode
<b>Usage Guide</b>	This command configures the node type as the primary or secondary node.
<b>Example</b>	Configure the switch to primary node. MRPP ring 4000. Switch(config)# mrpp ring 4000 Switch(mrpp-ring-4000)#node-mode master

### 14.1.15 show mrpp

<b>Command</b>	<code>show mrpp [&lt;ring-id&gt;]</code>
<b>parameter</b>	<i>ring-id</i> is MRPP ring ID, the valid range is from 1 to 4096, if not specified ID, it display all of MRPP ring configuration.
<b>default</b>	-
<b>Mode</b>	Admin and Configuration Mode
<b>Usage Guide</b>	This command is used to view the MRPP ring configuration.
<b>Example</b>	Display configuration of MRPP ring 4000 of switch Switch# show mrpp 4000



## 14.1.16 show mrpp statistics

<b>Command</b>	<code>show mrpp statistics [&lt;ring-id&gt;]</code>
<b>parameter</b>	<i>ring-id</i> is MRPP ring ID, the valid range is from 1 to 4096, if not specified ID, it displays all of MRPP ring statistic information.
<b>default</b>	-
<b>Mode</b>	Admin and Configuration Mode.
<b>Usage Guide</b>	This command is used to display the statistics of the MRPP loop receiving and transmitting packets.
<b>Example</b>	Display statistic information of MRPP ring 4000 of switch. Switch# show mrpp statistic 4000

## 14.2 ULPP

### 14.2.1 clear ulpp flush counter interface

<b>Command</b>	<code>clear ulpp flush counter interface &lt;name&gt;</code>
<b>parameter</b>	<i>name</i> is the name of the port
<b>default</b>	-
<b>Mode</b>	Admin mode
<b>Usage Guide</b>	Clear the statistics of the packets.
<b>Example</b>	Clear the statistic information of the flush packets for the port1/0/1 Switch#clear ulpp flush counter interface e1/0/1

## 14.2.2 control vlan

<b>Command</b>	<code>control vlan &lt;integer&gt;</code> <code>no control vlan</code>
<b>parameter</b>	<i>integer</i> is the control VLAN ID that sends the flush packets, range from 1 to 4094.
<b>default</b>	The default is VLAN 1
<b>Mode</b>	ULPP group configuration mode.
<b>Usage Guide</b>	Configure the control VLAN of ULPP group. This VLAN must correspond the existent VLAN, after it is configured, this VLAN can't be deleted. It must belong to the VLAN protected by ULPP group to avoid flush packets loopback.
<b>Example</b>	Configure the sending control VLAN of ULPP group as 10. Switch(config)# ulpp group 20 Switch(ulpp-group-20)# control vlan 10

### 14.2.3 description

<b>Command</b>	<b>description &lt;string&gt;</b> <b>no description</b>
<b>parameter</b>	<b>string</b> is the name of ULPP group, the max number of the characters is 128.
<b>default</b>	Do not configure ULPP name by default.
<b>Mode</b>	ULPP group configuration mode.
<b>Usage Guide</b>	Configure the description string for the ULPP group. Delete description no command.
<b>Example</b>	Configure the description of ULPP group as switch. Switch(config)# ulpp group 20 Switch(ulpp-group-20)# description switch

## 14.2.4 flush {enable |disable} arp

<b>Command</b>	flush {enable disable} arp
<b>parameter</b>	-
<b>default</b>	By default, enable the sending function of the flush packets which are deleted by ARP.
<b>Mode</b>	ULPP group configuration mode.
<b>Usage Guide</b>	If configure this command, when the link is switched, it will not actively send the flush packets to notify the upstream device to delete the entries of ARP.
<b>Example</b>	Disable sending the flush packets of deleting ARP. Switch(config)# ulpp group 20 Switch(ulpp-group-20)# flush disable arp

## 14.2.5 flush {enable |disable} mac

<b>Command</b>	flush {enable disable}mac
<b>parameter</b>	-
<b>default</b>	By default, enable sending the flush packets of updating MAC address.
<b>Mode</b>	ULPP group configuration mode.
<b>Usage Guide</b>	If configure this command, when the link is switched, it will not actively send the flush packets to notify the upstream device to update the MAC address table.
<b>Example</b>	Disable sending the flush packets of updating MAC address. Switch(config)# ulpp group 20 Switch(ulpp-group-20)# flush disable mac

## 14.2.6 flush {enable |disable} mac-vlan

<b>Command</b>	flush {enable disable}mac-vlan
<b>parameter</b>	-
<b>default</b>	Disable.
<b>Mode</b>	ULPP group configuration mode
<b>Usage Guide</b>	If configure this command, when the link is switched, it will not actively send the flush packets to notify the upstream device to delete the dynamic unicast mac according to vlan.
<b>Example</b>	Disable sending the flush packets deleted by mac-vlan. Switch(config)#ulpp group 1 Switch(ulpp-group-1)#flush disable mac-vlan

## 14.2.7 preemption delay

<b>Command</b>	<code>preemption delay &lt;integer&gt;</code> <code>no preemption delay</code>
<b>parameter</b>	<i>integer</i> the preemption delay, range from 1 to 600, in second.
<b>default</b>	The default preemption delay is 30.
<b>Mode</b>	ULPP group configuration mode.
<b>Usage Guide</b>	The preemption delay is the delay time before the master port is preempted as the forwarding state, for avoiding the link oscillation in a short time. After the preemption mode is enabled, the preemption delay takes effect.
<b>Example</b>	Configure the preemption delay as 50s for ULPP group. Switch(config)# ulpp group 20 Switch(ulpp-group-20)# preemption delay 50



## 14.2.8 preemption mode

<b>Command</b>	<b>preemption mode</b> <b>no preemption mode</b>
<b>parameter</b>	-
<b>default</b>	Do not preempt.
<b>Mode</b>	ULPP group configuration mode.
<b>Usage Guide</b>	If the preemption mode configured by ULPP group, and the slave port is in forwarding state, and the master port is in the standby state, the master port will turn into the forwarding state and the slave port turn into the standby state after the preemption delay.
<b>Example</b>	Configure the preemption mode of ULPP group. Switch(config)# ulpp group 20 Switch(ulpp-group-20)# preemption mode

## 14.2.9 protect vlan-reference-instance

<b>Command</b>	<code>protect vlan-reference-instance &lt;instance-list&gt;</code> <code>no protect vlan-reference-instance &lt;instance-list&gt;</code>
<b>parameter</b>	<i>instance-list</i> is MSTP instance list, such as: i; j-k. The number of the instances is not limited in the list.
<b>default</b>	Do not protect any VLANs by default that means any instances are not quoted.
<b>Mode</b>	ULPP group configuration mode.
<b>Usage Guide</b>	Quote the instances of MSTP to protect the VLANs. The VLAN corresponds to this instance is at the forwarding state on one port of this group, and at the blocked state on another port of this group. Each ULPP group can quotes all instances of MSTP. And it can quotes the inexistent MSTP instances that means any VLANs are not protected, the different ULPP groups can't quote the same instance.
<b>Example</b>	Configure the protective VLAN quoted from instance 1 for ULPP group. Switch(config)# ulpp group 20 Switch(ulpp-group-20)# protect vlan-reference-instance 1

## 14.2.10 show ulpp flush counter interface

<b>Command</b>	show ulpp flush counter interface {ethernet <IFNAME>   <IFNAME>}
<b>parameter</b>	<b>IFNAME</b> is the name of the ports.
<b>default</b>	-
<b>Mode</b>	Admin mode.
<b>Usage Guide</b>	Show the statistic information of the flush packets, such as: the information of the flush packets number which has been received, the time information that receive the flush packets finally.
<b>Example</b>	Show the statistic information of the flush packets for ULPP group1. Switch# show ulpp flush counter interface e1/0/1 Received flush packets: 10

## 14.2.11 show ulpp flush-receive-port

<b>Command</b>	show ulpp flush-receive-port
<b>parameter</b>	-
<b>default</b>	-
<b>Mode</b>	Admin mode.
<b>Usage Guide</b>	displays the port that receives the flush packet, flush type, and control VLAN.
<b>Example</b>	Show the information that the port receives flush packets. Switch# show ulpp flush-receive-port ULPP flush-receive portlist: Portname Type Control Vlan ----- Ethernet1/0/1 ARP 1 Ethernet1/0/3 MAC 1;3;5-10

## 14.2.12 show ulpp group

<b>Command</b>	<b>show ulpp group [group-id]</b>
<b>parameter</b>	<b>group-id</b> Show the information of the specific ULPP group
<b>default</b>	By default, show the information of all ULPP groups which have been configured
<b>Mode</b>	Admin mode.
<b>Usage Guide</b>	Show the configuration information of ULPP groups which have been configured, such as: the state of the master port and the slave port, the preemption mode, the preemption delay, etc.
<b>Example</b>	<p>Show the configuration information of ULPP group1.</p> <pre>Switch# show ulpp group 1 ULPP flush-receive portlist: Portname      Type          Control Vlan ----- -----  Switch#show ulpp group 20 ULPP group 20 information: Description: switch Preemption mode: ON Preemption delay: 50s Control VLAN: 10 Flush packet: NONE Protected VLAN: Reference Instance 1 Member        Role          State          Track-cfm-level ----- -----</pre>

## 14.2.13 ulpp control vlan

<b>Command</b>	<code>ulpp control vlan &lt;vlan-list&gt;</code> <code>no ulpp control vlan &lt;vlan-list&gt;</code>
<b>parameter</b>	<b><i>vlan-list</i></b> specify the control VLAN list that receives the flush packets, such as: i; j-k. The number of VLANs in Each character string cannot exceed 100. The receiving control VLAN of the port can be added.
<b>default</b>	The default is VLAN 1.
<b>Mode</b>	Port mode
<b>Usage Guide</b>	Configure the receiving control VLAN for the port. This VLAN must correspond the existent VLAN, after it is configured, this VLAN can't be deleted.
<b>Example</b>	Configure the receiving control VLAN as 10 Switch(config)# interface ethernet 1/0/1 Switch(config-If-Ethernet1/0/1)# ulpp control vlan 10

## 14.2.14 ulpp flush {enable|disable} arp

<b>Command</b>	ulpp flush {[enable disable} arp
<b>parameter</b>	-
<b>default</b>	By default, disable receiving the flush packets of deleting ARP
<b>Mode</b>	Port mode.
<b>Usage Guide</b>	If this command is configured, then it will not receive the flush packets of deleting ARP.
<b>Example</b>	Disable receiving the flush packets of deleting ARP. Switch(config)# interface ethernet 1/0/1 Switch(config-If-Ethernet1/0/1)# ulpp flush disable arp

## 14.2.15 ulpp flush {enable|disable} mac

<b>Command</b>	ulpp flush {enable disable} mac
<b>parameter</b>	-
<b>default</b>	By default, disable receiving the flush packets of updating MAC address.
<b>Mode</b>	Port mode.
<b>Usage Guide</b>	If this command is configured, then it will not receive the flush packets of updating MAC address.
<b>Example</b>	Disable receiving the flush packets of updating MAC address. Switch(config)# interface ethernet 1/0/1 Switch(config-If-Ethernet1/0/1)# ulpp flush disable mac



## 14.2.16 ulpp flush {enable|disable} mac-vlan

<b>Command</b>	ulpp flush {enable disable} mac-vlan
<b>parameter</b>	-
<b>default</b>	Disable
<b>Mode</b>	Port mode.
<b>Usage Guide</b>	If enabling this function, forward the hardware of the flush packets with mac-vlan type received in port. It will not be analyzed.
<b>Example</b>	Disable receiving the flush packets deleted by mac-vlan of port. Switch(config)#interface e1/0/2 Switch(config-if-ethernet1/0/2)#ulpp flush disable mac-vlan

## 14.2.17 ulpp group

<b>Command</b>	<code>ulpp group &lt;integer&gt;</code> <code>no ulpp group &lt;integer&gt;</code>
<b>parameter</b>	<i>integer</i> is the ID of ULPP group, range from 1 to 48.
<b>default</b>	Any ULPP groups are not configured.
<b>Mode</b>	Global Mode.
<b>Usage Guide</b>	Create a ULPP group. If the group exists, enter the configuration mode of the ULPP group. no command delete ULPP group.
<b>Example</b>	Configure ulpp group 20 or enter the mode of ulpp group 20. Switch(config)# ulpp group 20 Switch(ulpp-group-20)#

### 14.2.18 ulpp group {master|slave}

<b>Command</b>	<b>14.3 ulpp group &lt;integer&gt; {master slave}</b>
	<b>14.4 no ulpp group &lt;integer&gt; {master slave}</b>
<b>parameter</b>	<i>integer</i> is the ID of ULPP group, range from 1 to 48.
<b>default</b>	There is no master port configured by default.
<b>Mode</b>	Port mode
<b>Usage Guide</b>	There is no sequence requirement for the master and slave port configuration in a group, but the protective VLANs must be configured before the member ports. Each group has only one master port, if the master port exists, then the configuration fail.
<b>Example</b>	Configure the master port of ULPP group. Switch(config)# interface ethernet 1/0/2 Switch(config-If-Ethernet1/0/2)# ulpp group 20 slave

## 14.3 ULSM

### 14.3.1 show ulsm group

<b>Command</b>	<b>show ulsm group [group-id]</b>
<b>parameter</b>	<b>group-id</b> the ID of ULSM group.
<b>default</b>	By default, show the information of all ULSM groups which have been configured
<b>Mode</b>	Admin Mode
<b>Usage Guide</b>	This command is used to display configuration information for ULSM groups.
<b>Example</b>	Show the configuration information of ULSM group1. Switch# show ulsm group 1

### 14.3.2 ulsm group

<b>Command</b>	<code>ulsm group &lt;group-id&gt;</code> <code>no ulsm group &lt;group-id&gt;</code>
<b>parameter</b>	<b><i>group-id</i></b> is the ID of ULSM group, range from 1 to 32.
<b>default</b>	There is no ULSM group configured by default.
<b>Mode</b>	Global Mode.
<b>Usage Guide</b>	This command is used to create a ULSM group. no command delete ULSM group.
<b>Example</b>	Create ULSM group 10. Switch(config)# ulsm group 10

### 14.3.3 ulsm group {uplink | downlink}

<b>Command</b>	<ulsm &lt;group-id&gt;="" downlink}<br="" group="" {uplink=""  =""></ulsm> no ulsm group <group-id>	
<b>parameter</b>	<b>group-id</b>	The ID of ULSM group, the range from 1 to 32.
	<b>uplink</b>	Configure the port as the uplink port
	<b>downlink</b>	Configure the port as the downlink port.
<b>default</b>	The port does not belong to any ULSM group	
<b>Mode</b>	Port Mode	
<b>Usage Guide</b>	Configure the uplink/downlink ports of ULSM group. Each ULSM group can configure 8 uplink ports and 16 downlink ports at most ◦	
<b>Example</b>	Configure port1/0/3 as the uplink port of ULSM group10. Switch(config)# interface ethernet 1/0/3 Switch(config-If-Ethernet1/0/3)# ulsm group 10 uplink	

# Chapter 15 Mirroring Configuration

## 15.1 Mirroring Configuration

### 15.1.1 monitor session source interface

<b>Command</b>	<pre>monitor session &lt;session&gt; source {interface &lt;interface-list&gt;   cpu} {rx  tx  both} no monitor session &lt;session&gt; source {interface &lt;interface-list&gt;   cpu}</pre>
<b>parameter</b>	<p><b>session</b> is the session number for the mirror. Currently only 1 is supported</p> <hr/> <p><b>interface-list</b> is the list of source interfaces of the mirror which can be separated by "-" and ",".</p> <hr/> <p><b>cpu</b> means the CPU on the board to be the source of the mirror for debugging. Datagram received by or sent by the CPU</p> <hr/> <p><b>rx</b> means to filter the datagram received by the interface</p> <hr/> <p><b>tx</b> for the datagram sent out</p> <hr/> <p><b>both</b> means both of income and outcome datagram</p> <hr/>
<b>default</b>	Default does not match any mirror source port
<b>Mode</b>	Global mode
<b>Usage Guide</b>	<p>This command is used to configure the source interfaces for the mirror. It is not restricted the source interface of the mirror on the switch. The source can be one interface, or can be multiple interfaces. Both of the income and outcome datagram can be mirrored, or they can be mirrored selectively. If no [rx   tx   both] is specified, both are made to be the default. When multiple interfaces are mirrored, the direction of the mirror can be different, but they should be configured separately.</p>
<b>Example</b>	<p>Configure to mirror the datagram sent out by interface 1/0/1-4 and to mirror the datagram received by interface1/0/5</p> <pre>Switch(config)#monitor session 1 source interface ethernet 1/0/1-4 tx Switch(config)#monitor session 1 source interface ethernet1/0/5 rx</pre>

## 15.1.2 monitor session source interface access-list

<b>Command</b>	<pre>monitor session &lt;session&gt; source {interface &lt;interface-list&gt;} access-list &lt;num&gt; {rx tx both} no monitor session &lt;session&gt; source {interface &lt;interface-list&gt;} access-list &lt;num&gt;</pre>												
<b>parameter</b>	<table border="1"> <tr> <td><b>session</b></td> <td>is the session number for the mirror. Currently only 1 is supported</td> </tr> <tr> <td><b>interface-list</b></td> <td>is the list of source interfaces of the mirror which can be separated by '-' and ';'</td> </tr> <tr> <td><b>num</b></td> <td>is the number of the access list</td> </tr> <tr> <td><b>rx</b></td> <td>means to filter the datagram received by the interface</td> </tr> <tr> <td><b>tx</b></td> <td>for the datagram sent out</td> </tr> <tr> <td><b>both</b></td> <td>means both of income and outcome datagram</td> </tr> </table>	<b>session</b>	is the session number for the mirror. Currently only 1 is supported	<b>interface-list</b>	is the list of source interfaces of the mirror which can be separated by '-' and ';'	<b>num</b>	is the number of the access list	<b>rx</b>	means to filter the datagram received by the interface	<b>tx</b>	for the datagram sent out	<b>both</b>	means both of income and outcome datagram
<b>session</b>	is the session number for the mirror. Currently only 1 is supported												
<b>interface-list</b>	is the list of source interfaces of the mirror which can be separated by '-' and ';'												
<b>num</b>	is the number of the access list												
<b>rx</b>	means to filter the datagram received by the interface												
<b>tx</b>	for the datagram sent out												
<b>both</b>	means both of income and outcome datagram												
<b>default</b>	Default not configured												
<b>Mode</b>	Global Mode												
<b>Usage Guide</b>	<p>This command is used to configure the source interfaces for the mirror. It is not restricted the source interface of the mirror on the switch. The source can be one interface, or can be multiple interfaces. For flow mirror, only datagram received can be mirrored. The parameters can be rx, tx, both. The related access list should be prepared before this command is issued. For how to configure the access list, please refer to ACL configuration. The mirror can only be created after the destination interface of the corresponding session has been configured. In the moment, the command only IP ACL and MAC ACL</p>												
<b>Example</b>	<p>Configure the mirror interface 1/0/6 to filter with access list 120 in session 1.</p> <pre>Switch(config)#monitor session 1 source interface 1/0/6 access-list 120 rx</pre>												



### 15.1.3 monitor session destination interface

<b>Command</b>	<pre>monitor session &lt;session&gt; destination interface &lt;interface-number&gt; no monitor session &lt;session&gt; destination interface &lt;interface-number&gt;</pre>				
<b>parameter</b>	<table border="0" style="width: 100%;"> <tr> <td style="width: 20%;"><b>session</b></td> <td>is the session number of the mirror, which is currently limited to 1-4</td> </tr> <tr> <td><b>interface-number</b></td> <td>is the destination interface of the mirror.</td> </tr> </table>	<b>session</b>	is the session number of the mirror, which is currently limited to 1-4	<b>interface-number</b>	is the destination interface of the mirror.
<b>session</b>	is the session number of the mirror, which is currently limited to 1-4				
<b>interface-number</b>	is the destination interface of the mirror.				
<b>default</b>	Default does not match mirror destination port				
<b>Mode</b>	Global mode				
<b>Usage Guide</b>	<p>Only four destination mirror interface is supported on the switch. To be mentioned. The interface which is configured as the destination of the mirror should not be configured as the member of the interface trunk. And the maximum throughput of the interface is recommended to be larger than the total throughput of the interfaces to be mirrored. If the destination is removed, the mirror path configured will be removed at the same time. And if the destination interface is reconfigured, the interface, CPU mirror path will be recovered. To be mentioned, the flow mirror can only be recovered after the destination of the interface is re-configured.</p>				
<b>Example</b>	<p>Configure interface 1/0/7 as the destination of the mirror.</p> <pre>Switch(config)#monitor session 1 destination interface ethernet 1/0/7</pre>				

## 15.1.4 show monitor

---

<b>Command</b>	show monitor
----------------	--------------

---

<b>parameter</b>	-
<b>default</b>	-

---

<b>Mode</b>	Admin Mode
-------------	------------

---

<b>Usage Guide</b>	This command is used to display the source and destination ports for the configured mirror sessions. For port mirroring, CPU mirroring, and flow mirroring, the mirror mode of the source can be displayed.
--------------------	---

---

<b>Example</b>	View configuration information for the current image. Switch#show monitor
----------------	--

## 15.1.5 mirror sample rate

<b>Command</b>	<code>monitor session &lt;session&gt; sample rate &lt;num&gt;</code> <code>no monitor session &lt;session&gt; sample rate</code>
<b>parameter</b>	<b>session</b> is mirror session value, and it supports 1 to 4 at moment
	<b>num</b> is sampled value, and ranges from 0 to 65535
<b>default</b>	Default Unconfigured Sampling Rate
<b>Mode</b>	Global Mode
<b>Usage Guide</b>	It represents how many packets mirror to destination port and it ranges from 0 to 65535, such as, when rate value equals 100, the first, 101, 201 packets can mirror destination port, when rate value equal 0, it does not configure samping rate, the default is notconfigured samping rate.
<b>Example</b>	The sampling rate for configuring mirror session 1 is 100. <code>switch(config)#monitor session 1 sample rate 100</code>

## 15.2 sFlow

### 15.2.1 sflow agent-address

<b>Command</b>	<code>sflow agent-address &lt;agent-address&gt;</code> <code>no sflow agent-address</code>
<b>parameter</b>	<b>agent-address</b> is the sample proxy IP address which is shown in dotted decimal notation
<b>default</b>	None default value
<b>Mode</b>	Global Mode
<b>Usage Guide</b>	For configuring sflow proxy address, The proxy address is used to mark the sample proxy which is similar to OSPF or the Router ID in the BGP. However it is not necessary to make the sFlow sample proxy work properly.
<b>Example</b>	Sample the proxy address at global mode. switch (config)#sflow agent-address 192.168.1.200

## 15.2.2 sflow analyzer

---

<b>Command</b>	<b>sflow analyzer sflowtrend</b> <b>no sflow analyzer sflowtrend</b>
<b>parameter</b>	-
<b>default</b>	Do not configure
<b>Mode</b>	Global Mode
<b>Usage Guide</b>	This command is used to configure sFlow analyzer, no the command disables the analyzer,Configure this command when using sFlowTrend.
<b>Example</b>	Enable sFlow analyzer. Switch(config)#sflow analyzer sflowtrend

### 15.2.3 sflow counter-interval

<b>Command</b>	<b>sflow counter-interval &lt;interval-value&gt;</b> <b>no sflow counter-interval</b>
<b>parameter</b>	<b>interval-value</b> is the value of the interval with a valid range of 20~120 and shown in second.
<b>default</b>	No default value
<b>Mode</b>	Port Mode
<b>Usage Guide</b>	If no statistic sampling interval is configured, there will not be any statistic sampling on the interface.
<b>Example</b>	Set the statistic sampling interval on the interface e1/0/1 to 20 seconds. Switch(Config-If-Ethernet1/0/1)#sflow counter-interval 20

## 15.2.4 sflow data-len

<b>Command</b>	<b>sflow data-len &lt;length-value&gt;</b> <b>no sflow data-len</b>
<b>parameter</b>	<b>length-value</b> is the value of the length with a value range of 500-1470
<b>default</b>	The value is 1400 by default.
<b>Mode</b>	Port Mode
<b>Usage Guide</b>	For configuring sflow packet length. When combining several samples to a sFlow group to be sent, the length of the group excluding the MAC head and IP head parts should not exceed the configured value.
<b>Example</b>	Configure the max length of the sFlow packet data to 1000. switch (Config-If-Ethernet1/0/2)#sflow data-len 1000

## 15.2.5 sflow destination

<b>Command</b>	<code>sflow destination &lt;collector-address&gt; [&lt;collector-port&gt;]</code> <code>no sflow destination</code>
<b>parameter</b>	<b><i>collector-address</i></b> is the IP address of the analyzer, shown in dotted decimal notation <b><i>collector-port</i></b> is the destination port of the sent sFlow packets.
<b>default</b>	The destination port of the sFlow packet is defaulted at 6343, and the analyzer has no default address.
<b>Mode</b>	Global Mode and Port Mode.
<b>Usage Guide</b>	If the analyzer address is configured at Port Mode, this IP address and port configured at Port Mode will be applied when sending the sample packet. Or else the address and port configured at global mode will be applied. The analyzer address should be configured to let the sFlow sample proxy work properly.
<b>Example</b>	Configure the analyzer address and port at global mode. switch (config)#sflow destination 192.168.1.200 1025



## 15.2.6 sflow header-len

<b>Command</b>	<code>sflow header-len &lt;length-value&gt;</code> <code>no sflow header-len</code>
<b>parameter</b>	<i>length-value</i> is the value of the length with a valid range of 32-256.
<b>default</b>	128 by default.
<b>Mode</b>	Port Mode.
<b>Usage Guide</b>	Configure the length of header packets copied in sFlow data sampling. no" form reduction default value for this command. If the packet sample can not be identified whether it is IPv4 or IPv6 when sent to the CPU, certain length of the head of the group has to be copied to the sFlow packet and sent out. The length of the copied content is configured by this command.
<b>Example</b>	Configure the length of the packet data head copied in the sFlow data sampling to 50. Switch(Config-If-Ethernet1/0/2)#sflow header-len 50

## 15.2.7 sflow priority

---

<b>Command</b>	<b>sflow priority &lt;priority-value&gt;</b> <b>no sflow priority</b>
<b>parameter</b>	<b>priority-value</b> is the priority value with a valid range of 0-3.
<b>default</b>	The default value is 0.
<b>Mode</b>	Global Mode.
<b>Usage Guide</b>	This command is used to set the priority of the sample message. When sample packet is sent to the CPU, it is recommended not to assign high priority for the packet so that regular receiving and sending of other protocol packet will not be interfered. The higher the priority value is set, the higher its priority will be.
<b>Example</b>	Configure the priority when sFlow receives packet from the hardware at global mode. switch (config)#sflow priority 1

## 15.2.8 sflow rate

<b>Command</b>	<b>sflow rate { input &lt;input-rate&gt;   output &lt;output-rate &gt;}</b> <b>no sflow rate [input   output]</b>	
<b>parameter</b>	<b>input-rate</b>	is the rate of ingress group sampling, the valid range is 1000~16383500.
	<b>output-rate</b>	is the rate of egress group sampling, the valid range is 1000~16383500
<b>default</b>	No default value.	
<b>Mode</b>	Port Mode.	
<b>Usage Guide</b>	<p>The traffic sampling will not be performed if the sampling rate is not configured on the port. And if the ingress group sampling rate is set to 10000, this indicates there will be one group be sampled every 10000 ingress groups.</p>	
<b>Example</b>	<p>Configure the ingress sample rate on port e1/0/1 to 10000 and the egress sample rate to 20000.</p> <pre>Switch(Config-If-Ethernet1/0/1)#sflow rate input 10000 Switch(Config-If-Ethernet1/0/1)#sflow rate output 20000</pre>	

## 15.2.9 show sflow

<b>Command</b>	<b>show sflow</b>
<b>parameter</b>	-
<b>default</b>	-
<b>Mode</b>	All Modes.
<b>Usage Guide</b>	This command is used to acknowledge the operation state of sFlow.

**Example** View sFlow configuration information.  
Switch#show sflow

```
Sflow version 1.2
Agent address is 172.16.1.100
Collector address have not configured
Collector port is 6343
Sampler priority is 2
Sflow DataSource: type 2, index 194(Ethernet1/0/2)
Collector address is 192.168.1.200
Collector port is 6343
Counter interval is 0
Sample rate is input 0, output 0
Sample packet max len is 1400
Sample header max len is 50
Sample version is 4
```

Display information	describe
Sflow version 1.2	Indicates sFlow version 1.2
Agent address is 172.16.1.100	sFlow agent address :172.16.1.1100
Collector address have not configured	the sFlow global analyzer address is not configured
Collector port is 6343	the sFlow global destination port is the defaulted 6343
Sampler priority is 2	The priority of sFlow when receiving packets from the hardware is 2.
Sflow DataSource: type 2, index 194(Ethernet1/0/1)	One sample proxy data source of the sFlow is the

		interface e1/0/1 and its type is 2 (Ethernet), the interface index is 194.
Collector address is 192.168.1.200		The analyzer address of the sampling address of the E1/0/1 interface is 192.168.1.200
Collector port is 6343		Default value of the port on E1/0/1 interface sampling proxy is 6343.
Counter interval is 20		The statistic sampling interval on e1/0/1 interface is 20 seconds
Sample rate is input 10000, output 0		The ingress traffic rate of e1/0/1 interface sampling proxy is 10000 and no egress traffic sampling will be performed
Sample packet max len is 1400		The length of the sFlow group data sent by the e1/0/1 interface should not exceed 1400 bytes.
Sample header max len is 50		The length of the packet data head copied in the data sampling of the e1/0/1 interface sampling proxy is 50
Sample version is 4		The datagram version of the sFlow group sent by the E1/0/1 interface sampling proxy is 4.

## 15.3 RSPAN Configuration

### 15.3.1 remote-span

---

<b>Command</b>	<b>remote-span</b> <b>no remote-span</b>
<b>parameter</b>	-
<b>default</b>	Not configured
<b>Mode</b>	VLAN Configuration Mode
<b>Usage Guide</b>	<p>This command is used to configure the existing VLAN as RSPAN VLAN. Dedicated RSPAN VLAN should be configured before RSPAN can function. When configuring RSPAN VLAN, it should be made sure that specialized VLAN, such as the default VLAN, dynamic VLAN, private VLAN, multicast VLAN, and layer 3 interface enabled VLAN, should not be configured as RSPAN VLAN. If any existing sessions are still working when RSPAN is disabled, these sessions will be still working regardless the configuration change. However, if any layer 3 interface is configure in the VLAN after RSPAN is disable, the existing RSPAN session will be stopped.</p>
<b>Example</b>	<p>RSPAN VLAN. VLAN 5 configured. Switch(Config-Vlan5)#remote-span</p>

## 15.3.2 monitor session remote vlan

<b>Command</b>	<code>monitor session &lt;session&gt; remote vlan &lt;vid&gt;</code> <code>no monitor session &lt;session&gt; remote vlan</code>				
<b>parameter</b>	<table border="1"><tr><td><i>session</i></td><td>session ID, range between 1~4</td></tr><tr><td><i>vid</i></td><td>The id of RSPAN VLAN</td></tr></table>	<i>session</i>	session ID, range between 1~4	<i>vid</i>	The id of RSPAN VLAN
<i>session</i>	session ID, range between 1~4				
<i>vid</i>	The id of RSPAN VLAN				
<b>default</b>	Not configured				
<b>Mode</b>	Global Mode				
<b>Usage Guide</b>	To configure local mirror session to RSPAN. The VLAN id is the RSPAN VLAN. The mirrored data grams will be attached with RSPAN tags.				
<b>Example</b>	Configure the remote vlan of mirror session 1 to 5. Switch(config)#monitor session 1 remote vlan 5				

### 15.3.3 monitor session reflector-port

<b>Command</b>	<code>monitor session &lt;session&gt; reflector-port &lt;interface-number&gt;</code> <code>no monitor session &lt;session&gt; reflector-port &lt;interface-number&gt;</code>	
<b>parameter</b>	<i>session</i>	Session ID, range between 1~4
	<i>interface-number</i>	Interface number
<b>default</b>	Not configured	
<b>Mode</b>	Global Mode.	

**Usage Guide**

This command configures the reflector port for the destination of mirror data grams, and disables the MAC learning function of the specified port. The configuration of reflector port is to change the mode of the local port from the destination port mode to be the reflector mode. Hence, the configuration of reflector port and the destination port are exclusive. The no command is used to restore the reflector port to normal port. The source port, in access or trunk mode, should not be added to RSPAN VLAN. When the reflector port is configured as springboard of CPU TX direction mirroring, it must be configured as TRUNK port and allows the RSPAN VLAN data passing, the Native VLAN should not be configured as RSPAN VLAN. After configured RSPAN, the vlan tag will be added on the packet of the egress mirror. It will cause the abort error frame on the reflection port, so the default MTU value of the switch should be modified.

**Example**

Configure port 1/0/5 as a reflection port.

```
Switch(config)#monitor session 1 reflector-port ethernet1/0/5
```



# Chapter 16 Network Time Management

## 16.1 SNTP

### 16.1.1 clock timezone

<b>Command</b>	<b>clock timezone WORD {add   subtract} &lt;0-23&gt; [&lt;0-59&gt;]</b> <b>no clock timezone WORD</b>								
<b>Parameter</b>	<table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="border-top: 1px solid black; border-bottom: 1px solid black;"><b>WORD</b></td> <td>timezone name, the length should not exceed 16</td> </tr> <tr> <td style="border-top: 1px solid black; border-bottom: 1px solid black;"><b>add   subtract</b></td> <td>the action of timezone</td> </tr> <tr> <td style="border-top: 1px solid black; border-bottom: 1px solid black;"><b>&lt;0-23&gt;</b></td> <td>the hour value</td> </tr> <tr> <td style="border-top: 1px solid black; border-bottom: 1px solid black;"><b>&lt;0-59&gt;</b></td> <td>the minute value</td> </tr> </table>	<b>WORD</b>	timezone name, the length should not exceed 16	<b>add   subtract</b>	the action of timezone	<b>&lt;0-23&gt;</b>	the hour value	<b>&lt;0-59&gt;</b>	the minute value
<b>WORD</b>	timezone name, the length should not exceed 16								
<b>add   subtract</b>	the action of timezone								
<b>&lt;0-23&gt;</b>	the hour value								
<b>&lt;0-59&gt;</b>	the minute value								
<b>Default</b>	None.								
<b>Mode</b>	Global Mode								
<b>Usage Guide</b>	<p>This command configures timezone in global mode.</p> <p>The timezone name is invalid with the blank, the hour and minute value must be in the specific range.</p> <p>The no command deletes the configured timezone.</p>								
<b>Example</b>	<p>Configure the action as add for the eighth timezone globally.</p> <p><b>Switch(config)#clock timezone aaa add 8</b></p>								

## 16.1.2 sntp polltime

<b>Command</b>	<code>sntp polltime &lt;interval&gt;</code> <code>no sntp polltime</code>
<b>Parameter</b>	<code>&lt;interval&gt;</code> is the interval value from 16 to 16284
<b>Default</b>	The default polltime is 64 seconds.
<b>Mode</b>	Global Mode
<b>Usage Guide</b>	Sets the interval for SNTP clients to send requests to NTP/SNTP.  The no command cancels the polltime sets and restores the default setting.
<b>Example</b>	Setting the client to send request to the server every 128 seconds.  <b>Switch(config)#sntp polltime128</b>

### 16.1.3 sntp server

<b>Command</b>	<pre>sntp server {&lt;ip-address&gt;   &lt;ipv6-address&gt;} [source {vlan &lt;vlan no&gt;   loopback &lt;loopback no&gt;}] [version &lt;version_no&gt;] no sntp server {&lt;ip-address&gt;   &lt;ipv6-address&gt;} [source {vlan &lt;vlan no&gt;   loopback &lt;loopback no&gt;}] [version &lt;version_no&gt;]</pre>										
<b>Parameter</b>	<table border="1"> <tr> <td><b>&lt;ip-address&gt;</b></td> <td>IPv4 address of time server</td> </tr> <tr> <td><b>&lt;ipv6-address&gt;</b></td> <td>IPv6 address of time server</td> </tr> <tr> <td><b>&lt;vlan no&gt;</b></td> <td>Virtual LAN number, ranging from 1 to 4094</td> </tr> <tr> <td><b>&lt;loopback no&gt;</b></td> <td>Loopback identifier, ranging from 1 to 1024</td> </tr> <tr> <td><b>&lt;version_no&gt;</b></td> <td>Version number, ranging from 1 to 4, the default is 4</td> </tr> </table>	<b>&lt;ip-address&gt;</b>	IPv4 address of time server	<b>&lt;ipv6-address&gt;</b>	IPv6 address of time server	<b>&lt;vlan no&gt;</b>	Virtual LAN number, ranging from 1 to 4094	<b>&lt;loopback no&gt;</b>	Loopback identifier, ranging from 1 to 1024	<b>&lt;version_no&gt;</b>	Version number, ranging from 1 to 4, the default is 4
<b>&lt;ip-address&gt;</b>	IPv4 address of time server										
<b>&lt;ipv6-address&gt;</b>	IPv6 address of time server										
<b>&lt;vlan no&gt;</b>	Virtual LAN number, ranging from 1 to 4094										
<b>&lt;loopback no&gt;</b>	Loopback identifier, ranging from 1 to 1024										
<b>&lt;version_no&gt;</b>	Version number, ranging from 1 to 4, the default is 4										
<b>Default</b>	By default,do not configure the time server.										
<b>Mode</b>	Global Mode										
<b>Usage Guide</b>	<p>Enable the specified time server as clock source</p> <p>The no command deletes the specified time server.</p>										
<b>Example</b>	<p>Configure the time server address as 1.1.1.1, specify the interface of the source address as vlan1:</p> <pre>Switch(config)#sntp server 1.1.1.1 source vlan 1</pre>										

## 16.1.4 show sntp

<b>Command</b>	<b>show sntp</b>
<b>Parameter</b>	<b>none</b> none
<b>Default</b>	None.
<b>Mode</b>	Admin/Global mode
<b>Usage Guide</b>	Displays current SNTP client configuration and server status.
<b>Example</b>	Displaying current SNTP configuration.  <b>Switch(config)#show sntp</b>

## 16.2 NTP

### 16.2.1 ntp access-group

<b>Command</b>	<code>ntp access-group server &lt;acl&gt;</code> <code>no ntp access-group server &lt;acl&gt;</code>
<b>Parameter</b>	<code>&lt;acl&gt;</code> ACL number, range is from 1 to 99
<b>Default</b>	Not configure the access control of NTP Server by default.
<b>Mode</b>	Global Mode
<b>Usage Guide</b>	To configure/cancel the access control list of NTP Server.  The no command delete configuration.
<b>Example</b>	To configure access control list 2 on the switch.  <b>Switch(config)#ntp access-group server 2</b>

## 16.2.2 ntp authenticate

<b>Command</b>	<b>ntp authenticate</b> <b>no ntp authenticate</b>
<b>Parameter</b>	<b>none</b> none
<b>Default</b>	By default, NTP authentication is cancelled.
<b>Mode</b>	Global Mode
<b>Usage Guide</b>	To enable/cancel NTP authentication function.  The no command cancel NTP authentication function.
<b>Example</b>	To enable NTP authentication function.  <b>Switch(config)#ntp authenticate</b>

### 16.2.3 ntp authentication-key

<b>Command</b>	<pre>ntp authentication-key &lt;key-id&gt; md5 &lt;value&gt; no ntp authentication-key &lt;key-id&gt;</pre>				
<b>Parameter</b>	<table border="1"> <tr> <td><b>&lt;key-id&gt;</b></td> <td>The id of key, range is from 1 to 4294967295</td> </tr> <tr> <td><b>&lt;value&gt;</b></td> <td>The value of key, range between 1 to 16 of ascii code</td> </tr> </table>	<b>&lt;key-id&gt;</b>	The id of key, range is from 1 to 4294967295	<b>&lt;value&gt;</b>	The value of key, range between 1 to 16 of ascii code
<b>&lt;key-id&gt;</b>	The id of key, range is from 1 to 4294967295				
<b>&lt;value&gt;</b>	The value of key, range between 1 to 16 of ascii code				
<b>Default</b>	The authentication key of NTP authentication is not configured by default.				
<b>Mode</b>	Global Mode				
<b>Usage Guide</b>	<p>To enable/cancel NTP authentication function, and defined NTP authentication key.</p> <p>The no command cancel NTP authentication function</p>				
<b>Example</b>	<p>To define the authentication key of NTP authentication, the key-id is 20, the md5 is abc.</p> <pre>Switch(config)#ntp authentication-key 20 md5 abc</pre>				

## 16.2.4 ntp broadcast server count

<b>Command</b>	<code>ntp broadcast server count &lt;number&gt;</code> <code>no ntp broadcast server count</code>
<b>Parameter</b>	<code>&lt;number&gt;</code> the max number of broadcast servers, 1-100
<b>Default</b>	The default max number of broadcast servers is 50.
<b>Mode</b>	Global Mode
<b>Usage Guide</b>	Set the max number of broadcast or multicast servers supported by the NTP client.  The no operation will cancel the configuration and restore the default value.
<b>Example</b>	Configure the max number of broadcast servers is 70 on the switch.  <b>Switch(config)#ntp broadcast server count 70</b>



## 16.2.5 ntp disable

<b>Command</b>	ntp disable no ntp disable
<b>Parameter</b>	none                      none
<b>Default</b>	By default, NTP function are enabled on all ports.
<b>Mode</b>	VLAN Configuration Mode
<b>Usage Guide</b>	To disable/enable the NTP function on port.  The no command disables the NTP function on the port.
<b>Example</b>	To disable the NTP function on vlan1 interface.  <b>Switch(config)# interface vlan 1</b> <b>Switch(config-if-Vlan1)#ntp disable</b>

## 16.2.6 ntp enable

<b>Command</b>	ntp enable ntp disable
<b>Parameter</b>	none                      none
<b>Default</b>	By default, global disable NTP function.
<b>Mode</b>	Global Mode
<b>Usage Guide</b>	To enable/disable NTP function globally.  Disable command global disable NTP function.
<b>Example</b>	Configure switch global enable NTP function.  <b>Switch(config)# ntp enable</b>

## 16.2.7 ntp ipv6 multicast client

<b>Command</b>	<code>ntp ipv6 multicast client</code> <code>no ntp ipv6 multicast client</code>
<b>Parameter</b>	<code>none</code> <code>none</code>
<b>Default</b>	By default,Interface does not receive IPv6 NTP multicast packets.
<b>Mode</b>	VLAN Configuration mode
<b>Usage Guide</b>	Configure the specified interface to receive IPv6 NTP multicast packets  The no command will cancels the specified interface to receive IPv6 NTP multicast packets.
<b>Example</b>	Enable the function for receiving IPv6 NTP multicast packets on vlan1 interface.  <b>Switch(config)# interface vlan 1</b> <b>Switch(config-if-Vlan1)#ntp ipv6 multicast client</b>

## 16.2.8 ntp multicast client

<b>Command</b>	ntp multicast client no ntp multicast client
<b>Parameter</b>	none                      none
<b>Default</b>	By default,Interface does not receive NTP multicast packets.
<b>Mode</b>	VLAN Configuration mode
<b>Usage Guide</b>	Configure the specified interface to receive NTP multicast packets.  The no command will cancels the specified interface to receive NTP multicast packets.
<b>Example</b>	Enable the function for receiving NTP multicast packets on vlan1 interface.  <b>Switch(config)# interface vlan 1</b> <b>Switch(config-if-Vlan1)#ntp multicast client</b>

## 16.2.9 ntp server

<b>Command</b>	<pre>ntp server {&lt;ip-address&gt;   &lt;ipv6-address&gt;} [version &lt;version_no&gt;] [key &lt;key-id&gt;] no ntp server {&lt;ip-address&gt; &lt;ipv6-address&gt;}</pre>								
<b>Parameter</b>	<table border="1"> <tr> <td>&lt;ip-address&gt;</td> <td>IPv4 address of time server</td> </tr> <tr> <td>&lt;ipv6-address&gt;</td> <td>IPv6 address of time server</td> </tr> <tr> <td>&lt;version_no&gt;</td> <td>The version number of server, range is from 1 to 4, default is 4</td> </tr> <tr> <td>&lt;key-id&gt;</td> <td>The key id</td> </tr> </table>	<ip-address>	IPv4 address of time server	<ipv6-address>	IPv6 address of time server	<version_no>	The version number of server, range is from 1 to 4, default is 4	<key-id>	The key id
<ip-address>	IPv4 address of time server								
<ipv6-address>	IPv6 address of time server								
<version_no>	The version number of server, range is from 1 to 4, default is 4								
<key-id>	The key id								
<b>Default</b>	By default,disable.								
<b>Mode</b>	Global Mode								
<b>Usage Guide</b>	<p>To enable specified time server of time source.</p> <p>The no form of this command cancels the specified time server of time source.</p>								
<b>Example</b>	<p>To configure time server address as 1.1.1.1 on switch.</p> <pre>Switch(config)# ntp server 1.1.1.1</pre>								

## 16.2.10 ntp syn-interval

<b>Command</b>	<code>ntp syn-interval &lt;1-3600&gt;</code> <code>no ntp syn-interval</code>
<b>Parameter</b>	<code>&lt;1-3600&gt;</code> the request packet sending interval of ntp client as 1s-3600s
<b>Default</b>	By default,64s interval.
<b>Mode</b>	Global Mode
<b>Usage Guide</b>	<p>Configure the request packet sending interval of ntp client as 1s-3600s.</p> <p>For responding the risk of ntp adjusting the system time under the high latency network, ntp client will select the time information with the smallest latency for the system time synchronization after sent 8 ntp time requisitions. So at the default configuration, ntp client sends the requisition packet once every 64s, after 8 times, it will adjust the time. It means to adjust the system time every 8 minutes. If user wants to configure the interval, such as one hour, user should adjust the packet sending interval as <math>450(3600/8)</math> s.</p> <p>The no command recovers to be the default value of 64s.</p>
<b>Example</b>	<p>Configure to adjust the system time once an hour, and the packet sending time is 450s.</p> <pre>Switch(config)# ntp syn-interval 450</pre>

## 16.2.11 ntp trusted-key

<b>Command</b>	<code>ntp trusted-key &lt;key-id&gt;</code> <code>no ntp trusted-key &lt;key-id&gt;</code>
<b>Parameter</b>	<b>&lt;key-id&gt;</b> The id of key, range is from 1 to 4294967295
<b>Default</b>	Trusted key is not configured by default.
<b>Mode</b>	Global Mode
<b>Usage Guide</b>	To configure the trusted key.  The no command cancels the trusted key.
<b>Example</b>	To configure the specified key 20 to trusted key.  <b>Switch(config)# ntp trusted-key 20</b>

## 16.2.12 show ntp status

<b>Command</b>	<b>show ntp status</b>
<b>Parameter</b>	none                      none
<b>Default</b>	None.
<b>Mode</b>	Admin/Global Mode
<b>Usage Guide</b>	To display time synchronization status, include synchronized or not, layers, address of time source and so on.
<b>Example</b>	Display time synchronization status.  <b>Switch(config)# show ntp status</b> Clock status: synchronized Clock stratum: 3 Reference clock server: 1.1.1.2 Clock offset: 0.010 s Root delay: 0.012 ms Root dispersion: 0.000 ms Reference time: TUE JAN 03 01:27:24 2006



## 16.2.13 show ntp session

<b>Command</b>	<b>show ntp session [&lt;ip-address&gt;   &lt;ipv6-address&gt;]</b>				
<b>Parameter</b>	<table border="1"> <tr> <td><b>&lt;ip-address&gt;</b></td> <td>The IPv4 address of some specifics configured time server</td> </tr> <tr> <td><b>&lt;ipv6-address&gt;</b></td> <td>The IPv6 address of some specifics configured time server</td> </tr> </table>	<b>&lt;ip-address&gt;</b>	The IPv4 address of some specifics configured time server	<b>&lt;ipv6-address&gt;</b>	The IPv6 address of some specifics configured time server
<b>&lt;ip-address&gt;</b>	The IPv4 address of some specifics configured time server				
<b>&lt;ipv6-address&gt;</b>	The IPv6 address of some specifics configured time server				
<b>Default</b>	None.				
<b>Mode</b>	Admin/Global Mode				
<b>Usage Guide</b>	To display the information of all NTP session or one specific session, include server ID, server layer, and the local offset according to server. (The symbol * means this server is the selected local time source)				
<b>Example</b>	<p>To display the information of all NTP session.</p> <pre> Switch(config)# show ntp session   server  stream  type  rootdelay  rootdispersion  trustlevel *  1.1.1.2  2    unicast  0.010s      0.002s         10    2.2.2.2  3    unicast  0.005s      0.000s         10 </pre>				

## 16.3 Summer Time

### 16.3.1 clock summer-time absolute

<b>Command</b>	<pre>clock summer-time &lt;word&gt; absolute &lt;HH:MM&gt; &lt;YYYY.MM.DD&gt; &lt;HH:MM&gt; &lt;YYYY.MM.DD&gt; [&lt;offset&gt;] no clock summer-time</pre>												
<b>Parameter</b>	<table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="border: none;"><b>&lt;word&gt;</b></td> <td style="border: none;">the time zone name of summer time</td> </tr> <tr> <td style="border: none;"><b>&lt;HH:MM&gt;</b></td> <td style="border: none;">the start time, the format is hour (from 0 to 23):minute (from 0 to 59)</td> </tr> <tr> <td style="border: none;"><b>&lt;YYYY.MM.DD&gt;</b></td> <td style="border: none;">the start date, the format is year (from 1970 to 2038).month (from 1 to 12).date (from 1 to 31)</td> </tr> <tr> <td style="border: none;"><b>&lt;HH:MM&gt;</b></td> <td style="border: none;">the end time, the format is hour (from 0 to 23):minute (from 0 to 59)</td> </tr> <tr> <td style="border: none;"><b>&lt;YYYY.MM.DD&gt;</b></td> <td style="border: none;">the end date, the format is year (from 1970 to 2038).month (from 1 to 12).date (from 1 to 31)</td> </tr> <tr> <td style="border: none;"><b>&lt;offset&gt;</b></td> <td style="border: none;">the time offset, the range from 1 to 1440, unit is minute, default value is 60 minutes</td> </tr> </table>	<b>&lt;word&gt;</b>	the time zone name of summer time	<b>&lt;HH:MM&gt;</b>	the start time, the format is hour (from 0 to 23):minute (from 0 to 59)	<b>&lt;YYYY.MM.DD&gt;</b>	the start date, the format is year (from 1970 to 2038).month (from 1 to 12).date (from 1 to 31)	<b>&lt;HH:MM&gt;</b>	the end time, the format is hour (from 0 to 23):minute (from 0 to 59)	<b>&lt;YYYY.MM.DD&gt;</b>	the end date, the format is year (from 1970 to 2038).month (from 1 to 12).date (from 1 to 31)	<b>&lt;offset&gt;</b>	the time offset, the range from 1 to 1440, unit is minute, default value is 60 minutes
<b>&lt;word&gt;</b>	the time zone name of summer time												
<b>&lt;HH:MM&gt;</b>	the start time, the format is hour (from 0 to 23):minute (from 0 to 59)												
<b>&lt;YYYY.MM.DD&gt;</b>	the start date, the format is year (from 1970 to 2038).month (from 1 to 12).date (from 1 to 31)												
<b>&lt;HH:MM&gt;</b>	the end time, the format is hour (from 0 to 23):minute (from 0 to 59)												
<b>&lt;YYYY.MM.DD&gt;</b>	the end date, the format is year (from 1970 to 2038).month (from 1 to 12).date (from 1 to 31)												
<b>&lt;offset&gt;</b>	the time offset, the range from 1 to 1440, unit is minute, default value is 60 minutes												
<b>Default</b>	By default, there is no summer time range.												
<b>Mode</b>	Global Mode												
<b>Usage Guide</b>	<p>Configure summer time range, the time in this range is summer time.</p> <p>This command sets the absolute start and end time for summer time. When the system time reaches to the start time point of summer time, the clock is changed and increase &lt;offset&gt; value, the system enters summer time. When the system time reaches to the end time point of summer time, the clock is changed again, subtract &lt;offset&gt; value from system time, the system finishes summer time. Note: the end time should be bigger than the start time for configuring summer time.</p> <p>The no command deletes the configuration.</p>												
<b>Example</b>	<p>Configure the time range of summer time at 12:10 from april 6th to august 6th in 2010, offset value as 70 minutes, summer time is named as aaa.</p> <pre>Switch(config)#clock summer-time aaa absolute 12:10 2010.4.6 12:10 2010.8.6 70</pre>												

## 16.3.2 clock summer-time recurring

---

**Command**                    **clock summer-time <word> recurring <HH:MM> <MM.DD> <HH:MM> <MM.DD> [<offset>]**  
**no clock summer-time**

---

<b>Parameter</b>	<b>&lt;word&gt;</b>	the time zone name of summer time
	<b>&lt;HH:MM&gt;</b>	the start time, the format is hour (from 0 to 23):minute (from 0 to 59)
	<b>&lt;MM.DD&gt;</b>	the start date, the format is month(from 1 to 12).date(from 1 to 31)
	<b>&lt;HH:MM&gt;</b>	the end time, the format is hour(from 0 to 23):minute(from 0 to 59)
	<b>&lt;MM.DD&gt;</b>	the end date, the format is month(from 1 to 12).date(from 1 to 31)
	<b>&lt;offset&gt;</b>	the time offset, the range from 1 to 1440, unit is minute, default value is 60 minutes.

---

**Default**                    By default,there is no summer time range.

---

**Mode**                    Global Mode

---

**Usage Guide**            Configure the recurrent summer time range, the time in this range is summer time. This command sets the start and the end time for the recurrent summer time. When the system time reaches to the start time point of summer time, the clock is changed and increase <offset> value, the system enters summer time. When the system time reaches to the end time point of summer time, the clock is changed again, subtract <offset> value from system time, the system finishes summer time. There is no relation between the recurrent summer time to the year, the system clock will be changed when it reaches to the start and the end time point of summer time year after year. This command supports the summer time of southern hemisphere.

The no command delete summer time configuration.

---

**Example**                    Configure the time range of summer time at 12:10 from april 6th to august 6th year after year, offset value as 70 minutes, summer time is named as aaa.

**Switch(config)#clock summer-time aaa recurring 12:10 4.6 12:10 8.6 70**

---

### 16.3.3 clock summer-time recurring

<b>Command</b>	<p>clock summer-time &lt;word&gt; recurring&lt;HH:MM&gt; &lt;week&gt; &lt;day&gt; &lt;month&gt;&lt;HH:MM&gt; &gt; &lt;week&gt; &lt;day&gt; &lt;month&gt; [&lt;offset&gt;]</p> <p>no clock summer-time</p>																				
<b>Parameter</b>	<table border="1"> <tr> <td style="border-right: 1px solid black;"><b>&lt;word&gt;</b></td> <td>the time zone name of summer time</td> </tr> <tr> <td style="border-right: 1px solid black;"><b>&lt;HH:MM&gt;</b></td> <td>the start time, the format is hour(from 0 to 23):minute(from 0 to 59)</td> </tr> <tr> <td style="border-right: 1px solid black;"><b>&lt;week&gt;</b></td> <td>the week from 1 to 4, first or last</td> </tr> <tr> <td style="border-right: 1px solid black;"><b>&lt;day&gt;</b></td> <td>the week value, the value as "Sun", "Mon", "Tue", "Wed", "Thu", "Fri", "Sat"</td> </tr> <tr> <td style="border-right: 1px solid black;"><b>&lt;month&gt;</b></td> <td>the month, the value as "Jan", "Feb", "Mar", "Apr", "May", "Jun", "Jul", "Aug", "Sep", "Oct", "Nov", "Dec"</td> </tr> <tr> <td style="border-right: 1px solid black;"><b>&lt;HH:MM&gt;</b></td> <td>the end time, the format is hour(from 0 to 23):minute(from 0 to 59)</td> </tr> <tr> <td style="border-right: 1px solid black;"><b>&lt;week&gt;</b></td> <td>the week from 1 to 4, first or last</td> </tr> <tr> <td style="border-right: 1px solid black;"><b>&lt;day&gt;</b></td> <td>the week value, the value as "Sun", "Mon", "Tue", "Wed", "Thu", "Fri", "Sat"</td> </tr> <tr> <td style="border-right: 1px solid black;"><b>&lt;month&gt;</b></td> <td>the month, the value as "Jan", "Feb", "Mar", "Apr", "May", "Jun", "Jul", "Aug", "Sep", "Oct", "Nov", "Dec"</td> </tr> <tr> <td style="border-right: 1px solid black;"><b>&lt;offset&gt;</b></td> <td>the time offset, the range from 1 to 1440, unit is minute, default value is 60 minutes</td> </tr> </table>	<b>&lt;word&gt;</b>	the time zone name of summer time	<b>&lt;HH:MM&gt;</b>	the start time, the format is hour(from 0 to 23):minute(from 0 to 59)	<b>&lt;week&gt;</b>	the week from 1 to 4, first or last	<b>&lt;day&gt;</b>	the week value, the value as "Sun", "Mon", "Tue", "Wed", "Thu", "Fri", "Sat"	<b>&lt;month&gt;</b>	the month, the value as "Jan", "Feb", "Mar", "Apr", "May", "Jun", "Jul", "Aug", "Sep", "Oct", "Nov", "Dec"	<b>&lt;HH:MM&gt;</b>	the end time, the format is hour(from 0 to 23):minute(from 0 to 59)	<b>&lt;week&gt;</b>	the week from 1 to 4, first or last	<b>&lt;day&gt;</b>	the week value, the value as "Sun", "Mon", "Tue", "Wed", "Thu", "Fri", "Sat"	<b>&lt;month&gt;</b>	the month, the value as "Jan", "Feb", "Mar", "Apr", "May", "Jun", "Jul", "Aug", "Sep", "Oct", "Nov", "Dec"	<b>&lt;offset&gt;</b>	the time offset, the range from 1 to 1440, unit is minute, default value is 60 minutes
<b>&lt;word&gt;</b>	the time zone name of summer time																				
<b>&lt;HH:MM&gt;</b>	the start time, the format is hour(from 0 to 23):minute(from 0 to 59)																				
<b>&lt;week&gt;</b>	the week from 1 to 4, first or last																				
<b>&lt;day&gt;</b>	the week value, the value as "Sun", "Mon", "Tue", "Wed", "Thu", "Fri", "Sat"																				
<b>&lt;month&gt;</b>	the month, the value as "Jan", "Feb", "Mar", "Apr", "May", "Jun", "Jul", "Aug", "Sep", "Oct", "Nov", "Dec"																				
<b>&lt;HH:MM&gt;</b>	the end time, the format is hour(from 0 to 23):minute(from 0 to 59)																				
<b>&lt;week&gt;</b>	the week from 1 to 4, first or last																				
<b>&lt;day&gt;</b>	the week value, the value as "Sun", "Mon", "Tue", "Wed", "Thu", "Fri", "Sat"																				
<b>&lt;month&gt;</b>	the month, the value as "Jan", "Feb", "Mar", "Apr", "May", "Jun", "Jul", "Aug", "Sep", "Oct", "Nov", "Dec"																				
<b>&lt;offset&gt;</b>	the time offset, the range from 1 to 1440, unit is minute, default value is 60 minutes																				
<b>Default</b>	By default,there is no summer time range.																				
<b>Mode</b>	Global Mode																				
<b>Usage Guide</b>	<p>Configure the recurrent summer time range, the time in this range is summer time.</p> <p>This command sets the start and end time for the recurrent summer time flexibly. When the system time reaches to the start time point of summer time, the clock is changed and increase &lt;offset&gt; value, the system enters summer time. When the system time reaches to the end time point of summer time, the clock is changed again, subtract &lt;offset&gt; value from system time, the system finishes summer time. There is no relation between the recurrent summer time to the year, the system clock will be changed when it reaches to the start and the end time point of summer time year after year. This command supports summer time of southern hemisphere.</p> <p>The no command delete summer time configuration.</p>																				

---

**Example**

Configure summer time at 12:10 from the first Monday of april to the last Saturday of august year after year, offset value as 70 minutes, summer time is named as aaa.

```
Switch(config)#clock summer-time aaa recurring 12:10 1 mon apr 12:10 last sat aug  
70
```

---

# Chapter 17 Debugging and Diagnosis

## 17.1 SHOW

### 17.1.1 clear history all-users

<b>Syntax</b>	clear history all-users
<b>Parameter</b>	none
<b>Default</b>	none
<b>Mode</b>	Admin mode
<b>Usage</b>	Using this command can clear the command history of all users.
<b>Example</b>	Switch#clear history all-users

## 17.1.2 clear logging

<b>Syntax</b>	<code>clear logging sdram</code>
<b>Parameter</b>	none
<b>Default</b>	none
<b>Mode</b>	Admin mode
<b>Usage</b>	When the old information in the log buffer zone is no longer concerned, we can use this command to clear all the information.
<b>Example</b>	Clear all information in the log buffer zone sdram. <code>Switch#clear logging sdram</code>

### 17.1.3 history all-users max-length

<b>Syntax</b>	<b>history all-users max-length &lt;count&gt;</b>
<b>Parameter</b>	<b>&lt;count&gt;</b> the command history number can be saved, ranging from 100 to 1000
<b>Default</b>	The system can save 100 recent command history of all users at best by default
<b>Mode</b>	Global mode
<b>Usage</b>	using this command can set the max command history number
<b>Example</b>	Switch#config Switch(config)#history all-users max-length 500



## 17.1.4 logging

<b>Syntax</b>	<code>logging { &lt;ipv4-addr&gt;   &lt;ipv6-addr&gt; } [facility &lt;local-number&gt;] [level &lt;severity&gt;]</code> <code>no logging { &lt;ipv4-addr&gt;   &lt;ipv6-addr&gt; } [facility &lt;local-number&gt;]</code>								
<b>Parameter</b>	<table border="1"> <tr> <td><code>&lt;ipv4-addr&gt;</code></td> <td>IPv4 address of the host</td> </tr> <tr> <td><code>&lt;ipv6-addr&gt;</code></td> <td>IPv6 address of the host</td> </tr> <tr> <td><code>&lt;local-number&gt;</code></td> <td>recording equipment of the host with a valid range of local0~local7, which is in accordance with the facility defined in the RFC3164</td> </tr> <tr> <td><code>&lt;severity&gt;</code></td> <td>severity threshold of the log information severity level. The rule of the log information output is explained as follows: only those with a level equal to or higher than the threshold will be outputted. For detailed description on the severity please refer to the operation manual.</td> </tr> </table>	<code>&lt;ipv4-addr&gt;</code>	IPv4 address of the host	<code>&lt;ipv6-addr&gt;</code>	IPv6 address of the host	<code>&lt;local-number&gt;</code>	recording equipment of the host with a valid range of local0~local7, which is in accordance with the facility defined in the RFC3164	<code>&lt;severity&gt;</code>	severity threshold of the log information severity level. The rule of the log information output is explained as follows: only those with a level equal to or higher than the threshold will be outputted. For detailed description on the severity please refer to the operation manual.
<code>&lt;ipv4-addr&gt;</code>	IPv4 address of the host								
<code>&lt;ipv6-addr&gt;</code>	IPv6 address of the host								
<code>&lt;local-number&gt;</code>	recording equipment of the host with a valid range of local0~local7, which is in accordance with the facility defined in the RFC3164								
<code>&lt;severity&gt;</code>	severity threshold of the log information severity level. The rule of the log information output is explained as follows: only those with a level equal to or higher than the threshold will be outputted. For detailed description on the severity please refer to the operation manual.								
<b>Default</b>	No log information output to the log host by default. The default recorder of the log host is the local0; the default severity level is warnings.								
<b>Mode</b>	Global mode								
<b>Usage</b>	<p>The command is used to configure the output channel of the log host. The “no” form of this command will disable the output at the log host output channel.</p> <p>Only when the log host is configured by the logging command, this command will be available. We can configure many IPv4 and IPv6 log hosts.</p>								
<b>Example</b>	<p>Send the log information with a severity level equal to or higher than warning to the log server with an IPv4 address of 100.100.100.5, and save to the log recording equipment local1.</p> <pre>Switch#config Switch(config)#logging 100.100.100.5 facility local1 level warnings</pre>								

## 17.1.5 logging executed-commands

<b>Syntax</b>	<b>logging executed-commands {enable   disable}</b>
<b>Parameter</b>	<b>none</b>
<b>Default</b>	Disable state.
<b>Mode</b>	Global mode
<b>Usage</b>	After enable this command, the commands executed by user at the console, telnet or ssh terminal will record the log, so it should be used with the logging LOGHOST command.
<b>Example</b>	Enable the command and send the commands executed by user into log host (10.1.1.1) Switch#config Switch(config)#logging 10.1.1.1 Switch(config)#logging executed-commands enable

## 17.1.6 logging loghost sequence-number

<b>Syntax</b>	<b>logging loghost sequence-number</b> <b>no logging loghost sequence-number</b>
<b>Parameter</b>	<b>none</b>
<b>Default</b>	Do not include the sequence-number.
<b>Mode</b>	Global mode
<b>Usage</b>	Add the loghost sequence-number for the log; the no command does not include the loghost sequence-number. Use logging command to configure the loghost before this command is set.
<b>Example</b>	Open the loghost sequence-number Switch#config Switch(config) #logging loghost sequence-number

### 17.1.7 logging source-ip

<b>Syntax</b>	<code>logging source-ip { &lt;A.B.C.D&gt;   &lt;X:X::X:X&gt; }</code>
<b>Parameter</b>	<code>&lt;ipv4-addr&gt;</code> IPv4 address of the host
	<code>&lt;ipv6-addr&gt;</code> IPv6 address of the host
<b>Default</b>	None0000
<b>Mode</b>	Global mode
<b>Usage</b>	Appoint the source IP address of the log packet which is sent to the log server, the ipv4 or ipv6 addresses can be configured. After configured this command, the log information sent to the server has the IP address; if this command is not configured, the log information does not have the IP address.
<b>Example</b>	Configure the source IP address of the log packet which is sent to the log server. Switch#config Switch(config)#logging source-ip 2010::10

## 17.1.8 ping

<b>Syntax</b>	<code>ping [[src &lt;source-address&gt; ] { &lt;destination-address&gt;   host &lt;hostname&gt; }]</code>
<b>Parameter</b>	<p><b>&lt;source-address&gt;</b>      <b>&lt;source-address&gt;</b> is the source IP address where the ping command is issued, with IP address in dotted decimal format.</p> <p><b>&lt;destination-address&gt;</b>      <b>&lt;destination-address&gt;</b> is the target IP address of the ping command, with IP address in dotted decimal format</p> <p><b>&lt;hostname&gt;</b>      <b>&lt;hostname&gt;</b> is the target host name of the ping command, which should not exceed 64 characters.</p>
<b>Default</b>	5 ICMP echo requests will be sent. The default packet size and time out is 56 bytes and 2 seconds.
<b>Mode</b>	Admin mode
<b>Usage</b>	<p>Issue ICMP request to remote devices, check whether the remote device can be reached by the switch.</p> <p>When the ping command is entered without any parameters, interactive configuration mode will be invoked. And ping parameters can be entered interactively.</p>
<b>Example</b>	<p><b>Example 1 :</b> To ping with default parameters.</p> <pre>Switch#ping 10.1.128.160 Type ^c to abort. Sending 5 56-byte ICMP Echos to 10.1.128.160, timeout is 2 seconds. ...!! Success rate is 40 percent (2/5), round-trip min/avg/max = 0/0/0 ms</pre> <p>In the example above, the switch is made to ping the device at 10.1.128.160. The command did not receive ICMP reply packets for the first three ICMP echo requests within default 2 seconds timeout. The ping failed for the first three tries. However, the last two ping succeeded. So the success rate is 40%. It is denoted on the switch "." for ping failure which means unreachable link, while "!" for ping success, which means reachable link.</p> <p><b>Example 2 :</b> Ping with parameters entered interactively.</p> <pre>Switch#ping VRF name : Use IP Address[y]: y Target IP address : 10.1.128.160 Use source address option[n]: y Source IP address: 10.1.128.161 Repeat count [5]: 100 Datagram size in byte [56] : 1000 Timeout in milli-seconds [2000]: 500</pre>

Extended commands [n]: n

Display Information	Explanation
VRF name	VRM name. If MPLS is not enabled, this field will be left empty.
Target IP address :	The IP address of the target device.
Use source address option[n]	Whether or not to use ping with source address.
Source IP address	To specify the source IP address for ping.
Repeat count [5]	Number of ping requests to be sent. The default value is 5.
Datagram size in byte [56]	The size of the ICMP echo requests, with default as 56 bytes.
Timeout in milli-seconds [2000]:	Timeout in milli-seconds, with default as 2 seconds.
Extended commands [n]:	Whether or to use other extended options.

## 17.1.9 ping6

<b>Syntax</b>	<code>ping6 [&lt;dst-ipv6-address&gt;   host &lt;hostname&gt;   src &lt;src-ipv6-address&gt; {&lt;dst-ipv6-address&gt;   host &lt;hostname&gt;}]</code>						
<b>Parameter</b>	<table border="1"> <tr> <td><code>&lt;dst-ipv6-address&gt;</code></td> <td>target IPv6 address of the ping command</td> </tr> <tr> <td><code>&lt;src-ipv6-address&gt;</code></td> <td>source IPv6 address where the ping command is issued</td> </tr> <tr> <td><code>&lt;hostname&gt;</code></td> <td>target host name of the ping command, which should not exceed 64 characters.</td> </tr> </table>	<code>&lt;dst-ipv6-address&gt;</code>	target IPv6 address of the ping command	<code>&lt;src-ipv6-address&gt;</code>	source IPv6 address where the ping command is issued	<code>&lt;hostname&gt;</code>	target host name of the ping command, which should not exceed 64 characters.
<code>&lt;dst-ipv6-address&gt;</code>	target IPv6 address of the ping command						
<code>&lt;src-ipv6-address&gt;</code>	source IPv6 address where the ping command is issued						
<code>&lt;hostname&gt;</code>	target host name of the ping command, which should not exceed 64 characters.						
<b>Default</b>	Five ICMP6 echo request will be sent by default, with default size as 56 bytes, and default timeout to be 2 seconds.						
<b>Mode</b>	Admin mode						
<b>Usage</b>	<p>To check whether the destination network can be reached.</p> <p>When the ping6 command is issued with only one IPv6 address, other parameters will be default. And when the ipv6 address is a local data link address, the name of VLAN interface should be specified. When the source IPv6 address is specified, the command will fill the icmp6 echo requests with the specified source address for ping.</p>						
<b>Example</b>	<p><b>Example 1 :</b> To issue ping6 command with default parameters.</p> <pre>Switch#ping6 2001:1:2::4 Type ^c to abort. Sending 5 56-byte ICMP Echos to 2001:1:2::4, timeout is 2 seconds. !!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 1/320/1600 ms</pre> <p><b>Example 2 :</b> To issue the ping6 command with parameters input interactively.</p> <pre>Switch#ping6 Target IPv6 address:fe80::2d0:59ff:feb8:3b27 Output Interface: vlan1 Use source address option[n]:y Source IPv6 address: fe80::203:fff:fe0b:16e3 Repeat count [5]: Datagram size in byte [56]: Timeout in milli-seconds [2000]: Extended commands [n]: Type ^c to abort. Sending 5 56-byte ICMP Echos to fe80::2d0:59ff:feb8:3b27, using src address fe80::203:fff:fe0b:16e3, timeout is 2 seconds. !!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 1/4/16 ms</pre>						

Display Information	Explanation
ping6	The ping6 command
Target IPv6 address	The target IPv6 address of the command
Output Interface	The name of the VLAN interface, which should be specified when the target address is a local data link address.
Use source IPv6 address [n]:	Whether or not use source IPv6 address. Disabled by default.
Source IPv6 address	Source IPv6 address.
Repeat count[5]	Number of the ping packets.
Datagram size in byte[56]	Packet size of the ping command. 56 byte by default.
Timeout in milliseconds[2000]	Timeout for ping command. 2 seconds by default.
Extended commands[n]	Extended configuration. Disabled by default.
!	The network is reachable.
.	The network is unreachable.
Success rate is 100 percent(8/8), round-trip min/avg/max = 1/1/1ms	Statistic information, success rate is 100 percent of ping packet.



## 17.1.10 show boot-files

<b>Syntax</b>	<b>show boot-files</b>
<b>Parameter</b>	none
<b>Default</b>	none
<b>Mode</b>	Admin and Configuration Mode.
<b>Usage</b>	Display the first and second IMG files and the CFG file enabled by switch. After implementing this command, the booting sequence of IMG files in the corresponding storage device, which IMG file is currently used in booting, the configuration information of the CFG file in the storage device and the CFG file currently booted.
<b>Example</b>	Display the first and second IMG files and the CFG file enabled by switch. Switch#show boot-files Booted files on switch The primary img file at the next boot time: flash:/nos.img The backup img file at the next boot time: flash:/nos.img Current booted img file: flash:/nos.img The startup-config file at the next boot time: flash:/startup.cfg Current booted startup-config file: flash:/startup.cfg If the CFG file of the next booting is set as NULL, the CFG part mentioned above will be displayed as follows: The startup-config file at the next boot time: NULL Current booted startup-config file: flash:/startup.cfg

### 17.1.11 show flash

<b>Syntax</b>	<b>Show flash</b>
<b>Parameter</b>	<b>none</b>
<b>Default</b>	none
<b>Mode</b>	Admin and Configuration Mode.
<b>Usage</b>	Show the size of the files which are reserved in the system flash memory.
<b>Example</b>	To list the files and their size in the flash. Switch#show flash  total 12227K -rw- 12516553 nos.img -rw- 3224 startup.cfg  Drive : flash: Size:30.0M Used:13.0M Available:17.0M Use:43%

## 17.1.12 show history

<b>Syntax</b>	<b>show history</b>
<b>Parameter</b>	<b>none</b>
<b>Default</b>	none
<b>Mode</b>	Admin Mode
<b>Usage</b>	Display the recent user command history. The system holds up to 20 commands the user entered, the user can use the UP/DOWN key or their equivalent (ctrl+p and ctrl+n) to access the command history.
<b>Example</b>	Switch# show history enable config interface ethernet 1/0/3 enable dir show ftp

### 17.1.13 show history all-users

<b>Syntax</b>	<b>show history all-users [detail]</b>	
<b>Parameter</b>	<b>detail</b>	shows user name of the executing command. IP address of the user will be shown when logging in the executing command through Telnet or SSH
<b>Default</b>	none	
<b>Mode</b>	Admin and configuration mode	
<b>Usage</b>	<p>This command is used to show the recent command history of all users, including time, logging type, executing command, etc.</p> <p>Notice: The user can only check the command history of other users whose purview should not be higher than oneself.</p>	
<b>Example</b>	<pre>Switch# show history all-users detail Time Type User Command 0w 0d 0h 2m Telnet/SSH admin show history all-users detail 192.168.1.2:1419 0w 0d 0h 1m Telnet/SSH admin show history all-users 192.168.1.2:1419 0w 0d 0h 1m Console Null show history all-users 0w 0d 0h 1m Console Null end 0w 0d 0h 1m Console Null ip address 192.168.1.1 255.255.255.0 0w 0d 0h 0m Console Null in v 1 0w 0d 0h 0m Console Null telnet-server enable</pre>	

## 17.1.14 show logging buffered

<b>Syntax</b>	<code>show logging buffered [level {critical   warnings}   range &lt;begin-index&gt; &lt;end-index&gt;]</code>
<b>Parameter</b>	<p><code>level</code>    {critical         level of critical information</p> <p><code>warnings}</code></p> <hr/> <p><code>&lt;begin-index&gt;</code>            index start value of the log message, the valid range is 1-65535</p> <hr/> <p><code>&lt;end-index&gt;</code>                index end value of the log message, and the valid range is 1-65535. When only display logging buffered information of the line card must be added range parameter, but the main control has not the reques</p>
<b>Default</b>	No parameter specified indicates all the critical log information will be displayed.
<b>Mode</b>	Admin and configuration mode
<b>Usage</b>	<p>This command displays the detailed information in the log buffer channel. This command is not supported on low end switches.</p> <p>Warning and critical log information is saved in the buffer zone. When displayed to the terminal, their display format should be: index ID time &lt;level&gt; module ID [mission name] log information.</p>
<b>Example</b>	<p>Display the critical log information in the log buffer zone channel and related to the main control with index ID between 940 and 946.</p> <pre>Switch# show logging buffered level critical range 940 946</pre> <p>Current messages in SDRAM:0</p>

## 17.1.15 show logging executed-commands state

---

<b>Syntax</b>	<b>show logging executed-commands state</b>
<b>Parameter</b>	<b>none</b>
<b>Default</b>	none

---

<b>Mode</b>	Admin Mode
<b>Usage</b>	Use this command to display the state (enable or disable).
<b>Example</b>	Switch#show logging executed-commands state Logging executed command state is enable

---

## 17.1.16 show logging source

<b>Syntax</b>	<code>show logging source mstp</code>
<b>Parameter</b>	None
<b>Default</b>	None
<b>Mode</b>	Admin and configuration mode
<b>Usage</b>	Show the log information source of MSTP module.
<b>Example</b>	Show the log information source of MSTP.  Switch#show logging source mstp  system module log switch status:  Channel Onoff Severity  logbuff on warning  loghost on warning  terminal on warning

## 17.1.17 show running-config

<b>Syntax</b>	<b>show running-config</b>
<b>Parameter</b>	<b>none</b>
<b>Default</b>	None
<b>Mode</b>	Admin Mode
<b>Usage</b>	Display the current active configuration parameters for the switch. When the user finishes a set of configuration and needs to verify the configuration, show running-config command can be used to display the current active parameters. °
<b>Example</b>	Switch#show running-config



### 17.1.18 show running-config current-mode

<b>Syntax</b>	<code>show running-config current-mode</code>
<b>Parameter</b>	none
<b>Default</b>	none
<b>Mode</b>	All configuration modes.
<b>Usage</b>	Enter into any configuration mode and input this command under this mode, it can show all the configurations under the current mode.
<b>Example</b>	Switch(config-if-ethernet1/0/1)#show run c ! Interface Ethernet1/0/1 switchport access vlan 2 !

## 17.1.19 show startup-config

<b>Syntax</b>	<b>show startup-config</b>
<b>Parameter</b>	<b>none</b>
<b>Default</b>	If the configuration parameters read from the Flash are the same as the default operating parameter, nothing will be displayed.
<b>Mode</b>	Admin Mode
<b>Usage</b>	The <b>show running-config</b> command differs from <b>show startup-config</b> in that when the user finishes a set of configurations, <b>show running-config</b> displays the added-on configurations whilst <b>show startup-config</b> won't display any configurations. However, if <b>write</b> command is executed to save the active configuration to the Flash memory, the displays of <b>show running-config</b> and <b>show startup-config</b> will be the same.
<b>Example</b>	Switch#show startup-config

## 17.1.20 show switchport interface

<b>Syntax</b>	<code>show switchport interface [ethernet] &lt;IFNAME&gt;</code>
<b>Parameter</b>	<IFNAME>                      port number
<b>Default</b>	none

**Mode** Admin and configuration mode

**Usage** Show the VLAN port mode, VLAN number and Trunk port messages of the VLAN port mode on the switch.

**Example** Show VLAN messages of port ethernet 1/0/1

```
Switch#show switchport interface ethernet 1/0/1
Ethernet1/0/1
Type :Universal
Mode :Trunk
Port VID :1
Trunk allowed Vlan :1-4094
```

Displayed Information	Description
Ethernet1/0/1	Corresponding interface number of the Ethernet.
Type	Current interface type.
Mode: Trunk	Current interface VLAN mode.
Port VID :1	Current VLAN number the interface belongs.
Trunk allowed Vlan : ALL	VLAN permitted by Trunk

## 17.1.21 show tcp

<b>Syntax</b>	<b>show tcp</b>
<b>Parameter</b>	<b>none</b>
<b>Default</b>	none
<b>Mode</b>	Admin Mode
<b>Usage</b>	Display the current TCP connection status established to the switch.
<b>Example</b>	<pre>Switch#show tcp LocalAddress LocalPort ForeignAddress ForeignPort State 0.0.0.0 23 0.0.0.0 0 LISTEN 0.0.0.0 80 0.0.0.0 0 LISTEN</pre>

Displayed information	Description
LocalAddress	Local address of the TCP connection.
LocalPort	Local port number of the TCP connection.
ForeignAddress	Remote address of the TCP connection.
ForeignPort	Remote port number of the TCP connection.
State	Current status of the TCP connection.

## 17.1.22 show tcp ipv6

<b>Syntax</b>	<b>show tcp ipv6</b>																																		
<b>Parameter</b>	<b>none</b>																																		
<b>Default</b>	none																																		
<b>Mode</b>	Admin and configuration mode																																		
<b>Usage</b>	Show the current TCP connection.																																		
<b>Example</b>	<pre>Switch#show tcp ipv6</pre> <table border="1"> <thead> <tr> <th>LocalAddress</th> <th>LocalPort</th> <th>RemoteAddress</th> </tr> </thead> <tbody> <tr> <td>RemotePort</td> <td>State</td> <td>IF VRF</td> </tr> <tr> <td>::</td> <td>80</td> <td>::</td> </tr> <tr> <td>0</td> <td>LISTEN</td> <td>0 0</td> </tr> <tr> <td>::</td> <td>23</td> <td>::</td> </tr> <tr> <td>0</td> <td>LISTEN</td> <td>0 0</td> </tr> </tbody> </table> <table border="1"> <thead> <tr> <th>Displayed Information</th> <th>Explanation</th> </tr> </thead> <tbody> <tr> <td>LocalAddress</td> <td>Local IPv6 address of TCP connection</td> </tr> <tr> <td>LocalPort</td> <td>Local port of TCP connection</td> </tr> <tr> <td>RemoteAddress</td> <td>Remote IPv6 address of TCP connection</td> </tr> <tr> <td>RemotePort</td> <td>Remote Port of TCP connection</td> </tr> <tr> <td>State</td> <td>The current state of TCP connection</td> </tr> <tr> <td>IF</td> <td>Local port index of TCP connection</td> </tr> <tr> <td>VRF</td> <td>Virtual route forward instance</td> </tr> </tbody> </table>	LocalAddress	LocalPort	RemoteAddress	RemotePort	State	IF VRF	::	80	::	0	LISTEN	0 0	::	23	::	0	LISTEN	0 0	Displayed Information	Explanation	LocalAddress	Local IPv6 address of TCP connection	LocalPort	Local port of TCP connection	RemoteAddress	Remote IPv6 address of TCP connection	RemotePort	Remote Port of TCP connection	State	The current state of TCP connection	IF	Local port index of TCP connection	VRF	Virtual route forward instance
LocalAddress	LocalPort	RemoteAddress																																	
RemotePort	State	IF VRF																																	
::	80	::																																	
0	LISTEN	0 0																																	
::	23	::																																	
0	LISTEN	0 0																																	
Displayed Information	Explanation																																		
LocalAddress	Local IPv6 address of TCP connection																																		
LocalPort	Local port of TCP connection																																		
RemoteAddress	Remote IPv6 address of TCP connection																																		
RemotePort	Remote Port of TCP connection																																		
State	The current state of TCP connection																																		
IF	Local port index of TCP connection																																		
VRF	Virtual route forward instance																																		

## 17.1.23 show telnet login

---

<b>Syntax</b>	<b>show telnet login</b>
<b>Parameter</b>	<b>none</b>
<b>Default</b>	none
<hr/>	
<b>Mode</b>	Admin and configuration mode
<hr/>	
<b>Usage</b>	This command used to list the information of currently available telnet clients which are connected to the switch
<hr/>	
<b>Example</b>	Switch#show telnet login Authenticate login by local. Login user: aa
<hr/>	

## 17.1.24 show udp

<b>Syntax</b>	<b>show udp</b>																											
<b>Parameter</b>	<b>none</b>																											
<b>Default</b>	none																											
<b>Mode</b>	Admin Mode																											
<b>Usage</b>	Display the current UDP connection status established to the switch.																											
<b>Example</b>	<pre>Switch#show udp</pre> <table border="1"> <thead> <tr> <th>LocalAddress</th> <th>LocalPort</th> <th>ForeignAddress</th> <th>ForeignPort</th> <th>State</th> </tr> </thead> <tbody> <tr> <td>0.0.0.0</td> <td>32768</td> <td>0.0.0.0</td> <td>0</td> <td>CLOSE</td> </tr> <tr> <td>0.0.0.0</td> <td>3071</td> <td>0.0.0.0</td> <td>0</td> <td>CLOSE</td> </tr> </tbody> </table> <table border="1"> <thead> <tr> <th>Displayed Information</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>LocalAddress</td> <td>Local address of the UDP connection.</td> </tr> <tr> <td>LocalPort</td> <td>Local port number of the UDP connection.</td> </tr> <tr> <td>ForeignAddress</td> <td>Remote address of the UDP connection.</td> </tr> <tr> <td>ForeignPort</td> <td>Remote port number of the UDP connection.</td> </tr> <tr> <td>State</td> <td>Current status of the UDP connection.</td> </tr> </tbody> </table>	LocalAddress	LocalPort	ForeignAddress	ForeignPort	State	0.0.0.0	32768	0.0.0.0	0	CLOSE	0.0.0.0	3071	0.0.0.0	0	CLOSE	Displayed Information	Description	LocalAddress	Local address of the UDP connection.	LocalPort	Local port number of the UDP connection.	ForeignAddress	Remote address of the UDP connection.	ForeignPort	Remote port number of the UDP connection.	State	Current status of the UDP connection.
LocalAddress	LocalPort	ForeignAddress	ForeignPort	State																								
0.0.0.0	32768	0.0.0.0	0	CLOSE																								
0.0.0.0	3071	0.0.0.0	0	CLOSE																								
Displayed Information	Description																											
LocalAddress	Local address of the UDP connection.																											
LocalPort	Local port number of the UDP connection.																											
ForeignAddress	Remote address of the UDP connection.																											
ForeignPort	Remote port number of the UDP connection.																											
State	Current status of the UDP connection.																											

## 17.1.25 show udp ipv6

<b>Syntax</b>	<code>show udp ipv6</code>
<b>Parameter</b>	none
<b>Default</b>	none
<b>Mode</b>	Admin and configuration mode
<b>Usage</b>	Show the current UDP connection

**Example**

```
Switch#show udp ipv6
LocalAddress                               LocalPort  RemoteAddress
RemotePort  State
::                                                3071      ::
0          CLOSE
```

Displayed Information	Description
LocalAddress	Local IPv6 address of the UDP connection.
LocalPort	Local port number of the UDP connection.
RemoteAddress	Remote IPv6 address of the UDP connection.
RemotePort	Remote port number of the UDP connection.
State	Current status of the UDP connection.



## 17.1.26 show version

<b>Syntax</b>	<b>show version</b>
<b>Parameter</b>	<b>none</b>
<b>Default</b>	none
<b>Mode</b>	Admin Mode
<b>Usage</b>	Display the switch version. Use this command to view the version information for the switch, including hardware version and software version.
<b>Example</b>	Switch#show version

## 17.1.27 traceroute

<b>Syntax</b>	<code>traceroute [source &lt;ipv4-addr&gt; ] { &lt;ip-addr&gt;   host &lt;hostname&gt; } [hops &lt;hops&gt; ] [timeout &lt;timeout&gt; ]</code>										
<b>Parameter</b>	<table border="1"> <tr> <td><code>&lt;ipv4-addr&gt;</code></td> <td>assigned source host IPv4 address in dot decimal format</td> </tr> <tr> <td><code>&lt;ip-addr&gt;</code></td> <td>target host IP address in dot decimal format</td> </tr> <tr> <td><code>&lt;hostname&gt;</code></td> <td>hostname for the remote host</td> </tr> <tr> <td><code>&lt;hops&gt;</code></td> <td>maximum gateway number allowed by Traceroute command</td> </tr> <tr> <td><code>&lt;timeout&gt;</code></td> <td>timeout value for test packets in milliseconds, between 100 - 10000</td> </tr> </table>	<code>&lt;ipv4-addr&gt;</code>	assigned source host IPv4 address in dot decimal format	<code>&lt;ip-addr&gt;</code>	target host IP address in dot decimal format	<code>&lt;hostname&gt;</code>	hostname for the remote host	<code>&lt;hops&gt;</code>	maximum gateway number allowed by Traceroute command	<code>&lt;timeout&gt;</code>	timeout value for test packets in milliseconds, between 100 - 10000
<code>&lt;ipv4-addr&gt;</code>	assigned source host IPv4 address in dot decimal format										
<code>&lt;ip-addr&gt;</code>	target host IP address in dot decimal format										
<code>&lt;hostname&gt;</code>	hostname for the remote host										
<code>&lt;hops&gt;</code>	maximum gateway number allowed by Traceroute command										
<code>&lt;timeout&gt;</code>	timeout value for test packets in milliseconds, between 100 - 10000										
<b>Default</b>	The default maximum gateway number is 30, timeout in 2000 ms.										
<b>Mode</b>	Admin mode										
<b>Usage</b>	<p>This command is tests the gateway passed in the route of a packet from the source device to the target device. This can be used to test connectivity and locate a failed sector.</p> <p>Traceroute is usually used to locate the problem for unreachable network nodes.</p>										
<b>Example</b>	<pre>Switch#traceroute 192.168.2.36 Type ^c to abort. Traceroute to host 192.168.2.36, maxhops is 30, timeout is 2000ms.  1  0ms  192.168.2.36 Traceroute completed.</pre>										

## 17.1.28 traceroute6

<b>Syntax</b>	<code>traceroute6 [source &lt;addr&gt;] {&lt;ipv6-addr&gt;   host &lt;hostname&gt;} [hops &lt;hops&gt;] [timeout &lt;timeout&gt;]</code>										
<b>Parameter</b>	<table border="1"> <tr> <td><code>&lt;ipv4-addr&gt;</code></td> <td>assigned source host IPv6 address in colonned hex notation.</td> </tr> <tr> <td><code>&lt;ip-addr&gt;</code></td> <td>IPv6 address of the destination host, shown in colonned hex notation</td> </tr> <tr> <td><code>&lt;hostname&gt;</code></td> <td>name of the remote host</td> </tr> <tr> <td><code>&lt;hops&gt;</code></td> <td>max number of the gateways the traceroute6 passed through, ranging between 1-255</td> </tr> <tr> <td><code>&lt;timeout&gt;</code></td> <td>timeout period of the data packets, shown in millisecond and ranging between 100~10000</td> </tr> </table>	<code>&lt;ipv4-addr&gt;</code>	assigned source host IPv6 address in colonned hex notation.	<code>&lt;ip-addr&gt;</code>	IPv6 address of the destination host, shown in colonned hex notation	<code>&lt;hostname&gt;</code>	name of the remote host	<code>&lt;hops&gt;</code>	max number of the gateways the traceroute6 passed through, ranging between 1-255	<code>&lt;timeout&gt;</code>	timeout period of the data packets, shown in millisecond and ranging between 100~10000
<code>&lt;ipv4-addr&gt;</code>	assigned source host IPv6 address in colonned hex notation.										
<code>&lt;ip-addr&gt;</code>	IPv6 address of the destination host, shown in colonned hex notation										
<code>&lt;hostname&gt;</code>	name of the remote host										
<code>&lt;hops&gt;</code>	max number of the gateways the traceroute6 passed through, ranging between 1-255										
<code>&lt;timeout&gt;</code>	timeout period of the data packets, shown in millisecond and ranging between 100~10000										
<b>Default</b>	Default number of the gateways passes by the data packets is 30, and timeout period is defaulted at 2000ms.										
<b>Mode</b>	Admin mode										
<b>Usage</b>	<p>This command is for testing the gateways passed by the data packets from the source device to the destination device, so to check the accessibility of the network and further locating the network failure.</p> <p>Traceroute6 is normally used to locate destination network inaccessible failures.</p>										
<b>Example</b>	<pre>Switch#traceroute6 2004:1:2:3::4 Type ^c to abort. Traceroute to IPv6 host 2004:1:2:3::4, maxhops is 30, timeout is 2000ms. Traceroute6 error occured.</pre>										

### 17.1.29 reload after

<b>Syntax</b>	reload after {[<HH:MM:SS>] [days <days>]}	
<b>Parameter</b>	<HH:MM:SS>	specified time, HH (hours) ranges from 0 to 23, MM (minutes) and SS (seconds) range from 0 to 59
	<days>	specified days, unit is day, range from 1 to 30.
<b>Default</b>	none	
<b>Mode</b>	Admin mode	
<b>Usage</b>	With this command, users can reboot the switch without shutdown its power after a specified period of time, usually when updating the switch version. The switch can be rebooted after a period of time instead of immediately after its version being updated successfully. This command will not be reserved, which means that it only has one-time effect. After this command is configured, it will prompt the reboot information when user logging in the switch by telnet.	
<b>Example</b>	Set the switch to automatically reload after 2 days, 10 hours and 1 second. Switch#reload after 10:00:01 days 2 Process with reboot after? [Y/N] y	

### 17.1.30 reload cancel

<b>Syntax</b>	reload cancel
<b>Parameter</b>	none
<b>Default</b>	none
<b>Mode</b>	Admin mode
<b>Usage</b>	<p>Cancel the specified time period to reload the switch.</p> <p>With this command, users can cancel the specified time period to reload the switch, that is, to cancel the configuration of command "reload after". This command will not be reserved.</p>
<b>Example</b>	<p>Prevent the switch to automatically reboot after the specified time.</p> <pre>Switch#reload cancel</pre> <p>Reload cancel successful.</p>

### 17.1.31 show reload

---

<b>Syntax</b>	<b>show reload</b>
<b>Parameter</b>	none
<b>Default</b>	none

---

<b>Mode</b>	Admin and configuration mode
<b>Usage</b>	Display the user's configuration of command "reload after". With this command, users can view the configuration of command "reload after" and check how long a time is left before rebooting the switch.

---

<b>Example</b>	View the configuration of command "reload after". In the following case, the user set the switch to be rebooted in 10 hours and 1 second, and there are still 9 hours 59 minutes and 48 seconds left before rebooting it.  Switch#show reload  The original reload after configuration is 10:00:01.  System will be rebooted after 09:59:48 from now.
----------------	---

---

### 17.1.32 clear cpu-rx-stat protocol

<b>Syntax</b>	<code>clear cpu-rx-stat protocol [&lt;protocol-type&gt;]</code>
<b>Parameter</b>	<code>&lt;protocol-type&gt;</code> type of the protocol of the packet, , including dot1x, stp, snmp, arp, telnet, http, dhcp, igmp, ssh
<b>Default</b>	none
<b>Mode</b>	Admin mode
<b>Usage</b>	This command clear the statistics of the CPU received packets of the protocol type, it is supposed to be used with the help of the technical support.
<b>Example</b>	<p>Clear the statistics of the CPU receives ARP packets.</p> <pre>Switch#config Switch(config)#clear cpu-rx-stat protocol arp</pre>

### 17.1.33 cpu-rx-ratelimit protocol

<b>Syntax</b>	<pre>cpu-rx-ratelimit protocol &lt;protocol-type&gt; &lt;packets&gt; no cpu-rx-ratelimit protocol &lt;protocol-type&gt;</pre>
<b>Parameter</b>	<p><b>&lt;protocol-type&gt;</b> type of the protocol, including dot1x, stp, snmp, arp, telnet, http, dhcp, igmp, ssh</p> <p><b>&lt;packets&gt;</b> max rate of CPU receiving packets of the protocol type, its range is 1-2000 pps.</p>
<b>Default</b>	A different default rate is set for the different type of protocol.
<b>Mode</b>	Global mode
<b>Usage</b>	<p>Set the max rate of the CPU receiving packets of the protocol type, the no command set the max rate to default.</p> <p>The rate limit set by this command have an effect on CPU receiving packets, so it is supposed to be used with the help of the technical support.</p>
<b>Example</b>	<pre>set the rate of the ARP packets to 500pps. Switch#config Switch(config)#cpu-rx-ratelimit protocol arp 500</pre>



### 17.1.34 cpu-rx-ratelimit total

<b>Syntax</b>	<code>cpu-rx-ratelimit total &lt;packets&gt;</code> <code>no cpu-rx-ratelimit total</code>
<b>Parameter</b>	<packets>                      max number of CPU receiving packets per second
<b>Default</b>	1200pps
<b>Mode</b>	Global mode
<b>Usage</b>	Set the total rate of the CPU receiving packets, the no command sets the total rate of the CPU receiving packets to default. The total rate set by the command have an effect on CPU receiving packets, so it is supposed to be used with the help of the technical support.
<b>Example</b>	Set the total rate of the CPU receive packets to 1500pps. Switch#config Switch(config)# cpu-rx-ratelimit total 1500

### 17.1.35 show cpu-rx protocol

<b>Syntax</b>	<code>show cpu-rx protocol [&lt;protocol-type&gt;]</code>
<b>Parameter</b>	<code>&lt;protocol-type&gt;</code> protocol type of the packets, if do not input parameters, show all statistic packets.
<b>Default</b>	none
<b>Mode</b>	Admin and configuration mode
<b>Usage</b>	Show the statistics of the CPU received packets of the specified protocol type. This command is used to debug, it is supposed to be used with the help of the technical support.
<b>Example</b>	Show the statistics of CPU receiving ARP packets. Switch#show cpu-rx protocol arp Type Rate-limit TotPkts DropPkts DelayCount CurState ARP 300 0 0 0 allowed

# Chapter 18 PoE

## 18.1 PoE Configuration

### 18.1.1 power inline enable (Global)

<b>Command</b>	<code>power inline enable</code> <code>no power inline enable</code>
<b>parameter</b>	-
<b>default</b>	Disable.
<b>Mode</b>	Global Mode
<b>Usage Guide</b>	This command enables/disables global PoE. With PoE globally disabled, there would be no power output no matter what the power state of a specified port is.
<b>Example</b>	Globally disable PoE. Switch(Config)#no power inline enable

## 18.1.2 power inline enable (Port)

<b>Command</b>	<b>power inline enable</b> <b>no power inline enable</b>
<b>parameter</b>	-
<b>default</b>	Disable.
<b>Mode</b>	Port Mode.
<b>Usage Guide</b>	This command is used to enable/disable the specified port PoE, when the port disables the POE, there will be no power output regardless of the power state of the specified port.
<b>Example</b>	Disable power supply on ports1/0/1. Switch(config)#interface ethernet 1/0/1 Switch(config-if-ethernet1/0/1)#no power inline enable

### 18.1.3 power inline high-inrush

<b>Command</b>	<b>power inline high-inrush enable</b> <b>no power inline high-inrush enable</b>
<b>parameter</b>	-
<b>default</b>	The allowed high-inrush current is not enabled
<b>Mode</b>	Global mode
<b>Usage Guide</b>	<p>Power for non-standard PD instantaneously, this command is used to enable allowed high inrush output, no the command disables high inrush output.</p> <p>High-inrush current will be brought when nonstandard PD is powered instantaneously, it will result PSE self-protection to make PD power failure. Here, if this nonstandard PD must be powered, it needs to allow the high-inrush current.</p>
<b>Example</b>	<p>Enable the allowed high-inrush current when nonstandard PD is powered instantaneously.</p> <pre>Switch(config)#power inline high-inrush enable</pre>

## 18.1.4 power inline legacy

<b>Command</b>	<b>power inline legacy enable</b> <b>no power inline legacy enable</b>
<b>parameter</b>	-
<b>default</b>	Do not provide power supply for non-standard IEEE PD
<b>Mode</b>	Global Mode
<b>Usage Guide</b>	This command is used to enable non-standard IEEE PD detection functionality. No command disables non-standard IEEE PD detection function.
<b>Example</b>	Set the switch to provide power supply for non-standard IEEE PD. Switch(config)#power inline legacy enable

## 18.1.5 power inline max (Global)

<b>Command</b>	<code>power inline max &lt;max-wattage&gt;</code> <code>no power inline max</code>
<b>parameter</b>	<b><i>max-wattage</i></b> value of the max output power, in W. Any integer from 37 to 130 is valid
<b>default</b>	Default maximum output power 370W
<b>Mode</b>	Global Mode
<b>Usage Guide</b>	This command is used to set the global maximum output power of the POE no restore the default configuration.
<b>Example</b>	Set the global max output power to 50W. Switch(Config)#power inline max 50

## 18.1.6 power inline max (Port)

<b>Command</b>	<b>power inline max &lt;max-wattage&gt;</b> <b>no power inline max</b>	
<b>parameter</b>	<b>max-wattage</b>	the value of the max output power, in mW, ranging from 1 to 15400mW, with a granularity of 100mW. Any value less than 100mW will be taken as 100mW, that is, 1~100 equals 100, 15301~15400 equals 15400. But the value set by users will be maintained without being rounded up.
<b>default</b>	Default port maximum output power 32000mW	
<b>Mode</b>	Port Mode	
<b>Usage Guide</b>	This command can be used to set the maximum output power of the specified port.	
<b>Example</b>	Set the max output power of Port 1 to 0.8W. Switch(config)#interface ethernet 1/0/1 Switch(config-if-ethernet1/0/1)#power inline max 800	



## 18.1.7 power inline police

<b>Command</b>	<b>power inline police enable</b> <b>no power inline police enable</b>
<b>parameter</b>	-
<b>default</b>	The power priority management policy mode is disabled
<b>Mode</b>	Global Mode
<b>Usage Guide</b>	<p>This command is used to enable or disable priority management policy mode.</p> <p>In priority mode, when not enough PSE power is available, ports with low priority will be closed to satisfy the power supply for ports with high priority, no matter how long the access time of a PD is. If two ports have same priority, the one with smaller sequence number is higher privileged.</p> <p>In first-come-first-served mode, new PDs will not get power supply if available PSE power is not enough.</p>
<b>Example</b>	<p>Enable the power priority policy mode.</p> <pre>Switch(Config)#power inline police enable</pre>

## 18.1.8 power inline priority

<b>Command</b>	<b>power inline priority {critical   high   low}</b>						
<b>parameter</b>	<table border="1"> <tr> <td><b>critical</b></td> <td>the highest-level priority</td> </tr> <tr> <td><b>high</b></td> <td>high-level priority</td> </tr> <tr> <td><b>low</b></td> <td>low-level priority</td> </tr> </table>	<b>critical</b>	the highest-level priority	<b>high</b>	high-level priority	<b>low</b>	low-level priority
<b>critical</b>	the highest-level priority						
<b>high</b>	high-level priority						
<b>low</b>	low-level priority						
<b>default</b>	Port priority is low						
<b>Mode</b>	Port Mode						
<b>Usage Guide</b>	This command is used to set the priority level of the port. This command will take effect in the mode of "power inline police enable". Without enough available power for newly connected PD, ports with higher priority will get power supply first.						
<b>Example</b>	<p>Set the priority of Port 1 to high and that of Port 2 to critical.</p> <pre>Switch(Config)#interface ethernet 1/0/1 Switch(Config-Ethernet1/0/1)#power inline priority high Switch(Config)#interface ethernet 1/0/2 Switch(Config-Ethernet1/0/2)#power inline priority critical</pre>						

## 18.1.9 power inline monitor interval

<b>Command</b>	<b>power inline monitor interval &lt;30-36000&gt;</b>
<b>parameter</b>	<30-36000>                      Monitoring interval, size range :30-36000, per second
<b>default</b>	The default configuration interval is 150 seconds
<b>Mode</b>	Global mode
<b>Usage Guide</b>	this command is used to configure poe monitor interval time.
<b>Example</b>	The interval between switches is 3600 seconds. Switch(config)#power inline monitor interval 3600

### 18.1.10 power inline monitor {on|off }

<b>Command</b>	<b>18.2 power inline monitor {on off}</b>
<b>parameter</b>	-
<b>default</b>	Default disable poe monitor function
<b>Mode</b>	Port Configuration Mode
<b>Usage Guide</b>	This command is used to enable or disable poe monitoring function.
<b>Example</b>	enable poe detection function on port 1/0/1. Switch(config-if-ethernet1/0/1)#power inline monitor on

## 18.1.11 power inline power-off

<b>Command</b>	<b>power inline power-off time-range &lt;name&gt;</b>
<b>parameter</b>	<b>&lt;name&gt;</b> Time range name: This name is defined by the user and the character length is 1-64 bits
<b>default</b>	Default not configured
<b>Mode</b>	Port Mode
<b>Usage Guide</b>	this command is used to set poe timing off.
<b>Example</b>	The poe setting switch port 1/0/1 closes at t1. Switch(config-if-ethernet1/0/1)#power inline power-off time-range t1

## 18.1.12 power inline reset interval

<b>Command</b>	<b>power inline reset interval &lt;1-600&gt;</b>
<b>parameter</b>	<b>&lt;1-600&gt;</b> Refresh time interval size :1-600 per second
<b>default</b>	Default refresh time is 5 seconds
<b>Mode</b>	Global mode
<b>Usage Guide</b>	this command can be used to set poe refresh interval time.
<b>Example</b>	Sets the refresh interval poe the switch to 20 seconds. Switch(config)#power inline reset interval 20

## 18.2 PoE Monitoring and Debugging

### 18.2.1 show power inline

<b>Command</b>	show power inline
<b>parameter</b>	-
<b>default</b>	-
<b>Mode</b>	Admin Mode
<b>Usage Guide</b>	This command is used to view POE global configuration and state ◦
<b>Example</b>	View global POE configuration and status.Switch#show power inline ◦

```

PoE Work Status           : online
PoE Port Max Number      : 24
PoE Support Type         : 802.3at/802.3af
PoE MCU Software Version : V2.1
PoE Power Available      : 370 W
PoE Power Used           : 0 W
PoE Power Remaining     : 370 W
PoE Main Voltage         : 54.8 V
PoE Min Voltage          : 44 V
PoE Max Voltage          : 57 V
PoE Police               : Enable
PoE Legacy               : Enable
PoE High-inrush Status  : Disable
PoE Monitor Interval    : 150 s
PoE Reset Interval      : 5 s
  
```

Display entries	describe
PoE Work Status	POE working status
PoE Power Available	Global maximum of available power
PoE Power Used	Power currently in use
PoE Power Remaining	Remaining available power
PoE Min Voltage	minimum voltage
PoE Max Voltage	maximum voltage
PoE Police	Power Priority Policy Enable Status
PoE Legacy	Status of non-standard PD detection function
PoE High-inrush Status	Poe high inrush state

## 18.2.2 show power inline interface ethernet

<b>Command</b>	<code>show power inline interface [ethernet &lt;interface-number&gt;   &lt;interface-name&gt;]</code>
<b>parameter</b>	<i>interface-number</i> Ethernet port number
<b>default</b>	-
<b>Mode</b>	Admin Mode
<b>Usage Guide</b>	This command is used to view the configuration and status displayed on POE specified port.

**Example** View POE information on port 1/0/1.  
Switch#show power inline interface ethernet 1/0/1

Interface	Status	Oper	Power(mW)	Max(mW)	Current(mA)	Volt(V)	Priority	Class
Ethernet1/0/1	Disable	Off	0	800	0	54	Low	N/A

Display entries	describe
Oper	Working status: On : PD normal connection Off : PD no connection Faulty : PD detection failure Deny : Not enough power available or required to exceed the limit
Current(mA)	Current current at port
Volt(V)	Current voltage at port
Class	PD input power used: 0 Default 0.44~12.95 1 Optional 0.44~3.84 2 Optional 3.84~6.49 3 Optional 6.49~12.95 4 Reserved treated as class 0 and reserved for future use It is impossible for a compatible PD to provide a class 4 signal



# Chapter 19 Routing Protocol

## 19.1 RIP

### 19.1.1 accept-lifetime

<b>Command</b>	<p>accept-lifetime &lt;start-time&gt; {&lt;end-time&gt;  duration&lt;seconds&gt;  infinite}</p> <p><b>no accept-lifetime</b></p> <p>Use this command to specify a key accept on the key chain as a valid time period. The "no accept-lifetime" command deletes this configuration.</p>
<b>Parameter</b>	<p>&lt;start-time&gt; parameter specifies the start time of the time period, of which the form should be:</p> <p>&lt;start-time&gt;={&lt;hh:mm:ss&gt; &lt;month&gt; &lt;day&gt; &lt;year&gt; &lt;hh:mm:ss&gt; &lt;day&gt; &lt;month&gt; &lt;year&gt;}</p> <p>&lt;hh:mm:ss&gt; specify the concrete valid time of accept-lifetime in hours, minutes and second</p> <p>&lt;day&gt; specifies the date of valid, ranging between 1 -31</p> <p>&lt;month&gt; specifies the month of valid shown with the first three letters of the month, such as Jan</p> <p>&lt;year&gt; specifies the year of valid start, ranging between 1993 - 2035</p> <p>&lt;end-time&gt; specifies the due of the time period, of which the form should be:</p> <p>&lt;end-time&gt;={&lt;hh:mm:ss&gt; &lt;month&gt; &lt;day&gt; &lt;year&gt; &lt;hh:mm:ss&gt; &lt;day&gt; &lt;month&gt; &lt;year&gt;}&lt;hh:mm:ss&gt; specify the concrete valid time of accept-lifetime in hours, minutes and second</p> <p>&lt;day&gt; specifies the date of valid, ranging between 1 -31</p> <p>&lt;month&gt; specifies the month of valid shown with the first three letters of the month, such as Jan</p> <p>&lt;year&gt; specifies the year of valid start, ranging between 1993 - 2035</p> <p>&lt;seconds&gt; the valid period of the key in seconds, ranging between 1-2147483646</p> <p><b>Infinite</b> means the key will never be out of date.</p>
<b>Default</b>	No default configuration.
<b>Mode</b>	keychain-key Mode ◦
<b>Usage Guide</b>	<p>If only the authentication mode is configured and the key chain or password used by the interface is not configured, authentication will not work at all. If the mode is not configured before configuring this command, the mode will be set to clear text authentication after configuring this command. The no operation of this command will cancel the authentication, but it does not mean that the mode will be set to the non-authentication type, only that the authentication processing will not be performed when sending or receiving packets. You can enter ip rip authentication key-chain my key to indicate that the key chain name is my key, which is 6 characters in total.</p>

---

**Example**

The example below shows the accept-lifetime configuration of key 1 on the keychain named mychain.

```
Switch# config terminal
```

```
Switch(config)# key chain mychain
```

```
Switch(config-keychain)# key 1
```

```
Switch(config-keychain-key)# accept-lifetime 03:03:01 Dec 3 2004 04:04:02 Oct 6 2006
```

## 19.1.2 clear ip rip route

<b>Command</b>	<code>clear ip rip route {&lt;A.B.C.D/M&gt; kernel static connected rip ospf isis bgp all}</code>
	Clear specific route in the RIP route table.
<b>Parameter</b>	<b>&lt;A.B.C.D/M&gt;</b> Clear the routes which match the destination address from the RIP route table. Specifies the IP address prefix and its length of the destination address <b>kernel</b> delete kernel routes from the RIP route table <b>static</b> delete static routes from the RIP route table <b>connected</b> delete direct routes from the RIP route table <b>rip</b> only delete RIP routes from the RIP route table <b>ospf</b> only delete OSPF routes from the RIP route table <b>isis</b> only delete ISIS routes from the RIP route table <b>bgp</b> only delete BGP routes from the RIP route table <b>all</b> delete all routes from the RIP route table
<b>Default</b>	No default configuration
<b>Mode</b>	Admin mode
<b>Usage Guide</b>	Use this command with the all parameter will delete all learnt route in the RIP route which will be immediately recovered except for rip route. The dynamic learnt RIP route can only be recovered by studying one more time.
<b>Example</b>	Switch# clear ip rip route 10.0.0.0/8 Switch# clear ip rip route ospf

### 19.1.3 default-information originate

---

<b>Command</b>	default-information originate <b>no default-information originate</b>
	Allow the network 0.0.0.0 to be redistributed into the RIP. The “ <b>no default-information originate</b> ” disables this function.
<b>Parameter</b>	-
<b>Default</b>	Disabled
<b>Mode</b>	Router mode and address-family mode
<b>Usage Guide</b>	This command tells the router to insert the default route with the destination of 0.0.0.0 into the RIP routing database, and advertise the route as other routes.
<b>Example</b>	Switch# config terminal Switch(config)# router rip Switch(config-router)# default-information originate

## 19.1.4 default-metric

<b>Command</b>	<code>default-metric &lt;value&gt;</code> <b>no default-metric</b>  Set the default metric value of the introduced route. The “ <b>no default-metric</b> ” command restores the default value to 1.
<b>Parameter</b>	<b>&lt;value&gt;</b> is the metric value to be set, ranging between 1~16.
<b>Default</b>	Default route metric value is 1.
<b>Mode</b>	Router mode and address-family mode ◦
<b>Usage Guide</b>	<b>default-metric</b> command is used for setting the default route metric value of the routes from other routing protocols when distributed into the RIP routes. When using the <b>redistribute</b> commands for introducing routes from other protocols, the default route metric value specified by <b>default-metric</b> will be adopted if no specific route metric value is set.
<b>Example</b>	Set the default route metric value to 3 for introducing routes from other routing protocols into the RIP routes. Switch(config-router)#default-metric 3

## 19.1.5 distance

---

<b>Command</b>	<code>distance &lt;number&gt; [&lt;A.B.C.D/M&gt; ] [&lt;access-list-name access-list-number &gt;]</code> <code>no distance [&lt;A.B.C.D/M&gt; ]</code>
	Set the managing distance with this command. The " <b>no distance [&lt;A.B.C.D/M&gt;]</b> " command restores the default value to 120.
<b>Parameter</b>	<b>&lt;number&gt;</b> specifies the distance value, ranging from 1 to 255. <b>&lt;A.B.C.D/M&gt;</b> specifies the network prefix and its length. <b>&lt;access-list-name access-list-number &gt;</b> specifies the access-list number or name applied.
<b>Default</b>	The default managing distance of RIP is 120.
<b>Mode</b>	Router mode and address-family mode ◦
<b>Usage Guide</b>	In case there are routes from two different routing protocols to the same destination, the managing distance is then used for selecting routes. The less the managing distance of the route protocol is, the more reliable will be the route acquired from the protocol.
<b>Example</b>	Switch# config terminal Switch(config)# router rip Switch(config-router)# distance 8 10.0.0.0/8 mylist

## 19.1.6 distribute-list

---

<b>Command</b>	<pre>distribute-list{&lt;access-list-number access-list-name&gt;  prefix&lt;prefix-list-name&gt;} {in out} [&lt;ifname&gt;] no distribute-list{&lt;access-list-number access-list-name&gt;  prefix&lt;prefix-list-name&gt;} {in out} [&lt;ifname&gt;]</pre> <p>This command uses access-list or prefix-list to filter the route update packets sent and received. The “<b>no distribute-list {&lt;access-list-number&gt;  access-list-name&gt;  prefix&lt;prefix-list-name&gt;} {in out} [&lt;ifname&gt;]</b>” command cancels this route filter function.</p>
<b>Parameter</b>	<p><b>&lt;access-list-number  access-list-name&gt;</b> is the name or access-list number to be applied.</p> <p><b>&lt;prefix-list-name&gt;</b> is the name of the prefix-list to be applied.</p> <p><b>&lt;ifname&gt;</b> specifies the name of interface to be applied with route filtering.</p>
<b>Default</b>	The function in default situation is disabled.
<b>Mode</b>	Router mode and address-family mode ◦
<b>Usage Guide</b>	The filter will be applied to all the interfaces in case no specific interface is set.
<b>Example</b>	<pre>Switch# config terminal Switch(config)# router rip Switch(config-router)# distribute-list prefix myfilter in vlan 1</pre>

## 19.1.7 ip rip aggregate-address

<b>Command</b>	<code>ip rip aggregate-address A.B.C.D/M</code> <code>no ip rip aggregate-address A.B.C.D/M</code>
	To configure RIP aggregation route. The no form of this command will delete this configuration.
<b>Parameter</b>	<b>A.B.C.D/M</b> :IPv4 address and mask length.
<b>Default</b>	Disabled.
<b>Mode</b>	Router Mode or Interface Configuration Mode.
<b>Usage Guide</b>	If to configure aggregation route under router mode, RIP protocol must be enabled. If configured under interface configuration mode, RIP protocol may not be enabled, but the aggregation router can operation after the RIP protocol be enabled on interface.
<b>Example</b>	To configure aggregation route as 192.168.20.0/22 globally. Switch(config)#router rip Switch(config-router)#ip rip agg 192.168.20.0/22



## 19.1.8 ip rip authentication key-chain

---

<b>Command</b>	<pre>ip rip authentication key-chain &lt;name-of-chain&gt; no ip rip authentication key-chain</pre>
	<p>Use this command to enable RIPV2 authentication on an interface and further configures the adopted key chain. The “<b>no ip rip authentication key-chain</b>” command cancels the authentication.</p>
<b>Parameter</b>	<p><b>&lt;name-of-chain&gt;</b> is the name of the adopted key chain. There may be spaces in the string. The input ends with an enter and the string should not be longer than 256 bytes.</p>
<b>Default</b>	<p>Not configured.</p>
<b>Mode</b>	<p>Interface Configuration Mode.</p>
<b>Usage Guide</b>	<p>If the authentication is only configured without configuring the key chain or password used by the interface, the authentication does no effect. If mode has not been configured prior to configuring this command, the mode will be set to plaintext authentication. The “no ip rip authentication key” command will cancel the authentication which only cancels the authentication process when sending or receiving data packet other than set non authentication mode.</p>
<b>Example</b>	<pre>Switch#config terminal Switch(config)# interface vlan 1 Switch(config-if-vlan1)# ip rip authentication key-chain my key</pre>

---

## 19.1.9 ip rip authentication mode

<b>Command</b>	<b>ip rip authentication mode {text md5}</b> <b>no ip rip authentication mode {text md5}</b>  Configure the authentication mode; the “ <b>no ip rip authentication mode {ext md5}</b> ” command restores the default authentication mode namely text authentication mode.
<b>Parameter</b>	<b>text</b> means text authentication; <b>md5</b> means MD5 authentication.
<b>Default</b>	Not configured authentication.
<b>Mode</b>	Interface Configuration Mode.
<b>Usage Guide</b>	RIP-I do not support authentication which the RIP-II supports two authentication modes: text authentication (i.e. Simple authentication) and data packet authentication (i.e. MD5 authentication). This command should be used associating the ip rip authentication key or ip rip authentication string. Independently configuration will not lead to authentication process.
<b>Example</b>	Switch#config terminal Switch(config)# interface vlan 1 Switch(config-if-vlan1)# ip rip authentication mode md5

## 19.1.10 ip rip authentication string

---

<b>Command</b>	<pre>ip rip authentication string &lt;text&gt; no ip rip authentication string</pre>
	Set the password used in RIP authentication. The "no ip rip authentication string" cancels the authentication.
<b>Parameter</b>	<text> is the password used in authentication of which the length should be 1-16 characters with space available. The password should end with enter.
<b>Default</b>	-
<b>Mode</b>	Interface mode
<b>Usage Guide</b>	The ip rip authentication key will not be able to be configured when this command is configured, key id value is required in MD5 authentication which is 1 when use this command. The mode will be set to plaintext authentication in case no mode configuration is available. The "no ip rip authentication string" command will cancel the authentication which only cancels the authentication process when sending or receiving data packet other than set non authentication mode. Input ip rip authentication string aaa aaa to set the password as aaa aaa which is 7 characters.
<b>Example</b>	<pre>Switch# config terminal Switch(config)# interface vlan 1 Switch(config-if-vlan1)# ip rip authentication string guest</pre>

### 19.1.11 ip rip authentication cisco-compatible

<b>Command</b>	<b>ip rip authentication cisco-compatible</b> <b>no ip rip authentication cisco-compatible</b>
	After configured this command, the cisco RIP packets will be receivable by configuring the plaintext authentication or MD5 authentication
<b>Parameter</b>	-
<b>Default</b>	Not configured
<b>Mode</b>	Interface mode
<b>Usage Guide</b>	After authentication is configured on the cisco router, the RIP packets will exceeds the length of the defined standard length of the protocol once the number of route items is greater than 25. By configuring this command the over-lengthen RIP packets will be receivable other than denied.
<b>Example</b>	Switch# config terminal Switch(config)# interface vlan 1 Switch(config-if-vlan1)# ip rip authentication cisco-compatible

## 19.1.12 ip rip receive-packet

---

<b>Command</b>	<b>ip rip receive-packet</b> <b>no ip rip receive-packet</b>
	Set the interface to be able to receiveable RIP packets; the " <b>no ip rip receive-packet</b> " command sets the interface to be unable to receiveable RIP packets.
<b>Parameter</b>	-
<b>Default</b>	Interface receives RIP packets.
<b>Mode</b>	Interface Configuration Mode.
<b>Usage Guide</b>	-
<b>Example</b>	Switch# config terminal Switch(config)# interface vlan 1 Switch(config-if-vlan1)# ip rip receive-packet

### 19.1.13 ip rip receive version

<b>Command</b>	<code>ip rip receive version { 1   2 1 2 }</code> <code>no ip rip receive version</code>  Set the version information of the RIP packets the interface receives. The default version is 2; the “ <b>no ip rip receive version</b> ” command restores the value set by using the version command.
<b>Parameter</b>	<code>1</code> and <code>2</code> respectively stands for RIP version 1 and RIP version 2, <code>1 2</code> stands for the RIP versions 1, 2.
<b>Default</b>	Version 2 °
<b>Mode</b>	Interface Configuration Mode.
<b>Usage Guide</b>	-
<b>Example</b>	Switch# config terminal Switch(config)# interface vlan 1 Switch(config-if-vlan1)# ip rip receive version 1 2

## 19.1.14 ip rip send-packet

<b>Command</b>	<b>ip rip send-packet</b> <b>no ip rip send-packet</b>
	Set the Interface to be able to receive the RIP packets; the " <b>no ip rip send-packet</b> " sets the interface to be unable to receive the RIP packets.
<b>Parameter</b>	-
<b>Default</b>	Interface sends RIP packets.
<b>Mode</b>	Interface Configuration Mode.
<b>Usage Guide</b>	-
<b>Example</b>	Switch# config terminal Switch(config)# interface vlan 1 Switch(config-if-vlan1)# ip rip send-packet

## 19.1.15 ip rip send version

<b>Command</b>	<code>ip rip send version { 1   2   1-compatible   1 2 }</code> <code>no ip rip send version</code>  Set the version information of the RIP packets the interface receives. The default version is 2; the “ <b>no ip rip send version</b> ” command restores the value set by using the version command.
<b>Parameter</b>	<b>1</b> and <b>2</b> respectively stands for RIP version 1 and RIP version 2, <b>1 2</b> stands for the RIP versions 1, 2.
<b>Default</b>	Version 2 °
<b>Mode</b>	Interface Configuration Mode.
<b>Usage Guide</b>	-
<b>Example</b>	Switch# config terminal Switch(config)# interface vlan 1 Switch(config-if-vlan1)# ip rip send version 1



## 19.1.16 ip rip split-horizon

<b>Command</b>	<code>ip rip split-horizon [poisoned]</code> <code>no ip rip split-horizon</code>
	Enable split horizon. The " <b>no ip rip split-horizon</b> " disables the split horizon.
<b>Parameter</b>	<b>[poisoned]</b> means configure the split horizon with poison reverse.
<b>Default</b>	Split Horizon with poison reverse by default.
<b>Mode</b>	Interface Configuration Mode.
<b>Usage Guide</b>	The split horizon is for preventing the Routing Loops, namely preventing the layer 3 switches from broadcasting the routes which is learnt from the same interface on which the route to be broadcasted.
<b>Example</b>	Switch# config terminal Switch(config)# interface vlan 1 Switch(Config-if-Vlan1)# ip rip split-horizon poisoned

## 19.1.17 key

<b>Command</b>	<b>key &lt;keyid&gt;</b> <b>no key &lt;keyid&gt;</b>
	This command is for managing and adding keys in the key chain. The “ <b>no key &lt;keyid&gt;</b> ” command deletes one key.
<b>Parameter</b>	<b>&lt;keyid&gt;</b> is key ID, ranging between 0-2147483647.
<b>Default</b>	-
<b>Mode</b>	keychainMode and keychain-keyMode ◦
<b>Usage Guide</b>	The command permits entering the keychain-key mode and set the passwords corresponding to the keys.
<b>Example</b>	Switch#config terminal Switch(config)#key chain mychain Switch(config-keychain)#key 1 Switch(config-keychain-key)#

## 19.1.18 key chain

<b>Command</b>	<b>key chain &lt;name-of-chain&gt;</b> <b>no key chain &lt; name-of-chain &gt;</b>
	This command is for entering a keychain manage mode and configure a keychain. The “ <b>no key chain &lt; name-of-chain &gt;</b> ” deletes one keychain.
<b>Parameter</b>	<b>&lt;name-of-chain&gt;</b> is the name string of the keychain the length of which is not specifically limited.
<b>Default</b>	-
<b>Mode</b>	Global Mode
<b>Usage Guide</b>	-
<b>Example</b>	Switch#config terminal Switch(config)#key chain mychain Switch(config-keychain)#

## 19.1.19 key-string

<b>Command</b>	<b>key-string &lt;text&gt;</b> <b>no key-string &lt;text&gt;</b>  Configure a password corresponding to a key. The “ <b>no key-string &lt;text&gt;</b> ” command deletes the corresponding password.
<b>Parameter</b>	<b>&lt;text&gt;</b> is a character string without length limit. However when referred by RIP authentication only the first 16 characters will be used.
<b>Default</b>	-
<b>Mode</b>	keychain-key Mode ◦
<b>Usage Guide</b>	This command is for configure different passwords for keys with different ID.
<b>Example</b>	Switch# config terminal Switch(config)# key chain mychain Switch(config-keychain)# key 1 Switch(config-keychain-key)# key-string prime

## 19.1.20 maximum-prefix

<b>Command</b>	<b>maximum-prefix &lt;maximum-prefix&gt; [&lt;threshold&gt;]</b> <b>no maximum-prefix</b>
	Configure the maximum number of RIP routes in the route table. The “ <b>nomaximum-prefix</b> ” command cancels the limit.
<b>Parameter</b>	<b>&lt;maximum-prefix&gt;</b> the maximum number of RIP route, ranging between 1-65535; a warning is given when the number rate of current route exceeds <b>&lt;threshold&gt;</b> ranging between 1-100, default at 75.
<b>Default</b>	-
<b>Mode</b>	router mode
<b>Usage Guide</b>	The maximum RIP route only limits the number of routes learnt through RIP but not includes direct route or the RIP static route configured by the route command. The base on which the comparison is performed is the number of route marked R in the show ip route database, and also the number of RIP routes displayed in the show ip route statistics command.
<b>Example</b>	Switch# config terminal Switch(config)# router rip Switch(config-router)# maximum-prefix 150

## 19.1.21 neighbor

<b>Command</b>	<b>neighbor &lt;A.B.C.D&gt;</b> <b>no neighbor &lt;A.B.C.D&gt;</b>
	Specify the destination address requires targeted-peer sending. The “ <b>no neighbor &lt;A.B.C.D&gt;</b> ” command cancels the specified address and restores all gateways to trustable.
<b>Parameter</b>	<b>&lt;A.B.C.D&gt;</b> is the specified destination address for the sending, shown in dotted decimal notation.
<b>Default</b>	Not sending to any targeted-peer destination address.
<b>Mode</b>	router mode
<b>Usage Guide</b>	When used accompany with passive-interface command it can be configured to only sending routing messages to specific neighbor.
<b>Example</b>	Switch# config terminal Switch(config)# router rip Switch(config-router)# neighbor 1.1.1.1

## 19.1.22 network

<b>Command</b>	<code>network &lt;A.B.C.C/M ifname&gt;</code> <code>no network &lt;A.B.C.C/M ifname&gt;</code>
	Configure the RIP protocol network.
<b>Parameter</b>	<code>&lt;A.B.C.C/M &gt;</code> is the IP address prefix and its length in the network. <code>&lt;ifname&gt;</code> is the name of a interface.
<b>Default</b>	Not running RIP protocol
<b>Mode</b>	Router mode and address-family mode ◦
<b>Usage Guide</b>	Use this command to configure the network for sending or receiving RIP update packets. If the network is not configured, all interfaces of the network will not be able to send or receive data packets.
<b>Example</b>	Switch# config terminal Switch(config)# router rip Switch(config-router)# network 10.0.0.0/8 Switch(config-router)# network vlan 1

## 19.1.23 offset-list

---

<b>Command</b>	<b>offset-list &lt;access-list-number  access-list-name&gt; {in out }&lt;number &gt;[&lt;ifname&gt;]</b> <b>no offset-list &lt;access-list-number  access-list-name&gt; {in out }&lt;number &gt;[&lt;ifname&gt;]</b>
	Add an offset value to the metric value of the routes learnt by RIP. The “ <b>no offset-list &lt;access-list-number  access-list-name&gt; {in out} &lt;number &gt; [&lt;ifname&gt;]</b> ” command disables this function.
<b>Parameter</b>	<b>&lt; access-list-number  access-list-name&gt;</b> is the access-list or name to be applied <b>&lt;number &gt;</b> is the added offset value, ranging between 0-16; <b>&lt;ifname&gt;</b> is the specific interface name;
<b>Default</b>	Default offset value is the metric value defined by the system.
<b>Mode</b>	Router mode and address-family mode ◦
<b>Usage Guide</b>	-
<b>Example</b>	Switch# config terminal Switch(config)# router rip Switch(config-router)# offset-list 1 in 5 vlan 1

---



## 19.1.24 passive-interface

---

<b>Command</b>	<code>passive-interface &lt;ifname&gt;</code> <code>no passive-interface &lt;ifname&gt;</code>
	Set the RIP layer 3 switch blocks RIP broadcast on specified interface, on which the RIP data packets will only be sent to layer 3 switches configured with neighbor.
<b>Parameter</b>	<code>&lt;ifname&gt;</code> is the name of specific interface.
<b>Default</b>	Not configured
<b>Mode</b>	router mode
<b>Usage Guide</b>	-
<b>Example</b>	Switch# config terminal Switch(config)# router rip Switch(config-router)# passive-interface vlan 1

## 19.1.25 recv-buffer-size

<b>Command</b>	<b>recv-buffer-size&lt;size&gt;</b> <b>no recv-buffer-size</b>
	This command configures the size of UDP receiving buffer zone of RIP; the " <b>no recv-buffer-size</b> " command restores the system default.
<b>Parameter</b>	<b>&lt;size&gt;</b> is the buffer zone size in bytes, ranging between 8192-2147483647.
<b>Default</b>	8192 bytes.
<b>Mode</b>	router mode
<b>Usage Guide</b>	-
<b>Example</b>	Switch# config terminal Switch(config)# router rip Switch(config-router)# recv-buffer-size 23456789

## 19.1.26 redistribute

<b>Command</b>	<pre>redistribute {kernel  connected  static  ospf [&lt;process-id&gt;]  isis  bgp} [metric&lt;value&gt;] [route-map&lt;word&gt;] no redistribute {kernel  connected  static  ospf [&lt;process-id&gt;]  isis  bgp} [metric&lt;value&gt;] [route-map&lt;word&gt;]</pre>
	Introduce the routes learnt from other routing protocols into RIP.
<b>Parameter</b>	<p><b>kernel</b> introduce from kernel routes;</p> <p><b>connected</b> introduce from direct routes;</p> <p><b>static</b> introduce from static routes;</p> <p><b>ospf</b> introduce from OSPF routes. process-id is OSPF process ID, if there is no parameter that means the process by default, range between 1 to 65535;</p> <p><b>isis</b> introduce from ISIS routes;</p> <p><b>bgp</b> introduce from BGP routes;</p> <p><b>&lt;value&gt;</b> is the metric value assigned to the introduced route, ranging between 0 to 16;</p> <p><b>&lt;word&gt;</b> is the probe pointing to the route map for introducing routes.</p>
<b>Default</b>	-
<b>Mode</b>	Router mode and address-family mode ◦
<b>Usage Guide</b>	Under the address-family mode, the parameter kernel and ISIS is unavailable.
<b>Example</b>	<pre>Switch#config terminal Switch(config)#router rip Switch(config-router)#redistribute kernel route-map ipi To redistribute OSPFv2 routing information to RIP. Switch(config)#router rip Switch(config-router)#redistribute ospf 2</pre>

## 19.1.27 route

<b>Command</b>	<code>route &lt;A.B.C.D/M&gt;</code> <code>no route &lt;A.B.C.D/M&gt;</code>
	This command configures a static RIP route. The " <b>no route &lt;A.B.C.D/M&gt;</b> " command deletes this route.
<b>Parameter</b>	<code>&lt;A.B.C.D/M&gt;</code> Specifies this destination IP address prefix and its length.
<b>Default</b>	-
<b>Mode</b>	router mode
<b>Usage Guide</b>	The command adds a static RIP route, and is mainly used for debugging. Routes configured by this command will not appear in kernel route table but in the RIP route database.
<b>Example</b>	Switch# config terminal Switch(config)# router rip Switch(config-router)# route 1.0.0.0/8

## 19.1.28 router rip

<b>Command</b>	<b>router rip</b> <b>no router rip</b>
	Enable the RIP routing process and enter the RIP mode; the “ <b>no router rip</b> ” command closes the RIP routing protocol.
<b>Parameter</b>	-
<b>Default</b>	Not running RIP route.
<b>Mode</b>	Global mode
<b>Usage Guide</b>	This command is the switch for starting the RIP routing protocol which is required to be open before configuring other RIP protocol commands.
<b>Example</b>	Enable the RIP protocol mode Switch(config)#router rip Switch(config-router)#

## 19.1.29 send-lifetime

<b>Command</b>	<p><b>send-lifetime &lt;start-time&gt; {&lt;end-time&gt;  duration&lt;seconds&gt;  infinite}</b>  <b>no send-lifetime</b></p> <p>Use this command to specify a key on the keychain as the time period of sending keys. The "no send-lifetime" cancels this configuration.</p>
<b>Parameter</b>	<p><b>&lt;start-time&gt;</b> parameter specifies the starting time of the time period, which is:  <b>&lt;start-time&gt;={&lt;hh:mm:ss&gt; &lt;month&gt; &lt;day&gt; &lt;year&gt; &lt;hh:mm:ss&gt; &lt;day&gt; &lt;month&gt; &lt;year&gt;}</b></p> <p><b>&lt;hh:mm:ss&gt;</b>Specify the concrete valid time of accept-lifetime in hours, minutes and second ;</p> <p><b>&lt;day&gt;</b>Specifies the date of valid, ranging between 1 -31 ;</p> <p><b>&lt;month&gt;</b>Specifies the month of valid shown with the first three letters of the month, such as Jan ;</p> <p><b>&lt;year&gt;</b>Specifies the year of valid start, ranging between 1993 - 2035 ;</p> <p><b>&lt;end-time&gt;</b>Specifies the due of the time period, of which the form should be:  <b>&lt;end-time&gt;={&lt;hh:mm:ss&gt; &lt;month&gt; &lt;day&gt; &lt;year&gt; &lt;hh:mm:ss&gt; &lt;day&gt; &lt;month&gt; &lt;year&gt;}</b></p> <p><b>&lt;hh:mm:ss&gt;</b>Specify the concrete valid time of <b>send-lifetime</b> in hours, minutes and second ;</p> <p><b>&lt;seconds&gt;</b>is the valid period of the key in seconding and ranging between 1-2147483646 ;</p> <p><b>infinite</b> means the key will never be out of date.</p>
<b>Default</b>	No default configuration.
<b>Mode</b>	keychain-key Mode ◦
<b>Usage Guide</b>	<p>If only the authentication mode is configured and the key chain or password used by the interface is not configured, authentication will not work at all. If the mode is not configured before configuring this command, the mode will be set to clear text authentication after configuring this command. The no operation of this command will cancel the authentication, but it does not mean that the mode will be set to the non-authentication type, only that the authentication processing will not be performed when sending or receiving packets. You can enter ip rip authentication key-chain my key to indicate that the key chain name is my key, which is 6 characters in total.</p>
<b>Example</b>	<p>The example below shows the send-lifetime configuration on the keychain named mychain for key 1.</p> <pre>Switch# config terminal Switch(config)# key chain mychain Switch(config-keychain)# key 1 Switch(config-keychain-key)# send-lifetime 03:03:01 Dec 3 2004 04:04:02 Oct 6 2006</pre>

## 19.1.30 timers basic

<b>Command</b>	<b>timers basic &lt;update&gt; &lt;invalid&gt; &lt;garbage&gt;</b> <b>no timers basic</b>  Adjust the RIP timer update, timeout, and garbage collecting time. The “ <b>no timers basic</b> ” command restores each parameter to their default values.
<b>Parameter</b>	<b>&lt;update&gt;</b> time interval of sending update packet, shown in seconds and ranging between 5-2147483647; <b>&lt;invalid&gt;</b> time period after which the RIP route is advertised dead, shown in seconds and ranging between 5-2147483647 ; <b>&lt;garbage&gt;</b> is the hold time in which the a route remains in the routing table after advertised dead, shown in seconds and ranging between 5-2147483647.
<b>Default</b>	<b>&lt;update&gt;</b> defaulted at 30 ; <b>&lt;invalid&gt;</b> defaulted at 180 ; <b>&lt;garbage&gt;</b> defaulted at 120
<b>Mode</b>	router mode
<b>Usage Guide</b>	The system is defaulted broadcasting RIPng update packets every 30 seconds; and the route is considered invalid after 180 seconds but still exists for another 120 seconds before it is deleted from the routing table.
<b>Example</b>	Set the RIP update time to 20 seconds and the timeout period to 80 second, the garbage collecting time to 60 seconds. Switch(Config-Router)#timers basic 20 80 60

### 19.1.31 version

<b>Command</b>	<b>version {1  2}</b> <b>no version</b>  Configure the version of all RIP data packets sent/received by router interfaces: the " <b>no version</b> " restores the default configuration.
<b>Parameter</b>	<b>1</b> is version 1 rip; <b>2</b> is version 2 rip.
<b>Default</b>	Sent and received data packet is version 2 by default.
<b>Mode</b>	Router mode and address-family mode ◦
<b>Usage Guide</b>	1 refers to that each interface of the layer 3 switch only sends/receives the RIP-I data packets. 2 refers to that each interface of the layer 3 switch only sends/receives the RIP-II data packets. The RIP-II data packet is the default version.
<b>Example</b>	Configure the version of all RIP data packets sent/received by router interfaces to version 2. Switch(config-router)#version 2



### 19.1.32 show ip protocols rip

<b>Command</b>	show ip protocols rip
	Show the RIP process parameter and statistics information.
<b>Parameter</b>	-
<b>Default</b>	-
<b>Mode</b>	Any mode.
<b>Usage Guide</b>	-

**Example**

```

show ip protocols rip
Routing Protocol is "rip"
  Sending updates every 30 seconds with +/-50%, next due in 8 seconds
  Timeout after 180 seconds, garbage collect after 120 seconds
  Outgoing update filter list for all interface is not set
  Incoming update filter list for all interface is not set
  Default redistribution metric is 1
  Redistributing: static
  Default version control: send version 2, receive version 2
  Interface Send Recv Key-chain
Vlan1      2    2
  Routing for Networks:
Vlan1
Vlan2
  Routing Information Sources:
  Gateway Distance Last Update Bad Packets Bad Routes
20.1.1.1 120 00:00:31 0 0
  
```

Displayed information	Explanation
Sending updates every 30 seconds with +/-50%, next due in 8 seconds	Sending update every 30 secs
Timeout after 180 seconds, garbage collect after 120 seconds	The route time-out event period is 180 secs, the garbage collect time is 120 seconds
Outgoing update filter list for all interface is not set	Outgoing update filter list for all interface is not set
Incoming update filter list for all interface is not set	Incoming update filter list for all interface is not set
Default redistribution metric is 1	Default redistribution metric is 1

Redistributing: static	Redistributing the static route into the RIP route
Default version control: send version 2, receive version 2 Interface Send Recv Key-chain Ethernet1/3 2 2	The configuration of interface receiving and sending packets. Receive version is 2, keychain 1 not configured.
Routing for Networks: Vlan1 Vlan2	The segment running RIP is the Vlan 1 and Vlan 2
Routing Information Sources: Gateway Distance Last Update BadPackets Bad Routes 20.1.1.1 120 00:00:31 0 0	Routing information sources The badpacketand bad routes from the gateway 20.1.1.1 are all 0. 31 seconds have passed since the last route update. The manage distance is 120
Distance: (default is 120)	Default manage distance is 120

### 19.1.33 show ip rip

<b>Command</b>	<b>show ip rip</b>
	Show the routes in the RIP route data base.
<b>Parameter</b>	-
<b>Default</b>	-
<b>Mode</b>	Any mode.
<b>Usage Guide</b>	-
<b>Example</b>	<pre>show ip rip Codes: R - RIP, K - Kernel, C - Connected, S - Static, O - OSPF, I - IS-IS, B - BGP Network Next Hop Metric From If Time R 12.1.1.0/24 20.1.1.1 2 20.1.1.1 Vlan1 02:51 R 20.1.1.0/24 1 Vlan1</pre> <p>Amongst R stands for RIP route, namely a RIP route with the destination network address 12.1.1.0, the network prefix length as 24, next-hop address at 20.1.1.1. It is learnt from the Ethernet port E1/3 with a metric value of 2, and still has 2 minutes 51 seconds before time out.</p>

## 19.1.34 show ip rip database

---

<b>Command</b>	show ip rip database
	show the routes in the RIP route database.
<b>Parameter</b>	-
<b>Default</b>	-
<b>Mode</b>	Any mode.
<b>Usage Guide</b>	-

---

### Example

Switch# show ip rip database

Codes: R - RIP, K - Kernel, C - Connected, S - Static, O - OSPF, I - IS-IS,

B - BGP

Network	Next Hop	Metric	From	If	Time
---------	----------	--------	------	----	------

R	10.1.1.0/24	1		Vlan1	
---	-------------	---	--	-------	--

R	20.1.1.0/24	1		Vlan2	
---	-------------	---	--	-------	--

## 19.1.35 show ip rip interface

<b>Command</b>	<b>show ip rip interface [&lt;ifname&gt;]</b>
	Show the RIP related messages.
<b>Parameter</b>	<b>&lt;ifname&gt;</b> is the name of the interface to show the messages.
<b>Default</b>	-
<b>Mode</b>	Any mode.
<b>Usage Guide</b>	-
<b>Example</b>	Switch# show ip rip interface vlan 1 Vlan1 is up, line protocol is up Routing Protocol: RIP Receive RIP packets Send RIP packets Passive interface: Disabled Split horizon: Enabled with Poisoned Reversed IP interface address: 10.1.1.1/24

### 19.1.36 show ip rip aggregate

<b>Command</b>	<b>show ip rip aggregate</b>
	To display the information of IPv4 aggregation route.
<b>Parameter</b>	-
<b>Default</b>	-
<b>Mode</b>	Admin and Configuration Mode.
<b>Usage Guide</b>	This command is used to display which interface the aggregation route be configured, Metric, Count, Suppress and so on. If configured under global mode, then the interface display "----", "Metric" is metric. "Count" is the number of learned aggregation routes. "Suppress" is the times of aggregation.

**Example** To display the information of IPv4 aggregation route.

```
Switch(Config-if-Vlan1)#show ip rip agg
Aggregate information of rip
Network   Aggregated Ifname  Metric  Count  Suppress
192.168.0.0/16  Vlan1             1       2      0
192.168.4.0/22  ----              1       2      0
192.168.4.0/24  ----              1       1      1
                Vlan1             1       1      1
```

Displayed information	Explanation
Network	Route prefix and prefix length.
Aggregated Ifname	To configure the interface name of the aggregation route. If the route aggregated globally, then display "----".
Metric	Metric of aggregation route.
Count	The number of learned aggregation route.
Suppress	The times of aggregated for aggregation route.

## 19.1.37 show ip rip redistribute

<b>Command</b>	<b>show ip rip redistribute</b>
	To display the routing information introduced from external process of RIP.
<b>Parameter</b>	-
<b>Default</b>	Not shown by default.
<b>Mode</b>	Admin Mode and Configuration Mode.
<b>Usage Guide</b>	-
<b>Example</b>	Switch#show ip rip redistribute

## 19.2 OSPF

### 19.2.1 area authentication

<b>Command</b>	<b>area &lt;id&gt; authentication [message-digest]</b> <b>no area &lt;id&gt; authentication</b>
	Configure the authentication mode of the OSPF area; the “ <b>no area &lt;id&gt; authentication</b> ” command restores the default value.
<b>Parameter</b>	<b>&lt;id&gt;</b> is the area number which could be shown in digit, ranging from 0 to 4294967295, or in IP address <b>message-digest</b> is proved by MD5 authentication, or be proved by simple plaintext authentication if not choose this parameter.
<b>Default</b>	No authentication.
<b>Mode</b>	OSPF protocol mode
<b>Usage Guide</b>	Set the authentication mode to plaintext authentication or MD5 authentication. The authentication mode is also configurable under interface mode of which the priority is higher than those in the area. It is required to use <b>ip ospf authentication-key</b> to set the password while no authentication mode configured at the interface and the area is plaintext authentication, and use <b>ip ospf message-digest key</b> command to configure MD5 key if is MD5 authentication. The area authentication mode could not affect the authentication mode of the interface in this area.
<b>Example</b>	Set the authentication mode in area 0 to MD5. Switch(config-router)#area 0 authentication message-digest



## 19.2.2 area default-cost

<b>Command</b>	<b>area &lt;id&gt; default-cost &lt;cost&gt;</b> <b>no area &lt;id&gt; default-cost</b>
	Configure the cost of sending to the default summary route in stub or NSSA area; the “ <b>no area &lt;id&gt; default-cost</b> ” command restores the default value.
<b>Parameter</b>	<b>&lt;id&gt;</b> is the area number which could be shown as digits 0~4294967295, or as an IP address ; <b>&lt;cost&gt;</b> ranges between <0-16777215>
<b>Default</b>	Default OSPF cost is 1.
<b>Mode</b>	OSPF protocol mode
<b>Usage Guide</b>	The command is only adaptive to the ABR router connected to the stub area or NSSA area.
<b>Example</b>	Set the default-cost of area 1 to 10. Switch(config-router)#area 1 default-cost 10

### 19.2.3 area filter-list

<b>Command</b>	<p><b>[no] area &lt;id&gt; filter-list {access prefix} {in out}</b></p> <p>Configure the filter broadcasting summary routing on the ABR; the "<b>no area &lt;id&gt; filter-list {access prefix} {in out}</b>" command restores the default value.</p>
<b>Parameter</b>	<p><b>&lt;id&gt;</b> is the area number which could be shown in digits ranging between 0 ~ 4294967295, or as an IP address; access-list is appointed for use in access, so is prefix-list for prefix ;</p> <p><b>&lt;name&gt;</b> is the name of the filter, the length of which is between 1-256; in means from other areas to this area, out means from this area to other areas.</p>
<b>Default</b>	No filter configured.
<b>Mode</b>	OSPF protocol mode
<b>Usage Guide</b>	This command is used for restraining routes from specific area from spreading between this area and other areas.
<b>Example</b>	<p>Set a filter on the area 1.</p> <pre>Switch(config)#access-list 1 deny 172.22.0.0 0.0.0.255 Switch(config)#access-list 1 permit any-source Switch(config)#router ospf 100 Switch(config-router)#area 1 filter-list access 1 in</pre>

## 19.2.4 area nssa

<b>Command</b>	<pre>area &lt;id&gt; nssa [TRANSLATOR] no-redistribution [DEFAULT-ORIGINATE [no-summary] no area &lt;id&gt; nssa[TRANSLATOR] no-redistribution [DEFAULT-ORIGINATE [no-summary]</pre>
<b>Parameter</b>	<p>Set the area to Not-So-Stubby-Area (NSSA) area.</p> <p><b>&lt;id&gt;</b> is the area number which could be digits ranging between 0~4294967295, and also as an IP address.</p> <p><b>TRANSLATOR = translator-role {candidate never always}</b>, specifies the LSA translation mode for routes: <b>candidate</b> means if the router is elected translator, Type 7 LSA can be translated to Type-5 LSA, the default is <b>candidate</b>.</p> <p><b>never</b> means the router will never translate Type 7 LSA to Type 5 LSA.</p> <p><b>always</b> means the route always translate Type 7 LSA to Type 5 LSA.</p> <p><b>no-redistribution</b> means never distribute external-LSA to NSSA.</p> <p><b>DEFAULT-ORIGINATE=default-information-originate [metric &lt;0-16777214&gt;] [metric-type &lt;1-2&gt;]</b> , generate the Type-7 LSA.</p> <p><b>metric &lt;0-16777214&gt;</b> specifies the metric value.</p> <p><b>metric-type &lt;1-2&gt;</b> specifies the metric value type of external-LSA , default value is 2.</p> <p><b>no-summary</b> shows not injecting area route to the NSSA.</p>
<b>Default</b>	No NSSA area defined by default.
<b>Mode</b>	OSPF protocol mode
<b>Usage Guide</b>	The same area can not be both NSSA and stub at the same time.
<b>Example</b>	<pre>Set area 3 to NSSA. Switch#config terminal Switch(config)#router ospf 100 Switch(config-router)#area 0.0.0.51 nssa Switch(config-router)#area 3 nssa default-information-originate metric 34 metric-type 2 translator-role candidate no-redistribution</pre>

## 19.2.5 area range

<b>Command</b>	<pre>area &lt;id&gt; range &lt;address&gt; [advertise  not-advertise  substitute] no area &lt;id&gt; range &lt;address&gt;</pre> <p>Aggregate OSPF route on the area border. The “no area &lt;id&gt; range &lt;address&gt;” cancels this function.</p>
<b>Parameter</b>	<p>&lt;id&gt; is the area number which could be digits ranging between 0~4294967295, and also as an IP address. ;</p> <p>&lt;address&gt;=&lt;A.B.C.D/M&gt;, specifies the area network prefix and its length. ;</p> <p><b>advertise</b> : Advertise this area, which is the default ;</p> <p><b>not-advertise</b> : Not advertise this area ;</p> <p><b>substitute= substitute &lt;A.B.C.D/M&gt;</b> : advertise this area as another prefix ;</p> <p><b>&lt;A.B.C.D/M&gt;</b> : Replace the network prefix to be advertised in this area.</p>
<b>Default</b>	<p>Not set.</p>
<b>Mode</b>	<p>OSPF protocol mode</p>
<b>Usage Guide</b>	<p>Use this command to aggregate routes inside an area. If the network IDs in this area are not configured continuously, a summary route can be advertised by configuring this command on ABR. This route consists of all single networks belong to specific range.</p>
<b>Example</b>	<pre>Switch # config terminal Switch (config)# router ospf 100 Switch (config-router)# area 1 range 192.16.0.0/24</pre>

## 19.2.6 area stub

<b>Command</b>	<b>area &lt;id&gt; stub [no-summary]</b> <b>no area &lt;id&gt; stub [no-summary]</b>
	Define an area to a stub area. The “ <b>no area &lt;id&gt; stub [no-summary]</b> ” command cancels this function.
<b>Parameter</b>	<b>&lt;id&gt;</b> is the area number which could be digits ranging between 0~4294967295, and also as an IP address ; <b>no-summary</b> : The area border routes stop sending link summary announcement to the stub area.
<b>Default</b>	Not defined.
<b>Mode</b>	OSPF protocol mode
<b>Usage Guide</b>	Configure area stub on all routes in the stub area. There are two configuration commands for the routers in the stub area: stub and default-cost. All routers connected to the stub area should be configured with area stub command. As for area border routers connected to the stub area, their introducing cost is defined with area default-cost command.
<b>Example</b>	Switch # config terminal Switch (config)# router ospf 100 Switch (config-router)# area 1 stub

## 19.2.7 area virtual-link

<b>Command</b>	<pre>area &lt;id&gt; virtual-link A.B.C.D {AUTHENTICATION AUTH_KEY INTERVAL} no area &lt;id&gt; virtual-link A.B.C.D [AUTHENTICATION AUTH_KEY INTERVAL]</pre> <p>Configure a logical link between two backbone areas physically divided by non-backbone area. The "no area &lt;id&gt; virtual-link A.B.C.D [AUTHENTICATION   AUTH_KEY   INTERVAL]" command removes this virtual-link.</p>
<b>Parameter</b>	<p><b>&lt;id&gt;</b> is the area number which could be digits ranging between 0~4294967295, and also as an IP address.</p> <p><b>AUTHENTICATION</b> = authentication [message-digest[message-digest-key &lt;1-255&gt; md5 &lt;LINE&gt;]  null AUTH_KEY].</p> <p><b>authentication</b> : Enable authentication on this virtual link.</p> <p><b>message-digest</b> : Authentication with MD-5.</p> <p><b>null</b> : Overwrite password or packet summary with null authentication.</p> <p>AUTH_KEY= authentication-key &lt;key&gt;.</p> <p><b>&lt;key&gt;</b>: A password consists of less than 8 characters.</p> <p>INTERVAL= [dead-interval   hello-interval   message-digest-key&lt;1-255&gt;md5&lt;LINE&gt;   retransmit-interval   transmit-delay] &lt;value&gt;.</p> <p><b>&lt;value&gt;</b>&gt;: The delay or interval seconds, ranging between 1~65535.</p> <p><b>&lt;dead-interval&gt;</b>: A neighbor is considered offline for certain dead interval without its group messages which the default is 40 seconds.</p> <p><b>&lt;hello-interval&gt;</b>: The time interval before the router sends a hello group message, default is 10 seconds.</p> <p><b>&lt;message-digest-key&gt;</b>: Authentication key with MD-5.</p> <p><b>&lt;retransmit-interval&gt;</b>: The time interval before a router retransmitting a group message, default is 5 seconds.</p> <p><b>&lt;transmit-delay&gt;</b>: The time delay before a router sending a group messages, default is 1 second.</p>
<b>Default</b>	No default configuration.
<b>Mode</b>	OSPF protocol mode
<b>Usage Guide</b>	In the OSPF all non-backbone areas will be connected to a backbone area. If the connection to the backbone area is lost, virtual link will repair this connection. You can configure virtual link between any two backbone area routers connected with the public non-backbone area. The protocol treat routers connected by virtual links as a point-to-point network.
<b>Example</b>	<pre>Switch#config terminal Switch(config) #router ospf 100 Switch(config-router) #area 1 virtual-link 10.10.11.50 hello 5 dead 20</pre>

## 19.2.8 auto-cost reference-bandwidth

<b>Command</b>	<b>auto-cost reference-bandwidth &lt;bandwidth&gt;</b> <b>no auto-cost reference-bandwidth</b>
	This command sets the way in which OSPF calculate the default metric value. The “ <b>no auto-cost reference-bandwidth</b> ” command only configures the cost to the interface by types.
<b>Parameter</b>	<b>&lt;bandwidth&gt;</b> : reference bandwidth in Mbps, ranging between 1~4294967.
<b>Default</b>	Default bandwidth is 100Mbps.
<b>Mode</b>	OSPF protocol mode
<b>Usage Guide</b>	The interface metric value is acquired by divide the interface bandwidth with reference bandwidth. This command is mainly for differentiate high bandwidth links. If several high bandwidth links exist, their cost can be assorted by configuring a larger reference bandwidth value.
<b>Example</b>	Switch#config terminal Switch(config)#router ospf 100 Switch(config-router)#auto-cost reference-bandwidth 50

## 19.2.9 compatible rfc1583

<b>Command</b>	<b>compatible rfc1583</b> <b>no compatible rfc1583</b>
	This command configures to rfc1583 compatible. The " <b>no compatible rfc1583</b> " command close the compatibility.
<b>Parameter</b>	-
<b>Default</b>	Rfc 2328 compatible by default.
<b>Mode</b>	OSPF protocol mode
<b>Usage Guide</b>	-
<b>Example</b>	Switch#config terminal Switch(config)#router ospf 100 Switch(config-router)#compatible rfc1583



## 19.2.10 clear ip ospf process

<b>Command</b>	<b>clear ip ospf [&lt;process-id&gt;] process</b>
	Use this command to clear and restart OSPF routing processes. One certain OSPF process will be cleared by specifying the process ID, or else all OSPF processes will be cleared.
<b>Parameter</b>	-
<b>Default</b>	No default configuration.
<b>Mode</b>	Admin mode ◦
<b>Usage Guide</b>	-
<b>Example</b>	Switch#clear ip ospf process

## 19.2.11 default-information originate

<b>Command</b>	<b>default-information originate [always METRIC METRICTYPE ROTEMAP]</b> <b>no default-information originate</b>
	This command create a default external route to OSPF route area; the “ <b>no default-information originate</b> ” closes this feature.
<b>Parameter</b>	<b>always</b> : Whether default route exist in the software or not, the default route is always advertised. <b>METRIC = metric &lt;value&gt;</b> : Set the metric value for creating default route <b>&lt;value&gt;</b> ranges between 0~16777214, default metric value is 0. <b>METRICTYPE = metric-type {1 2}</b> set the OSPF external link type of default route. 1 Set the OSPF external type 1 metric value. 2 Set the OSPF external type 2 metric value. <b>ROTEMAP = route-map &lt;WORD&gt;</b> <b>&lt;WORD&gt;</b> specifies the route map name to be applied.
<b>Default</b>	Default metric value is 10; default OSPF external link type is 2.
<b>Mode</b>	OSPF protocol mode
<b>Usage Guide</b>	When introducing route into OSPF route area with this command, the system will behaves like an ASBR.
<b>Example</b>	Switch#config terminal Switch(config)#router ospf 100 Switch(config-router)#default-information originate always metric 23 metric-type 2 route-map myinfo

## 19.2.12 default-metric

<b>Command</b>	<b>default-metric &lt;value&gt;</b> <b>no default-metric</b>
	The command set the default metric value of OSPF routing protocol; the “ <b>no default-metric</b> ” returns to the default state.
<b>Parameter</b>	<b>&lt;value&gt;</b> , metric value, ranging between 0~16777214.
<b>Default</b>	Built-in, metric value auto translating.
<b>Mode</b>	OSPF protocol mode
<b>Usage Guide</b>	When the default metric value makes the metric value not compatible, the route introducing still goes through. If the metric value can not be translated, the default value provides alternative option to carry the route introducing on. This command will result in that all introduced route will use the same metric value. This command should be used associating redistribute.
<b>Example</b>	Switch#config terminal Switch(config)#router ospf 100 Switch(config-router)#default-metric 100

## 19.2.13 distance

<b>Command</b>	<b>distance {&lt;value&gt; ROUTEPARAMETER}</b> <b>no distance ospf</b>
<b>Parameter</b>	<p>Configure OSPF manage distance base on route type. The “<b>no distance ospf</b>” command restores the default value.</p> <hr/> <p>&lt;value&gt; › OSPF routing manage distance, ranging between 1~235</p> <p><b>ROUTEPARAMETER= ospf {ROUTE1 ROUTE2 ROUTE3}</b></p> <p><b>ROUTE1= external &lt;external-distance&gt;</b>, Configure the distance learnt from other routing area. <b>&lt;external-distance&gt;</b> distance value, ranging between 1~255.</p> <p><b>ROUTE2= inter-area &lt;inter-distance&gt;</b> › configure the distance value from one area to another area. <b>&lt;inter-distance&gt;</b> manage distance value, ranging between 1~255.</p> <p><b>ROUTE3= intra-area &lt;intra-distance&gt;</b> Configure all distance values in one area. <b>&lt;intra-distance&gt;</b> Manage distance value, ranging between 1~255.</p> <hr/>
<b>Default</b>	Default distance value is 110.
<b>Mode</b>	OSPF protocol mode
<b>Usage Guide</b>	Manage distance shows the reliability of the routing message source. The distance value may range between 1~255. The larger the manage distance value is, the lower is its reliability.
<b>Example</b>	<pre>Switch#config terminal Switch(config)#router ospf 100 Switch(config-router)#distance ospf inter-area 20 intra-area 10 external 40</pre>

## 19.2.14 distribute-list

<b>Command</b>	<b>distribute-list &lt;access-list-name&gt; out {kernel  connected  static  rip  isis  bgp}</b> <b>no distribute-list out {kernel  connected  static  rip  isis  bgp}</b>  Filter network in the routing update. The " <b>no distribute-list out {kernel  connected  static  rip  isis  bgp}</b> " command disables this function.
<b>Parameter</b>	<b>&lt; access-list-name&gt;</b> is the access-list name to be applied. <b>out:</b> Filter the sent route update. <b>kernel</b> Kernel route. <b>connected</b> Direct route ; <b>static</b> Static route ; <b>rip</b> RIP route ; <b>isis</b> ISIS route ; <b>bgp</b> BGP route.
<b>Default</b>	No default configuration.
<b>Mode</b>	OSPF protocol mode
<b>Usage Guide</b>	When distributing route from other routing protocols into the OSPF routing table, we can use this command.
<b>Example</b>	Example below is the advertisement based on the access-list list 1 of the BGP route. Switch#config terminal Switch(config)#access-list 11 permit 172.10.0.0 0.0.255.255 Switch(config)#router ospf 100 Switch(config-router)#redistribute rip Switch(config-router)#distribute-list 1 out rip

## 19.2.15 filter-policy

<b>Command</b>	<b>filter-policy &lt;access-list-name&gt;</b> <b>no filter-policy</b>
	Use access list to filter the route obtained by OSPF, the no command cancels the route filtering.
<b>Parameter</b>	<b>&lt;access-list-name&gt;</b> Access list name will be applied, it can use numeric standard IP access list and naming standard IP access list to configure.
<b>Default</b>	No default configuration.
<b>Mode</b>	OSPF protocol mode
<b>Usage Guide</b>	This command is used to filter the route obtained by OSPF. Do not filter any routes when the specified access list is not exist, for the routes which do not match permit rule of access list, they will be filtered. One access list can be set for this command, only the last configuration takes effect when configuring many times.
<b>Example</b>	Use access list 1 to filter the routes which do not belong to 172.10.0.0/16 segment. Switch#config terminal Switch(config)#access-list 1 permit 172.10.0.0 0.0.255.255 Switch(config)#router ospf Switch(config-router)#filter-policy 1

## 19.2.16 host area

<b>Command</b>	<code>host &lt;host-address&gt; area &lt;area-id&gt; [cost &lt;cost&gt;]</code> <code>no host &lt;host-address&gt; area &lt;area-id&gt; [cost &lt;cost&gt;]</code>
	Use this command to set a stub host entire belongs to certain area. The "[no] host <host-address> area <area-id> [cost <cost>]" command cancels this configuration.
<b>Parameter</b>	<b>&lt;host-address&gt;</b> is host IP address show in dotted decimal notation. <b>&lt;area-id&gt;</b> area ID shown in dotted decimal notation or integer ranging between 0~4294967295. <b>&lt;cost&gt;</b> specifies the entire cost, which is a integer ranging between 0~65535 and defaulted at 0.
<b>Default</b>	No entire set.
<b>Mode</b>	OSPF protocol mode
<b>Usage Guide</b>	With this command you can advertise certain specific host route out as stub link. Since the stub host belongs to special router in which setting host is not important.
<b>Example</b>	Switch#config terminal Switch(config)#router ospf 100 Switch(config-router)#host 172.16.10.100 area 1 Switch(config-router)#host 172.16.10.101 area 2 cost 10

## 19.2.17 ip ospf authentication

<b>Command</b>	<b>ip ospf [&lt;ip-address&gt;] authentication [message-digest null]</b> <b>no ip ospf [&lt;ip-address&gt;] authentication</b>
	Specify the authentication mode required in sending and receiving OSPF packets on the interfaces; the " <b>no ip ospf [&lt;ip-address&gt;] authentication</b> " command cancels the authentication.
<b>Parameter</b>	<b>&lt;ip-address&gt;</b> is the interface IP address, shown in dotted decimal notation. <b>message-digest</b> : Use MD5 authentication. <b>null</b> : no authentication applied, which resets the password or MD5 authentication applied on the interface.
<b>Default</b>	Authentication not required in receiving OSPF packets on the interface.
<b>Mode</b>	Interface Configuration Mode.
<b>Usage Guide</b>	-
<b>Example</b>	Switch#config terminal Switch(config)#interface vlan 1 Switch(config-if-vlan1)#ip ospf authentication message-digest



## 19.2.18 ip ospf authentication-key

<b>Command</b>	<b>ip ospf [&lt;ip-address&gt;] authentication-key &lt;0 LINE   7 WORD   LINE&gt;</b> <b>no ip ospf [&lt;ip-address&gt;] authentication</b>
	Specify the authentication key required in sending and receiving OSPF packet on the interface; the no command cancels the authentication key.
<b>Parameter</b>	<b>&lt;ip-address&gt;</b> is the interface IP address shown in dotted decimal notation; <b>&lt;LINE&gt;</b> specifies authentication key. If key option is 0, specify plaintext key. If key option is 7, specify encrypted string. If no option, specify plaintext key by default.
<b>Default</b>	Authentication not required in receiving OSPF packets on the interface.
<b>Mode</b>	Interface Configuration Mode.
<b>Usage Guide</b>	-
<b>Example</b>	Switch#config terminal Switch(config)#interface vlan 1 Switch(Config-if-Vlan1)#ip ospf authentication-key 0 password

## 19.2.19 ip ospf cost

<b>Command</b>	<pre>ip ospf [&lt;ip-address&gt;] cost &lt;cost&gt; no ip ospf [&lt;ip-address&gt;] cost</pre> <p>Specify the cost required in running OSPF protocol on the interface; the "no ip ospf [&lt;ip-address&gt;] cost" command restores the default value.</p>
<b>Parameter</b>	<p>&lt;ip-address&gt; is the interface IP address shown in dotted decimal notation.</p> <p>&lt;cost &gt; is the cost of OSPF protocol ranging between 1~65535.</p>
<b>Default</b>	Default OSPF cost on the interface is auto-figure out based bandwidth.
<b>Mode</b>	Interface Configuration Mode.
<b>Usage Guide</b>	-
<b>Example</b>	<pre>Switch#config terminal Switch(config)#interface vlan 1 Switch(config-if-vlan1)#ip ospf cost 3</pre>

## 19.2.20 ip ospf database-filter

<b>Command</b>	<b>ip ospf [&lt;ip-address&gt;] database-filter all out</b> <b>no ip ospf [&lt;ip-address&gt;] database-filter</b>
	The command opens LSA database filter switch on specific interface; the " <b>no ip ospf [&lt;ip-address&gt;] database-filter</b> " command closes the filter switch.
<b>Parameter</b>	<b>&lt;ip-address&gt;</b> is the interface IP address shown in dotted decimal notation; <b>all</b> : All LSAs. <b>out</b> : Sent LSAs.
<b>Default</b>	Filter switch Closed.
<b>Mode</b>	Interface Configuration Mode.
<b>Usage Guide</b>	-
<b>Example</b>	Switch#config terminal Switch(config)#interface vlan 1 Switch(config-if-vlan1)#ip ospf database-filter all out

## 19.2.21 ip ospf dead-interval

<b>Command</b>	<pre>ip ospf [&lt;ip-address&gt;] dead-interval &lt;time &gt; no ip ospf [&lt;ip-address&gt;] dead-interval</pre>
	Specify the dead interval for neighboring layer 3 switch; the “ <b>no ip ospf [&lt;ip-address&gt;] dead-interval</b> ” command restores the default value.
<b>Parameter</b>	<p><b>&lt;ip-address&gt;</b> is the interface IP address shown in dotted decimal notation;</p> <p><b>&lt;time &gt;</b> is the dead interval length of the neighboring layer 3 switches, shown in seconds and ranging between 1~65535.</p>
<b>Default</b>	The default dead interval is 40 seconds (normally 4 times of the hello-interval).
<b>Mode</b>	Interface Configuration Mode.
<b>Usage Guide</b>	If no Hello data packet received after the dead-interval period then this layer 3 switch is considered inaccessible and invalid. This command modifies the deadinterval value of neighboring layer 3 switch according to the actual link state. The set dead-interval value is written into the Hello packet and transmitted. To ensure the normal operation of the OSPF protocol, the dead-interval between adjacent layer 3 switches should be in accordance or at least 4 times of the hello-interval value.
<b>Example</b>	<pre>Switch#config terminal Switch(config)#interface vlan 1 Switch(config-if-vlan1)#ip ospf dead-interval 80</pre>

## 19.2.22 ip ospf disable all

<b>Command</b>	<code>ip ospf disable all</code> <code>no ip ospf disable all</code>
	Stop OSPF group process on the interface.
<b>Parameter</b>	-
<b>Default</b>	- °
<b>Mode</b>	Interface Configuration Mode.
<b>Usage Guide</b>	This command resets the network area command and stops group process on specific interface.
<b>Example</b>	Switch#config terminal Switch(config)#interface vlan 1 Switch(config-if-vlan1)#ip ospf disable all

## 19.2.23 ip ospf hello-interval

<b>Command</b>	<pre>ip ospf [&lt;ip-address&gt;] hello-interval &lt;time&gt; no ip ospf [&lt;ip-address&gt;] hello-interval</pre> <p>Specify the hello-interval on the interface; the “no ip ospf [&lt;ip-address&gt;] hello-interval” restores the default value.</p>
<b>Parameter</b>	<p>&lt;ip-address&gt; is the interface IP address shown in dotted decimal notation;</p> <p>&lt;time&gt; is the interval sending HELLO packet, shown in seconds and ranging between 1 ~ 65535.</p>
<b>Default</b>	The hello-interval on the interface is 10 seconds.
<b>Mode</b>	Interface Configuration Mode.
<b>Usage Guide</b>	HELLO data packet is the most common packet which is periodically sent to adjacent layer 3 switch to discover and maintain adjacent relationship, elect DR and BDR. The user set hello-interval value will be written into the HELLO packet and transmitted. The less the hello-interval value is, the sooner the network topological structure is discovered as well larger the cost. To ensure the normal operation of OSPF protocol the hello-interval parameter between the layer 3 switches adjacent to the interface must be in accordance.
<b>Example</b>	<pre>Switch#config terminal Switch(config)#interface vlan 1 Switch(config-if-vlan1)#ip ospf hello-interval 20</pre>

## 19.2.24 ip ospf message-digest-key

<b>Command</b>	<pre>ip ospf [&lt;ip-address&gt;] message-digest-key &lt;key_id&gt; MD5 &lt;0 LINE  7 WORD   LINE&gt; no ip ospf [&lt;ip-address&gt;] message-digest-key &lt;key_id&gt;</pre> <p>Specify the key id and value of MD5 authentication on the interface; the no command restores the default value.</p>
<b>Parameter</b>	<p><b>&lt;ip-address&gt;</b> is the interface IP address show in dotted decimal notation;</p> <p><b>&lt;key_id&gt;</b> ranges between 1-255;</p> <p><b>&lt;LINE&gt;</b> is OSPF key. If key option is 0, specify plaintext key. If key option is 7, specify encrypted string. If no option, specify plaintext key by default.</p>
<b>Default</b>	MD5 key is not configured.
<b>Mode</b>	Interface Configuration Mode.
<b>Usage Guide</b>	MD5 key encrypted authentication is used for ensure the safety between the OSPF routers on the network. Same key id and key should be configured between neighbors when using this command, or else no adjacent relationship will not be created.
<b>Example</b>	<pre>Switch#config terminal Switch(config)#interface vlan 1 Switch(config-if-vlan1)#ip ospf message-digest-key 2 MD5 0 yourpassword</pre>

## 19.2.25 ip ospf mtu

<b>Command</b>	<code>ip ospf mtu &lt;mtu&gt;</code> <code>no ip ospf mtu</code>
	Specify the mtu value of the interface as the OSPF group structure according; the "no ip ospf mtu" command restores the default value.
<b>Parameter</b>	<code>&lt;mtu &gt;</code> is the interface mtu value ranging between 576~65535
<b>Default</b>	Use the interface mtu acquired from the kernel.
<b>Mode</b>	Interface Configuration Mode.
<b>Usage Guide</b>	The interface value configured by this command is only used by OSPF protocol other than updated into kernel.
<b>Example</b>	Switch#config terminal Switch(config)#interface vlan 1 Switch(config-if-vlan1)#ip ospf mtu 1480



## 19.2.26 ip ospf mtu-ignore

<b>Command</b>	<code>ip ospf &lt;ip-address&gt; mtu-ignore</code> <code>no ip ospf &lt;ip-address&gt; mtu-ignore</code>
	Use this command so that the mtu size is not checked when switching DD; the “ <b>no ip ospf &lt;ip-address&gt; mtu-ignore</b> ” will ensure the mtu size check when performing DD switch.
<b>Parameter</b>	<code>&lt;ip-address&gt;</code> is the interface IP address show in dotted decimal notation.
<b>Default</b>	Check mtu size in DD switch.
<b>Mode</b>	Interface Configuration Mode.
<b>Usage Guide</b>	-
<b>Example</b>	Switch#config terminal Switch(config)#interface vlan 1 Switch(config-if-vlan1)#ip ospf mtu-ignore

## 19.2.27 ip ospf network

<b>Command</b>	<b>ip ospf network {broadcast non-broadcast point-to-point point-to-multipoint}</b> <b>no ip ospf network</b>
	This command configures the OSPF network type of the interface; the “ <b>no ip ospf network</b> ” command restores the default value.
<b>Parameter</b>	<b>broadcast</b> : Set the OSPF network type to broadcast. <b>non-broadcast</b> : Set the OSPF network type to NBMA. <b>point-to-point</b> : Set the OSPF network type to point-to-point. <b>point-to-multipoint</b> : Set the OSPF network type to point-to-multipoint.
<b>Default</b>	The default OSPF network type is broadcast.
<b>Mode</b>	Interface Configuration Mode.
<b>Usage Guide</b>	-
<b>Example</b>	The configuration below set the OSPF network type of the interface vlan 1 to point-to-point. Switch#config terminal Switch(config)#interface vlan 1 Switch(config-if-vlan1)#ip ospf network point-to-point

## 19.2.28 ip ospf priority

<b>Command</b>	<b>ip ospf [&lt;ip-address&gt;] priority &lt;priority&gt;</b> <b>no ip ospf [&lt;ip-address&gt;] priority</b>
	Configure the priority when electing "Defined layer 3 switch" at the interface. The " <b>no ip ospf [&lt;ip-address&gt;] priority</b> " command restores the default value.
<b>Parameter</b>	<b>&lt;ip-address&gt;</b> is the interface IP address show in dotted decimal notation. <b>&lt;priority&gt;</b> is the priority of which the valid value ranges between 0 ~ 255.
<b>Default</b>	The default priority when electing DR is 1.
<b>Mode</b>	Interface Configuration Mode.
<b>Usage Guide</b>	When two layer 3 switches connected to the same segments both want to be the "Defined layer 3 switch", the priority will decide which one should be chosen. Normally the one with higher priority will be elected, or the one with larger router-id number if the priorities are the same. A layer 3 switch with a priority equal to 0 will not be elected as "Defined layer 3 switch" or "Backup Defined layer 3 switch".
<b>Example</b>	Configure the priority of DR electing. Configure the interface vlan 1 to no election right, namely set the priority to 0. Switch#config terminal Switch(config)#interface vlan 1 Switch(config-if-vlan1)#ip ospf priority 0

## 19.2.29 ip ospf retransmit-interval

<b>Command</b>	<b>ip ospf [&lt;ip-address&gt;] retransmit-interval &lt;time&gt;</b> <b>no ip ospf [&lt;ip-address&gt;] retransmit-interval</b>
	Specify the retransmit interval of link state announcements between the interface and adjacent layer 3 switches. The “ <b>no ip ospf [&lt;ip-address&gt;] retransmit-interval</b> ” command restores the default value.
<b>Parameter</b>	<b>&lt;ip-address&gt;</b> is the interface IP address show in dotted decimal notation. <b>&lt;time&gt;</b> is the retransmit interveral of link state announcements between the interface and adjacent layer 3 switches, shown in seconds ang raning between 1~65535.
<b>Default</b>	Default retransmit interval is 5 seconds.
<b>Mode</b>	Interface Configuration Mode.
<b>Usage Guide</b>	When a layer 3 switch transmits LSA to its neighbor, it will maintain the link state announcements till confirm from the object side is received. If the confirm packet is not received within the interval, the LSA will be retransmitted. The retransmit interval must be larger than the time it takes to make a round between two layer 3 switches.
<b>Example</b>	Configure the LSA retransmit interval of interface vlan 1 to 10 seconds. Switch#config terminal Switch(config)#interface vlan 1 Switch(config-if-vlan1)#ip ospf retransmit-interval 10

## 19.2.30 ip ospf transmit-delay

<b>Command</b>	<b>ip ospf [&lt;ip-address&gt;] transmit-delay &lt;time&gt;</b> <b>no ip ospf [&lt;ip-address&gt;] transmit-delay</b>
	Set the transmit delay value of LSA transmitting; the “ <b>no ip ospf [&lt;ip-address&gt;] transmit-delay</b> ” restores the default value.
<b>Parameter</b>	<b>&lt;ip-address&gt;</b> is the interface IP address show in dotted decimal notation. <b>&lt;time&gt;</b> is the transmit delay value of link state announcements between the interface and adjacent layer 3 switches, shown in seconds ang raning between 1 ~ 65535.
<b>Default</b>	Default transmit delay value of link state announcements is 1 second.
<b>Mode</b>	Interface Configuration Mode.
<b>Usage Guide</b>	The LSA ages with time in the layer 3 switches, but not in the network transmitting process. By adding the transit-delay prior to sending the LSA, the LSA will be sent before aged.
<b>Example</b>	Set the LSA transmit delay of interface vlan1 to 3 seconds. Switch#config terminal Switch(config)#interface vlan 1 Switch(config-if-vlan1)#ip ospf transmit-delay 3

## 19.2.31 key

<b>Command</b>	<b>key &lt;keyid&gt;</b> <b>no key &lt;keyid&gt;</b>  This command is for managing and adding keys in the key chain. The “ <b>no key &lt;keyid&gt;</b> ” command deletes one key.
<b>Parameter</b>	<b>&lt;keyid&gt;</b> is key ID, ranging between 0-2147483647.
<b>Default</b>	- °
<b>Mode</b>	keychainMode and keychain-keyMode °
<b>Usage Guide</b>	The command permits entering the keychain-key mode and set the passwords corresponding to the keys.
<b>Example</b>	Switch#config terminal Switch(config)#key chain mychain Switch(config-keychain)#key 1 Switch(config-keychain-key)#

## 19.2.32 key chain

<b>Command</b>	<b>key chain &lt;name-of-chain&gt;</b> <b>no key chain &lt; name-of-chain &gt;</b>
	This command is for entering a keychain manage mode and configure a keychain. The “ <b>no key chain &lt; name-of-chain &gt;</b> ” command deletes one keychain.
<b>Parameter</b>	<b>&lt;name-of-chain&gt;</b> is the name string of the keychain the length of which is not specifically limited.
<b>Default</b>	- °
<b>Mode</b>	Global Mode and keychain Mode °
<b>Usage Guide</b>	-
<b>Example</b>	Switch#config terminal Switch(config)#key chain mychain Switch(config-keychain)#

### 19.2.33 log-adjacency-changes detail

<b>Command</b>	<b>log-adjacency-changes detail</b> <b>no log-adjacency-changes detail</b>
	Configure to keep a log for OSPF adjacency changes or not.
<b>Parameter</b>	-
<b>Default</b>	Don't I keep a log for OSPF adjacency changes by default.
<b>Mode</b>	OSPF Protocol Configuration Mode
<b>Usage Guide</b>	When this command is configured, the OSPF adjacency changes information will be recorded into a log.
<b>Example</b>	Switch#config terminal Switch(config)#router ospf 100 Switch(config-router)# log-adjacency-changes detail



## 19.2.34 max-concurrent-dd

<b>Command</b>	<b>max-concurrent-dd &lt;value&gt;</b> <b>no max-concurrent-dd</b>
	This command set the maximum concurrent number of dd in the OSPF process; the “no max-concurrent-dd” command restores the default.
<b>Parameter</b>	<b>&lt;value&gt;</b> ranges between <b>&lt;1-65535&gt;</b> , which is the capacity of processing the concurrent dd data packet.
<b>Default</b>	Not set, no concurrent dd limit.
<b>Mode</b>	OSPF protocol mode
<b>Usage Guide</b>	Specify the max concurrent number of dd in the OSPF process.
<b>Example</b>	Set the max concurrent dd to 20. Switch#config terminal Switch(config)#router ospf 100 Switch(config-router)#max-concurrent-dd 20

## 19.2.35 neighbor

<b>Command</b>	<b>neighbor A.B.C.D [&lt;cost&gt;  priority &lt;value&gt;   poll-interval &lt;value&gt;]</b> <b>no neighbor A.B.C.D [&lt;cost&gt;  priority &lt;value&gt;   poll-interval &lt;value&gt;]</b>
	This command configures the OSPF router connecting NBMA network. The “ <b>no neighbor A.B.C.D [&lt;cost&gt;  priority &lt;value&gt;   poll-interval &lt;value&gt;]</b> ” command removes this configuration.
<b>Parameter</b>	<b>&lt;cost&gt;</b> , OSPF neighbor cost value ranging between 1-65535 ; <b>priority &lt;value&gt;</b> , neighbor priority defaulted at 0 and ranges between 0-255 ; <b>poll-interval &lt;value&gt;</b> , 120s by default, which the polling time before neighbor relationship come into shape , ranging between 1-65535.
<b>Default</b>	No default configuration.
<b>Mode</b>	OSPF protocol mode
<b>Usage Guide</b>	Use this command on NBMA network to configure neighbor manually. Every known non-broadcasting neighbor router should be configured with a neighbor entry. The configured neighbor address should be the main address of the interface. The poll-interval should be much larger than the hello-interval.
<b>Example</b>	Switch#config terminal Switch(config)#router ospf 100 Switch(config-router)#neighbor 1.2.3.4 priority 1 poll-interval 90 Switch(config-router)#neighbor 1.2.3.4 cost 15

## 19.2.36 network area

<b>Command</b>	<b>network NETWORKADDRESS area &lt;area-id&gt;</b> <b>no network NETWORKADDRESS area &lt;area-id&gt;</b>
	This command enables OSPF routing function one the interface with IP address matched with the network address. The “ <b>no network NETWORKADDRESS area &lt;area-id&gt;</b> ” command removes the configuration and stop OSPF on corresponding interface.
<b>Parameter</b>	<b>NETWORKADDRESS = A.B.C.D/M   A.B.C.D X.Y.Z.W</b> , Shown with the network address prefix or the mask. Wildcast mask if shown in mask; <b>&lt;area-id&gt;</b> is the ip address or area number shown in point divided demical system, if shown in demcial integer, it ranges between 0~4294967295.
<b>Default</b>	No default configuration
<b>Mode</b>	OSPF protocol mode
<b>Usage Guide</b>	When certain segment belongs to certain area, interface the segment belongs will be in this area, starting hello and database interaction with the connected neighbor.
<b>Example</b>	Configuration 10.1.1.0/24 is in area 1. Switch#config terminal Switch(config)#router ospf 100 Switch(config-router)#network 10.1.1.0/24 area 1

### 19.2.37 ospf abr-type

<b>Command</b>	<b>ospf abr-type {cisco ibm shortcut standard}</b> <b>no ospf abr-type</b>
	Use this command to configure an OSPF ABR type. The “ <b>no ospf abr-type</b> ” command restores the default value.
<b>Parameter</b>	<b>cisco</b> , Realize through cisco ABR; <b>ibm</b> , Realize through ibm ABR; <b>shortcut</b> , Specify a shortcut-ABR; <b>standard</b> , Realize with standard(RFC2328)ABR.
<b>Default</b>	Cisco by default.
<b>Mode</b>	OSPF protocol mode
<b>Usage Guide</b>	For Specifying the realizing type of abr. This command is good for interactive operation among different OSPF realizing method and is especially useful in the multiple host environment.
<b>Example</b>	Configure abr as standard. Switch#config terminal Switch(config)#router ospf 100 Switch(config-router)#ospf abr-type standard

## 19.2.38 ospf router-id

<b>Command</b>	<b>ospf router-id &lt;address&gt;</b> <b>no ospf router-id</b>
	Specify a router ID for the OSPF process. The “ <b>no ospf router-id</b> ” command cancels the ID number.
<b>Parameter</b>	<b>&lt;address&gt;</b> , IPv4 address format of router-id.
<b>Default</b>	No default configuration
<b>Mode</b>	OSPF protocol mode
<b>Usage Guide</b>	The new router-id takes effect immediately.
<b>Example</b>	Configure router-id of ospf 100 to 2.3.4.5. Switch#config terminal Switch(config)#router ospf 100 Switch(config-router)#ospf router-id 2.3.4.5

### 19.2.39 overflow database

---

<b>Command</b>	<b>overflow database &lt;maxdbsize &gt; [{hard soft}]</b> <b>no overflow database</b>
	<p>This command is for configuring the max LSA number. The “no overflow database” command cancels the limit.</p>
<b>Parameter</b>	<p><b>&lt; maxdbsize &gt;</b> Max LSA numbers, ranging between 0~4294967294.</p> <p><b>soft</b> : Soft limit, warns when border exceeded.</p> <p><b>hard</b> : Hard limit, directly close ospf instance when border exceeded.</p> <p>If there is not soft or hard configured, the configuration is taken as hard limit.</p>
<b>Default</b>	Not configured
<b>Mode</b>	OSPF protocol mode
<b>Usage Guide</b>	-
<b>Example</b>	Switch#config terminal Switch(config)#router ospf Switch(config-router)#overflow database 10000 soft

## 19.2.40 overflow database external

---

<b>Command</b>	<b>overflow database external [&lt;maxdbsize &gt; &lt;maxtime&gt;]</b> <b>no overflow database external [&lt;maxdbsize &gt; &lt;maxtime&gt;]</b>
	<p>The command is for configuring the size of external link database and the waiting time before the route exits overflow state. The “<b>no overflow database external [&lt;maxdbsize &gt; &lt;maxtime&gt;]</b>” restores the default value.</p>
<b>Parameter</b>	<p><b>&lt; maxdbsize &gt;</b> size of external link database, ranging between 0~4294967294, defaulted at 4294967294.</p> <p><b>&lt; maxtime &gt;</b> the seconds the router has to wait before exiting the database overflow, ranging between 0~65535.</p>
<b>Default</b>	-
<b>Mode</b>	OSPF protocol mode
<b>Usage Guide</b>	-
<b>Example</b>	Switch#config terminal Switch(config)#router ospf Switch(config-router)#overflow database external 5 3

## 19.2.41 passive-interface

<b>Command</b>	<code>passive-interface&lt;ifname&gt; [&lt;ip-address&gt;]</code> <code>no passive-interface&lt;ifname&gt; [&lt;ip-address&gt;]</code>  Configure that the hello group not sent on specific interfaces. The “ <b>no passive-interface &lt;ifname&gt; [&lt;ip-address&gt;]</b> ”command cancels this function.
<b>Parameter</b>	<code>&lt;ifname&gt;</code> is the specific name of interface. <code>&lt;ip-address&gt;</code> IP address of the interface in dotted decimal format.
<b>Default</b>	Not configured
<b>Mode</b>	OSPF protocol mode
<b>Usage Guide</b>	-
<b>Example</b>	Switch#config terminal Switch(config)#router ospf Switch(config-router)#passive-interface vlan1



## 19.2.42 redistribute

<b>Command</b>	<pre>redistribute {kernel  connected  static  rip  isis  bgp} [metric&lt;value&gt;] [metric-type {1 2}][route-map&lt;word&gt;][tag&lt;tag-value&gt;] no redistribute {kernel  connected  static  rip  isis  bgp} [metric&lt;value&gt;] [metric-type {1 2}][route-map&lt;word&gt;][tag&lt;tag-value&gt;]</pre>
<b>Parameter</b>	<p>Introduce route learnt from other routing protocols into OSPF.</p> <p><b>kernel</b> introduce from kernel route.</p> <p><b>connected</b> introduce from direct route.</p> <p><b>static</b> introduce from static route.</p> <p><b>rip</b> introduce from the RIP route.</p> <p><b>isis</b> introduce from ISIS route.</p> <p><b>bgp</b> introduce from BGP route.</p> <p><b>metric &lt;value&gt;</b> is the introduced metric value, ranging between 0-16777214.</p> <p><b>metric-type {1 2}</b> is the metric value type of the introduced external route, which can be 1 or 2, and it is 2 by default.</p> <p><b>route-map &lt;word&gt;</b> point to the probe of the route map for introducing route.</p> <p><b>tag&lt;tag-value&gt;</b> external identification number of the external route, ranging between 0~4294967295, defaulted at 0.</p>
<b>Default</b>	-
<b>Mode</b>	OSPF protocol mode
<b>Usage Guide</b>	Learn and introduce other routing protocol into OSPF area to generate AS-external_LSAs.
<b>Example</b>	<pre>Switch#config terminal Switch(config)#router ospf Switch(config-router)#redistribute bgp metric 12</pre>

## 19.2.43 redistribute ospf

---

<b>Command</b>	<pre>redistribute ospf [&lt;process-id&gt;] [metric&lt;value&gt;] [metric-type {1 2}][route- map&lt;word&gt;] no redistribute ospf [&lt;process-id&gt;] [metric&lt;value&gt;] [metric-type {1 2}] [route- map&lt;word&gt;]</pre> <p>To redistribute of process ID routing to this process. The no form of command deletes the redistribution of process ID routing to this process. When input the optional parameters of metric, metric type and routermap, then restores default configuration.</p>
<b>Parameter</b>	<p><b>process-id</b> is OSPF process ID, 0 by default.</p> <p><b>metric &lt;value&gt;</b> is the metric for redistributed routing, range between 0 to 16777214.</p> <p><b>metric-type {1 2}</b> is the metric type for redistributed routing, only can be 1 or 2, and 2 by default.</p> <p><b>route-map &lt;word&gt;</b> is the pointer to the introduced routing map.</p>
<b>Default</b>	Not redistributed any OSPF routing by default.
<b>Mode</b>	OSPF protocol mode
<b>Usage Guide</b>	When process-id is not input, that means OSPF routing will be redistributed by default (Process-id is 0).
<b>Example</b>	Switch(config-router)#redistribute ospf

## 19.2.44 router ospf

<b>Command</b>	<code>router ospf &lt;process_id&gt;</code> <code>no router ospf &lt;process_id&gt;</code>
	This command is for relating the OSPF process.
<b>Parameter</b>	<code>&lt;process_id&gt;</code> specifies the ID of the OSPF process to be created, the ranging from 1 to 65535.
<b>Default</b>	-
<b>Mode</b>	Global Mode ◦
<b>Usage Guide</b>	-
<b>Example</b>	Switch#config terminal Switch(config)#router ospf 100 Switch(config-router)#network 10.1.1.0/24 area 0

## 19.2.45 summary-address

<b>Command</b>	<b>summary-address &lt;A.B.C.D/M&gt; [{not-advertise}tag&lt;tag-value&gt;]</b>
	Summarize or restrain external route with specific address scope.
<b>Parameter</b>	<b>&lt;A.B.C.D/M&gt;</b> address scope, shown in dotted decimal notation IPv4 address plus mask length. <b>not-advertised</b> restrain the external routes. <b>tag&lt;tag-value&gt;</b> is the identification label of the external routes, which ranges between 0~4294967295, and is defaulted at 0.
<b>Default</b>	-
<b>Mode</b>	OSPF protocol mode
<b>Usage Guide</b>	When routes are introduced into OSPF from other routing protocols, it is required to advertise every route in a external LSA. This command is for advertise one summary route for those introduced routes contained in specific network address and masks, which could greatly reduces the size of the link state database.
<b>Example</b>	Switch#config terminal Switch(config)#router ospf Switch(config-router)#summary-address 172.16.0.0/16 tag 3

## 19.2.46 timers spf

<b>Command</b>	<b>timers spf &lt;spf-delay&gt; &lt;spf-holdtime&gt;</b> <b>no timers spf</b>
	Adjust the value of the route calculating timer. The “ <b>no timers spf</b> ” command restores relevant values to default.
<b>Parameter</b>	<b>&lt;spf-delay&gt;</b> 5 seconds by default. <b>&lt;spf-holdtime&gt;</b> 10 seconds by default.
<b>Default</b>	-
<b>Mode</b>	OSPF protocol mode
<b>Usage Guide</b>	This command configures the delay time between receiving topology change and SPF calculation, further configured the hold item between two discontinuous SPF calculation.
<b>Example</b>	Switch#config terminal Switch(config)#router ospf Switch(config-router)#timers spf 5 10

## 19.2.47 show ip ospf

<b>Command</b>	<b>show ip ospf [&lt;process-id&gt;]</b>
	Display OSPF main messages.
<b>Parameter</b>	<b>&lt;process-id&gt;</b> is the process ID, ranging between 0~65535.
<b>Default</b>	Not displayed
<b>Mode</b>	Admin and Configuration Mode.
<b>Usage Guide</b>	-
<b>Example</b>	<pre>Switch#show ip ospf Routing Process "ospf 0" with ID 192.168.1.1 Process bound to VRF default Process uptime is 2 days 0 hour 30 minutes Conforms to RFC2328, and RFC1583Compatibility flag is disabled Supports only single TOS(TOS0) routes Supports opaque LSA SPF schedule delay 5 secs, Hold time between two SPFs 10 secs Refresh timer 10 secs Number of external LSA 0. Checksum Sum 0x000000 Number of opaque AS LSA 0. Checksum Sum 0x000000 Number of non-default external LSA 0 External LSA database is unlimited. Number of LSA originated 0 Number of LSA received 0 Number of areas attached to this router: 1   Area 0 (BACKBONE) (Inactive)     Number of interfaces in this area is 0(0)     Number of fully adjacent neighbors in this area is 0     Area has message digest authentication     SPF algorithm executed 0 times     Number of LSA 0. Checksum Sum 0x000000  Routing Process "ospf 10" with ID 0.0.0.0 Process bound to VRF test Process uptime is 4 days 23 hours 51 minutes Conforms to RFC2328, and RFC1583Compatibility flag is disabled</pre>

---

Supports only single TOS(TOS0) routes  
Supports opaque LSA  
SPF schedule delay 5 secs, Hold time between two SPFs 10 secs  
Refresh timer 10 secs  
Number of external LSA 0. Checksum Sum 0x000000  
Number of opaque AS LSA 0. Checksum Sum 0x000000  
Number of non-default external LSA 0  
External LSA database is unlimited.  
Number of LSA originated 0  
Number of LSA received 0  
Number of areas attached to this router: 1  
Area 0 (BACKBONE) (Inactive)  
Number of interfaces in this area is 0(0)  
Number of fully adjacent neighbors in this area is 0  
Area has no authentication  
SPF algorithm executed 0 times  
Number of LSA 0. Checksum Sum 0x000000

## 19.2.48 show ip ospf border-routers

<b>Command</b>	<b>show ip ospf [&lt;process-id&gt;] border-routers</b>
	Display the intra-domain route entries for the switch to reach ABR and ASBR of all instances.
<b>Parameter</b>	<b>&lt;process-id&gt;</b> is the process ID, ranging between 0~65535.
<b>Default</b>	Not displayed
<b>Mode</b>	Admin and Configuration Mode.
<b>Usage Guide</b>	-
<b>Example</b>	Switch#show ip ospf border-routers OSPF process 0 internal Routing Table Codes: i - Intra-area route, I - Inter-area route i 10.15.0.1 [10] via 10.10.0.1, Vlan1, ASBR, Area 0.0.0.0 i 172.16.10.1 [10] via 10.10.11.50, Vlan2, ABR, ASBR, Area 0.0.0.0



## 19.2.49 show ip ospf database

<b>Command</b>	<pre>show ip ospf [&lt;process-id&gt;] database[{{adv-router [{{&lt;linkstate_id&gt; self-originate  adv-router &lt;advertiser_router&gt;}}] asbr-summary[{{&lt;linkstate_id&gt;  self-originate  adv-router &lt;advertiser_router&gt;}}]  external [{{&lt;linkstate_id&gt;  self-originate  adv- router &lt;advertiser_router&gt;}}]  network [{{&lt;linkstate_id&gt; self-originate  adv-router &lt;advertiser_router&gt;}}] nssa-external [{{&lt;linkstate_id&gt; self-originate  adv-router &lt;advertiser_router&gt;}}] opaque-area [{{&lt;linkstate_id&gt; self-originate  adv-router &lt;advertiser_router&gt;}}] opaque-as [{{&lt;linkstate_id&gt; self-originate  adv-router &lt;advertiser_router&gt;}}] opaque-link [{{&lt;linkstate_id&gt; self-originate  adv-router &lt;advertiser_router&gt;}}] router [{{&lt;linkstate_id&gt; self-originate  adv-router &lt;advertiser_router&gt;}}] summary [{{&lt;linkstate_id&gt; self-originate  adv-router &lt;advertiser_router&gt;}}] self-originate   max-age }}]</pre>
	Display the OSPF link state data base messages.
<b>Parameter</b>	<p><b>&lt;process-id&gt;</b> is the process ID, ranging between 0~65535</p> <p><b>&lt;linkstate_id&gt;</b> Link state ID, shown in point divided demical system</p> <p><b>&lt;advertiser_router&gt;</b> is the ID of Advertising router, shown in point divided demcial IP address forma</p>
<b>Default</b>	Not displayed
<b>Mode</b>	Admin and Configuration Mode.
<b>Usage Guide</b>	According to the output messages of this command, we can view the OSPF link state database messages.
<b>Example</b>	<pre>Switch#show ip ospf database Router Link States (Area 0.0.0.2) Link ID ADV Router Age Seq# CkSum Link count 192.168.1.2 192.168.1.2 254 0x80000031 0xec21 1 192.168.1.3 192.168.1.3 236 0x80000033 0x0521 2  Net Link States (Area 0.0.0.2) Link ID ADV Router Age Seq# CkSum 20.1.1.2 192.168.1.2 254 0x8000002b 0xece4  Summary Link States (Area 0.0.0.2) Link ID ADV Router Age Seq# CkSum Route 6.1.0.0 192.168.1.2 68 0x8000002b 0x5757 6.1.0.0/22</pre>

---

6.1.1.0 192.168.1.2 879 0x8000002a 0xf8bc 6.1.1.0/24

22.1.1.0 192.168.1.2 308 0x8000000c 0xc8f0 22.1.1.0/24

ASBR-Summary Link States (Area 0.0.0.2)

Link ID ADV Router Age Seq# CkSum

192.168.1.1 192.168.1.2 1702 0x8000002a 0x89c7

AS External Link States

Link ID ADV Router Age Seq# CkSum Route

2.2.2.0 192.168.1.1 1499 0x80000056 0x3a63 E2 2.2.2.0/24 [0x0]

2.2.3.0 192.168.1.1 1103 0x8000002b 0x0ec3 E2 2.2.3.0/24 [0x0]

## 19.2.50 show ip ospf interface

<b>Command</b>	<b>show ip ospf interface &lt;interface&gt;</b>
	Display the OSPF interface messages.
<b>Parameter</b>	<b>&lt;interface&gt;</b> is the name of interface
<b>Default</b>	Not displayed
<b>Mode</b>	Admin and Configuration Mode.
<b>Usage Guide</b>	-
<b>Example</b>	Switch#show ip ospf interface Loopback is up, line protocol is up OSPF not enabled on this interface Vlan1 is up, line protocol is up Internet Address 10.10.10.50/24, Area 0.0.0.0 Process ID 0, Router ID 10.10.11.50, Network Type BROADCAST, Cost: 10 Transmit Delay is 5 sec, State Waiting, Priority 1 No designated router on this network No backup designated router on this network Timer intervals configured, Hello 35, Dead 35, Wait 35, Retransmit 5 Hello due in 00:00:16 Neighbor Count is 0, Adjacent neighbor count is 0

## 19.2.51 show ip ospf neighbor

<b>Command</b>	<code>show ip ospf [&lt;process-id&gt;] neighbor [{&lt;neighbor_id&gt;  all  detail [all]  interface&lt;ifaddress&gt;}]</code>
	Display the OSPF adjacent point messages.
<b>Parameter</b>	<p><b>&lt;process-id&gt;</b> is the process ID ranging between 0~65535</p> <p><b>&lt;neighbor_id&gt;</b> is the dotted decimal notation neighbor ID</p> <p><b>all</b> : Display messages of all neighbors</p> <p><b>detail</b> : Display detailed messages of all neighbors</p> <p><b>&lt;ifaddress&gt;</b> Interface IP address</p>
<b>Default</b>	Not displayed
<b>Mode</b>	Admin and Configuration Mode.
<b>Usage Guide</b>	OSPF neighbor state can be checked by viewing the output of this command.

<b>Example</b>	<pre>Switch#show ip ospf neighbor OSPF process 0: Neighbor ID Pri State Dead Time Address Interface 192.168.1.1 1 Full/Backup 00:00:32 6.1.1.1 Vlan1 192.168.1.3 1 Full/DR 00:00:36 20.1.1.3 Vlan2 192.168.1.3 1 Full/ - 00:00:30 20.1.1.3 VLINK2</pre> <table border="1"> <thead> <tr> <th>Displayed information</th> <th>Explanation</th> </tr> </thead> <tbody> <tr> <td>Neighbor ID</td> <td>ID Neighbor ID</td> </tr> <tr> <td>Priority</td> <td>Priority</td> </tr> <tr> <td>State</td> <td>Neighbor relation state</td> </tr> <tr> <td>Dead time</td> <td>Neighbor dead time</td> </tr> <tr> <td>Address</td> <td>Interface Address</td> </tr> <tr> <td>Interface</td> <td>Interface name</td> </tr> </tbody> </table>	Displayed information	Explanation	Neighbor ID	ID Neighbor ID	Priority	Priority	State	Neighbor relation state	Dead time	Neighbor dead time	Address	Interface Address	Interface	Interface name
Displayed information	Explanation														
Neighbor ID	ID Neighbor ID														
Priority	Priority														
State	Neighbor relation state														
Dead time	Neighbor dead time														
Address	Interface Address														
Interface	Interface name														

## 19.2.52 show ip ospf redistribute

<b>Command</b>	<b>show ip ospf [&lt;process-id&gt;] redistribute</b>
	To display the routing message redistributed from external process of OSPF.
<b>Parameter</b>	<b>&lt;process-id&gt;</b> is the process ID ranging between 0~65535.
<b>Default</b>	-
<b>Mode</b>	Admin Mode and Configuration Mode.
<b>Usage Guide</b>	-
<b>Example</b>	Switch#show ip ospf redistribute ospf process 1 redistribute information : ospf process 2 ospf process 3 bgp ospf process 2 redistribute information : ospf process 1 bgp ospf process 3 redistribute information : ospf process 1 bgp Switch#show ip ospf 2 redistribute ospf process 2 redistribute information : ospf process 1 bgp

## 19.2.53 show ip ospf route

<b>Command</b>	<code>show ip ospf [&lt;process-id&gt;] route</code>
	Display the OSPF routing table messages.
<b>Parameter</b>	<code>&lt;process-id&gt;</code> is the process ID ranging between 0~65535
<b>Default</b>	-
<b>Mode</b>	Admin and Configuration Mode.
<b>Usage Guide</b>	-
<b>Example</b>	<pre>Switch#show ip ospf route O 10.1.1.0/24 [10] is directly connected, Vlan1, Area 0.0.0.0 O 10.1.1.4/32 [10] via 10.1.1.4, Vlan1, Area 0.0.0.0 IA 11.1.1.0/24 [20] via 10.1.1.1, Vlan1, Area 0.0.0.0 IA 11.1.1.2/32 [20] via 10.1.1.1, Vlan1, Area 0.0.0.0 IA 12.1.1.0/24 [20] via 10.1.1.2, Vlan1, Area 0.0.0.0 IA 12.1.1.2/32 [20] via 10.1.1.2, Vlan1, Area 0.0.0.0 O 13.1.1.0/24 [10] is directly connected, Vlan4, Area 0.0.0.3 O 14.1.1.0/24 [10] is directly connected, Vlan5, Area 0.0.0.4 IA 15.1.1.0/24 [20] via 13.1.1.2, Vlan4, Area 0.0.0.3 IA 15.1.1.2/32 [20] via 13.1.1.2, Vlan4, Area 0.0.0.3 E1 100.1.0.0/16 [21] via 10.1.1.1, Vlan1 E1 100.2.0.0/16 [21] via 10.1.1.1, Vlan1</pre>

## 19.2.54 show ip ospf virtual-links

<b>Command</b>	<code>show ip ospf [&lt;process-id&gt;] virtual-links</code>
	Display the OSPF virtual link message.
<b>Parameter</b>	<code>&lt;process-id&gt;</code> is the process ID ranging between 0~65535.
<b>Default</b>	-
<b>Mode</b>	Admin and Configuration Mode.
<b>Usage Guide</b>	-
<b>Example</b>	<pre>Switch#show ip ospf virtual-links Virtual Link VLINK0 to router 10.10.0.9 is up   Transit area 0.0.0.1 via interface Vlan1   Transmit Delay is 1 sec, State Point-To-Point,   Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5   Hello due in 00:00:02   Adjacency state Full Virtual Link VLINK1 to router 10.10.0.123 is down   Transit area 0.0.0.1 via interface Vlan1   Transmit Delay is 1 sec, State Down,   Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5   Hello due in inactive   Adjacency state Down</pre>

## 19.2.55 show ip route process-detail

<b>Command</b>	<b>show ip route [database] process-detail</b>
	Display the IP routing table with specific process ID or Tag.
<b>Parameter</b>	The parameter of <b>database</b> means displaying all the routers, no parameter means only displaying effective routers.
<b>Default</b>	Not importing any router of OSPF process by default.
<b>Mode</b>	Admin and Configuration Mode.
<b>Usage Guide</b>	-
<b>Example</b>	<pre>Switch#show ip route database process-detail Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP O - OSPF, IA - OSPF inter area N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2 E1 - OSPF external type 1, E2 - OSPF external type 2 i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area &gt; - selected route, * - FIB route, p - stale info C *&gt; 127.0.0.0/8 is directly connected, Loopback O 192.168.2.0/24 [110/10] is directly connected, Vlan2, 00:06:13,process 12 C *&gt; 192.168.2.0/24 is directly connected, Vlan2</pre>



## 19.2.56 show ip protocols

<b>Command</b>	<b>show ip protocols</b>
	Display the running routing protocol messages.
<b>Parameter</b>	
<b>Default</b>	-
<b>Mode</b>	Admin and Configuration Mode.
<b>Usage Guide</b>	-
<b>Example</b>	<p>Switch#show ip protocols</p> <p>Use "show ip protocols" command will show the messages of the routing protocol running on current layer 3 switch</p> <p>For example, the displayed messages are:</p> <p>Routing Protocol is "ospf 0"</p> <p>Invalid after 0 seconds, hold down 0, flushed after 0</p> <p>Outgoing update filter list for all interfaces is</p> <p>Incoming update filter list for all interfaces is</p> <p>Redistributing:</p> <p>Routing for Networks:</p> <p>10.1.1.0/24</p> <p>12.1.1.0/24</p> <p>Routing Information Sources:</p> <p>Gateway Distance Last Update</p> <p>Distance: (default is 110)</p> <p>Address Mask Distance List</p> <p>Routing Protocol is "bgp 0"</p> <p>Outgoing update filter list for all interfaces is</p> <p>Incoming update filter list for all interfaces is</p> <p>IGP synchronization is disabled</p> <p>Automatic route summarization is disabled</p> <p>Neighbor(s):</p> <p>Address Filtn Filtn Distln DistOut Weight RouteMap</p> <p>Incoming Route Filter:</p>