CLI Reference Guide

(GEP-2652)

V1.0

Digital Data Communications GmbH.

http://www.level1.com

CLI Reference Guide

GEP-2652

26-Port Web Smart Gigabit PoE Switch,
2 x Gigabit SFP, 24 PoE Outputs, 370W

CLI Reference Guide

This guide includes detailed information on the switch software, including how to operate and use the management functions of the switch. To deploy this switch effectively and ensure trouble-free operation, you should first read the relevant sections in this guide so that you are familiar with all of its software features.

Who Should Read This Guide?

This guide is for network administrators who are responsible for operating and maintaining network equipment. The guide assumes a basic working knowledge of LANs (Local Area Networks), the Internet Protocol (IP), and Simple Network Management Protocol (SNMP).

How This Guide is Organized

This guide describes the switch's command line interface (CLI). For more detailed information on the switch's key features or information about the web browser management interface refer to the *Web Management Guide*.

The guide includes these section

- Section I "Getting Started" — Includes information on initial configuration.
- Section II "Command Line Interface" — Includes all management options

available through the CLI.

- Section III "Appendices" — Includes information on troubleshooting switch management access.

Related Documentation

This guide focuses on switch software configuration through the CLI.

For information on how to manage the switch through the Web management interface, see the following guide:

Web Management Guide

For information on how to install the switch, see the following guide:

Quick Start Guide

For all safety information and regulatory statements, see the following documents:

Quick Start Guide

Safety and Regulatory Information

Conventions

The following conventions are used throughout this guide to show information:

Note: Emphasizes important information or calls your attention to related features or instructions.

Caution: Alerts you to a potential hazard that could cause loss of data, or damage the system or equipment.

Revision History

This section summarizes the changes in each revision of this guide.

Revision	*Date*	*Change Description*
v103SP7D 190110	10/2018	Initial release

Table of Contents

1 Port basic configuration. 14

1.1 bpdu src-mac-check 14
1.2 description 14
1.3 dot1x auth-address-table 15
1.4 dot1x mac-auth-bypass 15
1.5 dot1x mac-auth-bypass multi-user 16
1.6 dot1x mac-auth-bypass timeout-activity 16
1.7 dot1x max-users 17
1.8 dot1x port-control auto 18
1.9 dot1x port-control-mode 18
1.10 duplex 19
1.11 flowcontrol 20
1.12 end 20
1.13 exit 21
1.14 line-detect 21
1.15 line-detect detail 21
1.16 list 22
1.17 lldp Enable 22
1.18 lldp encapsulation snap 23
1.20 lldp tlv-anble 24
1.21 logout 25
1.22 loopback 26
1.23 cross-over 26
1.24 port-isolate interface 27
1.25 port-security aging-time 27
1.26 port-security mac-address stick 28
1.27 port-security mac-address vlan 28
1.28 port-security max-mac-count 29
1.29 port-security clear mac-table unicast 29
1.30 rate-limit 30
1.31 speed 31
1.32 strom-control 31
1.33 shutdown 32
1.34 dot1q-tunnel Enable 33
1.35 dot1q-tunnel tpid 33
1.36 global 34
1.37 clear mac-address-table dynamic 35
1.38 clear mac-address-table static 36
1.39 show 36
1.40 default 38
1.41 no 40
1.42 help 41

2 VLAN 42

2.1 vlan 42
2.2 name 42
2.3 show vlan 43
2.4 switchport access 44
2.5 switchport mode 45
2.6 switchport trunk 46
2.7 switchport hybrid allowed vlan 47
2.8 switchport hybrid native vlan 48
2.9 mac-vlan mac 48
2.10 mac-vlan Enable 49

2.11 subnet-vlan ip-address 50
2.12 subnet-vlan Enable 51
2.13 protocol-vlan frametype 52
2.14 vlan-translation 53
2.15 vlan-translation Enable 54
2.16 dot1q-tunnel Enable 54
2.17 dot1q-tunnel tpid 55
2.18 dot1q-tunnel inner-vid 56
2.19 voice vlan 57
2.20 voice vlan cos 57
2.21 voice vlan aging 58
2.22 voice vlan mac-address 59
2.23 voice vlan Enable 60
2.24 voice vlan mode auto 60
2.25 voice vlan security Enable 61
2.26 private-vlan 61
2.27 private-vlan association 62
2.28 switchport mode private-vlan 63
2.29 switchport private-vlan association 64
2.30 show mac-vlan 64
2.31 show subnet-vlan 65
2.32 show protocol-vlan 66
2.33 show vlan-translation 67
2.34 show dotq1q-tunnel 67
2.35 show port vlan membership 68
2.36 show voice vlan 69
2.37 show voice vlan interface 70
2.38 show vlan private-vlan 70

3 ACL 72

3.1 IP standard access list 72
3.2 IP extended access list 72
3.3 MAC extended access list 74
3.4 Expert extended access list 76
3.5 IP standard access list 77
3.6 access list ip extended 78
3.7 access list mac extended 79
3.8 access list expert extended 80
3.9 ip access-list 82
3.10 mac access-list extended 82
3.11 expert access-list extended 83
3.12 access group 84
3.13 IPV6 standard access list 85
3.14 IPV6 extended access list 85
3.15 access group 87
3.16 show access-list 88
3.17 show access-group 88

4 PoE management 89

4.1 poe reset 89
4.2 poe Enable 89
4.3 poe mode 92
4.4 poe type 92
4.5 poe priority 93
4.6 poe max-power 94
4.7 poe alarmpower 95

4.8 poe reserve-power 96
4.9 poe individual 96
4.10 poe sysmarks method 97
4.11 poe uninterruptible-power 97
4.12 poe notification-control 98
4.13 ic-temp btsh-set 99

5 mstp 100

5.1 spanning-tree 100
5.2 spanning-tree loopguard default 101
5.3 spanning-tree max-hops 101
5.4 spanning-tree mode 102
5.5 spanning-tree mst configure 103
5.6 spanning-tree pathcost method 104
5.7 spanning-tree portfast bpdufilter default 105
5.8 spanning-tree portfast bpduguard default 106
5.9 spanning-tree portfast default 106
5.10 spanning-tree reset 106
5.11 spanning-tree priority 107
5.12 spanning-tree tc-protection 108
5.13 spanning-tree tc-protection tc-guard 108
5.14 spanning-tree tx-hold-count 108
5.15 spanning-tree autoedge 109
5.16 spanning-tree bpdufilter 109
5.17 spanning-tree bpduguard 110
5.18 spanning-tree compatible Enable 110
5.19 spanning-tree guard loop 111
5.20 spanning-tree guard none 111
5.21 spanning-tree guard root 112
5.22 spanning-tree ignore tc 112
5.23 spanning-tree link-type 112
5.24 spanning-tree mst cost 113
5.25 spanning-tree mst port-priority 114
5.26 spanning-tree port-priority 115
5.27 spanning-tree portfast 115
5.28 spanning-tree tc-guard 116
5.29 show spanning-tree 116
5.30 show spanning-tree interface 117
5.31 show spanning-tree mst 118

6.DHCP Relay & Server & Snooping 120

6.1 service dhcp 120
6.2 ip helper-address 120
6.3 ip dhcp relay information option 121
6.4 ip dhcp relay information trust-user-option 121
6.5 ip dhcp information option circuitid 122
6.6 ip dhcp information option remoteid 122
6.7 ip dhcp information option ip 123
6.8 show ip dhcp relay 124
6.9 ip dhcp snooping 125
6.10 ip dhcp snooping vlan 125
6.11 ip dhcp snooping trust 126
6.12 ip dhcp snooping suppression 126
6.13 ip dhcp snooping verify mac-address 128
6.14 ip dhcp snooping verify mac 128
6.15 ip dhcp snooping dhcpserver 129

6.16 ip dhcp snooping information option 129
6.17 ip dhcp snooping information client_option 130
6.18 ip dhcp snooping bingding mac 130
6.19 ip dhcp snooping database write-delay 131
6.20 ip dhcp snooping database write-to-flash 131
6.21 renew ip dhcp snooping database 132
6.22 clear ip dhcp snooping binding 132
6.23 show ip dhcp snooping 133
6.24 show ip dhcp snooping binding 134
6.25 show ip dhcp snooping trust 135
6.26 show ip dhcp snooping suppression 135
6.27 service dhcp-server 135
6.28 ip dhcp pool 136
6.29 network 137
6.30 lease 137
6.31 option 138
6.32 default-rouer 139
6.33 dns-server 140
6.34 domain-name 141
6.35 host 141
6.36 ip dhcp excluded-address 142
6.37 clear ip dhcp server binding 143
6.38 clear ip dhcp server conflict 143
6.39 show ip dhcp server 144
6.40 show ip dhcp server binding 145
6.41 show ip dhcp server conflict 145
6.42 show ip dhcp server host 146
6.43 show ip dhcp server exclude 146

7.DAI inspection 148

7.1 ip arp inspection 148
7.2 ip arp inspection vlan 148
7.3 ip arp inspection trust 149
7.4 ip arp entry 150
7.5 ip arp inspection rate-limit 150
7.6 ip arp inspection dhcp-snooping-entries 151
7.7 ip arp anti-spoofing 151
7.8 anti-arp-spoofing ip 152
7.9 ip arp static-binding 152
7.10 ip arp check 153
7.11 arp-check 154
7.12 ip arp gratuitous-arp 154
7.13 show ip arp 155
7.14 show anti-arp-spoofing 156

8 IP Source Guard 157

8.1 ip verify source 157
8.2 ip source binding 158
8.3 show ip verify source 158

9 .IGMP Snooping & MLD Snooping 160

9.1 ip igmp snooping 160
9.2 ip igmp snooping forwarding-mode 160
9.3 ip igmp snooping dyn-mr-aging-time 161
9.4 ip igmp snooping host-aging-time 162
9.5 ip igmp snooping query-max-response-time 163

9.6 ip igmp snooping suppression Enable 164
9.7 ip igmp snooping unknow-group-suppression 164
9.8 ip igmp snooping filter_mode Enable 165
9.9 ip igmp snooping filter auth 165
9.10 ip igmp profile 166
9.11 groups 167
9.12 ip igmp snooping vlan 167
9.13 ip igmp snooping vlan fast-leave Enable 168
9.14 ip igmp snooping vlan mrouter learn 169
9.15 ip igmp snooping vlan mrouter interface 169
9.16 ip igmp snooping querier 170
9.17 ip igmp snooping vlan querier address 171
9.18 ip igmp snooping vlan querier max-response-time 171
9.19 ip igmp snooping vlan querier query-interval 172
9.20 ip igmp snooping vlan querier timer expiry 173
9.21 ip igmp snooping vlan querier version 174
9.22 ip igmp snooping max-groups 174
9.23 ip igmp snooping filter 175
9.24 show ip igmp profile 176
9.25 show ip igmp snooping 177
9.26 show ip igmp snooping vlan 178
9.27 show ip igmp snooping mrouter 179
9.28 show ip igmp snooping interfaces 179
9.29 show ip igmp snooping groups 180
9.30 ipv6 mld snooping 181
9.31 ipv6 mld snooping forwarding-mode 181
9.32 ipv6 mld snooping dyn-mr-aging-time 182
9.33 ipv6 mld snooping host-aging-time 183
9.34 ipv6 mld snooping query-max-response-time 183
9.35 ipv6 mld snooping suppression Enable 184
9.36 ipv6 mld snooping unknow-group-suppression 185
9.37 ipv6 mld snooping filter_mode Enable 185
9.38 ipv6 mld snooping filter auth 186
9.39 ipv6 mld profile 187
9.40 groups 187
9.41 ipv6 mld snooping vlan 188
9.42 ipv6 mld snooping vlan fast-leave Enable 189
9.43 ipv6 mld snooping vlan mrouter learn 189
9.44 ipv6 mld snooping vlan mrouter interface 190
9.45 ipv6 mld snooping querier 191
9.46 ipv6 mld snooping vlan querier address 191
9.47 ipv6 mld snooping vlan querier max-response-time 192
9.48 ipv6 mld snooping vlan querier query-interval 193
9.49 ipv6 mld snooping vlan querier timer expiry 193
9.50 ipv6 mld snooping vlan vid querier version 194
9.51 ipv6 mld snooping max-groups 195
9.52 ipv6 mld snooping filter 195
9.53 show ipv6 mld profile 196
9.54 show ipv6 mld snooping 197
9.55 show ipv6 mld snooping vlan 198
9.56 show ipv6 mld snooping mrouter 199
9.57 show ipv6 mld snooping interfaces 199
9.58 show ipv6 mld snooping groups 200

10 QoS 201

10.1 mls qos map cos-queue 201

10.2 mls qos map dscp-cos 201
10.3 mls qos queue algorithm 202
10.4 mls qos queue wrr weight 203
10.5 mls qos queue wfq weight 204
10.6 mls qos cos 204
10.7 mls qos trust 205
10.8 class-map 206
10.9 match 207
10.10 policy-map 208
10.11 class 208
10.12 police 209
10.13 set 210
10.14 service-policy 211
10.15 show mls qos maps 211
10.16 show mls qos queueing 212
10.17 show mls qos interface 212
10.18 show class-map 213
10.19 show policy-map 213

11 MAC address 215

11.1 clear mac-address-table dynamic 215
11.2 mac-address-learning 215
11.3 mac-address dynamic-limit 216
11.4 mac-address-table aging-time 216
11.5 mac-address-table filtering 217
11.6 mac-address-table static 218
11.7 mac-address-table multicast 219
11.8 clear mac-address-table static 219
11.9 show mac-address-learning 220
11.10 show mac-address-table aging-time 220
11.11 show mac-address-table count 221
11.12 show mac-address-table dynamic 221
11.13 show mac-address-table filtering 222
11.14 show mac-address-table interface 223
11.15 show mac-address-table static 224

12 SNMP & RMON 225

12.1 Enable service snmp-agent 225
12.2 snmp-server community 225
12.3 snmp-server view 226
12.4 snmp-server view-rule 227
12.5 snmp-server group 228
12.6 snmp-server user 229
12.7 snmp-server host 230
12.8 show snmp 231
12.9 rmon statistics 232
12.10 rmon event 233
12.11 rmon alarm 234
12.12 rmon history 235
12.13 show rmon statistics 236
12.14 show rmon event 236
12.15 show rmon alarm 237
12.16 show rmon history 237

13 system status 239

13.1 ping 239

13.2 traceroute 239
13.3 tftp 240
13.4 copy running-config startup-config 240
13.5 Copy filename tftp: serveraddress 241
13.6 Copy tftp: server-address configfile 241
13.7 system config backup 242
13.8 system config upgrade 242
13.9 system upgrade 243
13.10 telnet-radius-auth 243
13.11 telnet tel_port 244
13.12 ssh-radius-auth 244

14 Basic Configuration Management 245

14.1 Enable 245
14.2 Enable password 245
14.3 clock set 246
14.4 Enable service 246
14.5 hostname 247
14.6 username 248
14.7 password 248
14.8 reload 249
14.9 write 249
14.10 line-detect 250
14.11 uptime 250
14.12 interface vlan 251
14.13 ip address dns 252
14.14 ip address 252
14.15 ip address mtu 253
14.16 ip address gateway 253
14.17 ip address pri 254
14.18 ip address ip-mode 254
14.19 ip address ip-mode dhcp 255
14.20 resetfactoryconfig 255
14.21 jumbo-frame 256
14.22 eee 256
14.23 SNTP Enable 257
14.24 show interfaces brief 258

15 System Log 259

15.1 Logging on 259
15.2 show logging 260
15.3 Logging Consolee 261
15.4 Logging buffered 262
15.5 Logging monitor 263
15.6 Logging file 263
15.7 Logging server 265
15.8 Logging trap 266
15.9 Logging source 267
15.10 Logging facility 268
15.11 Service sequence-numbers 269
15.12 Service timestamps 269
15.13 Service sysname 270
15.14 Clear logging 271
15.15 Terminal monitor 272
15.16 Dir 272
15.17 Delete 273

15.18 More 274
15.19 Debug 274

16 AAA 276

16.1 aaa new-model 276
16.2 aaa authentication dot1x 276
16.3 aaa authentication Enable 277
16.4 aaa authentication login 278
16.5 aaa group server 279
16.6 server 280
16.7 aaa domain Enable 281
16.8 aaa domain 281
16.9 state 282
16.10 username-format 283
16.11 aaa local authentication attempts 284
16.12 aaa local authentication lockout-time 284
16.13 show aaa method-list 285

17 802.1X 286

17.1 dot1x 286
17.2 dot1x port-control auto 286
17.3 dot1x port-control-mode 287
17.4 dot1x auto-req 288
17.5 dot1x auto-req packet-num 288
17.6 dot1x auto-req interval 289
17.7 dot1x auto-req user-detect 289
17.8 dot1x re-auth 290
17.9 dot1x req-max 291
17.10 dot1x pae-group-addr 291
17.11 dot1x timeout re-authperiod 292
17.12 dot1x timeout server-timeout 292
17.13 dot1x timeout supp-timeout 293
17.14 dot1x timeout tx-period 293
17.15 dot1x max-users 294
17.16 dot1x auth-address-table address 295
17.17 dot1x mac-auth-bypass 295
17.18 dot1x mac-auth-bypass multi-user 296
17.19 dot1x mac-auth-bypass timeout-activity 297
17.20 dot1x multi-mab quiet-period 297
17.21 dot1x guest-vlan 298
17.22 dot1x auth-fail max-attempt 299
17.23 dot1x auth-fail vlan 299
17.24 dot1x dynamic-vlan Enable 300
17.25 show dot1x 301
17.26 show dot1x port-control 302
17.27 show dot1x auto-req 302
17.28 show dot1x re-auth 303
17.29 show dot1x summary 303
17.30 show dot1x auth-address-table 304

18 RADIUS 305

18.1 radius-server host 305
18.2 radius-server attribute 306
18.3 radius-server retransmit 306
18.4 radius-server timeout 307
18.5 radius-server dead-criteria 308

18.6 radius-server deadtime 309
18.7 show radius 310
18.8 show radius server 311
18.9 show radius attribute 311

19 TACACS+ 313

19.1 tacacs-server host 313
19.2 tacacs-server key 314
19.3 tacacs-server timeout 314
19.4 tacacs-server attempts 315
19.5 tacacs-client session-sock 316
19.6 show tacacs 317

20 gvrp 318

20.1 gvrp Enable 318
20.2 gvrp timer 318

21 DHCP CLIENT 320

21.1 ipaddress vlan 1 ip-mode 320
21.2 ip address dhcp 320

22 FTP Client 322

22.1 Copy filename ftp: serveraddress 322
22.2 Copy ftp:serveraddress serverfile 323

23 Port Security 324

23.1 port-security violation 324
23.2 port-security aging-time 325
23.3 port-security mac-address 326
23.4 por-security max-mac-count 326
23.5 port-security mac-address stick 327
23.6 port-security block 327
23.7 port-security clear mac-table unicast 328
23.8 show port-security 329

24 Trunk & LACP 330

24.1 aggregateport load-balance 330
24.2 port-group 331
24.3 lacp Enable 332
24.4 lacp system-priority 332
24.5 lacp tick-time 333
24.6 lacp port-priority 333
24.7 lacp admin-key 334
24.8 show aggregateport 335
24.9 show lacp 336

25 Monitor 338

25.1 monitor session 338
25.2 show monitor 339

26 ERPS-Ethernet Ring Protection Switching 340

26.1 erps ring ring-id rplowner 340
26.2 erps ring ring-id rplneighbor 341
26.3 erps ring ring-id common 341
26.4 erps ring ring-id Enable 342

26.5 erps ring ring-id fs 343
26.6 erps ring ring-id ms 343
26.7 erps ring ring-id clear 344
26.8 erps ring ring-id subring 344
26.9 erps ring ring-id ring_role 345
26.10 erps ring ring-id mode 346
26.11 erps ring ring-id mac 347
26.12 erps delete ring 347
26.13 erps timeout 348
26.14 show erps ring 349
26.15 show erps timeout 350

27 Loopback 352

27.1 loopback 352
27.2 loopback action 352
27.3 loopback time 353
27.4 show loopback 353

1 Port basic configuration

1.1 bpdu src-mac-check

Open an interface bpdu source MAC inspection. Users can use the command no options close the interface of bpdus source MAC checking.

bpdu src-mac-check mac-address

no bpdu src-mac-check

Parameter Description

Parameter	Description
mac-address	Show only received the source MAC address to the address of the bpdu frame.
no	No said that port receive any bpdus frame .

Default Configuration The default is off.

Command mode Interface configuration mode.

Configuration Example

```
Console(config)# interface GigabitEthernet 1
Console(config-if-GigabitEthernet1)# bpdu src-mac-check 11:22:33:44:55:66
```

1.2 description

Set name for specified port; the no command cancels this configuration.

description string

no description

Parameter Description

Parameter	Description
string	Set name for specified port，range is 1-80 characters .

Default Configuration The default value is null.

Command mode Interface configuration mode and interface range configuration mode.

Configuration Example

```
Console(config)# interface GigabitEthernet 1
Console(config-if-GigabitEthernet1)#description abcd
```

1.3 dot1x auth-address-table

This command sets 802.1 X allow certification address table.
Use no option command to delete certification address.

dot1x auth-address-table address mac-address

no dot1x auth-address-table address mac-address

Parameter Description

Parameter	Description
mac-address	Certification of the physical address, dotted in hexadecimal fo

Default Configuration The default value is no any certification address

Command mode Interface configuration mode and interface range configuration mode.

Usage Guide Only in the address table address allows the use of 802.1 X attestation, use the show dot1x auth - address - table command to check the certification address table.

Configuration Example

Add the certification address on the interface.

```
Console(config)# interface GigabitEthernet 1
Console(config-if-GigabitEthernet1)# dot1x auth-address-table
address 00:D0:f8:00:00:00
```

Relative Command

Command	Description
show dot1x auth-address-table	Show 802.1 X allows certification address table.

1.4 dot1x mac-auth-bypass

Set the MAC bypass authentication.

dot1x mac-auth-bypass

no dot1x mac-auth-bypass

Default Configuration The default is not support MAC bypass authentication

Command mode Interface configuration mode and interface range configuration mode.

Usage Guide You can use the show dot1x port-control command view Settings.

Configuration Example The following are set examples of 802.1x MAC bypass authentication:

```
Console(config)# interface GigabitEthernet 1
Console(config-if-GigabitEthernet1)#dot1x mac-auth-bypass
```

Relative Command

Command	Description
show dot1x port-control	Show interface 802.1x information

1.5 dot1x mac-auth-bypass multi-user

Set x 802.1 MAC bypass certification violation.

dot1x mac-auth-bypass multi-user

no dot1x mac-auth-bypass multi-user

Default Configuration The default is no violation.

Command mode Interface configuration mode and interface range configuration mode.

Usage Guide Can be used to show running-config view 802.1 x Settings.

Configuration Example Set 802.1x MAC bypass certification violation case:

```
Console(config)# interface GigabitEthernet 1
Console(config-if-GigabitEthernet1)# dot1x mac-auth-bypass multi-user
```

Relative Command

Command	Description
show dot1x port-control	Show interface of 802.1x information.

1.6 dot1x mac-auth-bypass timeout-activity

Set 802.1x MAC address bypass authentication of online time.

dot1x mac-auth-bypass timeout-activity value

no dot1x mac-auth-bypass timeout-activity

Parameter Description

Parameter	Description
value	Online time, in seconds, range 1-65535.

Default Configuration

No default configuration values,expression never timeout.

Command mode

Interface configuration mode and interface range configuration mode.

Usage Guide

Can be used to show running-config view 802.1 x Settings.

Configuration Example

The following is examples of set 802.1x MAC bypass authentication timeout:
Console(config)# interface GigabitEthernet 1
Console(config-if-GigabitEthernet1)# dot1x mac-auth-bypass timeout-activity 3600

Relative Command

Command	Description
show dot1x port-control	Show interface of 802.1x information.

1.7 dot1x max-users

In the interface mode ,sets the maximum users number to allowed connect
port; the “no dot1x max-user” command restores the default setting.

dot1x max-users value

Parameter Description

Parameter	Description
value	Max-users number,range of 0-255.

Default Configuration

The default max-users allowed is 64.

Command mode

Interface configuration mode and interface range configuration mode.

Configuration Example

```
Console(config)# interface GigabitEthernet 1
Console(config-if-GigabitEthernet1)# dot1x max-users 200
```

Relative Command

Command	Description
show dot1x	Show interface of 802.1x information.

1.8 dot1x port-control auto

In the interface,Sets the 802.1x authentication status; the “no dot1x port-control” command restores the default setting.

dot1x port-control auto

no dot1x port-control

Default Configuration

Interfaces not add to 802.1 x authentication by default.

Command mode

Interface configuration mode and interface range configuration mode.

Usage Guide

use the show dot1x Command to view 802.1x configuration.

Configuration Example

Setting port 1 to require 802.1x authentication mode:

```
Console(config)# interface GigabitEthernet 1
Console(config-if-GigabitEthernet1)# dot1x port-control auto
```

Relative Command

Command	Description
show dot1x	Show interface of 802.1x information.

1.9 dot1x port-control-mode

802.1 x control of the user by default is based on the MAC users to control, only authenticated users can use the Internet, and for other users can't use the same port network, the control model based on port and said a port when there is a user authentication through the ports become certified, all meet under the port users to be able to normal use the Internet. Based on single user port control mode, the port allows only a single user authentication through the, the ports become certified, can the normal use network. Control in single user mode, when ports to become certified, if there are other users have found the port, the port all users under the clear, certification again. Configure authentication mode Command is as follows:

dot1x port-control-mode {**mac-based** | **port-based** }

no dot1x port-control-mode

Parameter Description

Parameter	Description
mac-based	802.1 x access control based on the MAC.
port-based	802.1 x access control based on the port.

Default Configuration

Default is based on MAC-based access control.

Command mode

Interface configuration mode and interface range configuration mode.

Usage Guide

can use the show dot1x port-control command to show interface 802.1x configuration.show dot1x port-control view port-based in the port, show running-config view dot1x port-control-mode port-based .
Set examples for port 802.1 x to participate in the certification:

Configuration Example

```
Console(config)# interface GigabitEthernet 1
Console(config-if-GigabitEthernet1)# dot1x port-control auto
Console(config-if-GigabitEthernet1)# dot1x port-control-mode port-based
```

Relative Command

Command	Description
show dot1x port-control	Show interface of 802.1x information.
show running-config	Show Console information

1.10 duplex

At the interface configuration mode, using the Command for the duplex Settings of the interface. The no command restores the default dulplex mode setting.

duplex {**auto** | **full** | **half**}

no duplex

Parameter Description

Parameter	Description
auto	Expression full-duplex and half-duplex adaptive
full	Expression full-duplex
half	Expression half-duplex

Default Configuration

The default is full duplex and half duplex adaptive.

Command mode

Interface configuration mode and interface range configuration mode.

Usage Guide

Interface of the duplex properties associated with the type of interface. You can use the show interfaces command to view the duplex configuration of the interface.

Configuration Example

Set interface duplex configuration is auto:

```
Console(config)# interface GigabitEthernet 1
Console(config-if-GigabitEthernet1)#  duplex auto
```

Relative Command

Command	Description
show interfaces	Show the interface Settings and statistics

1.11 flowcontrol

Enables the flow control function for the port: the "**no flow control**" command disables the flow control function for the port.

flowcontrol {**on** | **off**}

no flowcontrol

Parameter Description

Parameter	Description
on	Enable flowcontrol
off	Disable flowcontrol

Default Configuration

The default is off flow control.

Command mode

Interface configuration mode and interface range configuration mode.

Usage Guide

After the flow control function is Enabled, the port will notify the sending device to slow down the sending speed to prevent packet loss when traffic received exceeds the capacity of port cache.

Configuration Example

Open the flow control of gigabit Ethernet interface 1:

```
Console(config)# interface GigabitEthernet 1
Console(config-if-GigabitEthernet1)#  flowcontrol on
```

Relative Command

Command	Description
show interfaces	Show the interface Settings and statistics

1.12 end

Quit current mode and return to Admin mode when not at User Mode/ Admin Mode.

duplex {**auto** | **full** | **half**}

no duplex

Command mode

Interface configuration mode and interface range configuration mode.

Configuration Example

```
Console(config)# interface GigabitEthernet 1
Console(config-if-GigabitEthernet1)# end
Console(config)# interface range GigabitEthernet 1-4
Console(config-if)# end
```

1.13 exit

	Quit current mode and return to it's previous mode. **duplex** {**auto** | **full** | **half**} **no duplex**
Command mode	nterface configuration mode and interface range configuration mode.
Configuration Example	Console(config)# interface GigabitEthernet 1 Console(config-if-GigabitEthernet1)# exit Console(config)#

1.14 line-detect

	Perform line-detect Command,can be used to test the connection of the cable. **line-detect**
Command mode	Interface configuration mode.
Usage Guide	line-detect Command mainly used to check the status of cable and cable fault occur (such as open circuit), used to locate the fault location.
Configuration Example	Console(config)# interface aggregateport 1 Console(config-if-AggregatePort 1)# line-detect

1.15 line-detect detail

	Perform line-detect detail command,can be used to test the connection o the cable. **line-detect detail**
Command mode	Interface configuration mode.
Usage Guide	line-detect detail command mainly used in detail check the status of a wire and the cable fault occurs (such as open circuit), used to locate the fault location.
Configuration Example	Console(config)# interface aggregateport 1 Console(config-if-AggregatePort 1)# line-detect detail

1.16 list

Perform list command,Can be used to print out the Command list.

list

list string

Parameter Description

Parameter	Description
string	The list of print for string string matching

Command mode

Interface configuration mode and interface range configuration mode.

Configuration Example

```
Console(config)# interface aggregateport 1
Console(config-if-AggregatePort 1)# list ip
list <string>
  show ip arp
  show ip dhcp relay
  show ip dhcp snooping
  show ip dhcp snooping binding
  show ip igmp snooping config
  show ip igmp snooping m-vlan {<1-4094>}*1
  show ip igmp snooping unknow-group-suppression
  [no|default] description
  description <LINE>
  ip access-group [<1-199>|<WORD>] in
  no ip access-group [<1-199>|<WORD>] in
  ip igmp snooping max-groups <1-254>
  no ip igmp snooping max-groups
  default ip igmp snooping max-groups
```

1.17 lldp Enable

Globally and interface Enable LLDP function; no command globally or interface disables LLDP function.

lldp Enable

no lldpEnable

Default Configuration

Disable LLDP function.

Command mode

Interface configuration mode.

Usage Guide

If LLDP function is globally Enabled, it will be Enabled on port actively.

Configuration

Disable lldp in global and interface:

```
Console(config)# no lldp Enable
```

Example

```
Console(config)# interface aggregateport 1
Console(config-if-AggregatePort 1)# no lldp anable
```

Relative Command

Command	Description
show lldp status	Show LLDP status information

1.18 lldp encapsulation snap

Configuration LLDP packets encapsulation format, default using Ethernet II encapsulation format.

lldp encapsulation snap

no lldp encapsulation snap

Default Configuration

The default encapsulation using Ethernet II format.

Command mode

Interface configuration mode.

Usage Guide

In order to guarantee the normal communication of local equipment and neighbors, needs to be LLDP configured to the same message encapsulation format.

Configuration Example

Configuration LLDP packets encapsulation format for the SNAP:

```
Console(config)# interface aggregateport 1
Console(config-if-AggregatePort 1)# lldp encapsulation snap
```

Relative Command

Command	Description
show lldp status	Show LLDP status information

1.19 lldp mode

Configure the operating state of LLDP function of the port.

lldp mode {**rx** | **tx** | **txrx**}

no lldp mode

Parameter Description

Parameter	Description
tx	Configure the LLDP function as only being able to receive messages.
rx	Configure the LLDP function as only being able to send

	messages.
txrx	Configure the LLDP function as being able to both send and receive messages.

Default Configuration

the default is txrx

Command mode

Interface configuration mode

Usage Guide

Closed the LLDP working mode of the interface, the interface is no longer send and receive LLDP packets.

Configuration Example

set interface LLDP working mode is rx:

```
Console(config)# interface aggregateport 1
Console(config-if-AggregatePort 1)# lldp mode rx
```

Relative Command

Command	Description
show lldp status	Show LLDP status information

1.20 lldp tlv-anble

Configuration allows the release of the TLV type. Using the no option to cancel to distribute the TLV type.

lldp tlv-Enable { **basic-tlv** { all | port-description | system-capability | system-description | system-name } | **dot1-tlv** { all | port-vlan-id | protocol-vlan-id | vlan-name } | **dot3-tlv** { all | link-aggregation | mac-physic | max-frame-size | power } }

no lldp tlv-Enable { **basic-tlv** { all | port-description | system-capability | system-description | system-name } | **dot1-tlv** { all | port-vlan-id | protocol-vlan-id | vlan-name } | **dot3-tlv** { all | link-aggregation | mac-physic | max-frame-size | power } }

Parameter Description

Parameter	Description
basic-tlv	Basic manage TLV
port-description	Express port description TLV
system-capability	Express system capabilities TLV
system-description	Express system description TLV
system-name	Express system name TLV
dot1x-tlv	802.1 TLV

port-vlan-id	Express port vlan id TLV
protocol-vlan-id	Express port and protocol vlan id TLV
vlan-name	Express vlan name TLV
dot3-tlv	802.3 organizations defineTLV
link-aggregation	Express link aggregation TLV
mac-physic	Express MAC/PHY configuration/status TLV
max-frame-size	Express maximum frame size TLV
power	Express power via MDI TLV

Default Configuration

By default, for S12000 series products, the default only the TLV and IEEE 802.1 release, Basic the TLV, if you need to release the IEEE 802.3 the TLV and LLDP - MED the TLV, need through the LLDP the TLV - the Enable Command manually specify the release.

Command mode

Interface configuration mode

Usage Guide

The TLV, IEEE 802.1 configure basic management organizations define the TLV, IEEE 802.3 define the TLV, if all the Parameter is specified, will release all the types of optional the TLV.

Configuration Example

Configure all optional the TLV IEEE802.1 organization definitions:

```
Console(config)# interface aggregateport 1
Console(config-if-AggregatePort 1)# lldp tlv-Enable dot1x-tlv all
```

Relative Command

Command	Description
show lldp tlv-config interface	Show TLV configuration

1.21 logout

At the interface configuration mode using logout command exit CLI mode.

Command mode

Interface configuration mode and interface range configuration mode.

Configuration Example

```
Console(config)# interface GigabitEthernet 1
Console(config-if-GigabitEthernet1)# logout
Console>
```

1.22 loopback

	In global configuration mode use this Command is global configuration into the internal loop interface, using the no cancel configuration format. **loopback** **no loopback**
Default Configuration	no loopback
Command mode	Global Mode
Configuration Example	Console(config)# loopback

1.23 cross-over

	Interface configuration mode using cross - over this Command is the intersection line sequence features on the interface. **cross-over auto|mdi|mdix**
Default Configuration	The default is auto.
Command mode	Interface configuration mode and interface range configuration mode.
Usage Guide	After the intersection line sequence auto features, it is necessary to set the interface speed and duplex mode to auto (to be automatic), so that the interface can correct operation.
Configuration Example	Console(config)# interface GigabitEthernet 4 Console(config-if-GigabitEthernet4)# cross-over mdi

1.24 port-isolate interface

Configuration isolation between interfaces.

port-isolate interface {aggregateport [1-8] | GigabitEthernet [1-24]}

no port-isolate interface {aggregateport [1-8] | GigabitEthernet [1-24]}

Command mode

Interface configuration mode and interface range configuration mode.

Usage Guide

On Ethernet front ports can be isolated under multiple Ethernet front-end ports

Configuration Example

On Ethernet front ports GigabitEthernet 1 and 2、 3 isolation:

```
Console(config)# interface GigabitEthernet 1
Console(config-if-GigabitEthernet1)# port-isolate interface GigabitEthernet 2-3
```

1.25 port-security aging-time

Configure security MAC address aging time, using the no format back to default.

port-security aging-time time

no port-security aging-time

Parameter Description

Parameter	Description
Time	Aging time, integral form, the range is 0 to 1000000, the unit is second

Default Configuration

By default, the MAC address security aging time for 5 minutes.

Command mode

Interface configuration mode.

Usage Guide

Use this Command configuration interface secure MAC addresses of aging time. In the aging time, the interface secure MAC addresses will be aging. Aging time configuration is 0, not aging, safety all the MAC address will not be aging; Aging time is not configured to 0, namely the configuration of aging, aging time arrives, static security MAC and Sticky secure MAC will not be aging, dynamic security MAC will be aging.

Configuration Example

```
Console(config-if-GigabitEthernet2)# port-security aging-time 200
Console(config-if-GigabitEthernet2)#
```

1.26 port-security mac-address stick

Use this Command is open interface Stick learning function in interface configuration mode, using the no format this feature is prohibited.

port-security mac-address stick

no port-security mac-address stick

Parameter Description

Parameter	Description
Time	Aging time, integral form, the range is 0 to 1000000, the unit is ond

Default Configuration

The default interface Stick learning function is turned off.

Command mode

Interface configuration mode

Usage Guide

Use this Command configuration security the Sticky learning functions of the interface. After the feature Enabled, Sticky secure MAC address to take effect, and will not be aging; The interface to all dynamic security MAC into a Sticky secure MAC addresses; On the other hand, the interface Sticky learning function after the ban, the safety interface all Sticky secure MAC addresses into dynamic security MAC address.

Dynamic security MAC address is obtained by learning, users can be allowed to learn the MAC address of the largest number range, will learn the MAC address is set to secure MAC addresses, the secure MAC addresses can be aging, can also be transformed and Sticky secure MAC addresses, not aging.

Configuration Example

```
Console(config)# interface GigabitEthernet 1
Console(config-if-GigabitEthernet1)# port-security mac-address stick
```

1.27 port-security mac-address vlan

Use this Command in interface configuration mode is open interface Stic rning function, using the no format this feature is prohibited.

port-security mac-address mac-address **vlan** vlan-id

no port-security mac-address mac-address **vlan** vlan-id

Parameter Description

Parameter	Description
mac-address	Unicast MAC address, dotted in hexadecimal form.
vlan-id	VLAN ID value, integral form, the value range is 1-4094.

Command mode Interface configuration mode.

Configuration Example

```
Console(config)# interface GigabitEthernet 1
Console(config-if-GigabitEthernet1)# port-security mac-address 11:11:11:11:11
:11 vlan 1
```

Relative Command

Command	Description
show port-security	Show port-security information

1.28 port-security max-mac-count

Set maximum safe port address number, using the no format can restore default number.

port-security max-mac-count value

no port-security max-mac-count

Parameter Description

Parameter	Description
value	Range of 1-128

Default Configuration The default 128.

Command mode Interface configuration mode.

Usage Guide Security number address contains static configuration and dynamic learning security addresses the sum of the number, the default is 128, if set security address number is less than the current number of existing security address, you will be prompted to set up failure.

Configuration Example

Set port GigabitEthernet security address number is 2:1

```
Console(config)# interface GigabitEthernet 1
Console(config-if-GigabitEthernet1)# port-security max-mac-mount 2
```

Relative Command

Command	Description
show port-security	Show port-security information

1.29 port-security clear mac-table unicast

Use this Command is to clear the port under the MAC address list in interface configuration mode.

port-security clear mac-table unicast {**all** | **dynamic** | **static**}

Parameter Description

Parameter	Description
all	All of the unicast MAC address.
dynamic	The dynamic unicast MAC address.
static	The static unicast MAC address.

Command mode

Interface configuration mode.

Configuration Example

Clear unicast mac address in the interface:

```
Console(config)# interface GigabitEthernet 1
Console(config-if-GigabitEthernet1)# port-security clear mac-table unicast all
```

Relative Command

Command	Description
show port-security	Show port-security information

1.30 rate-limit

Set the max packet reception rate of a port.

rate-limit {**input** | **output**} bps

rate-limit bps

no rate-limit

Parameter Description

Parameter	Description
input	Input rate-limit
output	Output rate-limt
bps	The amount of bandwidth limit per second.
no	Restore the default value.

Command mode

Interface configuration mode and interface range configuration mode.

Configuration Example

```
Console(config)# interface GigabitEthernet 1
Console(config-if-GigabitEthernet1)# rate-limit input 1000
```

1.31 speed

To configure the rate of the interface, the interface configuration mode, t execution speed speed. To restore to the default rate of interface configuration using the no speed Command.

speed speed

No speed

Parameter Description

Parameter	Description
speed	The transmission rate of the interface, the unit is Mbps, rate values for 10, 100, 1000, 10000, auto. Speed value is not greater than the maximum rate of equipment.

Default Configuration

The default is auto.

Command mode

Interface configuration mode and interface range configuration mode.

Usage Guide

Speed rate value is not greater than setting the maximum rate of value, use the show interfacesCommand can view the interface configuration information.

Configuration Example

Configure the aggregation of port 1 rate of 100 Mbps:

```
Console(config)# interface GigabitEthernet 1
Console(config-if-GigabitEthernet1)#  speed 100
```

Relative Command

Command	Description
Show interfaces	Show the interface Settings and statistics.

1.32 strom-control

Set the storm control of the switch interface. Use this no command off the corresponding storm control function.

strom-control {**all** | **broadcast** | **multicast** | **unicast**} value

no storm-control {**all** | **broadcast** | **multicast** | **unicast**}

Parameter Description

Parameter	Description
all	Open all the storm control function.
broadcast	Open the control function of broadcast storm.

multicast	Open the control function of unknown multicast storm.
unicast	Open to the unknown list of control function of the storm.
value	Unit: Kbps, must be in multiples of 64, is set to 0 to disable the rm inhibition function.

Command mode

Interface configuration mode and interface range configuration mode.

Usage Guide

When a port to receive excessive broadcast, multicast or unicast packets, can produce a packet of storm, which can result in slow network and increase the timeou . The execution of the protocol stack errors or some error in the network configuratio is likely to lead to a storm.

Equipment can be broadcast, multicast and unicast data flow control the storm. When received a glut of broadcast and multicast or unicast package, equipment will temporarily banned from corresponding type FR packet forwarding until data flow back to normal (at this time the package data will be back to normal).

Configuration Example

```
Console(config)# interface GigabitEthernet 1
Console(config-if-GigabitEthernet1)# storm-control all 128
```

Relative Command

Command	Description
show storm-control	Show storm-control information

1.33 shutdown

In interface configuration mode, using the no command to open interface.

shutdown

no shutdown

Command mode

Interface configuration mode and interface range configuration mode.

Usage Guide

For interface (Ethernet interface, the Ap interface, SVI interface), the close command interface, the other configuration of the interface still exists, but doesn't work, use the show interfaces command view the interface state.

Configuration Example

Close the Ethernet interface 1:

```
Console(config)# interface GigabitEthernet 1
Console(config-if-GigabitEthernet1)# shutdown
```

Relative Command

Command	Description
show interfaces	Show the interface Settings and statistics.

1.34 dot1q-tunnel Enable

Using Command dot1q-tunnel Enable to open port dot1q-tunnel basic functions. No option of the Command is used to close port dot1q-tunnel function.

dot1q-tunnel Enable

no dot1q-tunnel Enable

Default Configuration

The default port dot1q-tunnel basic functions in the closed state.

Command mode

Interface configuration mode

Usage Guide

When open the basic function of dot1q-tunnel port, if the message originally did not carry out the Tag would be for the newspaper article to add a new Vlan Tag, the carry Vlan ID for the default VID of the port, and thus a new Vlan Tag as a packet forwarding.

- If the message has been carrying out the Tag, then no need to add a new Vlan Tag, direct to the newspaper article carries the Vlan Tag as the forwarding of a message.
- Only when a message in the first layer under the EtherType and interface dot1q-tunnel TPID consistent when that message to carry out the Tag.
- Under the Ethernet port view to execute the Command, then the configuration in the current port only comes into effect; Under the second aggregation port view to execute the Command, the second aggregation ports all members of the group and the corresponding aggregation effect; Under the view port group to execute the Command, then the configuration will take effect in all the ports in the port group.

Configuration Example

```
Console (config)# interface GigabitEthernet 2
Console (config-if-GigabitEthernet2)# dot1q-tunnel Enable
```

Relative Command

Command	Description
dot1q-tunnel tpid	The set port dot1q-tunnel protocol identification tags
show dot1q-tunnel	Show the port configuration information

1.35 dot1q-tunnel tpid

At the interface configuration mode using the label for the Command set port dot1q-tunnel protocol id. Using the no format restore to default values.

dot1q-tunnel tpid

no dot1q-tunnel tpid

Parameter Description

Parameter	Description
tpid	Identification tag agreement, the range is 0x0-0XFFFF.

Default Configuration

0x88a8

Command mode

Interface configuration mode

Configuration Example

Set the interface 2 dot1q-tunnel marks is 0x9100:

```
Console(config)# interface GigabitEthernet 2
Console(config-if-GigabitEthernet2)# dot1q-tunnel tpid 0x9100
```

Relative Command

Command	Description
dot1q-tunnel Enable	Enable dot1q-tunnel function
show dot1q-tunnel	Check the port configuration information

1.36 global

Use this Command in interface configuration mode set port global acl. Using the no format restore to default values.

global expert|ip|mac access-group {<2700-2799>|<1-199>|<700-799>} in

no global expert|ip|mac access-group {<2700-2799>|<1-199>|<700-799>} in

Parameter Description

Parameter	Description
access-group	Required Parameter：access-group value，range standard IP&extended IP access-group <1-199> Eatended MAC access-group <700-799> expert access-group <2700-2799>

Command mode

Interface configuration mode and interface range configuration mode.

Usage Guide

Use this Command for ACL is applied to all ports.

Configuration Example

At the interface 2 general ACL rule 100 is applied to all ports

```
Console(config)# ip access-list extended 100
Console(config-ext-nacl)# permit ip any any
Console(config-ext-nacl)# exit
Console(config)# interface GigabitEthernet 2
Console(config-if-GigabitEthernet2)# global ip access-group 100 in
```

Relative Command

Command	Description
show access-group	Show the application port

1.37 clear mac-address-table dynamic

Clear dynamic address.

clear mac-address-table dynamic[address mac-addr] [interface interface-id] [vlan vlan-id]

Parameter Description

Parameter	Description
dynamic	Clear all the dynamic address
address mac-addr	Clear the appoint address
interface interface-id	Clear the appoint dynamic address in the interface
vlan vlan-id	Clear the appoint dynamic address in the vlan

Command mode

Interface configuration mode and interface range configuration mode.

Usage Guide

use the show mac-address-table dynamic command to show all dynamic address

Configuration Example

clear the dynamic in the interface 2:

```
Console(config)# interface GigabitEthernet 2
Console(config-if-GigabitEthernet2)# clear mac-address-table dynamic
```

Relative Command

Command	Description
show mac-address-table dynamic	Show dynamic address table information.

1.38 clear mac-address-table static

Clear the static address of the interface

clear mac-address-table static {**address** mac-addr | **interface** [*interface -id*] | **vlan** [*vlan-id*]}

Parameter Description

Parameter	Description
static	Clear all the dynamic address
address mac-addr	Clear the appoint address
interface interface-id	Clear the appoint dynamic address in the interface
vlan vlan-id	Clear the appoint dynamic address in the vlan

Command mode

Interface configuration mode and interface range configuration mode.

Configuration Example

```
Console(config)# interface GigabitEthernet 2

Console(config-if-GigabitEthernet2)#clear mac-address-table static
```

Relative Command

Command	Description
show mac-address-table static	Show static address table information.

1.39 show

Show configuration information:

show history
show version
show memory
show cpu
show vlan
show vlan id <1-4094>
show statistics interface [management] {[no-zero]}*1
show statistics interface GigabitEthernet {<1-24>}*24 {[no-zero]}*1
show statistics interface aggregateport {<1-8>}*8 {[no-zero]}*1
show statistics interface sum {<1-24>}*24 {[no-zero]}*1
show statistics interface sum management {[no-zero]}*1
show [runtime-config|saved-config] [system|switch|qos|mac|dot1x]
show runtime-config interface GigabitEthernet <1-24> {<1-24>}*23
show saved-config interface GigabitEthernet <1-24> {<1-24>}*23
show runtime-config interface [GigabitEthernet|management]
show ip igmp snooping groups
show [runtime-config|saved-config] igmp [config|mv-cross]
show runtime-config igmp m-vlan {<1-4094>}*1
show saved-config igmp m-vlan

show runtime-config vlan {<1-4094>}*32
show saved-config vlan {<1-4094>}*32
show saved-config interface [GigabitEthernet|management]
show snmp
show snmp group
show snmp host
show snmp user
show snmp view
show runtime-config double-tag
show saved-config double-tag
show runtime-config qinq
show runtime-config link-trunk {group <1-8>}*8
show saved-config link-trunk {group <1-8>}*8
show runtime-config rstp bridge
show runtime-config rstp port {<1-24>}*1
show runtime-config qos remark-rule {number <1-64>}*1
show runtime-config qos remark-rule port-list <1-24> {<1-24>}*23
show saved-config qos remark-rule {number <1-64>}*1
show saved-config qos remark-rule port-list <1-24> {<1-24>}*23
show runtime-config mac
show saved-config mac
show runtime-config dhcp
show saved-config dhcp
show boot statistics
show ulf-forward
show clock
show dot1x
show dot1x
show dot1x re-auth
show dot1x port-control
show dot1x summary
show dot1x auto-req
show dot1x auth-address-table
show ip arp
show [telnetd | sshd]
show service
show ip dhcp relay
show ip dhcp snooping
show ip dhcp snooping binding
show ip igmp snooping
show ip igmp snooping interfaces
show aggregatePort <1-8> summary
show aggregatePort load-balance
show aggregatePort summary
show interfaces Aggregateport <1-8>
show interfaces
show loopback
show interfaces GigabitEthernet <LINE>
show mac-config
show mac-address-table
show mac-address-table filtering {[address] <HH:HH:HH:HH:HH:HH>}*1 {[vlan] <1-4094>}*1
show mac-address-table count
show mac-address-table count {interface GigabitEthernet <1-24> }*1
show mac-address-table count [vlan] <1-4094>
show mac-address-table [unicast|multicast]
show mac-address-table {[static|dynamic]}*1 {interface GigabitEthernet <1-24> }*1
show mac-address-learning
show mac-address-table aging-time
show monitor
show sntp

show time-range {<string>}
show logging
show running-config {interface aggregateport|GigabitEthernet <LINE>}
show mls qos maps
show mls qos queueing
show mls qos interface
show users
show [privilege]
show spanning-tree
show spanning-tree forward-time
show spanning-tree hello-time
show spanning-tree max-age
show spanning-tree max-hops
show spanning-tree tx-hold-count
show spanning-tree pathcost method
show spanning-tree summary
show spanning-tree counters
show spanning-tree tc-protection
show spanning-tree mst <0-16>
show spanning-tree mst configuration
show spanning-tree interface GigabitEthernet <1-24>
show spanning-tree interface GigabitEthernet <1-24> [bpdufilter|bpduguard|link-type|portfast]
show spanning-tree interface aggregateport <1-8>
show spanning-tree interface aggregateport <1-8> [bpdufilter|bpduguard|link-type|portfast]
show spanning-tree mst <0-16> interface GigabitEthernet <1-24>
show spanning-tree mst <0-16> interface aggregateport <1-8>
show lldp neighbors detail
show lldp interface GigabitEthernet <1-24>
show lldp statistics
show lldp statistics interface GigabitEthernet <1-24>
show lldp status
show lldp status interface GigabitEthernet <1-24>
show lldp tlv-config interface GigabitEthernet <1-24>
show lldp tlv-config
show lldp local-information global
show lldp local-information interface GigabitEthernet <1-24>
show gvrp configuration
show access-list {[<1-199>|<700-799>|<2700-2799>|<WORD>]}*1
show access-group {interface GigabitEthernet <1-24> }
show statistics {[no-zero]}*1
show eee status
show interfaces brief
show port-security
show ip dhcp snooping suppression
show ip dhcp snooping trust

1.40 default

Set config command is default

Parameter Description:
bpdu src-mac-check
description
dot1x mac-auth-by
pass multi-user
dot1x mac-auth-bypass timeout-activity

dot1x mac-auth-bypass
dot1x port-control auto
dot1x port-control
dot1x port-control-mode
duplex
flowcontrol
ip dhcp snooping suppression
ip igmp fast-leave Enable
jumbo-frame
mac-address-learning
qinq Enable
qinq innervid vlan-id
qinq set-tpid
shutdown
speed
switchport access vlan
switchport hybrid allowed vlan
switchport hybrid native vlan
switchport mode
switchport trunk allowed vlan
switchport trunk native vlan
spanning-tree autoedge disable
spanning-tree bpdufilter
spanning-tree bpduguard
spanning-tree compatible Enable
spanning-tree cost
spanning-tree guard loop
spanning-tree guard none
spanning-tree guard root
spanning-tree ignore tc
spanning-tree link-type
default spanning-tree mst [mst-id] cost
default spanning-tree mst [mst-id] port-priority
spanning-tree port-priority
spanning-tree portfast
spanning-tree tc-guard
spanning-tree
port-isolate all
default port-isolate interface aggregateport [port-num]
default port-isolate interface GigabitEthernet [port-num]
default port-isolate

Default Configuration:

Command mode Interface configuration mode.

Usage GuideFirst configuration interface, use the show interfaces to see before and after interface configuration information.Configuration Example Configuration interface duplex set to full duplex.

```
Console(config)# interface aggregateport 1
Console(config-if-AggregatePort 1)# duplex full
Console(config-if-AggregatePort 1)# default duplex
```

Relative Command:

Command	Description
show interfaces	Check the interface configuration before and after the change.

1.41 no

Restore the configuration for the default values.
[no|default] [shutdown]
[no|default] [duplex]
[no|default] {[speed]}*1
[no|default] description
no ip access-group [<1-199>|<WORD>] in
no mac access-group [<700-799>|<WORD>] in
no expert access-group [<2700-2799>|<WORD>] in
[no|default] {[flowcontrol]}*1
[no|default] {[jumbo-frame]}*1
[no|default] loopback
[no|default] storm-control [broadcast | multicast | unicast|all]
[no|default] rate-limit {[input|output]}*1
[no|default] port-isolate interface GigabitEthernet <LINE>
[no|default] port-isolate interface aggregateport <1-8>
[no|default] port-isolate {[all]}*1
[no|default] port-group mode {active|passive|static}
[no|default] switchport mode
[no|default] switchport access vlan
[no|default] switchport trunk native vlan
[no|default] switchport hybrid native vlan
[no|default] switchport trunk allowed vlan
[no|default] switchport hybrid allowed vlan
no ip igmp snooping max-groups
no ip igmp snooping control
no ip igmp snooping filter
no ip igmp tag-stripped Enable
[no|default] ip igmp fast-leave Enable
[no|default] qinq Enable
[no|default] qinq set-tpid
[no|default] port-security aging-time
[no|default] port-security mac-address <HH:HH:HH:HH:HH:HH> vlan <1-4094>
[no|default] port-security max-mac-count
[no|default] mac-address-learning
no ip dhcp snooping trust
no ip dhcp snooping suppression
no ip dhcp snooping binding mac <HH:HH:HH:HH:HH:HH> vlan <1-4094>
no eee Enable
no ip arp inspection trust
no ip arp entry src-ip <A.B.C.D> src-mac <HH:HH:HH:HH:HH:HH>
[no|default] dot1x port-control-mode
[no|default] dot1x port-control [auto]
no dot1x auth-address-table address <HH:HH:HH:HH:HH:HH>
[no | default] dot1x mac-auth-bypass
[no | default] dot1x mac-auth-bypass multi-user
[no | default] dot1x mac-auth-bypass timeout-activity
no anti-arp-spoofing ip <A.B.C.D>
no ip verify source
no ip source binding <HH:HH:HH:HH:HH:HH> vlan <1-4094> <A.B.C.D>
[no|default]gvrp Enable
[no|default]gvrp timer [join|leave|leaveall]
[no|default] spanning-tree
[no|default] spanning-tree bpduguard
[no|default] spanning-tree cost
[no|default] spanning-tree link-type
[no|default] spanning-tree mst <0-16> cost
[no|default] spanning-tree mst <0-16> port-priority

[no|default] spanning-tree port-priority
[no|default] spanning-tree portfast
[no|default] spanning-tree bpdufilter
[no|default] spanning-tree tc-guard
[no|default] spanning-tree ignore tc
[no|default] spanning-tree guard [loop|none|root]
[no|default] spanning-tree compatible Enable
[no|default] bpdu src-mac-check
no lldp Enable
no lldp mode
no lldp tlv-Enable basic-tlv [all|port-description|system-capability|system-description|system-name]
no lldp tlv-Enable dot1-tlv [all|port-vlan-id|protocol-vlan-id|vlan-name]
no lldp tlv-Enable dot3-tlv [all|link-aggregation|mac-physic|max-frame-size|power]
no lldp encapsulation snap

1.42 help

Check the system help information

Command mode

Global Mode

Usage Guide

When you want to get a Description of the Command all possible Parameter information, please enter the Command, and in the space after pressing the "?" The key. For example, by "show?" Will get all subsequent showCommand Parameter list.
When you want to get a Command to a few characters at the beginning of all the Parameter information, please input the corresponding character after the Command and then press the "?" The key. Such as "show m?" Will list all begin with m in showCommand subsequent Parameter.

Configuration Example

```
Console(config-if-GigabitEthernet1)# help

1. Anytime you need help, press "?", you'll
 see each possible command argument and its description.

 2. You can also input "list" and then press Enter
 to execute this helpful command to view the list of
 commands you can use.
```

2 VLAN

2.1 vlan

Configure the Command into the VLAN configuration mode.

Use this Command no option to delete existing vlans.

vlan *vlan-id*

vlan *vlan-id*

Parameter Description

Parameter	Description
vlan-id	Default VLAN 1 (VLAN) is not allowed to delete.

Command mode

Want to return to the privileged mode, Command input end, or type Ctrl + C key combination.

Usage Guide

To return to global configuration mode, type exit Command
For interface (Ethernet interface, the Ap interface, SVI interface), the close Command interface, the other configuration of the interface still exists, but doesn't work, use the show interfacesCommand view the interface state.

Configuration Example

```
Console(config)# vlan 1
Console(config-vlan)#
```

Relative Command

Command	Description
show vlan	show the information such as a member of the VLAN ports.

2.2 name

The name of the set VLAN. Use the Command no option set the back to the default value.

name *vlan-name*

no name

Parameter Description

Parameter	Description
vlan-name	VLAN name

Default Configuration

The default name for the VLAN VLAN + VLAN ID, such as the default name for "VLAN0002 VLAN 2"

Command mode

VLAN configuration mode

Usage Guide

Use the **show vlan c**ommand to view vlan configuration.

Configuration Example

Case 1: create vlan 20

```
Console(config)# vlan 20
Console(config-vlan)# name vlan20
```

Relative Command

Command	Description
show vlan	show the information such as a member of the VLAN ports.

2.3 show vlan

show the information such as a member of the VLAN ports.

show vlan [**id** *vlan-id*]

Parameter Description

Parameter	Description
vlan-id	VLAN ID number

Default Configuration

The default display all the information.

Command mode

Enable mode

Usage Guide

Want to return to the privileged mode, Command input end, or type Ctrl + C key combination.
To return to global configuration mode, type exit Command

Configuration Example

```
Console# show vlan id
```

Relative Command

Command	Description
name	Set VLAN name
switchport access	To add the interface to a Vlan.

2.4 switchport access

Use this Command to set a port to access port, and will it appointed a member of the VLAN ports. Use the Command no option to the port assigned to the default VLAN.

switchport access vlan vlan-id

no switchport access vlan

Parameter Description

Parameter	Description
vlan-id	port join the VLAN of ID .

Default Configuration

The default VLAN is the VLAN 1.

Command mode

Interface configuration mode and interface range configuration mode.

Usage Guide

Enter a VLAN ID. If the input is a new VLAN ID, device will create a VLAN, and set the port to the members of the VLAN. If the input is a VLAN ID already in existence, then increase the VLAN member ports. If the port is a trunkport, the operation will not have any effect.

Configuration Example

```
Console(config)# interface GigabitEthernet 1
Console(config-if-GigabitEthernet1)# switchport access vlan 3
```

Relative Command

Command	Description
switchport mode	Specify a second interface (the switch port) model
switchport trunk	Specify a native VLAN for a trunkport and configure it Licensing VLAN Trunk at the mouth of the list.

2.5 switchport mode

switchport mode {access | trunk | hybrid|private-vlan{community | isolated | promiscuous}}

no switchport mode

Parameter Description

Parameter	Description
access	Set a switch port is access port.
trunk	Set a switch port is trunk port.
hybrid	Set a switch port is hybrid port.
private-vlan	Set a switch port is **private-vlan** port.
sommunity	Set a switch port is **private-vlan** sommunity port.
isolated	Set a switch port is **private-vlan** isolated port.
promiscuous	Set a switch port is **private-vlan** promiscuous port.

Default Configuration

switchport default mode is trunk.

Command mode

Interface configuration mode and interface range configuration mode.

Usage Guide

If a switch port model is access, this interface can only as a member of the VLAN. You can use the switchport access vlan Command specifies the interface which is a member of the vlan.

If a switch port model is the trunk, then the interface can be members of more than one VLAN. The interface can belong to which VLAN is determined by the interface list of license of VLAN, trunk VLAN port is licensing in the list of all the members of the VLAN. You can use the switchport trunk Command to define the list of license VLAN interface.

Configuration Example

```
Console(config)# interface GigabitEthernet 1

Console(config-if-GigabitEthernet1)# switchport mode trunk
```

Relative Command

Command	Description
switchport mode	Specify a second interface (the switch port) mode
Switchport trunk	Specify a native VLAN for a trunkport and configure it Licensing VLAN Trunk at the mouth of the list.

2.6 switchport trunk

Specify a native VLAN for a trunkport and configure the list of license VLAN Trunk mouth. Use the Command of the trunk of the interface no option will revert to the default attribute values.

switchport trunk {**allowed vlan** {**all** | [**add** | **remove** | **except**] *vlan-list* }|

native vlan *vlan-id*}

no switchport trunk {**allowed vlan** | **native vlan**}

Parameter Description

Parameter	Description
allowed vlan *vlan-list*	Configure the list of license VLAN Trunk mouth. Parametervlan - the list could be a VLAN, also can be a series of VLAN, begin with small VLAN ID, ends in large VLAN ID, connection with a (-) symbol in the middle. Such as: 10 to 20. Period of separated (,) can be used between symbols, such as: 1-10, 20 and 25,30,33. All means permission VLAN list contains all supported VLAN; Add the specified VLAN list add said license VLAN list; Remove said will specify VLAN list from permission to delete VLAN list; Except, said it would except the VLAN lists all VLAN to join licensing VLAN list;
native vlan *vlan-id*	Configuration Native VLAN.

Default Configuration

The default permission Settings are all VLAN list, the default Native VLAN is the VLAN 1.

Command mode

Interface configuration mode and interface range configuration mode.

Usage Guide

Native VLAN：
As the Trunk, the mouth will belong to a native VLAN. The so-called native VLAN, is refers to UNTAG send or receive a message on the interface, is considered belongs to the VLAN. Obviously, the interface of the default VLAN ID (PVID) in the IEEE 802.1 Q VLAN ID is the native VLAN. At the same time, send belong to native VLAN frame on the Trunk, must adopt UNTAG
Way.

Allowing VLAN list:

A Trunk all mouth can transport the equipment support by default VLAN traffic (1-4094). But, also can by setting the permission VLAN Trunk at the mouth of the list to limit the flow of some VLAN can't through the Trunk.
The following is a VLAN 2 examples of removing from the port 1:

Configuration Example

```
Console(config)# interface GigabitEthernet 1

Console(config-if-GigabitEthernet1)# switchport trunk allowed vlan remove 2
```

Relative Command

Command	Description
show interfaces	Show interfaces information

2.7 switchport hybrid allowed vlan

The output of the configuration of hybrid port rules.

switchport hybrid allowed vlan {**add** [**tagged** | **untagged**] | **remove**}

vlan-list

no switchport hybrid allowed vlan

Parameter Description

Parameter	Description
no	Restore the hybrid default output rules.

Default Configuration

no configuration

Command mode

Interface configuration mode and interface range configuration mode.

Configuration Example

```
Console(config)# interface GigabitEthernet 1

Console(config-if-GigabitEthernet1)# switchport hybrid allowed vlan add tagged 3-5
```

Relative Command

Command	Description
show interfaces	show interfaces information

2.8 switchport hybrid native vlan

The default vlan configuration hybrid port

switchport hybrid native vlan vlan-*list*

no switchport hybrid native vlan

Parameter Description

Parameter	Description
no	Restore the hybrid default vlan.

Default Configuration

no configuration

Command mode

Interface configuration mode and interface range configuration mode.

Configuration Example

```
Console(config)# interface GigabitEthernet 1
Console(config-if-GigabitEthernet1)# switchport hybrid native vlan 5
```

Relative Command

Command	Description
show interfaces	show interfaces information

2.9 mac-vlan mac

Add the MAC address, the corresponding relationship between VLAN specifying the MAC address to join the specified VLAN; No form of the Command to delete specified corresponding relationship or delete all correspondence.

mac-vlan mac *mac-address* **[mask** *mac-mask***] vlan** *vlan-id* **[priority** *pri_vlan***]**

no mac-vlan { mac *mac-address* **[mask** *mac-mask***] | all }**

Parameter Description

Parameter	Description
mac-address	Appoint MAC address
mac-mask	Specifies the MAC address mask, binary high must

	continuously to 1. The default field for all F.
vlan-id	Specifies the MAC address corresponding VLAN, value range is 1 ~ 4094
pri_val	Specifies the MAC address of the corresponding VLAN 802.1 p, priority values of 0 ~ 7, the default is 0

Default Configuration

By default, there is no static MAC VLAN configuration table.

Command mode

global configuration mode

Usage Guide

The Command to add the specified MAC address in the specified VLAN. When we have the specified MAC address without a VLAN tag packets from the switch port, it will match to the specified VLAN number, to the specified VLAN. The Command packet with a VLAN tag is not to intervene.

Configuration Example

```
The MAC address for 00:00:02:00:00:02 network equipment delimit VLAN 100:
Console(config)# mac-vlan mac 00:00:00:00:00:02 vlan 100
Console(config)#
```

Relative Command

Command	Description
show mac-vlan	Show mac-vlan configuration information

2.10 mac-vlan Enable

On the port open the MAC-based VLAN function, no form of the Command close port the MAC -based VLAN function.

mac-vlan Enable

no mac-vlan Enable

Default Configuration

By default, the open port on MAC vlans.

Command mode

interface configuration mode

Usage Guide

When adding MAC addresses belong to the specified VLAN, MAC - -based global Enabled by default VLAN function, this Command can be shut on the specified port MAC - -based VLAN function, to adapt to the user's specific application.

Configuration

Close port 2 MAC - -based VLAN function:

```
Console(config)# interface GigabitEthernet 2
Console(config-if-GigabitEthernet2)# no mac-vlan Enable
```

Example

```
Console(config-if-GigabitEthernet2)#
```

Relative Command

Command	Description
show mac-vlan interface	Show the MAC - port configuration vlan information

2.11 subnet-vlan ip-address

The corresponding relationship between Add IP subnet and VLAN that specify the IP address to join the specified VLAN; No form of the Command or delete specified relation between all correspondence.

subnet-vlan ip-address *ip-address* **mask** *subnet-mask* **vlan** *vlan-id* **[priority** *pri_vlan***]**

no subnet-vlan { ip-address *ip-address* **mask** *subnet-mask* **| all }**

Parameter Description

Parameter	Description
ip-address	Specify the IP subnet address
subnet-mask	Specify the IP subnet mask
vlan-id	Specify the IP subnet addresses corresponding VLAN, value range is 1 ~ 4094
pri_val	Specify the IP subnet addresses corresponding VLAN 802.1 p priority, value of 0 ~ 7, the default is 0

Default Configuration

By default, items not have the static SUBNET VLAN configuration table.

Command mode

global configuration mode

Usage Guide

This Command will join the rest of the specified VLAN designated IP subnet. When we have designated IP subnet without a VLAN tag packets from the switch port, it will match to the specified VLAN number, to the specified VLAN. The Command packet with a VLAN tag is not to intervene.

Configuration Example

The IP subnet for 192.168.200.0/24 network equipment delimit VLAN 200:

```
Console(config)# subnet-vlan ip-address 192.168.200.0 mask 255.255.255.0 vlan
200
Console(config)#
```

Relative Command

Command	Description

show subnet-vlan	Show subnet-vlan configuration information

2.12 subnet-vlan Enable

Open the IP-subnet-based vlan configures on the port, no IP-subnet-based vlan command is close it on the port.

subnet-vlan Enable

no subnet-vlan Enable

Default Configuration

The default，open the IP-subnet-based VLAN fuction on the port.

Command mode

interface configuration mode

Usage Guide

When adding IP subnet belongs to the specified VLAN, global Enabled IP-subnet-based VLAN function by default,this no Command can be closed on the specified port IP-subnet-based VLAN function, to adapt to the user's specific application.

Configuration Example

Disable the IP-subnet-based VLAN function on the port 2：

```
Console(config)# interface GigabitEthernet 2
Console(config-if-GigabitEthernet2)# no subnet-vlan Enable
Console(config-if-GigabitEthernet2)#
```

Relative Command

Command	Description
show subnet-vlan interface	Show subnet-vlan port configuration information

2.13 protocol-vlan frametype

Add the corresponding relationship between the agreement and VLAN that specifying the agreement to join the specified VLAN; The Command no option to delete the specified corresponding relationship or delete all corresponding relations under the specified port or delete so corresponding relation.

protocol-vlan frametype {ether2 | snap | llc } ethertype *ethertype-val* **vlan** *vlan-id* **[priority** *pri_vlan***] [port** *port-num***]**

no protocol-vlan frametype {ether2 | snap | llc } ethertype *ethertype-val* **[port** *port-num***]**

no protocol-vlan { port *port-num* **| all }**

Parameter Description

Parameter	Description
ethertype-val	protocol type value
vlan-id	Specify the agreement corresponding VLAN, value range is 1 ~ 4094
pri_val	Specified agreement corresponding VLAN 802.1 p, priority values of 0 ~ 7, the default is 0
port-num	Application of port, the default said applied to all ports

Default Configuration

By default, items do not have the static PROTOCOL VLAN configuration table.

Command mode

global configuration mode

Usage Guide

This Command will be specified in the agreement to join in the specified VLAN. If there are not specified in the agreement with VLAN tag packets from the switch port, it will match to the specified VLAN number, to the specified VLAN. The Command packet with a VLAN tag is not to intervene.

Configuration Example

The Ethernet II encapsulated IP packets to a VLAN 100:

```
Console(config)# protocol-vlan frametype ether2 ethertype 0x0800 vlan 100
Console(config)#
```

Relative Command

Command	Description
show protocol-vlan	Show protocol-vlan configuration information

2.14 vlan-translation

Add a VLAN translation transformation rules, make the original VLAN ID and VLAN ID now produces a map; No form of the Command to delete the corresponding mapping.

vlan-translation *old-vlan-id* **to** *new-vlan-id* **{ in | out }**

no vlan-translation *old-vlan-id* **{ in | out }**

Parameter Description

Parameter	Description
old-vlan-id	The old VLAN ID, value range is 1 ~ 4094
new-vlan-id	Mapping the new VLAN ID, value range is 1 ~ 4094
in	The rules applied to a port on the entrance
out	The rules apply to a port on the export

Default Configuration

By default, no VLAN traslation mapping relation.

Command mode

global configuration mode

Usage Guide

The Command to set the VLAN translation mapping relationship. Packet is according to the mapping relationship set match, if the match is successful, is to change VLAN ID to set the VLAN ID of a item, if the match is not successful, according to the original VLAN forward.

Configuration Example

Take port 2 in VLAN100 packet delimit VLAN2 after entrance map:

```
Console(config)# interface GigabitEthernet 2
Console(config-if-GigabitEthernet2)# vlan-translation 200 to 2 in
```

Relative Command

Command	Description
show vlan-translation	Show vlan-translation configuration information

2.15 vlan-translation Enable

Enable the VLAN translation function on the port，no command to disbale the VLAN translation function.

vlan-translation Enable

no vlan-translation Enable

Default Configuration By default, can not make VLAN translation function.

Command mode interface configuration mode

Configuration Example Disable the VLAN translation function on the port 2：

```
Console(config)# interface GigabitEthernet 2
Console(config-if-GigabitEthernet2)# vlan-translation Enable
Console(config-if-GigabitEthernet2)#
```

Relative Command

Command	Description
show vlan-translation	Show vlan-translation configuration information

2.16 dot1q-tunnel Enable

Switches specified port can make QinQ function, no form of the Command close port QinQ function.

dot1q-tunnel Enable

no dot1q-tunnel Enable

Default Configuration By default, can not make QinQ function.

Command mode interface configuration mode

Usage Guide Port can make dot1q - tunnel, for from the port into the packet can play double tag, tag and outside layer and MAC address as the forwarding basis, until from untag port out strip outer tag.

Configuration Example Enabling QinQ function on port 2:

```
Console(config)# interface GigabitEthernet 2
Console(config-if-GigabitEthernet2)# dot1q-tunnel Enable
Console(config-if-GigabitEthernet2)#
```

Relative Command

Command	Description
show dot1q-tunnel	Show dot1q-tunnel configuration information

2.17 dot1q-tunnel tpid

Set message protocol type (TPID) to different TPID values compatible with third party vendors, no form of the Command to restore the port TPID as the default values.

dot1q-tunnel tpid *tpid-val*

no dot1q-tunnel tpid

Parameter Description

Parameter	Description
tpid-val	Set the TPID value of protocol

Default Configuration

By default, with 0 TPID x88a8.

Command mode

interface configuration mode

Usage Guide

This feature is for the convenience of the device interconnection with other manufacturers. Can be set up on the connected to the third party equipment export TPID value for third-party equipment TPID.

Configuration Example

The port 2 TPID value is set to 0x9100:

```
Console(config)# interface GigabitEthernet 2
Console(config-if-GigabitEthernet2)# dot1q-tunnel tpid 0x9100
Console(config-if-GigabitEthernet2)#
```

Relative Command

Command	Description
show dot1q-tunnel	Show dot1q-tunnel configuration information

2.18 dot1q-tunnel inner-vid

On the port Settings based on the inner Tag VID decision of outer VID strategy table, no form of the Command to delete the corresponding strategy table.

dot1q-tunnel inner-vid *ivid* **outer-vid** *ovid*

no dot1q-tunnel inner-vid *ivid*

Parameter Description

Parameter	Description
ivid	VID value of the packets inside the Tag
ovid	According to the inner VID decision outer Tag VID values

Default Configuration

By default, the strategy table is empty.

Command mode

interface configuration mode

Usage Guide

This Command set the mapping relationship of flexible QinQ, the lining of the packet will be set up according to the VID match, if the match is successful, will provide the outer Tag message encapsulation specified VID.

Configuration Example

Take port 2 enter VLAN100 data packet encapsulation layer of the VLAN200 outer Tag:

```
Console(config)# interface GigabitEthernet 2
Console(config-if-GigabitEthernet2)# dot1q-tunnel inner-vid 100 outer-vid 200
Console(config-if-GigabitEthernet2)#
```

Relative Command

Command	Description
show dot1q-tunnel	Show dot1q-tunnel configuration information

2.19 voice vlan

Global can make the Voice VLAN, and set a VLAN for the Voice VLAN, no command to close the Voice VLAN function .

voice vlan *vlan-id*

no voice vlan

Parameter Description

Parameter	Description
vlan-id	Expression the Voice VLAN ID, range of 2-4094

Default Configuration

The default is disable

Command mode

global configuration mode

Usage Guide

To configure the Voice VLAN before, need to first create the corresponding VLAN, VLAN1 is the default VLAN, cannot be set to Voice VLAN.

Configuration Example

Global Enabled Voice VLAN function of equipment, and set the Voice VLAN VLAN2 to:

```
Console(config)# vlan 2
Console(config-vlan)# exit
Console(config)# voice vlan 2
Console(config)#
```

Relative Command

Command	Description
show voice vlan	Show the Voice VLAN configuration information and the current state

2.20 voice vlan cos

Global Settings Voice VLAN Voice flow, the cosine value of the no form of the Command will be resumed the configuration to the default values.

voice vlan cos *cos-value*

no voice vlan cos

Parameter Description

Parameter	Description
cos-value	Expression the Voice VLAN Voice flow, the cosine value of the range of 0 ~ 7

Default Configuration The default is 6.

Command mode global configuration mode

Usage Guide Equipment by modifying the cosine value of the Voice VLAN Voice stream to provide Voice flow priority, guarantee the quality.

Configuration Example Configure the Voice VLAN Voice flow priority, CoS for 4:

```
Console(config)# voice vlan cos 4
Console(config)#
```

Relative Command

Command	Description
show voice vlan	Show the Voice VLAN configuration information and current state

2.21 voice vlan aging

Set the Voice VLAN aging time in the global，no command to restore default value.

voice vlan aging *minutes*

no voice vlan aging

Parameter Description

Parameter	Description
Minutes	Express Voice VLAN aging time,range 5 ~ 10000, unit: minutes.

Default Configuration The default value is 1440 minutes, which is 1 day.

Command mode global configuration mode

Usage Guide Users can be set up on the device Voice VLAN aging time, when the aging time, the equipment without any Voice message from the input port received, will give the port is removed from the Voice VLAN. Aging time only to automatic mode.

Configuration Example Set Voice VLAN aging time is 10 minute：

```
Console(config)# voice vlan aging 10
Console(config)#
```

Relative Command

Command	Description
show voice vlan	Show the Voice VLAN configuration information and the current state

2.22 voice vlan mac-address

Global Settings Voice VLAN identifiable Voice stream OUI address, no form of the Command delete equipment set on a particular OUI address.

voice vlan mac-address *mac-addr* **mask** *mac-mask* **[description** *text***]**

no voice vlan mac-address *mac-addr*

Parameter Description

Parameter	Description
mac-addr	Voice message of the source MAC address
mac-mask	The MAC address mask, binary high must continuously to 1. The default field for all F.
text	The Description of OUI addresses

Default Configuration

By default, the configuration, there are seven manufacturers OUI.

Command mode

global configuration mode

Usage Guide

Used to identify the manufacturer of the voice message. Voice equipment the MAC address of the first three bytes to sign makers, Voice VLAN can will receive the message of the source MAC address and OUI mask facies OUI, to decide whether the newspaper article is a Voice message.

Configuration Example

Add OUI address 00:12:34:00:00:00, **MASK 11:12:13：14：15：16**，description for the CompanyA:

```
Console(config)# voice vlan mac-address 00:12:34:00:00:00 mask
11:12:13:14:15:16 description CompanyA
Console(config)#
```

Relative Command

Command	Description
show voice vlan	Show the Voice VLAN configuration information and the current state

2.23 voice vlan Enable

Under the interface configuration mode can use this Command to make port Voice VLAN function, no form of the Command Voice VLAN function of the close port.

voice vlan Enable

no voice vlan Enable

Default Configuration The default case port closed Voice VLAN function.

Command mode Interface configuration mode

Usage Guide Through this Command to open the port Voice VLAN function, Voice VLAN function can only be Enabled on the physical port. In the global Voice VALN closed cases, also can make the Voice VLAN function of the port, but not to take effect.

Configuration Example Enable port 2 Voice VLAN function:

```
Console(config)# interface GigabitEthernet 2
Console(config-if-GigabitEthernet2)# voice vlan Enable
Console(config)#
```

Relative Command

Command	Description
show voice vlan interface	Show Voice VLAN port state and the working mode

2.24 voice vlan mode auto

In interface configuration mode Voice VLAN configuration port under working mode to automatic mode, the no form of the Command set port Voice VLAN work mode to manual mode.

voice vlan mode auto

no voice vlan mode auto

Default Configuration The default case port Voice VLAN work mode to manual mode.

Command mode interface configuration mode

Usage Guide Voice VLAN work mode can be divided into automatic mode and manual mode, based on the port configuration. Each port Voice VLAN work mode are independent of each other, each port can be set to different mode. Automatic mode, the port will automatically the port after receipt of the Voice and data to join the Voice VLAN, manual mode, the need to manually add the port Voice VLAN. Automatic mode, are not allowed by manually configure Command will join the Voice VLAN port or deleted from the Voice VLAN.

Configuration Set port 2 Voice VLAN mode to automatic mode:

Example

```
Console(config)# interface GigabitEthernet 2
Console(config-if-GigabitEthernet2)# voice vlan mode auto
Console(config)#
```

Relative Command

Command	Description
show voice vlan interface	According to Voice VLAN port state and the working mode

2.25 voice vlan security Enable

The global open the Voice VLAN security mode, the Command no form close security mode.

voice vlan security Enable

no voice vlan security Enable

Default Configuration

The default case Voice VLAN safe mode is turned off.

Command mode

global configuration mode

Usage Guide

In order to be able to better user separation Voice and data transmission, can open the Voice VLAN security mode. Open the safe mode after device will examine the source MAC address of a message, when the source MAC address is to recognize the Voice VLAN OUI, allowing the packet transmission within the Voice VLAN, otherwise will be discarded the newspaper article.

Configuration Example

Open the Voice VLAN security mode:

```
Console(config)# voice vlan security Enable
Console(config)#
```

Relative Command

Command	Description
show voice vlan	Show the Voice VLAN configuration information and the current state

2.26 private-vlan

Configuration Private VLAN primary VLAN and the VLAN, no form of the Command to cancel the Private VLAN attributes.

private-vlan { community | isolated | primary }

no private-vlan

Parameter Description

Parameter	Description
community	The specified VLAN to community VLAN
isolated	The specified VLAN to isolate VLAN
primary	The specified VLAN to primary VLAN

Default Configuration

The default case vlans belong to the ordinary VLAN, does not have the attribute of Private VLAN.

Command mode

VLAN mode

Configuration Example

Configuration Private VLAN attributes:

```
Console(config)# vlan 3
Console(config-vlan)# private-vlan primary
Console(config-vlan)# exit
Console(config)# vlan 4
Console(config-vlan)# private-vlan community
Console(config-vlan)# exit
Console(config)# vlan 5
Console(config-vlan)# private-vlan isolated
```

Relative Command

Command	Description
show vlan private-vlan	Show the Private VLAN configuration

2.27 private-vlan association

Associated auxiliary VLAN (secondary VLAN) on the second floor and primary VLAN (primary VLAN), no form of the Command to cancel all related auxiliary VLAN.

private-vlan association { *svlist* **| add** *svlist* **| remove** *svlist* }

no private-vlan association

Parameter Description

Parameter	Description
svlist	The associated secondary vlan(auxiliary VLAN)
add *svlist*	Add associated secondary vlan
remove *svlist*	Remove associated secondary vlan

Default Configuration

The default case there is no connection between the main VLAN and the auxiliary VLAN.

Command mode VLAN mode

Usage Guide Must be in the main VLAN configuration (primary VLAN). The associated VLAN must be a Private VLAN type of auxiliary VLAN.

Configuration Example Associated auxiliary VLAN:

```
Console(config)# vlan 3
Console(config-vlan)# private-vlan association 4,5
```

Relative Command

Command	Description
show vlan private-vlan	Show Private VLAN configuration

2.28 switchport mode private-vlan

Statement interface for private VLAN mode, no form of the Command to cancel the private VLAN mode of the interface, back into the access port.

switchport mode private-vlan { community | isolated | promiscuous }

no switchport mode

Parameter Description

Parameter	Description
community	Specified port to community port mode
isolated	Specified port to isolate port mode
promiscuous	Specified port to promiscuous mode

Default Configuration The default is access.

Command mode interface configuration mode

Usage Guide promiscuous port, belongs to the main port in the VLAN, can communication with any port, including the same private VLAN domain auxiliary VLAN isolation ports and group.

Isolated ports, VLAN ports, only with mixed oral communication.

Community port, belongs to the group, through a group of VLAN group port can be communication each other, can also be mixed with oral communication. Can't with other groups in the VLAN port and isolated VLAN port communication.

Configuration Example Specified port mode is promiscuous port mode：

```
Console(config)# interface GigabitEthernet 2
Console(config-if-GigabitEthernet2)# switchport mode private-vlan promiscuous
```

Relative Command

Command	Description
show vlan private-vlan	Show Private VLAN configuration
show interfaces GigabitEthernet	Show port information

2.29 switchport private-vlan association

Associated private VLAN mode under the VLAN interface is located, the no form of the Command to cancel the connection.

switchport private-vlan association *vid*

no switchport private-vlan association

Parameter Description

Parameter	Description
vid	Private VLAN Id

Default Configuration There is no connection default private VLAN.

Command mode interface configuration mode

Usage Guide Promiscuous port must be associated with the VLAN, groups mouth must be associated VLAN, isolated mouth must be associated with the VLAN.

Configuration Example Port 2 is promiscuous port，associate main VLAN 3：

```
Console(config)# interface GigabitEthernet 2
Console(config-if-GigabitEthernet2)# switchport private-vlan association 3
```

Relative Command

Command	Description
show vlan private-vlan	Show Private VLAN configuration
show interfaces GigabitEthernet	Show port information

2.30 show mac-vlan

Show switch MAC-based VLAN configuration

show mac-vlan [interface]

Command mode Enable mode

Configuration Example

Show current MAC-based VLAN configuration case：

```
Console(config)# show mac-vlan
  MAC Address         MAC Mask         VLAN ID     Priority
----------------   ----------------   --------   --------
00:00:00:00:03:01   FF:FF:FF:FF:FF:00   2          0

Console(config)#
Console(config)# show mac-vlan interface
Port 1     :  Enable
Port 2     :  disable
Port 3     :  Enable
Port 4     :  Enable
Port 5     :  Enable
Port 6     :  Enable
Port 7     :  Enable
Port 8     :  Enable
Port 9     :  Enable
Port 10    :  Enable
 __More__
```

Relative Command

Command	Description
mac-vlan mac	Add corresponding relations between the MAC address and VLAN
mac-vlan Enable	Open the MAC-based vlan function on the port

2.31 show subnet-vlan

Display switch IP-subnet-based VLAN configuration

show subnet-vlan

Command mode

Enable mode

Configuration Example

Show current IP-subnet-based VLAN configuration case：

```
Console(config)# show subnet-vlan
  IP Address         Mask          VLAN ID    Priority
---------------   ---------------   --------   --------
192.168.3.0       255.255.255.0     3          0
192.168.4.0       255.255.255.0     4          0

Console(config)#
Console(config)# show subnet-vlan interface
Port 1     :  Enable
Port 2     :  disable
Port 3     :  Enable
Port 4     :  Enable
```

```
Port 5    : Enable
Port 6    : Enable
Port 7    : Enable
Port 8    : Enable
Port 9    : Enable
Port 10   : Enable
 __More__
```

Relative Command

Command	Description
subnet-vlan ip-address	Add a corresponding relationship between the VLAN IP subnet and vlan
subnet-vlan Enable	Open the subnet-based-vlan function on the port

2.32 show protocol-vlan

Show switch Protocol-based VLAN configuration

show protocol-vlan

Command mode

Enable mode

Configuration Example

Show current Protocol-based VLAN configuration：

```
Console(config)# show protocol-vlan
 Frame Type     Ether Type    VLAN ID   Priority   Port
------------   ------------   -------   -------   -----
ether2         0x0800         4         0         all
ether2         0x0806         3         0         3

Console(config)#
```

Relative Command

Command	Description
protocol-vlan frametype	Add a corresponding relationship between the protocol-vlan and vlan

2.33 show vlan-translation

Show all in a state of VLAN translation port information

show vlan-translation

Command mode

Enable mode

Configuration Example

Show current VLAN translation information：

```
Console(config)# show vlan-translation
Port 2 :
   vlan-transldation is Enable
   vlan-translation 2 to 3 in
   vlan-translation 3 to 4 out

Console(config)#
```

Relative Command

Command	Description
vlan-translation	Add a VLAN translation transformation rules, make the original VLAN ID and VLAN ID now produces a map
vlan-translation Enable	Enable the VLAN translation function on the port

2.34 show dotq1q-tunnel

Show dotq-tunnel configuration

show dot1q-tunnel

Command mode

Enable mode

Configuration Example

Show dot1q-tunnel configuration information：

```
Console(config)# show dot1q-tunnel
Port 1   : disable          Tpid 0x88a8
Port 2   : disable          Tpid 0x88a8
Port 3   : Enable           Tpid 0x88a8
         inner vid = 3     outer vid = 2
Port 4   : disable          Tpid 0x88a8
Port 5   : disable          Tpid 0x88a8
Port 6   : disable          Tpid 0x88a8
Port 7   : disable          Tpid 0x88a8
Port 8   : disable          Tpid 0x88a8
Port 9   : disable          Tpid 0x88a8
Port 10  : disable          Tpid 0x88a8
__More__
```

Relative Command

Command	Description
dot1q-tunnel Enable	Switches specified port can make QinQ function
dot1q-tunnel tpid	Set a message protocol type (TPID) with different TPID values compatible with third party vendors
dot1q-tunnel inner-vid	On the port Settings based on the inner Tag VID decided to outer VID strategy table

2.35 show port vlan membership

Show port vlan membership configurtion

show port vlan membership

Command mode

Enable mode

Configuration Example

Show port vlan configuration information：

```
Console(config)# show port vlan membership
Port  Mode     Administrative VLANs                Operational VLANs
----- -------- ----------------------------------- -----------------------------------
1     access   1UP                                 1UP
2     access   1UP                                 1UP
3     access   1UP                                 1UP
4     access   1UP                                 1UP
5     access   1UP                                 1UP
6     access   1UP                                 1UP
7     access   1UP                                 1UP
8     access   1UP                                 2UP
9     access   1UP                                 1UP
10    access   1UP                                  1UP
11    access   1UP                                  1UP
12    access   1UP                                  1UP
13    access   1UP                                  1UP
14    access   1UP                                  1UP
15    access   1UP                                  1UP
16    access   1UP                                  1UP
17    access   1UP                                  1UP
18    access   1UP                                  1UP
19    access   1UP                                  1UP
20    access   1UP                                  1UP
21    access   1UP                                  1UP
22    access   1UP                                  1UP
23    access   1UP                                  1UP
24    access   1UP                                  1UP
25    access   1UP                                  1UP
26    access   1UP                                  1UP
```

2.36 show voice vlan

Show the Voice VLAN configuration information and current state, including equipment support OUI address, OUI mask, the Description information.

show voice vlan

Command mode

Enable mode

Configuration Example

Show the current state of Voice VLAN and OUI information:

```
Console(config)# show voice vlan
Voice VLAN status         : Enable
Voice VLAN ID        : 2
Voice VLAN security mode  : Enable
Voice VLAN aging time     : 1440 minutes
Voice VLAN cos            : 6
   OUI               Mask              Description
-----------------    -----------------    -------------------
00:01:E3:00:00:00    FF:FF:FF:00:00:00    Siemens phone
00:03:6B:00:00:00    FF:FF:FF:00:00:00    Cisco phone
00:04:0D:00:00:00    FF:FF:FF:00:00:00    Avaya phone
00:60:B9:00:00:00    FF:FF:FF:00:00:00    Philips/NEC phone
00:D0:1E:00:00:00    FF:FF:FF:00:00:00    Pingtel phone
00:E0:75:00:00:00    FF:FF:FF:00:00:00    Polycom phone
00:E0:BB:00:00:00    FF:FF:FF:00:00:00    3Com phone

Console(config)#
```

Relative Command

Command	Description
voice vlan	Enable Voice VLAN and set a VLAN is Voice VLAN in the global
voice vlan cos	Set Voice VLAN CoS value in the global
voice vlan aging	Set Voice VLAN aging time in the global
voice vlan mac-address	Set Voice VLAN identifiable Voice stream OUI address in the global
voice vlan security Enable	Enable Voice VLAN security mode in the global

2.37 show voice vlan interface

According to Voice VLAN port state and the working mode

show voice vlan interface

Command mode

Enable mode

Configuration Example

Show Voice VLAN configuration information：

```
Console(config)# show voice vlan interface
Port       Status     Mode
---------- ---------- ----------
Port 1     Enable     manual
Port 2     Enable      auto
Port 3     disable    manual
Port 4     disable    manual
Port 5     disable    manual
Port 6     disable    manual
Port 7     disable    manual
Port 8     disable    manual
Port 9     disable    manual
Port 10    disable     manual
__More__
```

Relative Command

Command	Description
voice vlan Enable	Enable Voice VLAN function
voice vlan mode auto	Set port Voice VLAN working mode is auto

2.38 show vlan private-vlan

Show Private VLAN configuration information

show vlan private-vlan

Command mode

Enable mode

Configuration Example

Show Private VLAN configuration information：

```
Console(config)# show vlan private-vlan
VLAN   Type        Associated VLANs          Ports
------ ----------- ------------------------ --------------------------
3      primary     4,5                       Gi0/2
4      community   3                           Gi0/3
5      isolated    3                        Gi0/4

Console(config)#
```

Relative Command

Command	Description
private-vlan	Set Private VLAN main VLAN and associated VLAN
private-vlan association	Associated auxiliary VLAN (secondary VLAN) on the second floor and primary VLAN (primary VLAN)
swithport mode private-vlan	The statement interface for private VLAN mode
switchport private-vlan association	The VLAN associated private VLAN mode interface

3 ACL

3.1 IP standard access list

In the global configuration mode using command access - the list in the acl filtering rules, use the no form of this command returns the default value.

access-list <idx> [deny|permit] [any|host|<A.B.C.D>] {time-range name}

Parameter Description

Parameter	Description
idx	Will choose the Parameter: index, scope of <1-99>
deny|permit	Will choose the Parameter: action, can only deny or permit
any|host|<A.B.C.D>	Will choose Parameter: Any means to match all of the source IP host | < A.B.C.D > means to match the source IP or mask
name	optional Parameter: binding time name

Command mode

global configuration mode

Configuration Example

Example 1: configuration matching SRC - IP for 192.168.2.5 message, to deny

access-list 1 deny host 192.168.2.5

Example 2: IP configuration matching SRC - for all message, action for the permit

access-list 1 permit any

Relative Command

Command	Description
no access-list <idx>	Delete idx entry access-list

3.2 IP extended access list

In the global configuration mode using Commandaccess - the list in the

acl filtering rules, use the no form of this Command returns the default value.

access-list <idx> [deny|permit] [ip-proto|ip] [any|[host|<A.B.C.D>]] [any|[host|<A.B.C.D>]] {dscp dscp-value}{time-range name}

access-list <idx> [deny|permit] [tcp|udp] [any|[host|<A.B.C.D>]] {eq src-port} [any|[host|<A.B.C.D>]] {eq dst-port} {dscp dscp-value}{time-range name}

Parameter Description

Parameter	Description
idx	Will choose the Parameter: index, range <100-199>
deny|permit	Will choose Parameter：action，only deny or permit
Ip-proto|ip	Will choose Parameter： Ip-proto value，range <0-255> Or all IP protocol
tcp|udp	Will choose Parameter： Tcp protocol Or UDP protocol
any|[host|<A.B.C.D>]	Will choose Parameter： Any means to match all the SRC - IP The host | < A.B.C.D > means to match the SRC IP or mask
Src-port	Optional Parameter: matching l4 - SRC - port, the scope of the < 0-65535 >
any|[host|<A.B.C.D>]	Will choose Parameter： Any means to match all the dst-IP The host | < A.B.C.D > means to match the dst-IP or mask
Dst-port	Optional Parameter: matching l4 - DST - port, the scope of the < 0-65535 >
dscp-value	Optional Parameter: message DSCP values, the range of 0-63 >
name	Optional Parameter: binding time name

Command mode

global configuration mode

Configuration

Case 1: configuration matching IP, DSCP values of 8 message,action is deny

Example access-list 100 deny ip any any dscp 8

Relative Command

Command	Description
no access-list <idx>	Delete idx entry access-list

3.3 MAC extended access list

In the global configuration mode using Commandaccess - the list in the acl filtering rules, use the no form of this Command returns the default value.

access-list <idx> [any|[host|<HH:HH:HH:HH:HH:HH>]] [any|[host|<HH:HH:HH:HH:HH:HH>]] [etype-any|eth-proto] {cos cos-value} {time-range name}

Parameter Description

Parameter	Description
idx	Will choose the Parameter: index, range <700-799>
deny|permit	Will choose Parameter：action，only deny or permit
any|[host|<HH:HH:HH:HH:HH:HH>]	Will choose Parameter： Any means to match all the SRC - IP The host | <HH:HH:HH:HH:HH:HH> means to match the SRC IP sk
any|[host|<HH:HH:HH:HH:HH:HH>]	Will choose Parameter： Any means to match all the dst-IP The host | <HH:HH:HH:HH:HH:HH> means to match the dst-IP o sk
etype-any|eth-proto	Will choose Parameter： Etype-any is all Ethernet protocol eth-proto is Ethernet protocol，range <0-0xffff>
cos-value	Optional Parameter:protocol cos value，range <0-7>
name	optional Parameter: binding time name

Command mode global configuration mode

Configuration Example Case 1: configuration matches all Ethernet protocol,

the cosine value of 5 message,action is deny

access-list 700 deny any any etype-any cos 5

Relative Command

Command	Description
no access-list <idx>	Delete idx entry access-list

3.4 Expert extended access list

In the global configuration mode using Commandaccess - the list in the a filtering rules, use the no form of this Command returns the default value.

access-list <idx> [any|[host|<HH:HH:HH:HH:HH:HH>]] [any|[host|<A.B.C.D>]]

[any|[host|<HH:HH:HH:HH:HH:HH>]] [any|[host|<A.B.C.D>]] {ip-proto|ip} {etype-any

eth-proto} {cos cos-value} {dscp dscp-value} {vid vid-value} {time-range name}

Parameter Description

Parameter	Description
idx	Will choose the Parameter: index, range <2700-2799>
deny|permit	Will choose Parameter：action，only deny or permit
any|[host|<HH:HH:H :HH:HH>]	Will choose Parameter： Any means to match all the SRC - IP The host | <HH:HH:HH:HH:HH:HH> means to match the SRC nask
any|[host|<A.B.C.D>	Will choose Parameter： Any means to match all the SRC - IP The host | < A.B.C.D > means to match the SRC IP or mask
any|[host|<HH:HH:H :HH:HH>]	Will choose Parameter： Any means to match all the dst- IP The host | <HH:HH:HH:HH:HH:HH> means to match the dst-I nask
any|[host|<A.B.C.D>	Will choose Parameter： Any means to match all the dst- IP The host | < A.B.C.D > means to match the dst IP or mask
etype-any|eth-proto	Will choose Parameter： Etype-any is all Ethernet protocol eth-proto is Ethernet protocol，range <0-0xffff>
Ip-proto|ip	Will choose Parameter： Ip-proto value，range <0-255> Or all IP protocol
cos-value	Optional Parameter:protocol cos value，range <0-7>

dscp-value	Optional Parameter: message DSCP values, the range of 0-6
vid-value	Optional Parameter：protocol vid value，range<0-4094>
name	optional Parameter: binding time name

Command mode

global configuration mode

Configuration Example

Case 1: configuration matching all agreements, action is deny

access-list 2700 deny any any any any

Relative Command

Command	Description
no access-list <idx>	Delete idx entry access-list

3.5 IP standard access list

In the global configuration mode using command access – the list in the acl filtering rules, use the no form of this command returns the default value

access-list <idx> [deny|permit] [any|host|<A.B.C.D>] {time-range name}

Parameter Description

Parameter	Description
idx	Will choose the Parameter: index, scope of <1-99>
deny|permit	Will choose the Parameter: action, can only deny or permit
any|host|<A.B.C.D>	Will choose Parameter： Any means to match all of the source IP host | < A.B.C.D > means to match the source IP or mask
name	optional Parameter: binding time name

Command mode

global configuration mode

Configuration Example

Example 1: configuration matching SRC - IP for 192.168.2.5 message, to deny

access-list 1 deny host 192.168.2.5

Example 2: IP configuration matching SRC - for all message, action for the

permit

access-list 1 permit any

Relative Command

Command	Description
no access-list <idx>	Delete idx entry access-list

3.6 access list ip extended

In the global configuration mode using Commandaccess - the list in the filtering rules, use the no form of this Command returns the default value

access-list <idx> [deny|permit] [ip-proto|ip] [any|[host|<A.B.C.D>]]

[any|[host|<A.B.C.D>]] {dscp dscp-value}{time-range name}

access-list <idx> [deny|permit] [tcp|udp] [any|[host|<A.B.C.D>]] {eq src-port}

[any|[host|<A.B.C.D>]] {eq dst-port} {dscp dscp-value}{time-range name}

Parameter Description

Parameter	Description
idx	Will choose the Parameter: index, range <100-199>
deny|permit	Will choose Parameter：action，only deny or permit
Ip-proto|ip	Will choose Parameter： Ip-proto value，range <0-255> Or all IP protocol
tcp|udp	Will choose Parameter： Tcp protocol Or UDP protocol
any|[host|<A.B.C.D	Will choose Parameter： Any means to match all the SRC - IP The host | < A.B.C.D > means to match the SRC IP or mask
Src-port	Optional Parameter: matching l4 - SRC - port, the scope of th 5535 >
any|[host|<A.B.C.D	Will choose Parameter： Any means to match all the dst-IP The host | < A.B.C.D > means to match the dst-IP or mask

Dst-port	Optional Parameter: matching l4 - DST - port, the scope of the 5535 >
dscp-value	Optional Parameter: message DSCP values, the range of 0-6
name	optional Parameter: binding time name

Command mode global configuration mode

Configuration Example

Case 1: configuration matching IP, DSCP values of 8 message,action is deny

access-list 100 deny ip any any dscp 8

Relative Command

Command	Description
no access-list <idx>	Delete idx entry access-list

3.7 access list mac extended

In the global configuration mode using Commandaccess - the list in the filtering rules, use the no form of this Command returns the default value

access-list <idx> [any|[host|<HH:HH:HH:HH:HH:HH>]] [any|[host|<HH:HH:HH:HH:HH:HH>]] [etype-any|eth-proto] {cos cos-value} {time-rangename}

Parameter Description

Parameter	Description
idx	Will choose the Parameter: index, range <700-799>
deny|permit	Will choose Parameter：action，only deny or permit
any|[host|<HH:HH:l:HH:HH>]	Will choose Parameter： Any means to match all the SRC - IP The host | <HH:HH:HH:HH:HH:HH> means to match the SRC nask
any|[host|<HH:HH:l:HH:HH>]	Will choose Parameter： Any means to match all the dst-IP The host | <HH:HH:HH:HH:HH:HH> means to match the dst-I

	nask
etype-any|eth-proto	Will choose Parameter： Etype-any is all Ethernet protocol eth-proto is Ethernet protocol，range <0-0xffff>
cos-value	Optional Parameter:protocol cos value，range <0-7>
name	optional Parameter: binding time name

Command mode

global configuration mode

Configuration Example

Case 1: configuration matches all Ethernet protocol, the cosine value of 5 message,action is deny

access-list 700 deny any any etype-any cos 5

Relative Command

Command	Description
no access-list <idx>	Delete idx entry access-list

3.8 access list expert extended

In the global configuration mode using Commandaccess - the list in the acl filtering rules, use the no form of this Command returns the default value.

access-list <idx> [any|[host|<HH:HH:HH:HH:HH:HH>]] [any|[host|<A.B.C.D>]] [any|[host|<HH:HH:HH:HH:HH:HH>]] [any|[host|<A.B.C.D>]] {ip-proto|ip} {etype-any|eth-proto} {cos cos-value} {dscp dscp-value} {vid vid-value} {time-range name}

Parameter Description

Parameter	Description
idx	Will choose the Parameter: index, range <2700-2799>
deny|permit	Will choose Parameter：action，only deny or permit
any|[host|<HH:HH:HH:HH:HH:HH>	Will choose Parameter： Any means to match all the SRC - IP The host | <HH:HH:HH:HH:HH:HH>

	means to match the SRC IP or mask
any|[host|<A.B.C.D>]	Will choose Parameter： Any means to match all the SRC - IP The host | < A.B.C.D > means to match the SRC IP or mask
any|[host| <HH:HH:HH:HH:HH:HH>	Will choose Parameter： Any means to match all the dst- IP The host | <HH:HH:HH:HH:HH:HH> means to match the dst-IP or mask
any|[host|<A.B.C.D>]	Will choose Parameter： Any means to match all the dst- IP The host | < A.B.C.D > means to match the dst IP or mask
etype-any|eth-proto	Will choose Parameter： Etype-any is all Ethernet protocol eth-proto is Ethernet protocol，range <0-0xffff>
Ip-proto|ip	Will choose Parameter： Ip-proto value，range <0-255> Or all IP protocol
cos-value	Optional Parameter:protocol cos value，range <0-7>
dscp-value	Optional Parameter: message DSCP values, the range of 0-63 >
vid-value	Optional Parameter：protocol vid value， range<0-4094>
name	optional Parameter: binding time name

Command mode global configuration mode

Configuration Example Case 1: configuration matching all agreements, action is deny

access-list 2700 deny any any any any

Relative Command

Command	Description
no access-list <idx>	Delete idx entry access-list

3.9 ip access-list

Create IP standard ACL or IP extended ACL,and enter ACL mode

ip access-list { extended | standard } id

Delete the ACL

no access-list { id | name } {index <10-1000>}

Parameter Description

Parameter	Description
idx	IP access list number, standard (1-99), extended (100-199)

Default Configuration

--no ACL

Command mode

global configuration mode

Configuration Example

Create an extended ACL numbered "123":

```
Console(config)# ip access-list extended 123
Console(config-ext-nacl)# show access-lists
ip access-list extended 123
```

Relative Command

Command	Description
no access-list <idx>	Delete idx index access-group
show access-list	Show ACL rule

3.10 mac access-list extended

Create MAC extended ACL，and enter ACL mode

mac access-list extended *id*

Delete MAC extended ACL

no access-list id {index <10-1000>}

Parameter Description

Parameter	Description
id	MAC Access list number（700-799）

Default Configuration no MAC extended ACL。

Command mode global configuration mode

Usage Guide -If you want to filter the Layer 2 packets in the network, you need to use the MAC extended ACL. You need to create a MAC extended ACL first.

Configuration Example 1：Create a MAC extended ACL numbered 704:

```
Console(config)# mac access-list extended 704
Console(config-mac-nacl)# show access-lists
mac access-list extended 704
```

Relative Command

Command	Description
no access-list <idx>	Delete idx index access-group
show access-list	Show ACL rule

3.11 expert access-list extended

Create an expert extended ACL and enter the configuration mode.

expert access-list extended *id*

Delete expert extended ACL

no access-list id {index <10-1000>}

Parameter Description

Parameter	Description
id	The number of the expert access list（2700-2799）

Default Configuration No expert-level extended ACLs are created

Command mode global configuration mode

Usage Guide If you want to achieve the IP standard ACL, IP extended ACL and MAC extended ACL filtering effect in an ACL, you can use the expert extended ACL.

Configuration Example Create an expert ACL number 2704:

```
Console(config)# expert access-list extended 2704
Console(config-exp-nacl)# show access-lists
expert access-list extended 2704
```

```
Console(config-exp-nacl)#
```

Relative Command

Command	Description
no access-list <idx>	Delete idx index access-group
show access-list	Show ACL rule

3.12 access group

The interface configuration mode using Commandaccess group in the acl filtering rules come into force in the interface, use the no form of this Command returns the default value.

[ip|mac|expert] access-group [access-list_value] in

Parameter Description

Parameter	Description
[ip|mac|expert]	Will choose the Parameter: choose what kind of access-list
access-list_value	Will choose Parameter：access-list value，range Standard IP access-list <1-99> Extended IP access-list <100-199> Extended MAC access-list <700-799> Expert expert access-list <2700-2799> Standard IPV6 access-list <500-599> Extended IPV6 access-list <600-699>

Command mode

interface configuration mode

Configuration Example

Case 1: configuration configuration access - the list in the current interface effect

ip access-group 1 in

Relative Command

Command	Description
no access-group <idx>	Delete idx entry access-group

3.13 IPV6 standard access list

In the global configuration mode using Commandipv6 access - the list in the acl filtering rules, use the no form of this Command returns the default value.

Ipv6 access-list <idx> [deny|permit] [any|host <X:X::X:X>|<X:X::X:X/M>] {time-range name}

Parameter Description

Parameter	Description
idx	Will choose the Parameter: index, scope of <500-599>
deny|permit	Will choose Parameter：action，only deny or permit
[any|host <X:X::X:X>|<X:X::X:X/M>]	Will choose the Parameter: Any means to match all of the source IPV6 host address The host < X: X: X: X > means to match the source IPV6 host address The < X: X: X: X/M > means to match the source IPV6 host address and the length of the mask
{time-range name}	optional Parameter: binding time name

Command mode

global configuration mode

Configuration Example

Example 1: configuration matching SRC - ipv6 for 4003: syntactic sugar for 1:2:3: : 1 message, action is deny

ipv6 access-list 500 deny host 4003:1:2:3::1

Example 2: SRC - ipv6 configuration matching for all messages，action is permit

ipv6 access-list 500 permit any

Relative Command

Command	Description
no ipv6 access-list <idx>	Delete idx entry ipv6 access-list

3.14 IPV6 extended access list

In the global configuration mode using Commandaccess - the list in the acl filtering rules, use the no form of this Command returns the default value.

ipv6 access-list <idx> [deny|permit] [<0-255>|tcp|udp] [any|host <X:X::X:X>|<X:X::X:X/M>] {[eq] <0-65535>} [any|host <X:X::X:X>|<X:X::X:X/M>] {[eq] <0-65535>} {time-range name}

Parameter Description

Parameter	Description
idx	Will choose the Parameter: index, scope of <500-599>
deny|permit	Will choose Parameter：action，only deny or permit
Ip-proto|ip	Will choose Parameter： Ip-proto value，range <0-255> Or all IP protocol
[any|host <X:X::X:X>|<X:X::X:X/M>]	Will choose the Parameter: Any means to match all of the source IPV6 host address The host < X: X: X: X > means to match the source IPV6 host address The < X: X: X: X/M > means to match the source IPV6 host address and the length of the mask
{[eq] <0-65535>}	Optional Parameter: matching l4 - DST - port, the scope of the 5535 >
[any|host <X:X::X:X>|<X:X::X:X/M>]	Will choose the Parameter: Any means to match all of the source IPV6 host address The host < X: X: X: X > means to match the destination IPV6 host address The < X: X: X: X/M > means to match the destination IPV6 host address and the length of the mask
{[eq] <0-65535>}	Optional Parameter: matching l4 - DST - port, the scope of the 5535 >
{time-range name}	optional Parameter: binding time name

Command mode

global configuration mode

Configuration Example

Case 1: configuration matching TCP protocol, the movement for the permit, the source address is 4003:1:2:3::1, L4 source port of 8, the destination address is 5003:1:2:3::1, L4 port to 9

ipv6 access-list 600 permit tcp host 4003:1:2:3::1 eq 8 host 5003:1:2:3::1 eq 9

Relative Command

Command	Description
no ipv6 access-list <idx>	Delete idx entry ipv6 access-list

3.15 access group

The interface configuration mode using Commandaccess group in the acl filtering rules come into force in the interface, use the no form of this Command returns the default value.

[ip|mac|expert] access-group [access-list_value] in

Parameter Description

Parameter	Description
[ip|mac|expert]	Will choose the Parameter: choose what kind of access-list
access-list_value	Will choose Parameter：access-list value，range Standard IP access-list <1-99> Extended IP access-list <100-199> Extended MAC access-list <700-799> Expert expert access-list <2700-2799> Standard IPV6 access-list <500-599> Extended IPV6 access-list <600-699>

Command mode

interface configuration mode

Configuration Example

Case 1: configuration configuration access - the list in the current interface effect

ip access-group 1 in

Relative Command

Command	Description
no access-group <idx>	Delete idx entry access-group

3.16 show access-list

Show the configuration of all ACLs or specified ACLs

show access-list [*id*]

Parameter Description

Parameter	Description
id	The number of ACL

Command mode global configuration mode

Usage Guide show the ACL configuration information. If no ACL number or name is specified, this command displays all ACL configuration information.

Configuration Example show ACL configuration information:

Console(config)# show access-list 102

ip access-list extended 102

Relative Command

Command	Description
no access-list <idx>	Delete idx index access-group
show access-list	Show ACL rule

3.17 show access-group

Show the ACL configuration applied on the interface

show access-group [**interface** *interface-name*]

Parameter Description

Parameter	Description
interface	Interface-name Specifies the interface name

Command mode global configuration mode

Usage Guide You can use this command if you want to check whether ACLs are applied on the specified interface, or if you want to see which interfaces have ACL applied.

Configuration Example show whether ACLs are applied to the interfaces on the device:

Console(config)show access-group

ip access-list standard 1 in

10 permit any

Applied On interface GigabitEthernet 0/1.

4 PoE management

4.1 poe reset

Restart the PoE function module.

poe reset

Command mode global configuration mode

Usage Guide Restart the PoE function module.

Configuration Example Restart the PoE function module.

```
Console# config
Console(config)# poe reset
Console(config)#
```

4.2 poe Enable

Enable/disable port supply power status.

poe Enable

no poe Enable

Default Configuration Default status：OFF.

Command mode interface configuration mode

Usage Guide The user can Enable or close port PoE function. By default, access convergence PoE function of switch port is closed. Please configure the following under the interface mode.

Configuration Example Below is the open port 1 state of power supply:

```
Console# config
Console(config)# interface GigabitEthernet 1
Console(config-if-GigabitEthernet1)# poe Enable
Console(config-if-GigabitEthernet1)#
```

Relative Command

Command	Description
show poe powersupply	Show poe system information.

show poe interfaces status	Show poe status
show poe interfaces configuration	Show poe configuration Parameter.

Command mode

Enable/disable port supply power status.

poe Enable

no poe Enable

Default Configuration

Default status：OFF.

Command mode

interface configuration mode

Usage Guide

The user can Enable or close port PoE function. By default, access convergence PoE function of switch port is closed. Please configure the following under the interface mode.

Configuration Example

Below is the open port 1 state of power supply:

```
Console# config
Console(config)# interface GigabitEthernet 1
Console(config-if-GigabitEthernet1)# poe Enable
Console(config-if-GigabitEthernet1)#
```

Relative Command

Command	Description
show poe powersupply	Show poe system information.
show poe interfaces status	Show poe status
show poe interfaces configuration	Show poe configuration Parameter.

Enable/disable port supply power status.

poe Enable

no poe Enable

Default Configuration Default status：OFF.

Command mode interface configuration mode

Usage Guide The user can Enable or close port PoE function. By default, access convergence PoE function of switch port is closed. Please configure the following under the interface mode.

Configuration Example Below is the open port 1 state of power supply:

```
Console# config
Console(config)# interface GigabitEthernet 1
Console(config-if-GigabitEthernet1)# poe Enable
Console(config-if-GigabitEthernet1)#
```

Relative Command

Command	Description
show poe powersupply	Show poe system information.
show poe interfaces status	Show poe status
show poe interfaces configuration	Show poe configuration Parameter.

Command mode Enable/disable port supply power status.

poe Enable

no poe Enable

Default Configuration Default status：OFF.

Command mode interface configuration mode

Usage Guide The user can Enable or close port PoE function. By default, access convergence PoE function of switch port is closed. Please configure the following under the interface mode.

Configuration Example Below is the open port 1 state of power supply:

```
Console# config
Console(config)# interface GigabitEthernet 1
Console(config-if-GigabitEthernet1)# poe Enable
```

```
Console(config-if-GigabitEthernet1)#
```

Relative Command

Command	Description
show poe powersupply	Show poe system information.
show poe interfaces status	Show poe status
show poe interfaces configuration	Show poe configuration Parameter.

4.3 poe mode

Choose the way to the PD distribution power of the device to connect. PoE switches support power management mode have automatic mode (Auto mode) and Static mode (Static mode).

poe mode [**auto** | **static**]

Parameter Description

Parameter	Description
auto	Auto mode
static	Static mode

Default Configuration By default, auto (automatic mode) as the default mode.

Command mode global configuration mode

Usage Guide This Command is used to select equipment connection way of PD distribution power.

Configuration Example The following is the set of power supply management mode for the energy saving mode:

```
Console# config
Console(config)# poe mode auto
Console(config)#
```

Relative Command

Command	Description
show poe powersupply	Show poe status

4.4 poe type

Set or disable port at&af mode .

poe type [af | at&af]

no poe type

Parameter Description

Parameter	Description
af	802.3af mode
at&af	802.3at mode

Default Configuration

Default is at&af mode .

Command mode

interface configuration mode

Configuration Example

Set port 1 mode is af:

```
Console# config
Console(config)# interface GigabitEthernet 1
Console(config-if-GigabitEthernet1)# poe type af
Console(config-if-GigabitEthernet1)#
```

Relative Command

Command	Description
show poe interfaces configuration	Show poe configuration Parameter.

4.5 poe priority

Set/close PoE power supply priority of the port. Priority order from High to Low is: Critical, High and Low. In automatic mode and mode of energy conservation, high priority as well as power supply port. At the time of PoE switch machine power shortage, low priority port first off electricity.

poe priority [**low** | **high** | **critical**]

no poe priority

Parameter Description

Parameter	Description
low	Low priority
high	High priority
critical	Critical priority

Default Configuration

Port of the default priority for all low (low).

Command

interface configuration mode

mode

Configuration Example

Below is a set of port 1 power as the highest priority:

```
Console# config
Console(config)# interface GigabitEthernet 1
Console(config-if-GigabitEthernet1)# poe priority critical
Console(config-if-GigabitEthernet1)#
```

Relative Command

Command	Description
show poe powersupply	Show poe system information.
show poe interfaces status	Show poe status
show poe interfaces configuration	Show poe configuration Parameter.

4.6 poe max-power

Set/close port maximum power. Users can configure port maximum power, to limit the maximum output power of a port.

poe max-power *values*

no poe max-power

Parameter Description

Parameter	Description
values	Maximum power range of 0-36 w

Default Configuration

The default maximum power port is 32 w.

Command mode

interface configuration mode

Usage Guide

This Command only in automatic mode and mode under the effect of energy conservation.

If under automatic mode and energy saving mode, the Max - power is set to 0, port of electricity, and no longer on the electricity.

If power supply management mode under automatic mode and configure the Max - power Command, then the power management algorithm according to the user's Max power - the power configuration Command to calculate the distribution of the port.

Configuration Example

Below is a set of port 1 maximum power of 30 w:

```
Console# config
Console(config)# interface GigabitEthernet 1
Console(config-if-GigabitEthernet1)# poe max-power 30
Console(config-if-GigabitEthernet1)#
```

Relative Command

Command	Description
show poe powersupply	Show poe system information.
show poe interfaces status	Show poe status
show poe interfaces configuration	Show poe configuration Parameter.

4.7 **poe** alarmpower

Configure the system of the alarm power.

poe alarmpower *power_values*

Parameter Description

Parameter	Description
power_values	The biggest warning power can be set up, the range is 15-300

Default Configuration

The default state: maximum.

Command mode

global configuration mode

Configuration Example

Below is the configuration system alarm power of 100 w:

```
Console# config
Console(config)# poe alarmpower 100
Console(config)#
```

Relative Command

Command	Description
show poe forcepower	Show system poe information

4.8 poe reserve-power

Set the system keep power Command.

poe reserve-power *value*

Parameter Description

Parameter	Description
value	Keep power setting percentage between 0 to 50.

Command mode

global configuration mode

Usage Guide

The current consumption of power will not exceed the limit of PoE switches itself, only in the current PoE switch power supply management mode for energy saving mode when it happened.

Configuration Example

The following is set up the system retains the power of 15 w:

```
Console# config
Console(config)# poe reserve-power 15
Console(config)#
```

Relative Command

Command	Description
show poe powersupply	Show poe status

4.9 poe individual

Set or disable poe individual.

poe individual

no poe individual

Configuration Example

Set poe individual Enable:

```
Console# config
Console(config)# poe individual
```

Relative Command

Command	Description
show poe powersupply	Show syatem poe information

4.10 poe sysmarks method

Set the system POE resistance capacitance mode.

poe sysmarks method [**res** | **res+cap**]

Parameter Description

Parameter	Description
res	Resistance mode
res+cap	Resistance and capacitance mode

Default Configuration

res-plus-cap(res+cap mode).

Command mode

global configuration mode

Configuration Example

Set poe is res mode：

```
Console# config
Console(config)# poe sysmarks method res
Console(config)#
```

Relative Command

Command	Description
show poe powersupply	Show poe status

4.11 poe uninterruptible-power

Open/close warm start uninterrupted power supply function. Warm start uninterrupted power supply function, at the time of system restart, has been in a state of power supply of PD equipment in the process of warm start PoE switches will not off electricity. Warm start, after the completion of the system back to the configuration file saved state.

poe uninterruptible-power

no poe uninterruptible-power

Default Configuration

The default state: close the warm start uninterrupted power supply.

Command mode

global configuration mode

Usage Guide

After open or close the function has to save the configuration to ensure effective in the reduction of the next.

Configuration Example

Poe uninterruptible-power Enable:

```
Console# config
Console(config)# poe uninterruptible-power
Console(config)#
```

Relative Command

Command	Description
show poe powersupply	Show poe status

4.12 poe notification-control

Open/close POE switch control trap sent. Control system is needed in the practical application in power changes and port whether on or off the electricity to send the trap. This function is used to set whether to send the trap.

poe notification-control Enable

no poe notification-control Enable

Default Configuration

The default state: close the POE switch control trap sent.

Command mode

global configuration mode

Usage Guide

This CLI command can only control RFC3621 defined in the trap to send, to the defined RFC3621 trap sending control is not effective. Open RFC3621 defined in trap send function, when the alarm of power since the childhood to or equal to the system power state changes to notice a greater than the power system, if subsequent alarm power has been greater than the system power, no longer send the trap; When the alarm power from greater than or equal to the system power state to less than the system power when notice once, if subsequent alarm has been less than the power system, power is no longer send the trap.

Configuration Example

Poe trap Enable :

```
Console# config
Console(config)# poe notification-control Enable
Console(config)#
```

Relative Command

Command	Description
show poe powersupply	Show poe status

4.13 ic-temp btsh-set

Set the IC Num temperature threshold.

ic-temp btsh-set icnum *icnum* **btsh** *values*

Parameter Description

Parameter	Description
icnum	Chip number: the range 1 to 3
values	Threshold temperature: it is recommended that 70 ° C to 120 ° C, the largest 150 ° C

Default Configuration

The default alarm temperature threshold value: 120°C

Command mode

global configuration mode

Configuration Example

Below is a set of IC 1 temperature threshold of 100°C:

```
Console# config
Console(config)# ic-temp btsh-set icnum 1 btsh 100
Console(config)#
```

5 mstp

5.1 spanning-tree

Open the MSTP, with the Parameter in the open of MSTP at the same time, set the MSTP global basic Settings. Using the Command no option to close spanning-tree function, if no Command Parameter option only to the corresponding Parameter to restore default, but it doesn't close the spanning tree.

spanning-tree [forward-time *seconds* | hello-time *seconds* | max-age *seconds*]

no spanning-tree [forward-time | hello-time | max-age]

Parameter Description

Parameter	Description
forward-time *seconds*	Port state change of time interval.
hello-time *seconds*	Equipment regularly sends bpdus in packet interval.
max-age *seconds*	BPDU packets news live the longest.

Default Configuration

spanning-tree is disable

Command mode

global configuration mode

Usage Guide

-Forward - time, hello - time, Max - the age of three values range is related to, Revised one of them will affect the value of the other two. There is a restriction relationship between these three values: 2 * (Hello Time + 1.0 SND) < = Max - Age Time < = 2 * (Forward - Delay - 1.0 SND)

Do not qualify for this value will also be setting is not successful.

Configuration Example

example 1：open the spanning-tree function：

```
Console(config)# spanning-tree
```

Example 2：set BridgeForwardDelay：

```
Console(config)# spanning-tree forward-time 10
```

Relative Command

Command	Description
show spanning-tree	Show STP global configuration information.
spanning-tree mst cost	Set STP interface PathCost.
spanning-tree tx-hold-count STP	TxHoldCount config

5.2 spanning-tree loopguard default

The global open loop guard features. Use this Command no option of closed loop guard features. Enable the loop guard function, can prevent root port or backup mouth due to not receive bpdus possible loop.

spanning-tree loopguard default

no spanning-tree loopguard default

Default Configuration The default closed loop guard function

Command mode global configuration mode

Configuration Example

```
Console(config)# spanning-tree loopguard default
```

5.3 spanning-tree max-hops

Under the global configuration mode using this Command can set the maximum number of jump bpdus frame (Max - hops Count), it specifies the bpdus within a Region after how many devices are discarded, and the Instance of all effective. Using the no option to the Command to restore to the default values.

spanning-tree max-hops *hop-count*

no spanning-tree max-hops

Parameter Description

Parameter	Description
Parameter	*Description*
hop-count	*Bpdus can pass before being discarded equipment number, range 1-40*

Default *hop-count default value is* 20

Configuration

Command mode global configuration mode

Usage Guide Within the Region, the Root Bridge, send bpdus contains a Hot item Count, starting from the Root Bridge, every equipment, Hop Count is minus 1, until timeout, 0 indicates the bpdus information device receives Hops value of 0 bpdus will discard it.

Change the Max - hops will affect all the Instance.

Configuration Example The next example to take all the MST Instance Max - hops a value of 10:

```
Console(config)# spanning-tree max-hops 10
```

Can also type in the show spanning - tree MST privileged Command to verify the above configuration

Relative Command

Command	Description
show spanning-tree	Show MSTP information

5.4 spanning-tree mode

Use this Command to STP version under global mode. Using the no option can be generated tree version back to the default value.

spanning-tree mode [**stp** | **rstp** | **mstp**]

no spanning-tree mode

Parameter Description

Parameter	Description
stp	Spanning tree protocol(IEEE 802.1d)
rstp	Rapid spanning tree protocol(IEEE 802.1w)
mstp	Multiple spanning tree protocol(IEEE 802.1s)

Default Configuration MSTP version

Command mode global configuration mode

Configuration Example

```
Console(config)# spanning-tree mode stp
```

Relative Command

Command	Description
show spanning-tree	Show sapnning-tree information

5.5 spanning-tree mst configure

Under the global mode can use this Command to enter the MST mode, configuration MSTP Region. Using the no option can be under the Command of all parameters (name, revision, vlan map) back to the default values.

spanning-tree mst configuration

no spanning-tree mst configuration

Default Configuration

The default instance and vlan corresponding relation is all vlan in instance 0.

name is empty.

revision is 0.

Command mode

global configuration mode

Usage Guide

Want to return to the privileged mode, Command input end, or type Ctrl + C key combination.

To return to global configuration mode, type exit Command.
After entering the MST configuration mode, you can use the following Command to configure the Parameter:
The instance instance id vlan vlan - range: add a vlan group to the MST instance. Here the instance - id of the range of 0-64. Vlan range 1-4095. Vlan - range can be a collection of vlan, vlan ID see use commas, continuous vlan ID can be used to '-' link end two vlan ID, such as: the instance 10 vlan 2,3,6-9 defines the vlan 2,3,6,7,8,9 added to the instance of 10. The default configuration is all VLAN in Instance 0. The VLAN is removed from the Instance method is to use the no Command: no Instance Instance - id (VLAN VLAN - range). (pay attention to the no Command of the Instance for the range of 1-64)
The name name: specify the MST name, most can contain 32 character string. You can use the no name back to its default value.
The MST revision version: set version number, the range of 0-65535. You can use the no revision will be back to the default value.
Show spanning - tree MST configuration: display the current the MST region information.

Configuration Example

The following examples to illustrate how to enter the MST mode, the VLAN 3, 5-10 mapped to the MST Instance 1:

```
Console(config)# spanning-tree mst configuration
Console(config-mst)# instance 1 vlan 3，5-10
Console(config-mst)# name region 1
```

```
Console(config-mst)# revision 1
Console(config-mst)# show spanning-tree mst configuration
MST configuration
Name [region1]
Revision 1
Instance Vlans Mapped
---------- --------------------
0 1-2,4,11-4094
1 3,5-10
---------------------------------
Console(config-mst)# exit
Console(config)#
```

If you would have a VLAN 3 is removed from the Instance 1, then after entering the MST configuration mode, perform the following process.

```
Console(config-mst)# no instance 1 vlan 3
```

If you would have the entire Instance 1 remove, the method is as follows:

```
Console(config-mst)# no instance 1
```

You can use the MST configuration Command show verification of the above process.

Relative Command

Command	Description
show spanning-tree mst	Show MST region configuration
instance instance-id vlan vlan-range	A Vlan group added to the MST Instance
name	MST configuration name
revision	Configuration MST revision

5.6 spanning-tree pathcost method

Configure port cost calculation method of the default path. Use the no command set the back to the default value.

spanning-tree pathcost method {{**long [standard]}** | **short**}

no spanning-tree pathcost method

Parameter Description

Parameter	Description
long [standard]	The 802.1 t standard set path - the cost value. Standard

	said according to the Standards recommended by the formula to calculate the cost value.
short	Using 802.1 d standard set path - the cost value.

Default Configuration The default set Path - cost by 802.1 T standard values.

Command mode global configuration mode

Configuration Example

```
Console(config-if)# spanning-tree pathcost method long
```

Relative Command

Command	Description
show spanning-tree interface	Show STP interface configuration .

5.7 spanning-tree portfast bpdufilter default

The global open bpdus filter. The user can use the Command no options for the closing of the global bpdus filter.

spanning-tree portfast bpdufilter default

no spanning-tree portfast bpdufilter default

Default Configuration The default close bpdus filter

Command mode global configuration mode

Usage Guide After open the bpdus Filter, corresponding port can neither send nor receive bpdus. Use show spanning - tree Command to check the Settings.

Configuration Example

```
Console(config)# spanning-tree portfast bpdufilter default
```

Relative Command

Command	Description
show spanning-tree interface	Show STP configuration

5.8 spanning-tree portfast bpduguard default

The global open bpdus guard. The user can use the no command for the closing of the global bpdus guard.

spanning-tree portfast bpduguard default

no spanning-tree portfast bpduguard default

Default Configuration The default close bpdus Guard.

Command mode global configuration mode

Usage Guide Open the bpdus guard, if received bpdus in the port, will enter the error - disabled state. Use show spanning - tree Command to check the Settings.

Configuration Example

```
Console(config)# spanning-tree portfast bpduguard default
```

Relative Command

Command	Description
show spanning-tree interface	Show STP configuration

5.9 spanning-tree portfast default

The global open all the Portfast switch of the interface. Use the no Command to close global Portfast switch of the all interfaces.

spanning-tree portfast default

no spanning-tree portfast default

Default Configuration The default close all the Portfast switch of the interface.

Command mode global configuration mode

5.10 spanning-tree reset

Set the whole spanning - tree revert to the default value. This Command does not have no option.

spanning-tree reset

Command mode global configuration mode

Configuration Example

```
Console(config)# spanning-tree reset
```

Relative Command

Command	Description
show spanning-tree	Show STP configuration information in the global
show spanning-tree interface	Show STP interface configuration

5.11 spanning-tree priority

Configure the spanning-tree priority; the "**no spanning-tree priority**" command restores the default priority.

spanning-tree priority <0-61440>

Default Configuration

32768

Command mode

global configuration mode

Usage Guide

The bridge ID can be altered by changing the priority of the switch. Further, the priority information can also be used for voting of the root bridge and the specified ports. The bridge priority value of the switch is smaller, however the priority is higher.

Configuration Example

```
Console(config)# spanning-tree priority 4096
```

Relative Command

Command	Description
show spanning-tree	Show STP configuration information in the global
show spanning-tree interface	Show STP interface configuration

5.12 spanning-tree tc-protection

Set the port is tc-protection port, “**no spanning-tree tc-protection**” command sets the port is non-tc-protection port.

spanning-tree tc- protection

Default Configuration The default open tc-protection switch.

Command mode global configuration mode

Configuration Example

```
Console(config)# spanning-tree tc- protection
```

5.13 spanning-tree tc-protection tc-guard

The global open tc - guard switch. Use this Command no option global close tc-guard switch. Enable the tc-guard function, can prevent the spread of the tc message.

spanning-tree tc-protection tc-guard

no spanning-tree tc-protection tc-guard

Default Configuration The default close tc - guard switch.

Command mode global configuration mode

Configuration Example

```
Console(config)# spanning-tree tc-protection tc-guard
```

5.14 spanning-tree tx-hold-count

STP global TxHoldCount setup, configure a second number up to send bpdus. Use the Command no option set the back to the default value.

spanning-tree tx-hold-count *tx-hold-count*

no spanning-tree tx-hold-count

Parameter Description

Parameter	Description
x-hold-count TxHoldCount config	Range 1 to 10

Default Configuration The default value is 3.

Command mode global configuration mode

Configuration Example

```
Console(config)# spanning-tree tx-hold-count 5
```

Relative Command

Command	Description
show spanning-tree interface	Show STP configuration

5.15 spanning-tree autoedge

Open an interface Autoedge switch. The user can use the Command is disabled option close the interface Autoedge switch.

spanning-tree autoedge disable

Parameter Description

Parameter	Description
disable	Close the interface Autoedge switch.

Default Configuration The default is disable.

Command mode Interface configuration mode

Configuration Example

```
Console(config)# interface GigabitEthernet 1
Console(config-if-GigabitEthernet1)# spanning-tree autoedge disable
```

Relative Command

Command	Description
show spanning-tree interface	Show port STP configuration

5.16 spanning-tree bpdufilter

Open the bpdus filter switch of an interface. The user can use this Command to Enable or disable option to open or close the interface bpdus filter switch.

spanning-tree bpdufilter {**Enable** | **disable**}

Parameter Description

Parameter	Description
disable	Close the interface of bpdus filter switch.
Enable	Open the bpdus filter of the interface switch.

Default Configuration The default is off.

Command mode Interface configuration mode.

Configuration Example

```
Console(config)# interface GigabitEthernet 1
Console(config-if-GigabitEthernet1)# spanning-tree bpdufilter Enable
```

Relative Command

Command	Description
show spanning-tree interface	Show port STP configuration

5.17 spanning-tree bpduguard

Open the bpdus Guard switch of an interface. The user can use this Command to Enable or disabled option to open or close the interface bpdus Guard switch.

spanning-tree bpduguard {**Enable** | **disable**}

Parameter Description

Parameter	Description
disable	Close the interface of bpdus Guard switch.
Enable	Open the interface of bpdus Guard switch.

Default Configuration the default is disable

Command mode Interface configuration mode.

Configuration Example

```
Console(config)# interface GigabitEthernet 1
Console(config-if-GigabitEthernet1)# spanning-tree bpduguard Enable
```

Relative Command

Command	Description
show spanning-tree interface	Show port STP configuration

5.18 spanning-tree compatible Enable

Based on the current port interface attribute information selective carry MSTI information to send, in order to realize the interconnection between with other producers.

spanning-tree compatible Enable

no spanning-tree compatible Enable

Default Configuration	the default is disable
Command mode	Interface configuration mode
Configuration Example	Console(config)# interface GigabitEthernet 1 Console(config-if-GigabitEthernet1)# spanning-tree compatible Enable

5.19 spanning-tree guard loop

Interface on the open loop guard features. Use this Command no option of closed loop guard features. Enable the loop guard function, can prevent to port or backup mouth due to not receive bpdus possible loop.

spanning-tree guard loop

no spanning-tree guard loop

Default Configuration	the default is disable
Command mode	Interface configuration mode
Configuration Example	Console(config)# interface GigabitEthernet 1 Console(config-if-GigabitEthernet1)# spanning-tree guard loop

5.20 spanning-tree guard none

The interface properties off guard. Use this Command no option to cancel the guard on the interface features.

spanning-tree guard none

no spanning-tree guard none

Default Configuration	The default is off guard function.
Command mode	Interface configuration mode
Configuration Example	Console(config)# interface GigabitEthernet 1 Console(config-if-GigabitEthernet1)# spanning-tree guard none

5.21 spanning-tree guard root

Open the root guard feature on the interface. Use the Command no option off the root guard feature. To Enable root guard function, can prevent the current caused by wrong configuration or illegal packet attack position changes the root bridge.

spanning-tree guard root

no spanning-tree guard root

Default Configuration The default is off guard function.

Command mode Interface configuration mode

Configuration Example

```
Console(config)# interface GigabitEthernet 1
Console(config-if-GigabitEthernet1)# spanning-tree guard root
```

5.22 spanning-tree ignore tc

Open tc filter switch interface. Use this Command no option close tc filter switch. Enable the tc filtering function, the port tc message will not be received.

spanning-tree ignore tc

no spanning-tree ignore tc

Default Configuration The default is close TC filtering capabilities.

Command mode Interface configuration mode

Configuration Example

```
Console(config)# interface GigabitEthernet 1
Console(config-if-GigabitEthernet1)# spanning-tree ignore tc
```

5.23 spanning-tree link-type

Configuration of the interface connection type is " point-to-point" connections. Users can use the Command no option will set back to default values.

spanning-tree link-type {**point-to-point** | **share**}

no spanning-tree link-type

Parameter Description

Parameter	Description
point-to-point	Mandatory set the interface connection type to point - to - point
share	Mandatory set the interface connection type to share

Default Configuration

Interface type double working hours for the whole, the interface of the connection types of point-to-point; Interface type for two hours, the interface connection type to share.

Command mode

Interface configuration mode.

Configuration Example

```
Console(config)# interface GigabitEthernet 1
Console(config-if-GigabitEthernet1)# spanning-tree link-type share
```

Relative Command

Command	Description
show spanning-tree interface	Show STP port configuration

5.24 spanning-tree mst cost

Under the interface mode use this Command to set each instance of the path cost. Using the no option to the Command to restore to the default values.

spanning-tree {**mst** instance-id} **cost** cost-value

no spanning-tree {**mst** instace-id} **cost**

Parameter Description

Parameter	Description
instance-id	The Instance number, range of 0-16
cost-value	Path cost values, the range of 1-200 000 000 or auto

Default Configuration

The instance id of the default value is 0.

The default value is automatically according to the link rate of interface is calculated.

1000 Mbps——20000

100 Mbps——200000

10 Mbps——2000000

Command mode Interface configuration 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.

Configuration Example On the port 1, set the MSTP port cost in the instance 3 to 300.

```
Console(config)# interface GigabitEthernet 1
Console(config-if-GigabitEthernet1)# spanning-tree mst 3 cost 300
```

Relative Command

Command	Description
show spanning-tree mst configuration	Show port MSTP information

5.25 spanning-tree mst port-priority

Use this command to set the interface under the interface mode for different instance in different port priority, this will affect the region formed in the loop of the port status will be sent. Using the no option to the command to restore to the default values.

spanning-tree {**mst** instance-id} **priority** priority-value

no spanning-tree {**mst** instace-id} **priority**

Parameter Description

Parameter	Description
instance-id	Instance number, range of 0-16
priority-value	The port priority, can choose 0,16,32,48,64,80,96,112,128,144,160 and so on, a total of 16 integer, all is a multiple of 16.

Default Configuration The instance id of the default value is 0. Priority - the value of the default value is 128.

Command mode Interface configuration mode.

Usage Guide By setting the port priority, users can control the port ID of the instance in order to control the root port and designated port of the instance. The lower the value of the port priority is, the higher the priority is.

Configuration Example Set the port priority as 16 on the port 1 for the instance 3.

```
Console(config)# interface GigabitEthernet 1
Console(config-if-GigabitEthernet1)# spanning-tree mst 3 port-priority 16.
```

Relative Command

Command	Description
show spanning-tree mst configuration	Show port MSTP information

5.26 spanning-tree port-priority

The interface configuration mode by using this Command is to configure spanning tree the priority of the interface.

spanning-tree priority priority-value

no spanning-tree priority

Parameter Description

Parameter	Description
priority-value	The port priority, can choose 0,16,32,48,64,80,96,112,128,144,160, 176,192,208,224,240, a total of 16 integer, all is a multiple of 16.

Default Configuration

Priority - the value of the default value is 128.

Command mode

Interface configuration mode.

Usage Guide

To form the loop within the region, preferred a high-priority port in the sending state. Priority phase at the same time, choose to smaller port number.

Configuration Example

Give an interface GigabitEthernet 1 configuration priority value 16:

```
Console(config)# interface GigabitEthernet 1
Console(config-if-GigabitEthernet1)# spanning-tree port-priority 16.
```

5.27 spanning-tree portfast

Open the portfast switch of an interface. The user can use the Command disable options close the portfast switch of the interface.

spanning-tree portfast {disable}

Parameter Description

Parameter	Description
disable	Close the interface of the portfast switch.

Default Configuration

The default is off.

Command mode

Interface configuration mode.

Configuration Example

```
Console(config)# interface GigabitEthernet 1
Console(config-if-GigabitEthernet1)# spanning-tree portfast
```

Relative Command

Command	Description
show spanning-tree interface	According to the STP port configuration information.

5.28 spanning-tree tc-guard

Open tc-guard on the interface. Use this command no option is close the interface of tc - guard switch. Enable the tc-guard function, can prevent the spread of the tc message.

spanning-tree tc-guard

no spanning-tree tc-guard

Default Configuration

The default is close tc - guard switch.

Command mode

Interface configuration mode.

Configuration Example

```
Console(config)# interface GigabitEthernet 1
Console(config-if-GigabitEthernet1)# spanning-tree tc-guard
```

5.29 show spanning-tree

Show information about the global configuration and spanning tree.

show spanning-tree [**summary** | **forward-time** | **hello-time** | **max-age** | **inconsistentports|tx-hold-count** | **pathcost method** | **max_hops** | **counters**]

Parameter Description

Parameter	Description
summary	Show information about the each instance of MSTP and its port forwarding state information.

forward-time	Show BridgeForwardDelay.
hello-time	Show BridgeHelloTime.
max-age	Show BridgeMaxAge.
max-hops	Show instance max-hops
tx-hold-count	Show TxHoldCount.
pathcost method	Show how to determine the path cost.
counters	Show the STP contract awarding statistics.

Command mode Enable mode .

Configuration Example Console# show spanning-tree hello-time

Relative Command

Command	Description
spanningtree pathcost method	Show how to determine the path cost.
spanning-tree forward-time	Set BridgeForwardDelay.
spanning-tree hello-time	Set BridgeHelloTime.
spanning-tree max-age	Set BridgeMaxAge.
spanning-tree max-hops	Set instance max-hops
spanning-tree tx-hold-count	Show TxHoldCount.

5.30 show spanning-tree interface

According to the STP interface Settings. Including the optional spanning tree configuration.

show spanning-tree interface *interface-id* [{bpdufilter | portfast | bpduguard | link-type }]

Parameter Description

Parameter	Description
interface-id	Port nomber
bpdufilter	Show bpdufilter status
portfast	Show portfast status

bpduguard	Show bpduguard status
link-type	Show port linktype

Command mode

Enable mode .

Configuration Example

```
Console# show spanning-tree interface GigabitEthernet 1/5
```

Relative Command

Command	Description
spanning-tree bpdufilter	Open the bpdus filter switch of an interface.
spanning-tree portfast	Open the portfast switch of an interface.
spanning-tree bpduguard	Open the bpdus guard switch of an interface.
spanning-tree link-type	Configuration of the interface connection type is "the point-to-point connections”.

5.31 show spanning-tree mst

Under the Enable mode use this Command to view the MST configuration, the Instance of the information.

show spanning-tree mst { configuration | *instance-id* [interface *interface-id*] }

Parameter Description

Parameter	Description
configuration	Device mst configuration
instance-id	*Instance number*
interface-id	Port ID

Command mode

Enable mode .

Configuration Example

```
Console# show spanning-tree mst configuration
```

Relative Command

Command	Description
spanning-tree mst configuration	Enter MST region configuration
spanning-tree mst cost	show instance path cost

spanning-tree mst max-hops	show instance max-hops
spanning-tree mst priority	Show instance priority
spanning-tree mst port-priority	show instance port priority

6.DHCP Relay & Server & Snooping

6.1 service dhcp

Enable the DHCP relay agent. No form of the Command shut down the DHCP relay agent.
service dhcp
no service dhcp

Default Configuration
By default, shut down the DHCP relay agent.

Command mode
global configuration mode

Usage Guide
DHCP relay DHCP request can be forwarded to other servers, and will return the DHCP reply packet is forwarded to the DHCP client, to play the role of a transit DHCP message.

Configuration Example
Enable the DHCP relay function：

```
Console(config)# service dhcp
Console(config)#
```

Relative Command

Command	Description
show ip dhcp relay	Show dhcp relay configuration information

6.2 ip helper-address

The purpose of configuration relay forwarding the address of the server. No form of the Command to delete relay server address.
ip helper-address *address*
no ip helper-address *address*

Parameter Description

Parameter	Description
address	Server IP address, configurable up to 10 server address

Default Configuration
By default, no configuration relay server address

Command mode
global configuration mode

Usage Guide
Can support up to configure server 10 purpose. If open the function of relay agent, then receives the broadcast DHCP message, to be delivered in the form of unicast to configure on the server.
The following are examples of configuration relay server address:

Configuration Example

```
Console(config)# ip helper-address 192.168.2.30
Console(config)#
```

Relative Command

Command	Description
show ip dhcp relay	Show dhcp relay configuration information

6.3 ip dhcp relay information option

Open relay agent option82 function. No form closed option82 function of the Command.
ip dhcp relay information option
no ip dhcp relay information option

Default Configuration

By default for open option82 functions.

Command mode

global configuration mode

Usage Guide

After open relay agent option82 function, forwarded to the proxy server message will add relay agent information on option.

Configuration Example

The following is an example of an open option82 configuration:

```
Console(config)# ip dhcp relay information option
Console(config)#
```

Relative Command

Command	Description
show ip dhcp relay	Show dhcp relay configuration information

6.4 ip dhcp relay information trust-user-option

Trust option82 information from the client. The no form of this Command is a distrust of the discarded with option82 information message from the client.
ip dhcp relay information trust-user-option
no ip dhcp relay information trust-user-option

Default Configuration

Default for trust option82 information from the client.

Command mode

global configuration mode

Usage Guide

Trust mode, when the client received the DHCP message with option82 information, keep, or add a switch their option82 information forwarded. The trust mode, discarding belt option82 information message from the client.

Configuration Example

The following are examples of configuration closed option82 trust the client information:

```
Console(config)# no ip dhcp relay information trust-user-option
Console(config)#
```

Relative Command

Command	Description
show ip dhcp relay	Show dhcp relay configuration information

6.5 ip dhcp information option circuitid

Configuration option82 sub - option1 circuit ID of options for the user custom content (storage format for the ASCII) and forward. The no form of the Command to delete the content of the custom.
ip dhcp information option circuitid *circuit-id* **fromvlan** *vid* **acsii-string** *string*
no ip dhcp information option fromvlan *vid* **suboption circuited**

Parameter Description

Parameter	Description
circuit-id	Circuit ID number type, scope of 1 ~ 254
vid	The DHCP request message in the VLAN, value range is 1 ~ 4094
string	Circuit ID to populate the user custom content, scope of string length is 3 ~ 63

Command mode

global configuration mode

Usage Guide

Based on vlan choose to use DHCP message take under the vlan configuration of circuit ID options content, if there is no configuration, the default use the circuit ID 0 type, content of vlan ID + interface number, namely the DHCP client's vlan and port.

Configuration Example

The following are examples of configuration circuit ID sub options content:

```
Console(config)# ip dhcp information option circuitid 1 fromvlan 1 acsii-string test
Console(config)#
```

Relative Command

Command	Description
show ip dhcp relay	Check the DHCP relay configuration information
show ip dhcp snooping	Check the DHCP snooping configuration information
ip dhcp relay information option	Open relay agent option82 function
ip dhcp snooping information option	Open DHCP Snooping option82 function

6.6 ip dhcp information option remoteid

Configuration option82 sub - option2 remote ID of options for the user custom content (storage format for the ASCII) and forward. The no form of the Command to delete the content of the custom.
ip dhcp information option remoteid *remote-id* **fromvlan** *vid* **acsii-string** *string*
no ip dhcp information option fromvlan *vid* **suboption remoteid**

Parameter Description

Parameter	Description
remote-id	Remote-ID number type, scope of 1 ~ 254
vid	The DHCP request message in the VLAN, value range is 1 ~ 4094
string	Circuit ID to populate the user custom content, scope of string length is 3 ~ 63

Command mode

global configuration mode

Usage Guide

Based on VLAN choose to use DHCP message take under the VLAN configuration of the remote ID options content, if there is no configuration, the default use remote ID 0 type, content to switch MAC address.

Configuration Example

Configure the remote ID are options below examples of content:

```
Console(config)# ip dhcp information option remoteid 1 fromvlan 1 acsii-string test
Console(config)#
```

Relative Command

Command	Description
show ip dhcp relay	Show the DHCP relay configuration information
show ip dhcp snooping	Show the DHCP snooping configuration information
ip dhcp relay information option	Open relay agent option82 function
ip dhcp snooping information option	Open DHCP Snooping option82 function

6.7 ip dhcp information option ip

Configuration option82 sub - option5 IP option content. No form of the Command to delete IP options for the configuration of the content.
ip dhcp information option ip *address* **fromvlan** *vid*
no ip dhcp information option fromvlan *vid* **suboption ip**

Parameter Description

Parameter	Description
adresss	IP address dotted decimal
vid	Vlan id value, value range is 1 ~ 4094

Command mode

global configuration mode

Usage Guide

Based on the vlan choose to use DHCP message take under the vlan configuration of IP options content, if there is no configuration, no send this option.

Configuration Example

Below are examples of son configure IP options content:

```
Console(config)# ip dhcp information option ip 192.168.2.3 fromvlan 1
Console(config)#
```

Relative Command

Command	Description
show ip dhcp relay	Show the DHCP relay configuration information
show ip dhcp snooping	Show the DHCP snooping configuration information
ip dhcp relay information option	Open relay agent option82 function
ip dhcp snooping information option	Open DHCP Snooping option82 function

6.8 show ip dhcp relay

Show the DHCP relay configuration information
show ip dhcp relay

Command mode

Enable mode

Usage Guide

Use this Command to view the DHCP relay and option82 related configuration information.

Configuration Example

The following are examples of show DHCP relay configuration:

```
Console(config)# show ip dhcp relay

        relay status                    :start3relay
        option82 status                   :Enable
        trust user option82               :Enable
        dhcp serverip                   :192.168.2.30,Status:valid
        option82 ip                     :
                        From Vlan | Ip Addr
                        ---------   -------
                              1 | 192.168.2.3

        option82 cid                      :
                        From Vlan | Id     String
                        ---------   --     ------
                              1 | 1      test

        option82 rid                      :
                        From Vlan | Id     String
                        ---------   --     ------
                              1 | 1      test

Console(config)#
```

Relative Command

Command	Description
service dhcp	Enable the DHCP relay agent
ip helper-address	The purpose of configuration relay forwarding the address of the server
ip dhcp relay information option	Open relay agent option82 function
ip dhcp relay information trust-	Trust the client option82 information

user-option	
ip dhcp information option circuitid	Configuration option82 sub - option1 circuit ID options
ip dhcp information option remoteid	Configure option82 sub - option2 remote ID options
ip dhcp information option ip	Configuration option82 sub - option5 IP option content

6.9 ip dhcp snooping

Open DHCP Snooping global function. The no form of the Command will shut down the DHCP Snooping function
ip dhcp snooping
no ip dhcp snooping

Default Configuration By default, shut down the DHCP Snooping function

Command mode global configuration mode

Usage Guide After open the DHCP Snooping function, use the show IP DHCP snoopingCommand can see DHCP Snooping function is on.
The following is an example of an open DHCP Snooping global function:

Configuration Example

```
Console(config)# ip dhcp snooping
Console(config)#
```

Relative Command

Command	Description
show ip dhcp snooping	Show the DHCP Snooping configuration information

6.10ip dhcp snooping vlan

Open the specified VLAN DHCP Snooping function, the no form of the Command closes the corresponding VLAN DHCP Snooping function.
ip dhcp snooping vlan *vlan-list*
no ip dhcp snooping vlan *vlan-list*

Parameter Description

Parameter	Description
vlan-list	lan list, such as 1, 3-5,7,9-11. Vlan range is 1 ~ 4094

Default Configuration By default, without any vlan open DHCP Snooping function.

Command mode global configuration mode

Usage Guide In addition to the global open DHCP Snooping function, still need other also

Configuration Example

open DHCP Snooping function on the VLAN，
Otherwise the study will not be able to monitor the binding table of VLAN.
The following are examples of configuration open DHCP snooping function of vlan1:

```
Console(config)# ip dhcp snooping vlan 1
Console(config)
```

Relative Command

Command	Description
ip dhcp snooping	The global open DHCP Snooping function
show ip dhcp snooping	Show the DHCP Snooping configuration information

6.11ip dhcp snooping trust

Configure port for trust port. No form of the Command configuration ports for distrust.
ip dhcp snooping trust
no ip dhcp snooping trust

Default Configuration

By default for untrusted port

Command mode

interface configuration mode

Usage Guide

Trust port forwarding normal receive DHCP message, distrust port discards the DHCP response message, thus connecting the DHCP server and other DHCP Snooping device ports need to be set to trust.

Configuration Example

The following are examples of configuration 1 port for trust port:

```
Console(config)# interface GigabitEthernet 1
Console(config-if-GigabitEthernet1)# ip dhcp snooping trust
Console(config-if-GigabitEthernet1)#
```

Relative Command

Command	Description
show ip dhcp snooping	Show the DHCP Snooping configuration information
show ip dhcp snooping trust	Show whether the port port for trust

6.12 ip dhcp snooping suppression

Configure port to curb the status. No form of the Command set port to the inhibition of the status.
ip dhcp snooping suppression
no ip dhcp snooping suppression

Default Configuration

By default for the inhibition of the status

Command mode interface configuration mode

Usage Guide Through this Command, but refused to port under all the DHCP request packet,

namely prohibited under the port's application for all users by DHCP address.

Configuration Example In the port 1， set is dhcp snooping suppression port:

```
Console(config)# interface GigabitEthernet 1
Console(config-if-GigabitEthernet1)# ip dhcp snooping suppression
Console(config-if-GigabitEthernet1)#
```

Relative Command

Command	Description
show ip dhcp snooping suppression	Show to see if port for inhibition of port

6.13 ip dhcp snooping verify mac-address

The global open source MAC address validation function. No form of the Command closed source MAC address validation functions.
ip dhcp snooping verify mac-address
no ip dhcp snooping verify mac-address

Default Configuration By default the shut down

Command mode global configuration mode

Usage Guide The source MAC address validation function, is to the DHCP CLIENT issued a request message, check the link layer header MAC address is the same and the DHCP CLIENT MAC field in the message. The source MAC address validation fails, a message will be discarded.

Configuration Example Examples of open DHCP to use MAC check:

```
Console(config)# ip dhcp snooping verify mac-address
Console(config)#
```

Relative Command

Command	Description
show ip dhcp snooping	Show the DHCP Snooping configuration information
ip dhcp snooping verify mac	Set on whether a particular MAC source MAC address check

6.14 ip dhcp snooping verify mac

Whether can be set separately for a particular MAC source MAC address check. No form of this Command does not need to source MAC address of the MAC.
ip dhcp snooping verify mac *mac-address*
no ip dhcp snooping verify mac *mac-address*

Parameter Description

Parameter	Description
mac-address	MAC address format for HH: HH: HH: HH: HH: HH

Command mode global configuration mode

Usage Guide This feature can be based on the global open source MAC address check, use the no form for one MAC don't check.

Configuration Example

```
Console(config)# no ip dhcp snooping verify mac 00:00:00:00:00:01
Console(config)#
```

Relative Command

Command	Description
show ip dhcp snooping	Show the DHCP Snooping configuration information

ip dhcp snooping verify mac-address	The global open source MAC address validation function

6.15 ip dhcp snooping dhcpserver

Use this Command to add a trusted the DHCP server address. The no form of the Command to delete the corresponding server address
ip dhcp snooping dhcpserver *ip-address*
no ip dhcp snooping dhcpserver *ip-address*

Parameter Description

Parameter	Description
ip-address	Server IP address

Command mode

global configuration mode

Usage Guide

When have configurations trusted the DHCP server address, after receiving the response from the DHCP server packages, need to check whether the server address is one of the trusted server address configuration, if the check fails, will discard the packet. Do not have any trusted address configuration, do not need to do this check.

Configuration Example

Below are examples of add a trusted server address:

```
Console(config)# ip dhcp snooping dhcpserver 192.168.2.30
Console(config)#
```

Relative Command

Command	Description
show ip dhcp snooping	Show the DHCP Snooping configuration information

6.16 ip dhcp snooping information option

Open DHCP Snooping option82 function. Turn this feature off the no form of the Command
ip dhcp snooping information option
no ip dhcp snooping information option

Default Configuration

The default is off.

Command mode

global configuration mode

Usage Guide

By configuring the Command, will be added in the DHCP request packet option82 information forwarded to the server, the DHCP server can be flexible allocation according to this information. About user defined sub - option1, sub - option2, sub - option5 configuration described above.

Configuration Example

Below is the open DHCP Snooping option82 example:

```
Console(config)# ip dhcp snooping information option
Console(config)#
```

Relative Command

Command	Description
show ip dhcp snooping	Show the DHCP Snooping configuration information

6.17 ip dhcp snooping information client_option

Configure trust take option82 DHCP message from the client. The no form of the Command is configured for distrust.
ip dhcp snooping information client_option
no ip dhcp snooping information client_option

Default Configuration

By default for the trust

Command mode

global configuration mode

Usage Guide

Trust mode will keep client option82 option, and forward a message, and don't trust mode, if you receive from the client with option82 DHCP message, will discard the packet.

Configuration Example

The following are examples of configuration trust client option82 packet:

```
Console(config)# ip dhcp snooping information client_option
Console(config)#
```

Relative Command

Command	Description
show ip dhcp snooping	Show the DHCP Snooping configuration information

6.18 ip dhcp snooping bingding mac

Add a static binding information. No form of the Command to delete the corresponding static binding.
ip dhcp snooping binding mac *mac-address* **vlan** *vid* **expire** *lease-time*
no ip dhcp snooping binding mac *mac-address* **vlan** *vid*

Parameter Description

Parameter	Description
mac-address	The DHCP client MAC address
vid	Location VLAN ID
lease-time	Lease expiration time, value range is 1-100000 seconds

Command mode

interface configuration mode

Usage Guide

The Command static binding on a client in a port and a VLAN, so if you receive the client's DHCP request message from other ports or VLAN will be discarded. Static Settings, there is no corresponding IP information, the IP information needed by dynamic monitoring learning get assigned to the MAC client server IP address.

Configuration Example

Here is to a port on the 1 static add an example of the binding information:

```
Console(config)# interface GigabitEthernet 1
Console(config-if-GigabitEthernet1)# ip dhcp snooping binding mac
```

```
00:00:00:00:00:01 vlan 1 expiry 20
Console(config-if-GigabitEthernet1)#
```

Relative Command

Command	Description
show ip dhcp snooping binding	Show DHCP Snooping binding data information

6.19 ip dhcp snooping database write-delay

Timing of DHCP Snooping database configuration switches binding information written to the FLASH. No form of the Command close timing write FLASH function.
ip dhcp snooping database write-delay *time*
no ip dhcp snooping database write-delay

Parameter Description

Parameter	Description
time	Time interval, the range of 600-600 seconds

Default Configuration

By default to shut down

Command mode

global configuration mode

Usage Guide

Through this Command, DHCP Snooping database can be written to FLASH files regularly, prevent the equipment after the restart, user information is missing, cause the user must to obtain IP address, can the normal communication.

Configuration Example

The following are examples of configuration timing will be binding database written to flash:

```
Console(config)# ip dhcp snooping database write-delay 1000
Console(config)#
```

Relative Command

Command	Description
show ip dhcp snooping	Show the DHCP Snooping configuration information

6.20 ip dhcp snooping database write-to-flash

The DHCP Snooping binding information database immediately written to the FLASH file.
ip dhcp snooping database write-to-flash

Command mode

global configuration mode

Usage Guide

By executing this Command, the binding information table can be immediately written to the FLASH stored.

Configuration Example

Below is information immediately written to the flash of DHCP binding database example:

```
Console(config)# ip dhcp snooping database write-to-flash
Console(config)#
```

6.21 renew ip dhcp snooping database

The information in the current FLASH into the DHCP Snooping binding database.
renew ip dhcp snooping database

Command mode

global configuration mode

Usage Guide

By executing the Command, can real-time information to import flash files to the DHCP Snooping database.

Configuration Example

Here is the flash file information import DHCP Snooping database examples:

```
Console(config)# renew ip dhcp snooping database
Console(config)#
```

6.22 clear ip dhcp snooping binding

Delete the DHCP Snooping binding the dynamic user data.
clear ip dhcp snooping binding [*ip***] [***mac***] [***vid***] [interface** *interface-id***]**

Parameter Description

Parameter	Description
ip	Specify the IP address of the user
mac	Specify the delete user's MAC address
vid	Specify the delete user VLAN ID
interface-id	Specify the delete user belongs to port

Command mode

Enable mode

Usage Guide

To perform this Command, you can delete all or specified DHCP Snooping database dynamic user.

Configuration Example

Below is to remove the DHCP Snooping database all the examples of dynamic user:

```
Console# clear ip dhcp snooping binding
Console#
```

Relative Command

Command	Description
Show ip dhcp snooping binding	Show DHCP Snooping binding data information

6.23 show ip dhcp snooping

Check the DHCP Snooping the current configuration.
show ip dhcp snooping

Command mode

Enable mode

Usage Guide

To perform this Command, you can view the current configuration of DHCP Snooping.

Configuration Example

Show current DHCP Snooping configuration：

```
Console# show ip dhcp snooping

        snoop status                  :Enable
        option82 status               :Enable
        client option82 status        :Enable
        verfiy status                 :Enable
        cycle save bind status        :Enable
        cycle save bind times         :1000 s
        trust port                    :Gi0/1
        snoop vlan                    :1
        dhcpserver ipaddr             :192.168.2.30

        mac verfiy table              :
                    Mac Address | Verfiy Status
                    -----------   -------------
              00:00:00:00:00:01 | disable

        option82 ip                   :
                    From Vlan | Ip Addr
                    ---------   -------
                          1 | 192.168.2.3

        option82 cid                  :
                    From Vlan | Id    String
                    ---------   --    ------
                          1 | 1     test

        option82 rid                  :
                    From Vlan | Id    String
                    ---------   --    ------
                          1 | 1     test
Console#
```

Relative Command

Command	Description
ip dhcp snooping	DHCP Snooping global configuration switch
ip dhcp snooping vlan	Open the specified VLAN DHCP Snooping function

ip dhcp snooping trust	Configure port for trust port
ip dhcp snooping verify mac-address	The global open source MAC address validation function
ip dhcp snooping verify mac	Set on whether a particular MAC source MAC address check
ip dhcp snooping dhcpserver	Add a trust the DHCP server address
ip dhcp snooping information option	Open DHCP Snooping option82 function
ip dhcp snooping information client_option	Configure trust take option82 DHCP message from the client
ip dhcp snooping database write-delay	Timing of DHCP Snooping database configuration switches binding information written to the FLASH
ip dhcp information option circuitid	Configuration option82 sub - option1 circuit ID option content
ip dhcp information option remoteid	Configure option82 sub - option2 remote ID option content
ip dhcp information option ip	Configuration option82 sub - option5 IP option content

6.24 show ip dhcp snooping binding

Show DHCP Snooping data of user information
show ip dhcp snooping binding

Command mode

Enable mode

Usage Guide

Use the Command，show current DHCP Snooping data all user information.

Configuration Example

Console# show ip dhcp snooping binding

Mac address	IP address	Vlan	Interface	Lease	Status
00:00:00:00:00:01	**0.0.0.0**	**1**	**Gi0/1**	**20**	**Static**
00:05:16:09:13:09	**192.168.2.2**	**1**	**Gi0/10**	**172800**	**Dynamic**

Relative Command

Command	Description
ip dhcp snooping bingding mac	Static add binding mac
clear ip dhcp snooping binding	Delete DHCP Snooping binding dynamic user

6.25 show ip dhcp snooping trust

In interface configuration mode， show trust port

show ip dhcp snooping trust

Command mode interface configuration mode

Usage Guide Use the Command，the port whether is a trust port.

Configuration Example

```
Console(config)# interface GigabitEthernet 1
Console(config-if-GigabitEthernet1)# show ip dhcp snooping trust

 snoop trust status: Enable
Console(config-if-GigabitEthernet1)#
```

Relative Command

Command	Description
ip dhcp snooping trust	Config trust port

6.26 show ip dhcp snooping suppression

In interface configuration mode， show port wether suppression DHCP protocol.
show ip dhcp snooping suppression

Command mode interface configuration mode

Usage Guide Use the Command，the port whether is a suppression port.

Configuration Example

```
Console(config)# interface GigabitEthernet 1
Console(config-if-GigabitEthernet1)# show ip dhcp snooping suppression

 snoop suppression status: Enable
Console(config-if-GigabitEthernet1)#
```

Relative Command

Command	Description
ip dhcp snooping suppression	Config port is suppression status

6.27 service dhcp-server

Open DHCP server function.The no option command disable DHCP sever.

service dhcp-server

no service dhcp-server

Default Configuration

By default, shut down the DHCP server function.

Command mode

global configuration mode

Usage Guide

The DHCP server automatically assign IP addresses to client. The DHCP server can not open in conjunction with DHCP relay agent.

Configuration Example

Below is the open DHCP server features:

```
Console(config)# service dhcp-server
Console(config)#
```

Relative Command

Command	Description
show ip dhcp server	Show the DHCP server configuration information

6.28 ip dhcp pool

Create a DHCP address and enter the DHCP pool pool configuration mode. No form of the Command to delete a DHCP address pool.

ip dhcp pool *pool-id*

no ip dhcp pool *pool-id*

Parameter Description

Parameter	Description
pool-id	Pool address id, the range of 1-65535

Default Configuration

By default the DHCP pool is not defined

Command mode

global configuration mode

Configuration Example

Here is to create the pool with ID 1 DHCP address pool, and into the pool configuration mode:

```
Console(config)# ip dhcp pool 1
Console(dhcp-config)#
```

Relative Command

Command	Description
show ip dhcp server	Show the DHCP server configuration information

6.29 network

Define the DHCP pool of network and network mask. No form of the Command to delete the configuration of the network number and mask.

network *network-number net-mask [low-ipaddress high-ip-address]*

no network

Parameter Description

Parameter	Description
network-number	The IP address of the DHCP pool network number
net-mask	The IP address of the DHCP pool network mask.
low-ip-address	starting IP address
high-ip-address	ending IP address

Default Configuration

By default does not define the network number and network mask

Command mode

DHCP pool configuration mode

Usage Guide

Define new address pool and subnet mask, DHCP server provides a can be assigned to the client's address space.

Configuration Example

Here is to configure the DHCP pool network number for 192.168.2.0, mask is 255.255.255.0:

```
Console(dhcp-config)# network 192.168.2.0 255.255.255.0
Console(dhcp-config)#
```

Relative Command

Command	Description
show ip dhcp server	Show the DHCP server configuration information

6.30 lease

Define the DHCP server assigned to client address lease time. The no form of the Command to restore the default configuration.

lease *{day [hours] [minutes]* | **infinite***}*

no lease

Parameter Description

Parameter	Description
days	Define the lease time, the unit for the day
hours	Define the lease time, the unit for hours
minutes	Define the lease time, the unit is minutes.
infinite	There is no limit to the definition of the lease

Default Configuration

The default lease for one day

Command mode

DHCP pool configuration mode

Usage Guide

When the lease, then the DHCP client sends request for renewal. The DHCP server will generally allow relet, renewal and address remains the same.

Configuration Example

The following example will set the DHCP lease time for 2 hours and 30 minutes:

```
Console(dhcp-config)# lease 0 2 30
Console(dhcp-config)#
```

Relative Command

Command	Description
show ip dhcp server	Show the DHCP server configuration information

6.31 option

Configure the DHCP server option. No form of the Command to delete option configuration.

option *code* **{ascii** *sting* **| hex** *string* **| ip** *ip-address***}**

no option

Parameter Description

Parameter	Description
code	Define the DHCP option code
ascii *sting*	Define the DHCP option ascii value
hex *string*	Define the dhcp option hex value
ip *ip-address*	Define IP address list

Default Configuration

The default lease for one day

Command mode DHCP pool configuration mode

Usage Guide DHCP provides a mechanism to allow in the heart of the TCP/IP network configuration information transmitted to the host. DHCP message have option fields, the part of the content can change the content, the user can be defined according to actual condition, the DHCP client must be able to accept option information carrying at least 312 bytes of the DHCP message. Another DHCP message of fixed data field is also known as an option. Regarding the definition of the current DHCP option, please see RFC 2132 documents.

Configuration Example The following examples to define option code 43, this option is for the supplier to custom information:

```
Console(dhcp-config)# option 43 ip 192.168.2.44
Console(dhcp-config)#
```

Relative Command

Command	Description
show ip dhcp server	Show the DHCP server configuration information

6.32 default-rouer

Define the DHCP client default gateway. No form of the Command to delete the default gateway configured.

default-router *ip-address [ip-adress2 … ip-address8]*

no default-router

Parameter Description

Parameter	Description
ip-address	The default gateway address, at least one configuration
ip-adress2 … ip-address8	(optional) up to eight gateway can be configured.

Default Configuration The default does not define the default gateway

Command mode DHCP address configuration mode

Usage Guide Usually the client need to get the default gateway information from the DHCP server. The DHCP server will need at least specify a gateway IP address for the client.

Configuration Example The following example defines 192.168.2.11 as the default gateway:

```
Console(dhcp-config)# default-router 192.168.2.11
Console(dhcp-config)#
```

Relative Command

Command	Description
show ip dhcp server	Show DHCP server configuration information

6.33 dns-server

Defining DHCP client's DNS server. The Command's no form to delete the definition of DNS servers.

dns-server *ip-address [ip-adress2 … ip-address8]*

no dns-server

Parameter Description

Parameter	Description
ip-address	Defining DNS server IP address, configure at least one
ip-adress2 … ip-address8	(Optional) You can configure up to eight DNS server.

Default Configuration

By default, no defined default gateway

Command mode

DHCP address configuration mode

Usage Guide

When you define multiple DNS servers, EDITORIAL priority to engage, DHCP client and DNS server and only the top head of communications failure, will select the next DNS server.

Configuration Example

The following example defines 192.168.2.3 as the DNS server:

```
Console(dhcp-config)# dns-server 192.168.2.3
Console(dhcp-config)#
```

Relative Command

Command	Description
show ip dhcp server	Show DHCP server configuration information

6.34 domain-name

Defining DHCP client domain name suffix. The Command's no form to remove the domain name suffix.

domain-name *domain-name*

no domain-name

Parameter Description

Parameter	Description
domain-name	Domain name suffix string defined DHCP client

Default Configuration

By default, no domain name suffix

Command mode

DHCP address configuration mode

Usage Guide

DHCP client to obtain the domain name suffix specified later, when accessing a host with the same domain name suffix, the host name directly through it.

Configuration Example

The following example to define a DHCP client domain name suffix test.com.cn:

```
Console(dhcp-config)# domain-name test.com.cn
Console(dhcp-config)#
```

Relative Command

Command	Description
show ip dhcp server	Show DHCP server configuration information

6.35 host

Defining DHCP client hardware address of the host IP static binding. The Command's no form to remove the configuration.

host *hardware-address ip-address*

no host *hardware-address*

Parameter Description

Parameter	Description
hardware-address	Defining DHCP client's MAC address
ip-address	Defining DHCP client host IP address

Command mode DHCP address configuration mode

Usage Guide If the definition of a static host binding for the hardware address of the host will give priority to configure the corresponding IP address assignment.

Configuration Example Here is a static set the hardware address is 00: 23: 44: 56: 03: IP address 22 is 192.168.2.15:

```
Console(dhcp-config)# host 00:23:44:56:03:22 192.168.2.15
Console(dhcp-config)#
```

Relative Command

Command	Description
show ip dhcp server host	Show DHCP static host address binding configuration

6.36 ip dhcp excluded-address

Define certain IP address, the DHCP server does not assign to DHCP clients. The Command's no form to remove the configuration.

ip dhcp excluded-address *low-ip-address [high-ip-address]*

no ip dhcp excluded-address *low-ip-address [high-ip-address]*

Parameter Description

Parameter	Description
low-ip-address	IP address exclusion, which excluded IP address range starting IP address
high-ip-address	End IP address exclusion address range.

Default Configuration The default DHCP server address pool to allocate the entire range of IP addresses

Command mode global configuration mode

Usage Guide If you do not exclude an IP address, DHCP server assigned DHCP address pool view all IP addresses. The Command can reserve some IP addresses for a particular host, avoid these addresses to DHCP clients.

Configuration Example The following example DHCP server will not attempt to assign IP addresses 192.168.2.100 ~ 192.168.2.120 range:

```
Console(config)# ip dhcp excluded-address 192.168.2.100 192.168.2.120
Console(config)#
```

Relative Command

Command	Description
show ip dhcp server exclude	show DHCP server configuration excluded addresses

6.37 clear ip dhcp server binding

Clear DHCP binding table.

clear ip dhcp binding *[ip-address]*

Parameter Description

Parameter	Description
ip-address	Delete the specified IP address is recorded, is not specified, then remove all DHCP bindings

Command mode Enable mode

Configuration Example The following example clears the IP address of 192.168.2.100 DHCP binding:

```
Console# clear ip dhcp server binding 192.168.2.100
Console#
```

Relative Command

Command	Description
show ip dhcp server binding	Show DHCP address binding information

6.38 clear ip dhcp server conflict

Clear DHCP conflict record.

clear ip dhcp conflict *[ip-address]*

Parameter Description

Parameter	Description
ip-address	Delete the specified IP address conflicts recorded is not specified, then remove all address conflicts recorded

Command mode Enable mode

Configuration Example The following example clears all address conflicts recorded:

```
Console# clear ip dhcp server conflict
Console#
```

Relative Command

Command	Description
show ip dhcp server conflict	show DHCP server conflict address

6.39 show ip dhcp server

Show DHCP server configuration information

show ip dhcp server

Command mode Enable mode

Configuration Example The following are examples show DHCP server configuration:

```
Console#show ip dhcp server

server status              : Enable


pool id                    : 1
-----------------------------------------
network                    : 192.168.2.0
netmask                    : 255.255.255.0
lease time                 : 240 secs
start ip                   : 192.168.2.1
end ip                     : 192.168.2.255
domain name                : test.com.cn
default router             : 192.168.2.11 192.168.2.12
dns server                 : 192.168.2.3 192.168.2.4
option-43                  : 192.168.2.44
Console#
```

Relative Command

Command	Description
service dhcp-server	Enable DHCP server function
ip dhcp pool	Create a DHCP address pool and enter DHCP address configuration mode
network	Defining DHCP address pool of the network number and network mask
lease	Defining DHCP server assigned to the client's address lease time
option	Configuring the DHCP server options

default-router	Default Gateway Defining DHCP clients
dns-server	Defining DHCP client's DNS server
domain-name	Domain name suffix defined DHCP client

6.40 show ip dhcp server binding

Show DHCP address binding information

show ip dhcp server binding

Command mode Enable mode

Configuration Example The following are examples show DHCP server configuration:

```
Console#show ip dhcp server binding

        ip address      hw type  hw address           expire time
        ----------      -------  ----------          ---------------
        192.168.2.2     Ethernet f0:de:f1:0a:1f:52  0Day 0Hour 2Min
Console#
```

Relative Command

Command	Description
clear ip dhcp server binding	Clear DHCP binding table

6.41 show ip dhcp server conflict

Show DHCP server Duplicate records

show ip dhcp server conflict

Command mode Enable mode

Usage Guide Address List of conflicts in the Command show DHCP server detected

Configuration Example The following are examples of conflict records show DHCP server:

```
Console# show ip dhcp server conflict

        IP Address              Detection Time
        ----------          --------------------
        192.168.2.2         Mon Mar  7 16:13:26 2016

Console#
```

Relative Command

Command	Description
clear ip dhcp server conflict	Clear DHCP conflict record

6.42 show ip dhcp server host

Show DHCP static host address binding configuration

show ip dhcp server host

Command mode

Enable mode

Configuration Example

```
Console#show ip dhcp server host

        pool id   hardware address     ip address
        -------- ------------------ ----------------
        1        00:23:44:56:03:22  192.168.2.15

Console#
```

Relative Command

Command	Description
host	IP address of the host hardware defined DHCP client static binding

6.43 show ip dhcp server exclude

Show DHCP server configuration excluded addresses

show ip dhcp server exclude

Command mode

Enable mode

Configuration Example

The following discharge address entry:

```
Console#show ip dhcp server exclude

        start ip          end ip
        ---------------   ---------------
        20.2.2.2          20.2.2.10
        19.1.1.1          10.1.1.10

Console#
```

Relative Command

Command	Description
ip dhcp excluded-address	Define certain IP address, the DHCP server does not assign to DHCP clients

7.DAI inspection

7.1 ip arp inspection

Enable DAI (Dynamic Arp Inspection) detection. The Command's no closed form DAI detection.

ip arp inspection

no ip arp inspection

Default Configuration By default, closed.

Command mode global configuration mode

Usage Guide The Command for a global open DAI detection

Configuration Example Here is an example of detection to be open:

```
Console(config)# ip arp inspection
Console(config)#
```

Relative Command

Command	Description
show ip arp	show DAI detection configurations.

7.2 ip arp inspection vlan

Use this Command to Enable the corresponding VLAN of DAI packet checking function. The Command's no closed form corresponding to the VLAN DAI detection.

ip arp inspection vlan *vlan-id*

no ip arp inspection vlan *vlan-id*

Parameter Description

Parameter	Description
vlan-id	VLAN ID number

Default Configuration Close DAI on all VLAN packets check.

Command mode global configuration mode

Usage Guide

For this Command to play a role, you must first Enable the feature

Configuration Example

Here is an example of open ARP packets received on a test VLAN1:

```
Console(config)# ip arp inspection vlan 1
Console(config)#
```

Relative Command

Command	Description
show ip arp	show DAI detection configurations.
ip arp inspection	Enable DAI band detection

7.3 ip arp inspection trust

Setting the port is trusted. Use the Command's no form to restore the port as untrusted status.

ip arp inspection trust

no ip arp inspection trust

Default Configuration

All ports are in default trust status

Command mode

interface configuration mode

Usage Guide

Port trust status to indicate that not need to check received on the port ARP packets, they are legitimate. If a non-trusted status, the need to detect incoming ARP packets and host IP and MAC port is located in the static ARP Entry configuration.

Configuration Example

Here is the untrusted port 4 status:

```
Console(config)# interface GigabitEthernet 4
Console(config-if-GigabitEthernet4)# no ip arp inspection trust
Console(config-if-GigabitEthernet4)#
```

Relative Command

Command	Description
show ip arp	show DAI detection configurations.
ip arp inspection	Enable DAI band detection
ip arp inspection vlan	DAI is Enabled in the VLAN packet checking function
ip arp entry	Setting ARP Detection Anti private static entry

7.4 ip arp entry

Setting ARP detection Anti private static IP address, static entries IP + MAC + interface.

ip arp entry src-ip *ipv4-address* **src-mac** *mac-addr*

no ip arp entry { all | src-ip *ipv4-address* **src-mac** *mac-addr* **}**

Parameter Description

Parameter	Description
ipv4-address	Source IP address
mac-addr	Source MAC address

Command mode

global configuration mode and interface configuration mode

Usage Guide

The Command supported configurations in both mode, globally and interface mode, if configured in global mode indicates that the item belongs to all ports in the specified port if configured to indicate that only part of the port.

Configuration Example

The following is a configuration example of a static IP + MAC entry address in global mode:

```
Console(config)# ip arp entry src-ip 192.168.2.10 src-mac 00:30:ab:0a:c0:c6
Console(config)#
```

Relative Command

Command	Description
show ip arp	show DAI detection configurations.

7.5 ip arp inspection rate-limit

Setting ARP packet rate limit of detection, to prevent ARP attack.

ip arp inspection rate-limit *rate-value*

Parameter Description

Parameter	Description
rate-value	Set the speed limit, the unit is 16Kbps, 0 indicates no limit rate

Default Configuration

Do not set the ARP packet rate limit function.

Command mode

global configuration mode

Usage Guide

The Command can limit the rate of ARP packets to prevent ARP attack.

Configuration

```
Here is the ARP packet rate limit is an example of 16kbps:
Console(config)# ip arp inspection rate-limit 1
```

Example

```
Console(config)#
```

Relative Command

Command	Description
show ip arp	show DAI detection configurations.

7.6 ip arp inspection dhcp-snooping-entries

Open dhcp snooping automatically synchronizes ARP entry, the Command's no form to turn off automatic synchronization.

ip arp inspection dhcp-snooping-entries

Default Configuration

Auto-sync.

Command mode

global configuration mode

Usage Guide

While the auto-sync, then learn from that DHCP Snooping listens to the IP + MAC + Port information is automatically synchronized to the ARP Entry.

Configuration Example

Here is an example turn on auto-sync:

```
Console(config)# ip arp inspection dhcp-snooping-entries
Console(config)#
```

Relative Command

Command	Description
show ip arp	show DAI detection configurations.

7.7 ip arp anti-spoofing

Open gateway anti-spoofing function. The Command's no form of closed gateway anti-spoofing function.

ip arp anti-spoofing

no ip arp anti-spoofing

Default Configuration

Close gateway anti-spoofing function.

Command mode

global configuration mode

Usage Guide

The Command and DAI detection and static binding function are mutually exclusive

Configuration Example

Here is the open gateway anti-spoofing example:

```
Console(config)# ip arp anti-spoofing
Console(config)#
```

Relative Command

Command	Description
show anti-arp-spoofing	show gateway anti-spoofing configuration information

7.8 anti-arp-spoofing ip

Setting deception gateway ipv4 address.

anti-arp-spoofing ip *ipv4-address*

no anti-arp-spoofing ip *ipv4-address*

Parameter Description

Parameter	Description
ipv4-address	Gateway IP address

Command mode

interface configuration mode and range interface configuration mode

Usage Guide

The Command Set the IP address of an interface for gateway address spoofing, if a host address is set after the deception gateway address from the port over the ARP packets from the host will be discarded.

Configuration Example

Here is set the port 4 of the IP address 192.168.2.10 as the gateway address spoofing examples:

```
Console(config)# interface GigabitEthernet 4
Console(config-if-GigabitEthernet4)# anti-arp-spoofing ip 192.168.2.10
Console(config-if-GigabitEthernet4)#
```

Relative Command

Command	Description
show anti-arp-spoofing	show gateway anti-spoofing configuration information

7.9 ip arp static-binding

Enable static IP + MAC binding function. The Command's no closed form static binding.

ip arp static-binding

no ip arp static-binding

Default Configuration

Close static binding

Command mode

global configuration mode

Usage Guide

This function DAI detection and gateway anti-spoofing functions are mutually exclusive. If you turn static binding feature, not only to view the host whether the gateway address spoofing, also to the host IP to check ARP Entry entry, if configured, the host of the MAC address must correspond to the configuration items (here only concern IP + MAC ignored Port), if not configured, the default release.

Configuration Example

Here is an example of open static IP + MAC binding function:

```
Console(config)# ip arp static-binding
Console(config)#
```

Relative Command

Command	Description
show ip arp	show DAI detection configurations.
ip arp entry	Setting ARP Detection Anti private static entry
anti-arp-snoofing ip	Setting deception gateway ipv4 address

7.10 ip arp check

Enable check function. The Command's no closed form static binding.

ip arp check

no ip arp check

Default Configuration

Close detection.

Command mode

global configuration mode

Usage Guide

This function DAI detection, static binding, and gateway anti-spoofing function are mutually exclusive. Dhcp entries will automatically detect IP Source Guard entry and the port, ip, Mac information.

Configuration Example

Here is an example of open check:

```
Console(config)# ip arp check
Console(config)#
```

Relative Command

Command	Description
show ip arp	show DAI detection configurations.

7.11 arp-check

Enable check function. The Command's no closed form static binding.

arp-check

no ip arp-check

Default Configuration Close detection.

Command mode interface configuration mode

Usage Guide This feature requires first check under the global mode feature is turned on;

Configuration Example Here is an example of open check:

```
Console(config)# ip arp check
Console(config)# interface GigabitEthernet 2
Console(config-if-GigabitEthernet2)# arp-check
```

Relative Command

Command	Description
show ip arp	show DAI detection configurations.

7.12 ip arp gratuitous-arp

Enable the gratuitous ARP sending function. The no form of this command turns off gratuitous ARP sending.

ip arp gratuitous-arp

no ip arp gratuitous-arp

Default Configuration The gratuitous ARP sending function is disabled.

Command mode global configuration mode

Usage Guide When the gratuitous ARP sending function is Enabled in the global configuration mode, gratuitous ARP sending is Enabled for all Layer 3 interfaces in the system.

Configuration Example

```
The following are examples of gratuitous-arp Enabled:
Console(config)# ip arp gratuitous-arp
```

Relative Command

Command	Description
show ip arp gratuitous-arp	Show **gratuitous-arp configuration status**

7.13 show ip arp

show DAI detection configurations.

show ip arp

Command mode

Enable mode

Configuration Example

Here is an example of view configuration information to be:

```
Console#show ip arp

        Mac address | IP address    Interface
        ------------ ---------------- -----------------
  00:30:AB:0A:C0:C6 192.168.2.10         AllPort

        ------------ ---------------- -----------------

        arp entries counter             :1
        dynamic arp inspection          :on
        static binding                  :off
        arp vlan list                   :1
        arp trust port                  :1 2 3 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21
22 23 24 25 26
        dhcp snooping entries           :on
        rate limit                      :16 kpbs

Console#
```

Relative Command

Command	Description
ip arp inspection	Enable DAI band detection
ip arp inspection vlan	DAI is Enabled in the VLAN packet checking function
ip arp entry	Setting ARP Detection Anti private static entry
ip arp inspection trust	Setting the port is trusted
ip arp inspection rate-limit	Setting ARP detection packets rate limit
ip arp inspection dhcp-snooping-entries	Open dhcp snooping automatically synchronizes ARP entries

7.14 show anti-arp-spoofing

Show gateway anti-spoofing configuration information.

Show anti-arp-spoofing

Command mode

Enable mode

Configuration Example

Here is an example of view configuration information to be:

```
Console#show anti-arp-spoofing

          Interface          IP
         ---------------  ------------------------
                   4              192.168.2.10
         ---------------  ------------------------

         anti gateway spoofing          :on

Console#
```

Relative Command

Command	Description
ip arp anti-spoofing	Open gateway anti-spoofing detection feature
anti-arp-snoofing ip	Setting deception gateway ipv4 address

8 IP Source Guard

8.1 ip verify source

Open IP Source Guard on the interface. The Command's no closed form the corresponding function.

ip verify source

no ip verify source

Default Configuration By default, closed.

Command mode interface configuration mode

Usage Guide You can open an interface through which the Command IP Source Guard feature, the user can be based on IP + MAC + VLAN + Port detection, IP Source Guard-- law turned on the DHCP Snooping trust port.

Configuration Example Here is the open IP Source Guard feature on the example of the interface 2:

```
Console(config)# interface GigabitEthernet 2
Console(config-if-GigabitEthernet2)# ip verify source
Console(config-if-GigabitEthernet2)#
```

Relative Command

Command	Description
show ip verify source	Show IP Source Guard configuration information

Configuration Example Here is the open IP Source Guard feature on the example of the interface 2:

```
Console(config)# interface GigabitEthernet 2
Console(config-if-GigabitEthernet2)# ip verify source
Console(config-if-GigabitEthernet2)#
```

Relative Command

Command	Description
show ip verify source	Show IP Source Guard configuration information

8.2 ip source binding

Add a static IP source address of the user information in the binding database, the Command's no form to delete the corresponding static user.

ip source bingding *mac-address* **vlan** *vlan-id ip-address*

no ip source binding *mac-address* **vlan** *vlan-id ip-address*

Parameter Description

Parameter	Description
mac-address	Static MAC address to add users
vlan-id	Add static user vlan id
ip-address	Add static user ip address

Command mode interface configuration mode

Usage Guide By configuring this Command allows some users by IP Source Guard detected.

Configuration Example Here it is to allow a user by way of example IP Source Guard detected:

```
Console(config)# interface GigabitEthernet 2
Console(config-if-GigabitEthernet2)# ip source binding 00:30:ab:0a:c0:c6 vlan 1
192.168.2.10 Console(config-if-GigabitEthernet2)#
```

Relative Command

Command	Description
show ip verify source	Show IP Source Guard configuration information

8.3 show ip verify source

Show IP Source Guard configuration information

show ip verify source

Command mode global configuration mode

Configuration Example Here is an example of view IP Source Guard configuration information:

```
Console(config)# show ip verify source
        MacAddress    IpAddress    Lease(sec)    Type     VLAN       Interface
        ----------- ----------- ------------ ------------ ------------ -----------
  00:30:AB:0A:C0:C6 192.168.2.10    infinite     static        1          2
        ----------- ----------- ------------ ------------ ------------ -----------
```

```
        deny-all 2

Console(config)
```

Relative Command

Command	Description
ip verify source	Open IP Source Guard on the interface
ip source binding	Add a static IP source address of the user information in the binding database

9 .IGMP Snooping & MLD Snooping

9.1 ip igmp snooping

Global Enable igmp snooping. The Command's no form to restore the off status

ip igmp snooping

no ip igmp snooping

Default Configuration By default, igmp snooping Close

Command mode global configuration mode

Usage Guide The Command is used to Enable igmp snooping

Configuration Example The following are open igmp snooping functions:

```
Console(config)# ip igmp snooping
Console(config)#
```

Relative Command

Command	Description
show ip igmp snooping	show global IGMP Snooping configuration information

9.2 ip igmp snooping forwarding-mode

Multicast forwarding mode. The Command's no form to restore the default values

ip igmp snooping forwarding-mode {mac | ip}

no ip igmp snooping forwarding-mode

Parameter Description

Parameter	Description
mac	Based on the destination multicast forwarding based on mac
ip	Based on source ip and destination ip multicast forwarding based

Default Configuration The default is mac forwarding mode

Command mode global configuration mode

Usage Guide IGMPv3 need ip forwarding mode used together in order to see the effect, under the mac forwarding mode, will be backward compatible to IGMPv2 IGMPv3 effect.

Configuration Example Below is the forwarding mode examples:

```
Console(config)# ip igmp snooping forwarding-mode ip
Console(config)#
```

Relative Command

Command	Description
show ip igmp snooping	show global IGMP Snooping configuration information

9.3 ip igmp snooping dyn-mr-aging-time

Set the aging time for dynamic routing port. The Command's no form to restore the aging time of dynamic router port configuration.

ip igmp snooping dyn-mr-aging-time *seconds*

no ip igmp snooping dyn-mr-aging-time

Parameter Description

Parameter	Description
seconds	Aging time of dynamic router port, and in seconds, ranging from 1 to 3600

Default Configuration 300 second

Command mode global configuration mode

Usage Guide If a dynamic routing connection port in its aging timer does not receive IGMP general query messages, the device will route from the port connector removed from the list.
In connection port Enable dynamic learning routing function, you can adjust the aging time of dynamic router port through this Command. If the aging time is set too short may lead to route the connection port frequent additions and deletions.

Configuration Example Below is the dynamic router port aging time is 100s:

```
Console(config)# ip igmp snooping dyn-mr-aging-time 100
Console (config)#
```

Relative Command

Command	Description
show ip igmp snooping	show global IGMP Snooping configuration information

9.4 ip igmp snooping host-aging-time

Configuring IGMP dynamic member port aging time. The Command's no form to restore the dynamic member port aging time.

ip igmp snooping host-aging-time *seconds*

no ip igmp snooping host-aging-time

Parameter Description

Parameter	Description
seconds	Aging time. In seconds, in the range 1-65535

Default Configuration

Default 260 seconds

Command mode

global configuration mode

Usage Guide

Dynamic member port aging time is when the device receives a port aging time to join an IP multicast group when the host sends IGMP join messages for the dynamic member port settings.
After receiving the IGMP join message, it resets the aging timer for the dynamic member port, the timer for the host-aging-time. If the timer expires, it is considered non-existent hosts receive multicast packets at the port, it will multicast device removes the port from the IGMP Snooping in members.

Configuration Example

Configuring dynamic port aging time IGMP 30s:

```
Console(config)# ip igmp snooping host-aging-time 30
```

Relative Command

Command	Description
show ip igmp snooping	show global IGMP Snooping configuration information

9.5 ip igmp snooping query-max-response-time

Configure the query maximum packet response time. The Command's no form to restore the configuration.

Ip igmp snooping query-max-response-time *seconds*

no ip igmp snooping query-max-response-time

Parameter Description

Parameter	Description
seconds	Query messages maximum response time, in seconds, in the range 1-65535.

Default Configuration

The default configuration of 10 seconds

Command mode

global configuration mode

Usage Guide

After receiving IGMP general query packet, a multicast device reset all dynamic member port aging timer, the timer time query-max-response-time. If the timer expires, it is considered non-existent hosts receive multicast packets at the port, it will multicast device removes the port from the IGMP Snooping member ports. After receiving IGMP group-specific query message, a multicast device reset all the members of the particular group dynamic port aging timer, the timer time query-max-response-time. If the timer expires, it is considered non-existent hosts receive multicast packets at the port, the device will multicast the port is removed from the mouth of a member of IGMP Snooping.

Configuration Example

Below is the message query maximum response time for 100s:

```
Console(config)# ip igmp snooping query-max-response-time 100
Console(config)#
```

Relative Command

Command	Description
show ip igmp snooping	show global IGMP Snooping configuration information

9.6 ip igmp snooping suppression Enable

Setting Report message suppression. The Command's no form Close Report message suppression.

ip igmp snooping suppression Enable

no ip igmp snooping suppression Enable

Default Configuration Disable this function.

Command mode global configuration mode

Usage Guide When Enabled Report message suppression function within a query interval only the first received specific vlan Group Report and forwards the packets to route the connection port, the subsequent Report packets will not continue to route the connection port forwarding this can reduce the number of network packets.

Configuration Example Enable Report message suppression:

```
Console(config)# ip igmp snooping suppression Enable
Console(config)#
```

Relative Command

Command	Description
show ip igmp snooping	show global IGMP Snooping configuration information

9.7 ip igmp snooping unknow-group-suppression

Settings for handling unknown multicast data can be discarded or broadcast. The Command's no form to restore the default values.

ip igmp unknow-group-suppression {drop | flood}

no ip igmp unknow-group-suppression

Parameter Description

Parameter	Description
drop	Discard unknown multicast data
flood	For unknown multicast data broadcast in vlan

Default Configuration By default broadcast

Command mode global configuration mode

Configuration Example

```
Console(config)# ip igmp snooping unknow-group-suppression drop
Console(config)#
```

Relative Command

Command	Description
show ip igmp snooping	show global IGMP Snooping configuration information

9.8 ip igmp snooping filter_mode Enable

Globally Enable multicast filtering. The Command's no closed form the corresponding function.

ip igmp snooping filter_mode Enable

no ip igmp snooping filter_mode Enable

Default Configuration

By default Close

Command mode

global configuration mode

Usage Guide

Before using IGMP Snooping Filter feature, use the Command Enable global.

Configuration Example

Here is an example of the configuration Enable global IGMP Snooping Filter is:

```
Console(config)# ip igmp snooping filter_mode Enable
Console(config)#
```

Relative Command

Command	Description
show ip igmp snooping	show global IGMP Snooping configuration information

9.9 ip igmp snooping filter auth

Configure multicast filter default mode. The Command's no form to restore the default mode

ip igmp filter auth [permit | deny]

no ip igmp filter auth

Parameter Description

Parameter	Description
permit	This is the default rule of igmp profile to allow
deny	This is the default rule of igmp profile is rejected

Default Configuration By default, to allow

Command mode global configuration mode

Usage Guide When the port is not configured corresponding filter profile, then the default behavior of the filter configured here.

Configuration Example Here is the default filter mode setting to deny:

```
Console(config)# ip igmp snooping filter auth deny
Console(config)#
```

Relative Command

Command	Description
show ip igmp snooping	show global IGMP Snooping configuration information

9.10 ip igmp profile

Create a profile, enter the profile mode.

ip igmp profile *profile-name* **[permit | deny]**

no ip igmp profile *profile-name*

Parameter Description

Parameter	Description
profile-name	Profile name
perimit	The profile indicates when all the group matches have failed to allow the implementation of the action, not configured, the default permission.
deny	The profile indicates execution refused action when all group failed to match

Default Configuration By default, it did not create any profile

Command mode global configuration mode

Usage Guide profile is a group for the "Filter", a reference for other functions. Configuration steps:
1. Use the ip igmp profileCommand create a profile, enter the profile mode.
2. Use groupsCommand define a set range and behavior.
3. Use applyCommand, application and exit.

Configuration Example Below is the profile 1, allows the group 224.2.2.2 ~ 224.2.2.244, and reject other groups:

```
Console(config)# ip igmp 1 deny
Console(igmp/profile/1)# groups permit range 224.2.2.2 224.2.2.244
```

```
Console(igmp/profile/1)# apply
Console(config)#
```

Relative Command

Command	Description
show ip igmp profile	Show profile configuration information

9.11 groups

igmp profile configured range of multicast groups and behavior. The Command's no form to remove Multicast Configuration

groups { permit | deny } { *ipv4-address* | **all** | **range** *low-ipaddr high-ipaddr*}

no groups {permit | deny } *low-ipaddr* [high-ipaddr]

no groups all

Parameter Description

Parameter	Description
ipv4-address	Multicast group address
all	All Multicast group
range	Range of multicast

Command mode

Igmp profile configuration mode

Configuration Example

Here is an example of the configuration groups permit:

```
Console(config)# ip igmp snooping profile 11
Console(igmp/profile/11)# groups permit 239.2.2.2
Console(igmp/profile/11)# apply
Console(config)#
```

Relative Command

Command	Description
show ip igmp profile	Show profile configuration information

9.12 ip igmp snooping vlan

Enabling IGMP Snooping on vlan. The Command's no closed form on IGMP Snooping vlan.

ip igmp snooping vlan *vid*

no ip igmp snooping vlan *vid*

Parameter Description

Parameter	Description
vid	VLAN ID, in the range 1-4094

Default Configuration

The default is disable.

Command mode

global configuration mode

Configuration Example

Here is to Enable igmp snooping on vlan1:

```
Console(config)# ip igmp snooping vlan 1
Console(config)#
```

Relative Command

Command	Description
show ip igmp snooping vlan	Show IGMP Snooping VLAN configuration information

9.13 ip igmp snooping vlan fast-leave Enable

Enabling fast leave. The Command's no form of closed fast leave.

ip igmp snooping vlan *vid* **fast-leave Enable**

no ip igmp snooping vlan *vid* **fast-leave Enable**

Parameter Description

Parameter	Description
vid	VLAN ID, in the range 1-4094

Default Configuration

The default is disable.

Command mode

global configuration mode

Usage Guide

Enabling fast leave port after, when the device is a port receives Leave messages directly issued from the mouth of a member of the forwarding entry to remove the port.
Thereafter, when the device receives the corresponding group-specific query, the device is no longer forwarded to the port.
The fast leave feature only applies to a device port connections only one host, you can save bandwidth and resources.

Configuration Example

Here is an example of vlan 1 Enable fast leave function:

```
Console(config)# ip igmp snooping vlan 1 fast-leave Enable
Console(config)#
```

Relative Command

Command	Description
show ip igmp snooping vlan	Show IGMP Snooping VLAN configuration information

9.14 ip igmp snooping vlan mrouter learn

Enable dynamic routing connector learning function. The Command's no closed form dynamic learning routes connecting port function.

ip igmp snooping vlan *vid* **mrouter learn**

no ip igmp snooping vlan *vid* **mrouter learn**

Parameter Description

Parameter	Description
vid	VLAN ID, in the range 1-4094

Default Configuration

The default is disable.

Command mode

global configuration mode

Usage Guide

Route connecting port is open on the port IGMP Snooping multicast device and Enable the multicast multicast routing protocol multicast devices directly connected neighbors. When you start learning dynamic routing connection port function, the device automatically listen for IGMP Query messages, dynamic routing to identify the connection port.

Configuration Example

Enable dynamic learning routes connecting port functions on vlan1:

```
Console(config)# ip igmp snooping vlan 1 mrouter learn
Console(config)#
```

Relative Command

Command	Description
show ip igmp snooping mrouter	Show IGMP Snooping router interface configuration information

9.15 ip igmp snooping vlan mrouter interface

Configuring static routes connecting port. The Command's no form to cancel the configuration.

ip igmp snooping vlan *vid* **mrouter interface GigabitEthernet** *interface-number*

no ip igmp snooping vlan *vid* **mrouter interface GigabitEthernet** *interface-number*

Parameter Description

Parameter	Description
vid	VLAN ID, in the range 1-4094
interface-number	Interface number

Default Configuration

Default - static routing connection port

Command mode

global configuration mode

Usage Guide

If a port is configured as a static route connecting port, then all multicast traffic received on the device it can be transmitted via this port.
Static routing connector does not age.

Configuration Example

Below is the static routing port 1 connector:

```
Console(config)# ip igmp snooping vlan 1 mrouter interface GigabitEthernet 1
Console(config)#
```

Relative Command

Command	Description
show ip igmp snooping mrouter	Show IGMP Snooping router interface configuration information

9.16 ip igmp snooping querier

Enable IGMP Snooping querier. The Command's no form close IGMP Snooping querier.

ip igmp snooping [**vlan** *vid*] **querier**

no ip igmp snooping [**vlan** *vid*] **querier**

Parameter Description

Parameter	Description
vlan *vid*	VLAN ID, in the range 1-4094

Default Configuration

This feature is disabled by default.

Command mode

global configuration mode

Usage Guide

When the global startup query function, then Enable query function on a VLAN,

VLAN feature to its inquiry on the force. If the global function on a closed query, the query function on all VLAN will be closed.

Configuration Example

Enabling Query function on a VLAN:

```
Console(config)# ip igmp snooping querier
Console(config)# ip igmp snooping vlan 2 querier
```

Relative Command

Command	Description
show ip igmp snooping	show global IGMP Snooping configuration information
show ip igmp snooping vlan	Show IGMP Snooping VLAN configuration information

9.17 ip igmp snooping vlan querier address

Configuring IGMP Snooping query the source IP address. The Command's no form to remove the configuration.

ip igmp snooping vlan *vid* **querier address** *a.b.c.d*

no ip igmp snooping vlan *vid* **querier address**

Parameter Description

Parameter	Description
vid	VLAN ID, in the range 1-4094
a.b.c.d	Source IP address

Command mode

global configuration mode

Configuration Example

IGMP Snooping querier on VLAN1 source IP address of 192.168.2.1:

```
Console(config)# ip igmp snooping vlan 1 querier address 192.168.2.1
Console(config)#
```

Relative Command

Command	Description
show ip igmp snooping vlan	Show IGMP Snooping VLAN configuration information

9.18 ip igmp snooping vlan querier max-response-time

Configuring IGMP Snooping querier maximum response time. The

Command's no form to restore the configuration to the default values.

ip igmp snooping vlan *vid* **querier max-response-time** *seconds*

no ip igmp snooping vlan *vid* **querier max-response-time**

Parameter Description

Parameter	Description
vid	VLAN ID, in the range 1-4094
seconds	The maximum response time. In seconds, in the range 1-25

Default Configuration

Default 10 seconds

Command mode

global configuration mode

Configuration Example

Configuring VLAN query maximum response time of 1 to 15 seconds:

```
Console(config)# ip igmp snooping vlan 1 querier max-response-time 15
Console(config)#
```

Relative Command

Command	Description
show ip igmp snooping vlan	Show IGMP Snooping VLAN configuration information

9.19 ip igmp snooping vlan querier query-interval

Configuring IGMP Snooping querier query interval. The Command's no form to restore the configuration to the default values.

ip igmp snooping vlan *vid* **querier query-interval** *seconds*

no ip igmp snooping vlan *vid* **querier query-interval**

Parameter Description

Parameter	Description
vid	VLAN ID, in the range 1-4094
seconds	Query interval. In seconds, in the range 1-18000

Default Configuration

Default 60 seconds

Command mode

global configuration mode

Configuration Example

Query interval configured VLAN 1 to 100 seconds:

```
Console(config)# ip igmp snooping vlan 1 querier query-interval 100
Console(config)#
```

Relative Command

Command	Description
show ip igmp snooping vlan	Show IGMP Snooping VLAN configuration information

9.20 ip igmp snooping vlan querier timer expiry

Configuring IGMP Snooping querier timeout. The Command's no form to restore the configuration to the default values.

ip igmp snooping vlan *vid* **querier timer expiry** *seconds*

no ip igmp snooping vlan *vid* **querier timer expiry**

Parameter Description

Parameter	Description
vid	VLAN ID, in the range 1-4094
seconds	overtime time. In seconds, in the range 60-300

Default Configuration

Default 125 seconds

Command mode

global configuration mode

Usage Guide

After the query function is Enabled, it may also be lost in the election. If the loser in "Query timeout period" does not receive query messages emitted by the current query is considered the current query its failure to launch the next round of elections.
When a plurality of query exists, the election interrogator mac address mainly small.

Configuration Example

Configure VLAN 1 querier timeout to 60 seconds:

```
Console(config)# ip igmp snooping vlan 1 querier timer expiry 60
Console(config)#
```

Relative Command

Command	Description
show ip igmp snooping vlan	Show IGMP Snooping VLAN configuration information

9.21 ip igmp snooping vlan querier version

Configuring IGMP Snooping Query running version. The Command's no form to restore the configuration to the default values.

ip igmp snooping vlan *vid* **querier version { 1 | 2 | 3}**

no ip igmp snooping vlan *vid* **querier version**

Parameter Description

Parameter	Description
vid	VLAN ID, in the range 1-4094
1 | 2 | 3	Running version IGMPv1 / IGMPv2 / IGMPv3

Default Configuration

Default running IGMPv2

Command mode

global configuration mode

Configuration Example

Setting VLAN 1 on the query run IGMP v1:

```
Console(config)# ip igmp snooping vlan 1 querier version 1
Console(config)#
```

Relative Command

Command	Description
show ip igmp snooping vlan	Show IGMP Snooping VLAN configuration information

9.22 ip igmp snooping max-groups

The maximum number of the interface can be dynamically added to the group. The Command's no form to restore the default configuration.

ip igmp snooping max-groups *number*

no ip igmp snooping max-groups

Parameter Description

Parameter	Description
number	Maximum group number, in the range 0-254
flood	For unknown multicast data broadcast in vlan

Default Configuration

The default is 42

Command mode interface configuration mode

Usage Guide If you configure this Command, it is in the interface, when the group dynamic learning group to exceed the maximum number of recording device will not learn IGMP Report messages to create a new forwarding entry.
The number of multicast groups that the interface statistics are based VLAN interface belongs statistics, such as the interface belongs to VLAN 3, on each VLAN receives a request to the multicast group 224.1.1.1, that while three VLAN on both receive the multicast group 224.1.1.1 demand request, the number of groups at this time of the statistics interface is three, not one.

Configuration Example A port can dynamically join 20 Group 1:

```
Console(config)# interface GigabitEthernet 1
Console(config-if-GigabitEthernet1)# ip igmp snooping max-groups 20
```

Relative Command

Command	Description
show ip igmp snooping interfaces	Show IGMP Snooping interfaces configuration information

9.23 ip igmp snooping filter

Configure a port can only receive a number of specific multicast data streams associated with the implementation of the Command particular profile in the interface mode. The Command's no form to remove the associated profile.

ip igmp snooping filter *profile-name*

no ip igmp snooping filter *profile-name*

Parameter Description

Parameter	Description
profile-name	Profile name

Command mode interface configuration mode

Usage Guide The IGMP Profile applied at a port if the port receives IGMP Report messages, the device will find out whether the port to be added in IGMP Profile multicast address this within the allowable range. If so, then allowed to join, only after further processing. You must create the specified profile, then you can perform the associated filter.

Configuration Example On port 1 is associated profile 1:

```
Console(config)# interface GigabitEthernet 1
Console(config-if-GigabitEthernet1)# ip igmp snooping filter 1
Console(config-if-GigabitEthernet1)#
```

Relative Command

Command	Description
show ip igmp snooping interfaces	Show IGMP Snooping interfaces configuration information

9.24 show ip igmp profile

Show profile configuration information

show ip igmp profile [*profile-name*]

Parameter Description

Parameter	Description
profile-name	profile name, the default configuration of all the show's profile

Command mode Enable mode

Usage Guide By this Command to view the configured profile information

Configuration Example View profile information configured:

```
Console(config)# show ip igmp profile
ip igmp profile 2 permit
  groups deny 239.255.255.254
ip igmp profile 1 deny
  groups permit range 224.2.2.2 225.2.2.254
Console(config)#
```

Relative Command

Command	Description
ip igmp profile	Create a profile, enter the profile mode
groups	igmp profile configured range of multicast groups and behavior

9.25 show ip igmp snooping

show global IGMP Snooping configuration information

show ip igmp snooping

Command mode Enable mode

Configuration Example Show Global IGMP Snooping Information:

```
Console(config)# show ip igmp snooping
IGMP Global snooping status   : Disable
Forwarding Mode               : MAC Group Address
Filter mode                   : disable
MLD Global querier            : disable
MLD Report suppress           : disable
Unknow Group suppression      : flood
Default Filter auth           : deny
Query max response time       : 10(Seconds)
Mrouter aging time            : 200(Seconds)
Host aging time               : 260(Seconds)
```

Relative Command

Command	Description
ip igmp snooping	Enable igmp snooping
ip igmp snooping forwarding-mode	Multicast forwarding mode
ip igmp snooping dyn-mr-aging-time	The aging time of dynamic router port
ip igmp snooping host-aging-time	Configuring IGMP dynamic member port aging time
ip igmp snooping query-max-response-time	Configure the maximum response time of Query messages
ip igmp snooping suppression Enable	Setting Report message suppression
ip igmp snooping unknow-group-suppression	Settings for handling unknown multicast data can be discarded or broadcast
ip igmp snooping filter_mode Enable	Globally Enable multicast filtering
ip igmp snooping filter auth	Configuring the default mode multicast filtering
ip igmp snooping querier	Enable IGMP Snooping querier feature

-

9.26 show ip igmp snooping vlan

Show IGMP Snooping VLAN configuration information.

show ip igmp snooping vlan *vid*

Parameter Description

Parameter	Description
vid	VLAN ID, in the range 1-4094

Command mode Enable mode

Configuration Example Show the configuration of the igmp snooping vlan 1 under:

```
Console(config)# show ip igmp snooping vlan 1
VLAN 1
------------------------------------

IGMP Snooping state: Enable
IGMP Fast-Leave: disable
Mrouter dyanmic learn: disable
IGMP VLAN querier: Disable
IGMP querier version: 2
IGMP querier source address: 192.168.2.1
IGMP querier interval: 60s
IGMP querier max response time: 10s
IGMP querier timer expiry: 125s
```

Relative Command

Command	Description
ip igmp snooping vlan	Enabling IGMP Snooping on vlan
ip igmp snooping vlan fast-leave Enable	Enabling fast leave
ip igmp snooping querier	Enable IGMP Snooping querier feature
ip igmp snooping vlan querier address	Configuring IGMP Snooping query the source IP address
ip igmp snooping vlan querier max-response-time	Configuring IGMP Snooping querier maximum response time
ip igmp snooping vlan querier query-interval	Configuring IGMP Snooping querier query-interval
ip igmp snooping vlan querier timer expiry	Configuring IGMP Snooping querier timer expiry
ip igmp snooping vlan querier version	Configuring IGMP Snooping querier version

ip igmp snooping vlan querier version	Configuring IGMP Snooping querier version

9.27 show ip igmp snooping mrouter

show IGMP Snooping is routed interface configuration information.

show ip igmp snooping mrouter [**vlan** *vid*]

Parameter Description

Parameter	Description
vlan *vid*	VLAN ID, in the range 1-4094

Command mode Enable mode

Configuration Example Show routed interface configuration information:

```
Console(config)# show ip igmp snooping mrouter
Vlan   Interface    State
----   ----------   -----
1      Gi0/2        static
1      Gi0/3        static
Switch(config)#
```

Relative Command

Command	Description
ip igmp snooping vlan mrouter learn	Enable dynamic routing connector learning function
ip igmp snooping vlan mrouter interface	Configuring static routes connecting port

9.28 show ip igmp snooping interfaces

Show IGMP Snooping interface configuration information.

show ip igmp snooping interfaces [**GigabitEthernet** *interface-num*]

Parameter Description

Parameter	Description
GigabitEthernet *interface-num*	show configuration information for the specified interface under default show represents all ports.

Command mode Enable mode

Configuration Example Show port configuration information 1:

```
Console(config)# show ip igmp snooping interface GigabitEthernet 1
Interface  Filter Profile Name  max-groups
---------- -------------------- ----------
```

```
Gi0/1      1                  10
Console(config)#
```

Relative Command

Command	Description
ip igmp snooping max-groups	The maximum number of the interface can be dynamically added to the group
ip igmp snooping filter	Configure the associated port profile

9.29 show ip igmp snooping groups

Show IGMP Snooping multicast group information learned.

show ip igmp snooping groups [**detail**]

Parameter Description

Parameter	Description
detail	Show Multicast group learning details

Command mode

Enable mode

Configuration Example

Show multicast group information learned:

```
Console(config)# show ip igmp snooping groups
VLAN  Group Address         Source Address        Included Ports   Excluded
Ports
---------------------------------------------------------------------------
1     224.0.2.0             11.0.0.1              Gi6              --
1     224.0.2.0             22.0.0.2              Gi6              --
1     224.0.2.0             33.0.0.3              Gi6              --
1     239.255.255.250       *                      Gi6              --

Console(config)#
Console(config)# show ip igmp snooping groups detail
8100:0001 224.0.2.0
       Gi0/6 (D) (04:02)
       8100:0001 192.168.0.2     00:00:04:00:00:00

8100:0001 239.255.255.250
       Gi0/6 (D) (03:40)
       8100:0001 fe80::39e2:df93:2f58:e677 00:30:ab:0a:c0:c6

Console(config)#
```

9.30 ipv6 mld snooping

Global Enable MLD snooping. The Command's no form to restore the off status

ipv6 mld snooping

no ipv6 mld snooping

Default Configuration By default,MLD snooping Close

Command mode global configuration mode

Usage Guide The Command is used to Enable MLD snooping

Configuration Example The following are open MLD snooping functions:

```
Console(config)# ipv6 mld snooping
Console(config)#
```

Relative Command

Command	Description
show ipv6 mld snooping	show global mld Snooping configuration information

9.31 ipv6 mld snooping forwarding-mode

Multicast forwarding mode. The Command's no form to restore the default values

Ipv6 mld snooping forwarding-mode {mac | ip}

no ipv6 mld snooping forwarding-mode

Parameter Description

Parameter	Description
mac	Based on the destination multicast forwarding based on mac
ip	Based on source ip and destination ip multicast forwarding based

Default Configuration The default is mac forwarding mode

Command mode global configuration mode

Usage Guide MLDv3 need ip forwarding mode used together in order to see the effect,

under the mac forwarding mode, will be backward compatible to mldv2 mldv3 effect.

Configuration Example

Below is the forwarding mode examples:

```
Console(config)# ipv6 mld snooping forwarding-mode ip
Console(config)#
```

Relative Command

Command	Description
show ipv6 mld snooping	show global mld Snooping configuration information

9.32 ipv6 mld snooping dyn-mr-aging-time

Set the aging time for dynamic routing port. The Command's no form to restore the aging time of dynamic router port configuration.

Ipv6 mld snooping dyn-mr-aging-time *seconds*

no ipv6 mld snooping dyn-mr-aging-time

Parameter Description

Parameter	Description
seconds	Aging time of dynamic router port, and in seconds, ranging from 1 to 3600

Default Configuration

300 second

Command mode

global configuration mode

Usage Guide

If a dynamic routing connection port in its aging timer does not receive mld general query messages, the device will route from the port connector removed from the list.
In connection port Enable dynamic learning routing function, you can adjust the aging time of dynamic router port through this Command. If the aging time is set too short may lead to route the connection port frequent additions and deletions.

Configuration Example

Below is the dynamic router port aging time is 100s:

```
Console(config)# ipv6 mld snooping dyn-mr-aging-time 100
Console (config)#
```

Relative Command

Command	Description
show ipv6 mld snooping	show global mld Snooping configuration information

9.33 ipv6 mld snooping host-aging-time

Configuring MLD dynamic member port aging time. The Command's no form to restore the dynamic member port aging time.

Ipv6 mld snooping host-aging-time *seconds*

no ipv6 mld snooping host-aging-time

Parameter Description

Parameter	Description
seconds	Aging time. In seconds, in the range 1-65535

Default Configuration

Default 260 seconds

Command mode

global configuration mode

Usage Guide

Dynamic member port aging time is when the device receives a port aging time to join an IPv6 multicast group when the host sends MLD join messages for the dynamic member port settings.
After receiving the MLD join message, it resets the aging timer for the dynamic member port, the timer for the host-aging-time. If the timer expires, it is considered non-existent hosts receive multicast packets at the port, it will multicast device removes the port from the MLD Snooping in members.

Configuration Example

Configuring dynamic port aging time MLD 30s:

```
Console(config)# ipv6 mld snooping host-aging-time 30
```

Relative Command

Command	Description
show ipv6 mld snooping	show global MLD Snooping configuration information

9.34 ipv6 mld snooping query-max-response-time

Configure the query maximum packet response time. The Command's no form to restore the configuration.

Ipv6 mld snooping query-max-response-time *seconds*

no ipv6 mld snooping query-max-response-time

Parameter Description

Parameter	Description
seconds	Query messages maximum response time, in seconds, in the range 1-65535.

Default Configuration	The default configuration of 10 seconds
Command mode	global configuration mode
Usage Guide	After receiving MLD general query packet, a multicast device reset all dynamic member port aging timer, the timer time query-max-response-time. If the timer expires, it is considered non-existent hosts receive multicast packets at the port, it will multicast device removes the port from the MLD Snooping member ports. After receiving MLD group-specific query message, a multicast device reset all the members of the particular group dynamic port aging timer, the timer time query-max-response-time. If the timer expires, it is considered non-existent hosts receive multicast packets at the port, the device will multicast the port is removed from the mouth of a member of MLD Snooping.

Configuration Example	Below is the message query maximum response time for 100s:
	`Console(config)# ipv6 mld snooping query-max-response-time 100`
	`Console(config)#`

Relative Command

Command	Description
show ipv6 mld snooping	show global MLD Snooping configuration information

9.35 ipv6 mld snooping suppression Enable

Setting Report message suppression. The Command's no form Close Report message suppression.

Ipv6 mld snooping suppression Enable

no ipv6 mld snooping suppression Enable

Default Configuration	Disable this function.
Command mode	global configuration mode
Usage Guide	When Enabled Report message suppression function within a query interval only the first received specific vlan Group Report and forwards the packets to route the connection port, the subsequent Report packets will not continue to route the connection port forwarding this can reduce the number of network packets.

Configuration Example	Enable Report message suppression:
	`Console(config)# ipv6 mld  snooping suppression Enable`
	`Console(config)#`

Relative Command

Command	Description
show ipv6 mld snooping	show global MLD Snooping configuration information

9.36 ipv6 mld snooping unknow-group-suppression

Settings for handling unknown multicast data can be discarded or broadcast. The Command's no form to restore the default values.

ipv6 mld unknow-group-suppression {drop | flood}

no ipv6 mld unknow-group-suppression

Parameter Description

Parameter	Description
drop	Discard unknown multicast data
flood	For unknown multicast data broadcast in vlan

Default Configuration

By default broadcast

Command mode

global configuration mode

Usage Guide

--

Configuration Example

```
Console(config)# ipv6 mld  snooping unknow-group-suppression drop
Console(config)#
```

Relative Command

Command	Description
show ipv6 mld snooping	show global MLD Snooping configuration information

9.37 ipv6 mld snooping filter_mode Enable

Globally Enable multicast filtering. The Command's no closed form the corresponding function.

Ipv6 mld snooping filter_mode Enable

no ipv6 mld snooping filter_mode Enable

Default Configuration

By default Close

Command mode	global configuration mode
Usage Guide	Before using MLD Snooping Filter feature, use the Command Enable global.

Configuration Example	Here is an example of the configuration Enable global MLD Snooping Filter is:
	`Console(config)# ipv6 mld snooping filter_mode Enable`
	`Console(config)#`

Relative Command

Command	Description
show ipv6 mld snooping	show global MLD Snooping configuration information

9.38 ipv6 mld snooping filter auth

Configure multicast filter default mode. The Command's no form to restore the default mode

Ipv6 mld filter auth [permit | deny]

no ipv6 mld filter auth

Parameter Description

Parameter	Description
permit	This is the default rule of mld profile to allow
deny	This is the default rule of mld profile is rejected

Default Configuration	By default, to allow
Command mode	global configuration mode
Usage Guide	When the port is not configured corresponding filter profile, then the default behavior of the filter configured here.

Configuration Example	Here is the default filter mode setting to deny:
	`Console(config)# ipv6 mld  snooping filter auth deny`
	`Console(config)#`

Relative Command

Command	Description
show ipv6 mld snooping	show global MLD Snooping configuration information

9.39 ipv6 mld profile

Create a profile, enter the profile mode.

Ipv6 mld profile *profile-name* **[permit | deny]**

no ipv6 mld profile *profile-name*

Parameter Description

Parameter	Description
profile-name	Profile name
perimit	The profile indicates when all the group matches have failed to allow the implementation of the action, not configured, the default permission.
deny	The profile indicates execution refused action when all group failed to match

Default Configuration

By default, it did not create any profile

Command mode

global configuration mode

Usage Guide

profile is a group for the "Filter", a reference for other functions. Configuration steps:
1. Use the ipv6 mld profileCommand create a profile, enter the profile mode.
2. Use groups Command define a set range and behavior.
3. Use apply Command, application and exit.

Configuration Example

Below is the profile 1, allows the group ff02::2～ff02::f, and reject other groups:

```
Console(config)# ipv6 mld profile 1 deny
Console(mld/profile/1)# groups permit range ff02::2 ff02::f
Console(mld/profile/1)# apply
Console(config)#
```

Relative Command

Command	Description
show ipv6 mld profile	Show profile configuration information

9.40 groups

MLD profile configured range of multicast groups and behavior. The Command's no form to remove Multicast Configuration

groups { permit | deny } { *ipv6-address* | **all** | **range** *low-ipaddr high-ipaddr*}

no groups {permit | deny } *low-ipaddr* [high-ipaddr]

no groups all

Parameter Description

Parameter	Description
Ipv6-address	Multicast group address
all	All Multicast group
range	Range of multicast

Command mode

MLD profile configuration mode

Configuration Example

Here is an example of the configuration groups permit:

```
Console(config)# ipv6 mld profile 11
Console(mld/profile/11)# groups permit ff02::3
Console(mld/profile/11)# apply
Console(config)#
```

Relative Command

Command	Description
show ipv6 mld profile	Show profile configuration information

9.41 ipv6 mld snooping vlan

Enabling MLD Snooping on vlan. The Command's no closed form on MLD Snooping vlan.

Ipv6 mld snooping vlan *vid*

no ipv6 mld snooping vlan *vid*

Parameter Description

Parameter	Description
vid	VLAN ID, in the range 1-4094

Default Configuration

The default is disable.

Command mode

global configuration mode

Configuration Example

Here is to Enable MLDsnooping on vlan1:

```
Console(config)# ipv6 mld snooping vlan 1
Console(config)#
```

Relative Command

Command	Description
show ipv6 mld snooping vlan	Show MLD Snooping VLAN configuration information

9.42 ipv6 mld snooping vlan fast-leave Enable

Enabling fast leave. The Command's no form of closed fast leave.

Ipv6 mld snooping vlan *vid* **fast-leave Enable**

no ipv6 mld snooping vlan *vid* **fast-leave Enable**

Parameter Description

Parameter	Description
vid	VLAN ID, in the range 1-4094

Default Configuration

The default is disable.

Command mode

global configuration mode

Usage Guide

Enabling fast leave port after, when the device is a port receives Leave messages directly issued from the mouth of a member of the forwarding entry to remove the port.
Thereafter, when the device receives the corresponding group-specific query, the device is no longer forwarded to the port.
The fast leave feature only applies to a device port connections only one host, you can save bandwidth and resources.

Configuration Example

Here is an example of vlan 1 Enable fast leave function:

```
Console(config)# ipv6 mld snooping vlan 1 fast-leave Enable
Console(config)#
```

Relative Command

Command	Description
show ipv6 mld snooping vlan	Show MLD Snooping VLAN configuration information

9.43 ipv6 mld snooping vlan mrouter learn

Enable dynamic routing connector learning function. The Command's no closed form dynamic learning routes connecting port function.

Ipv6 mld snooping vlan *vid* **mrouter learn**

no ipv6 mld snooping vlan *vid* **mrouter learn**

Parameter Description

Parameter	Description
vid	VLAN ID, in the range 1-4094

Default Configuration

The default is disable.

Command mode

global configuration mode

Usage Guide

Route connecting port is open on the port MLD Snooping multicast device and Enable the multicast multicast routing protocol multicast devices directly connected neighbors. When you start learning dynamic routing connection port function, the device automatically listen for MLD Query messages, dynamic routing to identify the connection port.

Configuration Example

Enable dynamic learning routes connecting port functions on vlan1:

```
Console(config)# ipv6 mld snooping vlan 1 mrouter learn
Console(config)#
```

Relative Command

Command	Description
show ipv6 mld snooping mrouter	Show MLD Snooping router interface configuration information

9.44 ipv6 mld snooping vlan mrouter interface

Configuring static routes connecting port. The Command's no form to cancel the configuration.

Ipv6 mld snooping vlan *vid* **mrouter interface GigabitEthernet** *interface-number*

no ipv6 mld snooping vlan *vid* **mrouter interface GigabitEthernet** *interface-number*

Parameter Description

Parameter	Description
vid	VLAN ID, in the range 1-4094
interface-number	Interface number

Default Configuration

Default - static routing connection port

Command mode

global configuration mode

Usage Guide

If a port is configured as a static route connecting port, then all multicast traffic received on the device it can be transmitted via this port.
Static routing connector does not age.

Configuration Example

Below is the static routing port 1 connector:

```
Console(config)# ipv6 mld snooping vlan 1 mrouter interface GigabitEthernet 1
Console(config)#
```

Relative Command

Command	Description
show ipv6 mldsnooping mrouter	Show MLD Snooping router interface configuration information

9.45 ipv6 mld snooping querier

Enable MLD Snooping querier. The Command's no form close MLD Snooping querier.

Ipv6 mld snooping [**vlan** *vid*] **querier**

no ip v6 mld snooping [**vlan** *vid*] **querier**

Parameter Description

Parameter	Description
vlan *vid*	VLAN ID, in the range 1-4094

Default Configuration

This feature is disabled by default.

Command mode

global configuration mode

Usage Guide

When the global startup query function, then Enable query function on a VLAN, VLAN feature to its inquiry on the force. If the global function on a closed query, the query function on all VLAN will be closed.

Configuration Example

Enabling Query function on a VLAN:

```
Console(config)# ipv6 mld snooping querier
Console(config)# ipv6 mld snooping vlan 2 querier
```

Relative Command

Command	Description
show ipv6 mld snooping	show global MLD Snooping configuration information
show ipv6 mld snooping vlan	Show MLD Snooping VLAN configuration information

9.46 ipv6 mld snooping vlan querier address

Configuring MLD Snooping query the source IPv6 address. The Command's no form to remove the configuration.

Ipv6 mld snooping vlan *vid* **querier address** *a.b.c.d*

no ipv6 mld snooping vlan *vid* **querier address**

Parameter Description

Parameter	Description
vid	VLAN ID, in the range 1-4094
x:x::x:x	Source IPv6 address

Command mode

global configuration mode

Configuration Example

MLD Snooping querier on VLAN1 source IPv6 address of 2001::2:

```
Console(config)# ipv6 mld snooping vlan 1 querier address 2001::2
Console(config)#
```

Relative Command

Command	Description
show ipv6 mld snooping vlan	Show MLD Snooping VLAN configuration information

9.47 ipv6 mld snooping vlan querier max-response-time

Configuring MLD Snooping querier maximum response time. The Command's no form to restore the configuration to the default values.

Ipv6 mld snooping vlan *vid* **querier max-response-time** *seconds*

no ipv6 mld snooping vlan *vid* **querier max-response-time**

Parameter Description

Parameter	Description
vid	VLAN ID, in the range 1-4094
seconds	The maximum response time. In seconds, in the range 1-25

Default Configuration

Default 10 seconds

Command mode

global configuration mode

Configuration Example

Configuring VLAN query maximum response time of 1 to 15 seconds:

```
Console(config)# ipv6 mld snooping vlan 1 querier max-response-time 15
Console(config)#
```

Relative Command

Command	Description
show ipv6 mld snooping vlan	Show MLD Snooping VLAN configuration information

9.48 ipv6 mld snooping vlan querier query-interval

Configuring MLD Snooping querier query interval. The Command's no form to restore the configuration to the default values.

Ipv6 mld snooping vlan *vid* querier query-interval *seconds*

no ipv6 mld snooping vlan *vid* querier query-interval

Parameter Description

Parameter	Description
vid	VLAN ID, in the range 1-4094
seconds	Query interval. In seconds, in the range 1-18000

Default Configuration

Default 60 seconds

Command mode

global configuration mode

Configuration Example

Query interval configured VLAN 1 to 100 seconds:

```
Console(config)# ipv6 mld snooping vlan 1 querier query-interval 100
Console(config)#
```

Relative Command

Command	Description
show ipv6 mld snooping vlan	Show MLD Snooping VLAN configuration information

9.49 ipv6 mld snooping vlan querier timer expiry

Configuring MLD Snooping querier timeout. The Command's no form to restore the configuration to the default values.

Ipv6 mld snooping vlan *vid* **querier timer expiry** *seconds*

no ipv6 mld snooping vlan *vid* **querier timer expiry**

Parameter Description

Parameter	Description
vid	VLAN ID, in the range 1-4094

seconds	overtime time. In seconds, in the range 60-300

Default Configuration

Default 125 seconds

Command mode

global configuration mode

Usage Guide

After the query function is Enabled, it may also be lost in the election. If the loser in "Query timeout period" does not receive query messages emitted by the current query is considered the current query its failure to launch the next round of elections.
When a plurality of query exists, the election interrogator mac address mainly small.

Configuration Example

Configure VLAN 1 querier timeout to 60 seconds:

```
Console(config)# ipv6 mld snooping vlan 1 querier timer expiry 60
Console(config)#
```

Relative Command

Command	Description
show ipv6 mld snooping vlan	Show MLD Snooping VLAN configuration information

9.50 ipv6 mld snooping vlan vid querier version

Configuring MLD Snooping Query running version. The Command's no form to restore the configuration to the default values.

Ipv6 mld snooping vlan *vid* **querier version { 1 | 2 | 3}**

no ipv6 mld snooping vlan *vid* **querier version**

Parameter Description

Parameter	Description
vid	VLAN ID, in the range 1-4094
1 | 2 | 3	Running version MLDv1 /MLDv2 / MLDv3

Default Configuration

Default running MLDv2

Command mode

global configuration mode

Configuration Example

Setting VLAN 1 on the query run MLDv1:

```
Console(config)# ipv6 mld snooping vlan 1 querier version 1
Console(config)#
```

Relative Command

Command	Description
show ipv6 mld snooping vlan	Show MLD Snooping VLAN configuration information

9.51 ipv6 mld snooping max-groups

The maximum number of the interface can be dynamically added to the group. The Command's no form to restore the default configuration.

Ipv6 mld snooping max-groups *number*

no ipv6 mld snooping max-groups

Parameter Description

Parameter	Description
number	Maximum group number, in the range 0-254
flood	For unknown multicast data broadcast in vlan

Default Configuration

The default is 42

Command mode

interface configuration mode

Usage Guide

If you configure this command, on the interface, when the group dynamic learning group to exceed the maximum number of recording device will not learn MLD Report messages create a new forwarding entry.
The number of multicast groups on the interface statistics are based VLAN interface belongs to the statistics.

Configuration Example

A port can dynamically join 20 Group 1:

```
Console(config)# interface GigabitEthernet 1
Console(config-if-GigabitEthernet1)# ipv6 mld snooping max-groups 20
```

Relative Command

Command	Description
show ipv6 mld snooping interfaces	Show MLD Snooping interfaces configuration information

9.52 ipv6 mld snooping filter

Configure a port can only receive a number of specific multicast data streams associated with the implementation of the Command particular profile in the interface mode. The Command's no form to remove the associated profile.

Ipv6 mld snooping filter *profile-name*

no ipv6 mld snooping filter *profile-name*

Parameter Description

Parameter	Description
profile-name	Profile name

Command mode interface configuration mode

Usage Guide The MLD Profile applied at a port if the port receives MLD Report messages, the device will find out whether the port to be added in MLD Profile multicast address this within the allowable range. If so, then allowed to join, only after further processing. You must create the specified profile, then you can perform the associated filter.

Configuration Example On port 1 is associated profile 1:

```
Console(config)# interface GigabitEthernet 1
Console(config-if-GigabitEthernet1)# ipv6 mld snooping filter 1
Console(config-if-GigabitEthernet1)#
```

Relative Command

Command	Description
show ipv6 mld snooping interfaces	Show MLD Snooping interfaces configuration information

9.53 show ipv6 mld profile

Show ipv6 mld profile configuration information

show ipv6 mld profile [*profile-name*]

Parameter Description

Parameter	Description
profile-name	profile name, the default configuration of all the show's profile

Command mode Enable mode

Usage Guide By this Command to view the configured profile information

Configuration Example View profile information configured:

```
Console(config)# show ipv6 mld profile
ipv6 mld profile 2 permit
  groups deny ff02::3
ipv6 mld profile 1 deny
  groups permit range ff02::1 ff02::f
Console(config)#
```

Relative Command

Command	Description
Ipv6 mld profile	Create a profile, enter the profile mode
groups	MLD profile configured range of multicast groups and behavior

9.54 show ipv6 mld snooping

show global MLD Snooping configuration information

show ipv6 mld snooping

Command mode Enable mode

Configuration Example Show Global MLD Snooping Information:

```
Console(config)# show ipv6 mld snooping
MLD Global snooping status   : Disable
Forwarding Mode              : MAC Group Address
Filter mode                  : disable
MLD Global querier           : disable
MLD Report suppress          : disable
Unknow Group suppression     : flood
Default Filter auth          : deny
Query max response time      : 10(Seconds)
Mrouter aging time           : 200(Seconds)
Host aging time              : 260(Seconds)
```

Relative Command

Command	Description
Ipv6 mld snooping	Enable MLD snooping
Ipv6 mld snooping forwarding-mode	Multicast forwarding mode
Ipv6 mld snooping dyn-mr-aging-time	The aging time of dynamic router port
Ipv6 mld snooping host-aging-time	Configuring MLD dynamic member port aging time
Ipv6 mld snooping query-max-response-time	Configure the maximum response time of Query messages
Ipv6 mld snooping suppression Enable	Setting Report message suppression
Ipv6 mld snooping unknow-group-suppression	Settings for handling unknown multicast data can be discarded or broadcast

Ipv6 mld snooping filter_mode Enable	Globally Enable multicast filtering
Ipv6 mld snooping filter auth	Configuring the default mode multicast filtering
Ipv6 mld snooping querier	Enable MLD Snooping querier feature

9.55 show ipv6 mld snooping vlan

Show MLD Snooping VLAN configuration information.

show ipv6 mld snooping vlan *vid*

Parameter Description

Parameter	Description
vid	VLAN ID, in the range 1-4094

Command mode Enable mode

Configuration Example Check the configuration of the MLD snooping vlan 1 under:

```
Console(config)# show ipv6 mld snooping
MLD Global snooping status    : Enable
Forwarding Mode               : Source Specific IP Group Address
Filter mode                   : Enable
MLD Global querier            : Enable
MLD Report suppress           : Enable
Unknow Group suppression      : drop
Default Filter auth           : permit
Query max response time       : 30(Seconds)
Mrouter aging time(Seconds)   : 300
Host aging time(Seconds)      : 200

Console(config)#
```

Relative Command

Command	Description
ipv6 mld snooping vlan	Enabling MLD Snooping on vlan
ipv6 mld snooping vlan	Enabling fast leave
ipv6 mld snooping vlan	Enable MLD Snooping querier feature
ipv6 mld snooping vlan	Configuring MLD Snooping query the source IP address
ipv6 mld snooping vlan	Configuring MLD Snooping querier maximum response time

ipv6 mld snooping vlan	Configuring MLD Snooping querier query-interval
ipv6 mld snooping vlan	Configuring MLD Snooping querier timer expiry
ipv6 mld snooping vlan	Configuring MLD Snooping querier version

9.56 show ipv6 mld snooping mrouter

show MLD Snooping is routed interface configuration information.

show ipv6 mld snooping mrouter [**vlan** *vid*]

Parameter Description

Parameter	Description
vlan *vid*	VLAN ID, in the range 1-4094

Command mode Enable mode

Configuration Example View is routed interface configuration information:

```
Console(config)# show ipv6 mld snooping mrouter
Vlan   Interface    State
----   ----------   -----
1      Gi0/2        static
1      Gi0/3        static
Console(config)#
```

Relative Command

Command	Description
Ipv6 mldsnooping vlan mrouter learn	Enable dynamic routing connector learning function
Ipv6 mld snooping vlan mrouter interface	Configuring static routes connecting port

9.57 show ipv6 mld snooping interfaces

Show MLD Snooping interface configuration information.

show ipv6 mld snooping interfaces [**GigabitEthernet** *interface-num*]

Parameter Description

Parameter	Description
GigabitEthernet *interface-num*	show configuration information for the specified interface under default show represents all ports.

Command mode Enable mode

Configuration Example

Check port configuration information 1:

```
Console(config)# show ipv6 mld snooping interface GigabitEthernet 1
Interface  Filter Profile Name  max-groups
---------- -------------------- ----------
Gi0/1      1                    10
Console(config)#
```

Relative Command

Command	Description
Ipv6 mld snooping max-groups	The maximum number of the interface can be dynamically added to the group
Ipv6 mld snooping filter	Configure the associated port profile

9.58 show ipv6 mld snooping groups

Show MLD Snooping multicast group information learned.

show ipv6 mld snooping groups [**detail**]

Parameter Description

Parameter	Description
detail	Show Multicast group learning details

Command mode

Enable mode

Configuration Example

View multicast group information learned:

```
Console(config)# show ipv6 mld snooping groups
VLAN  Group Address          Source Address          Included Ports   Excluded Ports
-------------------------------------------------------------------------------
1     ff02::1:3              *                       Gi6              --
1     ff02::c                *                       Gi6              --
1     ff02::1:ff58:e677      *                       Gi6              --

Console(config)#
Console(config)# show ipv6 mld snooping groups detail
8100:0001 ff02::1:3
       Gi0/6 (D) (03:07)
       8100:0001 fe80::39e2:df93:2f58:e677 00:30:ab:0a:c0:c6

8100:0001 ff02::c
       Gi0/6 (D) (03:04)
       8100:0001 fe80::39e2:df93:2f58:e677 00:30:ab:0a:c0:c6

8100:0001 ff02::1:ff58:e677
       Gi0/6 (D) (03:04)
       8100:0001 fe80::39e2:df93:2f58:e677 00:30:ab:0a:c0:c6

Console(config)#
```

10 QoS

10.1 mls qos map cos-queue

Configure the mapping between the cos and queue queues. The no form of the command is restored to the default state

mls qos map cos-queue <*queue0…queue7*>

no mls qos map cos-queue

Parameter Description

Parameter	description
<*queue0…queue7*>	CoS 0 to 7 The queues are mapped in the range of 0 to 7

Default Configuration

Cos0 is mapped to queue0, cos1 is mapped to queue1, ..., cosN is mapped to queueN

Command mode

global configuration mode

Usage Guide

Use this command to configure the mapping between cos and queue

Configuration Example

The following is an example of configuring a mapping relationship:

```
Console(config)#  mls qos map cos-queue 7 6 5 4 3 2 1
Console(config)#
```

Relative Command

command	description
show mls qos maps	Show the mapping information of DSCP-CoS and CoS-Queue

10.2 mls qos map dscp-cos

Configure DSCP-to-CoS mapping. The no form of the command is restored to the default state

mls qos map dscp-cos <*dscp-list*> **to** <*cos*>

no mls qos map dscp-cos

Parameter Description

Parameter	description
dscp-list	DSCP list to be mapped to CoS, in the range 0 to 63
cos	DSCP CoS value to be mapped, in the range 0 to 7

Default Configuration By default, DSCP 0 to 7 are mapped to CoS0, DSCPs 8 to 15 to CoS 1, DSCP 16 to 23 to CoS 2, DSCP 24 to 31 to CoS 3, DSCP 32 to 39 to CoS 4, DSCP 40 to 47 to CoS 5, DSCPs 48 to 55 to CoS 6, and DSCPs 56 to 63 to CoS 7.

Command mode global configuration mode

Usage Guide This command is used to configure the mappings between dscp and cos, and to map to which queue the cos to queue mapping is combined.

Configuration Example Here is an example of configuring dscp 5 to cos 2:

```
Console(config)# mls qos map dscp-cos 5 to 2
Console(config)#
```

Relative Command

command	description
show mls qos maps	Show the mapping information of DSCP-CoS and CoS-Queue

10.3 mls qos queue algorithm

Configure the scheduling policy for the output queue. The no form of the command is restored to the default value.

mls qos queue algorithm { sp | rr | wrr | wfq }

no mls qos queue algorithm

Parameter Description

Parameter	description
sp	The scheduling policy of the output queue is strict priority scheduling
rr	The output scheduling policy is configured as polling scheduling
wrr	The scheduling policy for output queues is weighted polling
wfq	Set the scheduling policy of the output queue to WFQ

Default Configuration By default, the scheduling policy is WFQ.

Command mode global configuration mode

Usage Guide Use this command to set the scheduling mode between queues.

Configuration Example The following output queue scheduling policy is strict priority scheduling:

```
Console(config)# mls qos queue algorithm sp
Console(config)#
```

Relative Command

command	description
show mls qos queueing	Show queueing policy and polling weight ratio information

10.4 mls qos queue wrr weight

Configure WRR queue scheduling weight, and restore the command to no default.

mls qos queue wrr weight <*weight0..weight7*>

no mls qos queue wrr weight

Parameter Description

Parameter	description
<*weight0..weight7*>	The weight value corresponding to queues 0 through 7, in the range of 0 to 127

Default Configuration

The weight of the default queue 0 ~ 7 is 1 2 3 4 5 6 7

Command mode

global configuration mode

Usage Guide

If the queue weight is set to 0, the queue is scheduled according to the SP algorithm. In this case, the WRR algorithm evolves to the SWRR algorithm. When the queue is scheduled, the system will give priority to ensuring that the SP queue is scheduled. When no packets are sent in the SP queue, the WRR queue is scheduled. The SP queue performs the strict priority scheduling mode, and the WRR queue performs the weighted polling scheduling mode.

Configuration Example

Set the polling weight of the WRR queue scheduling policy to 1: 2: 3: 4: 4: 3: 2: 1:

```
Console(config)# mls qos queue wrr weight 1 2 3 4 4 3 2 1
Console(config)#
```

Relative Command

command	description
show mls qos queueing	Show queueing policy and polling weight ratio information

10.5 mls qos queue wfq weight

Configure the WFQ queue scheduling weight, and the no form of this command is restored to the default value.

mls qos queue wfq weight *<weight0..weight7>*

no mls qos queue wfq weight

Parameter Description

Parameter	description
<weight0..weight7>	The weight value of the eight output queues, in the range of 0 to 127

Default Configuration

The weight of the default queue 0 ~ 7 is 1 2 3 4 5 6 7

Command mode

global configuration mode

Configuration Example

Set the polling weight of the WFQ output queue queueing policy to 1: 1: 2: 2: 4: 6: 8

```
Console(config)# mls qos queue wfq weight 1 1 1 2 2 4 6 8
Console(config)#
```

Relative Command

command	description
show mls qos queueing	Show queueing policy and polling weight ratio information

10.6 mls qos cos

Configure the default CoS value for the interface.the no form of this command is restored to the default value.

mls qos cos *<default-cos>*

no mls qos cos

Parameter Description

Parameter	description
default-os	The default CoS value is 0 in the interface, in the range of 0 to 7.

Default Configuration

By default, all ports are mapped to cos 0

Command mode

Interface configuration mode

Configuration Example

Configure the default CoS value of port 1 to 7:

```
Console(config)# interface GigabitEthernet 1
Console(config-if-GigabitEthernet1)# mls qos cos 7
Console(config-if-GigabitEthernet1)#
```

Relative Command

command	description
show mls qos interface	Show interface QoS information

10.7 mls qos trust

Configure the trust mode of the interface.the no form of this command is restored to the default value.

mls qos trust {cos | dscp | cos-dscp}

no mls qos trust

Parameter Description

Parameter	description
cos	Trust CoS
dscp	Trust DSCP

Default Configuration

The default trust mode is not.

Command mode

Interface configuration mode

Configuration Example

Configure the trust mode of port 1 as CoS:

```
Console(config)# interface GigabitEthernet 1
Console(config-if-GigabitEthernet1)# mls qos trust cos
Console(config-if-GigabitEthernet1)#
```

Relative Command

command	description
show mls qos interface	Show QoS information in the interface

10.8 class-map

Create a class and enter the class configuration mode. The no form of the command deletes the existing class.

class-map <*class-map-name*>

no class-map <*class-map-name*>

Parameter Description

Parameter	description
class-map-name	The name of the class to create, the name of the class can not exceed 31 characters.

Default Configuration

By default, no classes are created

Command mode

global configuration mode

Configuration Example

1.create MAC ACL 700：

```
Console(config)# access-list 700 permit host 00:00:00:11:22:33 any etype-any
Console(config)#
```

2.create class c1,match ACL 700：

```
Console(config)# class-map c1
Console(config-cmap)# match access-group 700
Console(config-cmap)# exit
```

3.create c2,match DSCP 8～15：

```
Console(config)# class-map c2
Console(config-cmap)# match ip dscp 8 mask 0x7
Console(config-cmap)# exit
```

Relative Command

command	description
show class-map	Show class-map information

10.9 match

In the class configuration mode, the rule matches the rule. The no form of the command deletes the class matching rule.

match { access-group <*access_id*> **| ip { dscp** <*dscp-value*> [**mask** <dscp-mask>] **| precedence** <pre-value> [**mask** <pre-mask>] **} }**

no match { access-group | ip {dscp | precedence} }

Parameter Description

Parameter	description
access_id	Match ACL rule
dscp-value	Match DSCP rule,It can match a single DSCP or DSCP + mask, in the range 0 to 63
dscp-mask	Matches DSCPMask, in the range of 0x0 to 0x3F
pre-val	Match IP PRE rule, which can match a single IP PRE or IP PRE + Mask, in the range of 0 to 7
pre-mask	Match the IP PRE Mask

Default Configuration

By default, the class does not match any rules

Command mode

Class configuration mode

Configuration Example

1.create class c1,match DSCP 8～15：

```
Console(config)# class-map c1
Console(config-cmap)# match ip dscp 8 mask 0x7
```

Relative Command

command	description
show class-map	Show class information

10.10 policy-map

Create a policy and enter the policy configuration mode. The no form of the command deletes the existing policy.

policy-map <*policy-map-name*>

no policy-map <*policy-map-name*>

Parameter Description

Parameter	description
policy-map-name	The name of the policy to create, the name of the class can not exceed 31 characters.

Default Configuration

By default, no policy is created

Command mode

global configuration mode

Configuration Example

1.Create the policy p1 and enter the policy configuration mode. Associate the class c1 with the policy class configuration mode.

```
Console(config)# policy-map p1
Console(config-pmap)# class c1
```

2. Configure the traffic behavior as 10 Mbps for the limited data flow and 256 K for the triggering traffic, and discard the packets exceeding the limit:

```
Console(config-pmap-c)# police 10240 256 exceed-action drop
```

Relative Command

command	description
Show policy-map	Show policy-map information

10.11 class

Associates the class with the policy configuration mode. The no form of this command deletes the class associated with the policy.

class <*class-map-name*>

no class <*class-map-name*>

Parameter Description

Parameter	description
class-map-name	the class associate with name.

Default

By default, no class is associated with a policy

Configuration

Command mode Policy configuration mode

Configuration Example 1.create class c1, match DCSP5：

```
Console(config)# class-map c1
Console(config-cmap)# match ip dscp 5
Console(config-cmap)# exit
```

2. Create p1,asscicated witch c1：

```
Console(config)# policy-map p1
Console(config-pmap)# class c1
Console(config-pmap-c)# end
```

Relative Command

command	description
Show policy-map	Show policy-map information

10.12 police

In the policy class configuration mode, bind the bandwidth limit of the flow. The no form of the command deletes the bound traffic behavior.

police *<rate-bps>* *<burst-byte>* **[exceed-action drop]**

no police

Parameter Description

Parameter	description
rate-bps	Bandwidth limit per second (KBits), in kbps, in the range of 1-10000000
burst-byte	Burst flow limit value (Kbytes), in the range of 1-1000000

Default Configuration By default, no traffic behavior is specified for a class associated with a policy

Command mode Policy class configuration mode

Configuration Example 1.Create policy p1, enter policy configuration mode, associate class c1, and enter policy class configuration mode.

```
Console(config)# policy-map p1
Console(config-pmap)# class c1
```

2.Configure the traffic behavior to limit the bandwidth of the data flow to 100 Mbps, burst traffic to 4096 K, and the excess traffic to drop:

```
Console(config-pmap-c)# police 102400 4096 exceed-action drop
```

Relative Command

command	description
Show policy-map	Show policy-map information

10.13 set

In the policy class configuration mode, binding changes the CoS and DSCP behavior of the flow, and the no form of the command deletes the bound traffic behavior.

set { ip dsco <*new-dscp*> **| cos** <*new-cos*> **}**

no set { ip dscp | cos }

Parameter Description

Parameter	description
new-dscp	The DSCP value of the modified stream is new-dscp, ranging from 0 to 63.
new-cos	The modified CoS value is new-cos, and the value ranges from 0 to 7.

Default Configuration

The DSCP value of the modified flow is new-dscp, in the range of 0 to 63

Command mode

Policy class configuration mode

Configuration Example

1.Create policy p1, enter policy configuration mode, associate class c1, and enter policy class configuration mode.

```
Console(config)# policy-map p1
Console(config-pmap)# class c1
```

2.Configure the traffic behavior to modify the CoS value of packets to

```
Console(config-pmap-c)# set cos 3
```

Relative Command

command	description
Show policy-map	Show policy-map information

10.14 service-policy

Apply the policy to the interface. The no form of the command will contact the policy applied to the interface.

service-policy input <*policy-map-name*>

no service-policy input { <*policy-map-name*> **}**

Parameter Description

Parameter	description
policy-map-name	The name of the policy to apply

Default Configuration

By default, no policy is applied on an interface

Command mode

Interface configuration mode

Configuration Example

1.Enter interface configuration mode and apply the policy p1 to the input direction:

```
Console(config)# interface GigabitEthernet 3
Console(config-if-GigabitEthernet3)# service-policy input p1
```

Relative Command

command	description
show mls qos interface	show mls qos interface information

10.15 show mls qos maps

Show DSCP-CoS、CoS-Queue maps information

show mls qos maps [dscp-cos | cos-queue]

Parameter Description

Parameter	description
dscp-cos	DSCP-CoS map information
cos-queue	CoS-Queue map information

Default Configuration

no

Command mode

Global configuration mode

Configuration Example

Show all qos map information：

```
Console(config)# show mls qos maps
  cos map to queue :
       cos id| 0 1 2 3 4 5 6 7
        -----|---------------
```

```
        queue| 0 1 2 3 4 5 6 7

  dscp map to cos :
          cos 0: 0  1  2  3  4  5  6  7
          cos 1: 8  9  10 11 12 13 14 15
          cos 2: 16 17 18 19 20 21 22 23
          cos 3: 24 25 26 27 28 29 30 31
          cos 4: 32 33 34 35 36 37 38 39
          cos 5: 40 41 42 43 44 45 46 47
          cos 6: 48 49 50 51 52 53 54 55
          cos 7: 56 57 58 59 60 61 62 63

Console(config)#
```

10.16 show mls qos queueing

Show queueing policy and polling weight ratio information

show mls qos queueing

Parameter Description

Parameter	description

Default Configuration

no

Command mode

Global configuration mode

Configuration Example

Show queueing policy and polling weight ratio information：

```
Console(config)# show mls qos queueing
  queue algorithm : RR

  wrr queue  weight:
     queue id|  0  1  2  3  4  5  6  7
        -----|------------------------
       weight|  1  2  3  4  5  6  7  8

  wfq queue  weight:
     queue id|  0  1  2  3  4  5  6  7
        -----|------------------------
       weight|  1  2  3  4  5  6  7  8
Console(config)
```

10.17 show mls qos interface

Show QoS information in the interface

show mls qos interface [GigabitEthernet <*port-num*> **]**

Parameter Description

Parameter	description
port-num	Show port-num

Default Configuration

no

Command mode Global configuration mode

Configuration Example Show port 3 information：

```
Console(config)# show mls qos interface GigabitEthernet 3
interface GigabitEthernet 3
Default cos: 0
Default trust: cos-dscp
Attached input policy-map:

Console(config)#
```

10.18 show class-map

Show class information

show class-map [<*class-map-name*> **]**

Parameter Description

Parameter	description
class-map-name	Show class-map name

Default Configuration no

Command mode Global configuration mode

Configuration Example Show all class information：

```
Console(config)# show class-map
Class Map c1
  Match access-group 700

Class Map c2
  Match ip dscp 5

Console(config)#
```

10.19 show policy-map

Show policy-map information

show policy-map [<*policy-map-name*> **]**

Parameter Description

Parameter	description
policy-map-name	Show policy name

Default Configuration no

Command mode Global configuration mode

Configuration Example

Show all the policy-map p1 information：

```
Console(config)# show policy-map p1
Policy Map p1
  Class c1
    police 10240 256 exceed-action drop

  Class c2
       set ip dscp 6

Console(config)#
```

11 MAC address

11.1 clear mac-address-table dynamic

clear mac-address-table

clear mac-address-table dynamic[address mac-addr] [interface interface-id] [vlan vlan-id]

Parameter Description

Parameter	Description
dynamic	Clears all dynamic address.
address mac-addr	Clear the dynamic address.
interface interface-id	Clear all the dynamic address specified interface.
vlan vlan-id	Clears all dynamic VLAN address.

Command mode

Enable mode .

Usage Guide

-You can use the show mac-address-table dynamic Command to view the entire contents of the dynamic address table.

Configuration Example

Delete all dynamic address

```
Console# clear mac-address-table dynamic
```

Relative Command

Command	Description
show mac-address-table dynamic	show the dynamic address table.

11.2 mac-address-learning

The ability to open a port address learning. Use the Command's no option to shut down the port address learning.

mac-address-learning

no mac-address-learning

Default Configuration

Address learning Enable

Command mode

Interface configuration mode and interface range configuration mode.

Usage Guide

Can not disable MAC address learning on the security features of open port, close port address learning ability can not configure security features;

Configuration Example

Example 1: Close the interface address learning ability:

```
Console(config-if-GigabitEthernet2)# no mac-address-learning
```

Relative Command

Command	Description
show running-config	Check the non-default configuration information

11.3 mac-address dynamic-limit

Designated port dynamic learning limit. 0: Disable Default Learning 8191.

mac-address dynamic-limit[0-8191] [default]

Parameter Description

Parameter	Description
<0-8191>	Max learn number,see 0 will disable learning
default	Default learning number

Default Configuration

default of 8191

Command mode

Interface configuration mode and interface range configuration mode.

Usage Guide

MAC address learning limit, the default is the maximum capacity;

Configuration Example

Example 1: The interface address learning limit is 8:

```
Console(config-if-GigabitEthernet2)# mac-address dynamic-limit 8
```

Relative Command

Command	Description
show running-config	Check the non-default configuration information

11.4 mac-address-table aging-time

Set up a dynamic address aging time. Use the Command's no option to return the setting to the default.

mac-address-table aging-time seconds

no mac-address-table aging-time

Parameter Description

Parameter	Description
seconds	Dynamic address aging time, in seconds. Worth range

	determined by the device.

Default Configuration

The default value is 300 seconds.

Command mode

global configuration mode

Usage Guide

use show mac-address-table aging-time Command view configuration.

use show mac-address-table dynamic Command view Dynamic Address table.

Configuration Example

```
Console# mac-address-table aging-time 150
```

Relative Command

Command	Description
show mac-address-table aging-time	show dynamic address aging time.
show mac-address-table dynamic	show the dynamic address table.

11.5 mac-address-table filtering

Set filters address. Use the Command's no option to remove the filter ad dress.

mac-address-table filtering mac-address vlan vlan-id [source | destination]

clear mac-address-table filtering mac-address vlan vlan-id

Parameter Description

Parameter	Description
mac-address	Filter address
vlan vlan-id	VLAN ID, a range determined by the device.
source	Only filter based on the source MAC address. That is, only to filter received from the VLAN set to the source MAC address is the MAC address set in the data frame.
destination	Only filter based on the purpose of MAC. That is only received from the filter settings to the destination VLAN. MAC address is the MAC address set in the data frame.

Default Configuration

Default not set any address filtering.

If the configuration is not specified source or destination, when it receives from the set VLAN data source MAC address or destination MAC address of the set MAC address will be filtered.

Command mode Global Mode

Usage Guide Filtering address can not be a multicast address. Use show mac-address-table filtering Command View address filtering settings.

Configuration Example

```
Console(config)# mac-address-table filtering 00:d0:f8:00:07:3c vlan 1
```

Relative Command

Command	Description
show mac-address-table filtering	show address filtering information table.

11.6 mac-address-table static

Set a static address. Use the Command's no option to delete a static address.

mac-address-table static mac-addr vlan vlan-id interface interface-id

clear mac-address-table static {**address** mac-addr | **interface** [*interface-id*] | **vlan** [*vlan-id*]}

Parameter Description

Parameter	Description
mac-addr	Specifies the entry corresponding to the destination MAC address.
vlan-id	Specified entry corresponding VLAN.
interface-id	Package will be forwarded to the interface (can be a physical port or AggregatePort).

Default Configuration Default not set any static address.

Command mode Global Mode

Usage Guide The following example shows how to configure a static address 00d0.f800.073c, when the VLAN 4 in the received packet destination address is the address of the packet is forwarded to the specified interface GigabitEthernet 1.

Configuration Example

```
Console(config)# mac-address-table static 00:d0:f8:00:07:3c vlan 4
interface GigabitEthernet 1
```

Relative Command

Command	Description
show mac-address-table static	show static address.

11.7 mac-address-table multicast

Set a static address. Use the Command's no option to delete a static address.

mac-address-table multicast mac-addr vlan vlan-id interface interface-id

clear mac-address-table multicast {**address** mac-addr | **interface** [*interface-id*] | **vlan** [*vlan-id*]}

Parameter Description

Parameter	Description
mac-addr	Specifies the entry corresponding to the destination MAC address.
vlan-id	Specified entry corresponding VLAN.
interface-id	Package will be forwarded to the interface (can be a physical port or AggregatePort).

Default Configuration

Default not set any multicast address.

Command mode

Global Mode

Usage Guide

The following example shows how to configure a multicast address 01:00:5e:02:03:04, when the VLAN 4 in the received packet destination address is the address of the packet is forwarded to the specified interface GigabitEthernet 1.

Configuration Example

Console(config)# mac-address-table multicast 01:00:5e:02:03:04 vlan 4 interface GigabitEthernet 1

Relative Command

Command	Description
show mac-address-table multicast	show multicast address.

11.8 clear mac-address-table static

Clear static addresses Interface

clear mac-address-table static {**address** mac-addr | **interface** [*interface-id*] | **vlan** *vlan-id*]}

Parameter Description

Parameter	Description
static	Clear all static address.
address mac-addr	Clear known static address.

interface interface-id	Clear all static address specified interface.
vlan vlan-id	Clear all static address specified VLAN.

Command mode Interface configuration mode and interface range configuration mode.

Usage Guide You can use the show mac-address-table static Command to view the entire contents of the dynamic address table.

Configuration Example

```
Console(config)# interface aggregateport 1
Console(config-if-AggregatePort 1)#clear mac-address-table static
```

Relative Command

Command	Description
show mac-address-table static	show static address list information.

11.9 show mac-address-learning

Show the port address learning ability.

show mac-address-learning

Command mode Enable mode

Configuration Example Example 1: show port address learning capability: switch(config)# show mac-address-learning

11.10 show mac-address-table aging-time

Show dynamic address aging time.

show mac-address-table aging-time

Command mode Enable mode

Configuration Example

```
Console# show mac-address-table aging-time
Aging time : 300
```

Relative Command

Command	Description
mac-address-table aging-time	Set up a dynamic address aging time.

11.11 show mac-address-table count

Statistics show the number of addresses in the address table entries.

show mac-address-table count [interface interface-id | vlan vlan-id]

Parameter Description

Parameter	Description
interface *interface-id*	Interface number.
vlan *vlan-id*	VLAN number

Command mode

Enable mode

Usage Guide

show mac-address-table count Command, according to the type of MAC address entries statistics entry number;
show mac-address-table count interface Command, according to the number of the interface statistics entry corresponding to the MAC address table entries;
show mac-address-table count vlan Command, the number of statistics entries based on the MAC address table entry belongs VLAN.

Configuration Example

Console# show mac-address-table count1

Dynamic Address Count : 51

Static Address Count : 0

Filter Address Count : 0

Total Mac Addresses : 51

Total Mac Address Space Available: 8139

Relative Command

Command	Description
show mac-address-table static	show static address.
show mac-address-table filtering	Show filtering address
show mac-address-table dynamic	Show dynamic address

11.12 show mac-address-table dynamic

Statistics show the number of addresses in the address table entries.

show mac-address-table dynamic [address mac-addr] [interface interface-id] [vlan vlan-id]

Parameter Description

Parameter	Description
mac-addr	Specifies the entry corresponding to the destination MAC address.
vlan-id	Specified entry corresponding VLAN.
interface-id	Package will be forwarded to the interface (can be a physical port or AggregatePort).

Default Configuration

Default show all available data.

Command mode

Enable mode

Configuration Example

```
Console# show mac-address-table dynamic
Vlan MAC Address Type Interface
---- ------------ ------ ------------------
1 00:00:00:00:00:01 DYNAMIC GigabitEthernet 1
1 00:01:96:0c:a7:40 DYNAMIC GigabitEthernet 1
1 00:07:95:c7:df:f9 DYNAMIC GigabitEthernet 1
1 00:07:95:cf:ee:e0 DYNAMIC GigabitEthernet 1
1 00:07:95:cf:f4:1f DYNAMIC GigabitEthernet 1
1 00:09:b7:15:d4:00 DYNAMIC GigabitEthernet 1
1 00:50:ba:de:63:c4 DYNAMIC GigabitEthernet 1
```

11.13 show mac-address-table filtering

Show filter address table.

show mac-address-table filtering [addr mac-addr] [vlan vlan-id]

Parameter Description

Parameter	Description
mac-addr	Specifies the entry corresponding to the destination MAC address.
vlan-id	Specified entry corresponding VLAN.

Command mode Enable mode

Configuration Example

```
Console# show mac-address-table filtering

Vlan MAC Address Type Interface

------ ------------------- -------- -----------

1 00:d0:f8:00:10:02 FILTER Not available
```

Relative Command

Command	Description
mac-address-table filtering	Set filters address.

11.14 show mac-address-table interface

show the specified address information for all types of interfaces (including dynamic addresses, static address).

show mac-address-table interface [interface-id] [vlan vlan-id]

Parameter Description

Parameter	Description
interface-id	Specified interface (can be a physical port or AggregatePort).
vlan-id	Specify the corresponding VLAN entry

Command mode Enable mode

Configuration Example

```
Console# show mac-address-table interface GigabitEthernet 1

Vlan MAC Address Type Interface

------ --------------- ----- -----------

1 00:d0:f8:00:10:01 STATIC GigabitEthernet 1

1 00:d0:f8:00:10:02 STATIC GigabitEthernet 1

1 00:d0:f8:00:10:03 STATIC GigabitEthernet 1

1 00:d0:f8:00:10:04 STATIC GigabitEthernet 1
```

Relative Command

Command	Description
show mac-address-table static	show static address.
show mac-address-table filtering	show filtering address
show mac-address-table dynamic	show dynamic address

11.15 show mac-address-table static

show static address.

show mac-address-table static [addr mac-addr] [interface interface-id] [vlan vlan-id]

Parameter Description

Parameter	Description
mac-addr	Specifies the entry corresponding to the destination MAC address.
vlan-id	Specify the corresponding VLAN entry
interface-id	Package will be forwarded to the interface (can be a physical port or AggregatePort)

Command mode

Enable mode

Configuration Example

```
Console# show mac-address-table static

Vlan MAC Address Type Interface

----- ----------- -------- ------------------

1 00:d0:f8:00:10:01 STATIC GigabitEthernet 1

1 00:d0:f8:00:10:02 STATIC GigabitEthernet 1

1 00:d0:f8:00:10:03 STATIC GigabitEthernet 1
```

Relative Command

Command	Description
mac-address-table static	Set a static address.

12 SNMP & RMON

12.1 Enable service snmp-agent

Opening devices SNMP agent function. The Command's no shield in the form of SNMP agent function.

Enable service snmp-agent

no Enable service snmp-agent

Default Configuration By default, the SNMP agent function.

Command mode global configuration mode

Usage Guide The Command globally Enabled device SNMP agent function.

Configuration Example

```
Here is on the SNMP agent function examples:
Console(config)# Enable service snmp-agent
Console(config)#
```

Relative Command

Command	Description
show snmp	Show SNMP configuration information

12.2 snmp-server community

Specify access SNMP community character. The Command's no access character will cancel the specified SNMP community.

snmp-server community *string* **{ ro | rw}**

no snmp-server community *string*

Parameter Description

Parameter	Description
string	Community string, equivalent to communication password between NMS and SNMP Agent
ro	Specifies the NMS (SNMP host) for MIB variables can only be read, can not be modified
rw	NMS of MIB variables readable and writable

Command mode global configuration mode

Usage Guide When the Command to add a community name and specify the attributes of the group, using SNMPv1, SNMPv2 connection with the device, you must use the group name.

Configuration Example Here is to add a group called the public can write:

```
Console(config)# snmp-server community public rw
Console(config)#
```

Relative Command

Command	Description
show snmp community	show group information

12.3 snmp-server view

Add an SNMP view name. The Command's no form to delete the name.

snmp-server view *view-name*

no snmp-server view view-name

Parameter Description

Parameter	Description
view-name	View name

Command mode global configuration mode

Usage Guide The Command just add a view, specifically the rule uses snmp-server view-rule configuration.

Configuration Example The Command just add a view, specifically the rule uses snmp-server view-rule configuration:

```
Console(config)# snmp-server view v1
Console(config)#
```

Relative Command

Command	Description
show snmp view	Show SNMP view configuration information
snmp-server view-rule	Setting view rules

12.4 snmp-server view-rule

Setting view rules to allow or disable access to certain MIB objects. The Command's no form to delete the corresponding rule.

snmp-server view-rule *view-name* **{ included | excluded } oid** *oid-tree* **[mask** *oid-mask***]**

no snmp-server view-rule *view-name* **{ included | excluded } oid** *oid-tree*

Parameter Description

Parameter	Description
view-name	View name
include	The MIB objects indicate the number of children to be included in the view of
exclude	The MIB objects indicate the number of children being excluded from view
oid-tree	MIB objects associated views, is a number of sub-MIB
oid-mask	MIB OID mask

Command mode

global configuration mode

Usage Guide

The Command which can be controlled to allow or prohibit access to MIB objects.

Configuration Example

Below is the view v1 rules to include all MIB-2 Sub Number:

```
Console(config)# snmp-server view-rule v1 included oid 1.3.6.1
Console(config)#
```

Relative Command

Command	Description
show snmp view	Show SNMP view configuration information
snmp-server view	Add view name

12.5 snmp-server group

Set the SNMP user group. The Command's no form to remove a user group.

snmp-server group *groupname* **security-level {auth | noauth | priv} read-view** view-name **write-view** *view-name* **notify-view** *view-name*

no snmp-server group *groupname*

Parameter Description

Parameter	Description
groupname	User group name
auth	Message-user transmission needs to be verified but the group does not need data confidentiality
noauth	Message does not require user authentication data transmission of the group nor the need for confidentiality
priv	The group of users simultaneously transmit messages need to verify the need for confidentiality of data transmission
view-name	View name associated

Command mode

global configuration mode

Usage Guide

Adding a user group, set the encryption method and associated views.

Configuration Example

Here is an example of adding a user group:

```
Console(config)# snmp-server group g1 security-level auth read-view v1 write-view v1 notify-view v1
Console(config)#
```

Relative Command

Command	Description
show snmp group	Show SNMP User Group Configuration
snmp-server view	Add view name
snmp-server view-rule	Setting view rules

12.6 snmp-server user

Set the SNMP user. The Command's no form to remove a user.

snmp-server user *username* **{ auth {md5 | sha}** *auth-password* **priv {aes | des}** *priv-password* **| authnopriv {md5 | sha}** *auth-password* **| noauthnopriv } group** *groupname*

no snmp-server user *username*

Parameter Description

Parameter	Description
username	*username*
auth	And the need to verify the data is encrypted
authnopriv	But the need to verify the data is not encrypted
noauthnopriv	No authentication and the data is not encrypted
md5	Specifies MD5 authentication protocol
sha	Specifies SHA authentication protocol
auth-password	Password authentication
aes	Specify the use of AES encryption protocol
des	Specify the use of DES encryption protocol
priv-password	Encryption Password
groupname	*groupname*

Command mode

global configuration mode

Usage Guide

Add a user authentication and encryption methods used by the user and group configuration belongs, the user will be used for SNMPv3 connection.

Configuration Example

Here is add a SNMPv3 user, use MD5 authentication, encryption does not use the examples:

```
Console(config)# snmp-server user u1 authnopriv md5 1234567890 group g1
Console(config)#
```

Relative Command

Command	Description
show snmp user	Show SNMP user configuration information
snmp-server group	Set the SNMP user group

12.7 snmp-server host

Specifies to send SNMP trap messages from the host (NMS). The Command's no form to cancel the specified SNMP host.

snmp-server host {*host-addr* | *ipv6-addr*} **traps version {v1 | v2c | v3** *username***}**

no snmp-server host {*host-addr* | *ipv6-addr*} **traps version {v1 | v2c |v3** *username***}**

Parameter Description

Parameter	Description
host-addr	SNMP host ipv4 address
ipv6-addr	SNMP host ipv6 address
v1 | v2c | v3	SNMP version
username	SNMPV3 username

Command mode

global configuration mode

Usage Guide

You can configure a number of different SNMP host to receive trap messages. Time has triggered the trap message: Linkup / LinkDown, the cold-start device port (power down restart) / warm-start (warm restart), set the ports as well as RMON statistics upper and lower threshold.

Configuration Example

Here is to add a SNMP host, receives trap messages examples:

```
Console(config)# snmp-server host 192.168.2.10 traps version v2c
Console(config)#
```

Relative Command

Command	Description
show snmp host	Show SNMP host conmfiguration
snmp-server user	Set SNMP user
rmon event	Define RMON event

12.8 show snmp

Show SNMP configuration information

show snmp [community | view | group | user | host]

Parameter Description

Parameter	Description
community	Show community information
view	Show view information
group	Show group information
user	Show user information
host	show host information

Command mode

Enable mode

Usage Guide

Use this Command to show SNMP configuration information

Configuration Example

Here is an example show SNMP configuration:

```
Console# show snmp
SNMP: Enable
Switch# show snmp view
View Name: v1

Console# show snmp group
groupname: g1
securityLevel: authNoPriv
readview: v1
writeview: v1
notifyview: v1

Console# show snmp user
User name: u1
Security level: authNoPriv
Auth protocol: MD5
Priv protocol:
Group-name: g1

Console# show snmp host
Notification host: 192.168.2.10
udp-port: 162
type: trap
user:
security model: v2c

Console#
```

Relative Command

Command	Description
Enable service snmp-agent	Opening devices SNMP agent function
snmp-server community	Specifies the SNMP community access character
snmp-server view	Add view name
snmp-server view-rule	Setting view rules
snmp-server group	Set the SNMP user group
snmp-server user	Set the SNMP user
snmp-server host	Specifies to send trap messages SNMP host

12.9 rmon statistics

Set up monitoring an Ethernet interface statistics. The Command's no form to cancel monitoring

rmon statistics *index interface* **owner** *ownername*

no rmon statistics *index*

Parameter Description

Parameter	Description
index	Statistics entry index, which ranges from 1 to 65535
interface	To monitor source port
ownername	Setting entry creator, ownername of 1 to 30 characters

Command mode global configuration mode

Usage Guide The statistics set Command listening port

Configuration Example Here is an example of setting monitor Ethernet port 4:

```
Console(config)# rmon statistics 1 4 owner xmh
add statistics entry successfully.
Console(config)#
```

Relative Command

Command	Description
show rmon statistics	Show Statistics information

12.10 rmon event

Define an event, the Command's no form to delete the event.

rmon event *number* **description {trap | log | trap&log | none} owner** *ownername*

no rmon event *number*

Parameter Description

Parameter	Description
number	Event entry index, which ranges from 1 to 65535
trap	Trap event, when the event is triggered, the system will send a Trap message
log	Log event when the event is triggered, the system will log
trap&log	When an event is triggered, both logging and trap sending
none	When an event occurs, not action
ownername	Setting entry creator, ownername of 1 to 30 characters

Command mode

global configuration mode

Usage Guide

When the Command defined event trigger recording events.

Configuration Example

Here is an example of the configuration of events:

```
Console(config)# rmon event 1 description BroadcastPkts_too_much trap owner xmh
add event entry successfully.
Console(config)#
```

Relative Command

Command	Description
show rmon event	show event information table

12.11 rmon alarm

Add a monitor alarms. The Command's no form to cancel monitoring.

rmon alarm *number statistics-item statistics-index interval* **{absolute | delta} rising-threshold** *value event-number* **falling-threshold** *value event-number* **owner** *ownername*

no ip dhcp snooping trust

Parameter Description

Parameter	Description
number	No alarm entry index, which ranges from 1 to 65535
statistics-item	Statistics Type Value:3:DropEvents; 4:Octets; 5:Pkts; 6:BroadcastPkts; 7:MulticastPkts; 8:CRCAlignErrors; 9:UndersizePkts; 10:OversizePkts; 11:Fragments; 12:Jabbers; 13:Collisions; 14:Pkts64Octets; 15:Pkts65to127Octets; 16:Pkts128to255Octets; 17:Pkts256to511Octets; 18:Pkts512to1023Octets; 19:Pkts1024to1518Octets
statistic-index	Statistics Statistics set corresponding index number to determine statistical listening port number
interval	Sampling interval, in the range of 5 to 65,535 seconds
absolute	Sampling sampling type to absolute, that is extracted directly sampling time is reached when the variable value
delta	Sampling type to change the value of the sampling, the sampling time is reached when the extracted value is variable change in the sampling interval
rising-threshold *value*	Parameter set the upper limit value
falling-threshold *value*	Parameter sets the lower limit value
event-number	Upper / lower limit is reached, each corresponding event number
ownername	Setting entry creator, ownername of 1 to 30 characters

Command mode global configuration mode

Usage Guide The Joint Command rmon statistics nuclear rmon event Command finalize port statistics monitor alarm setting.

Configuration Here is an example of setting the alarm:

Example

```
Console(config)# rmon alarm 1 6 1 30 delta rising-threshold 300 1 falling-
threshold 10 1 owner xmh
add alarm entry successfully.
Console(config)#
```

Relative Command

Command	Description
show rmon alarm	show alarm entry
rmon statistics	Setting an Ethernet interface statistics monitoring
rmon event	Define an event

12.12 rmon history

Record history information for a Ethernet interface. The Command's no form of off the record.

rmon history *index interface buckets-number interval* **owner** *ownername*

no rmon history *index*

Parameter Description

Parameter	Description
index	History control entry index, which ranges from 1 to 65535
interface	Ethernet interface number to be recorded
buckets-number	Setting history entry control history table size, the number of recorded history table can accommodate up to, in the range of 1 to 65535
interval	Set statistics, in the range of 5 to 3600 seconds
ownername	Setting entry creator, ownername of 1 to 30 characters

Command mode

global configuration mode

Usage Guide

By this Command, you can cycle to the historical statistical data ports, and set the number of historical data retention.

Configuration Example

Here is the history information to monitor Ethernet port 4 examples:

```
Console(config)# rmon history 1 4 10 20 owner xmh
add history entry successfully.
Console(config)#
```

Relative Command

Command	Description
show rmon history	show history information table

12.13 show rmon statistics

Show Statistics information.

show rmon statistics

Command mode

global configuration mode

Configuration Example

The following tables show examples of information are:

```
Console(config)# show rmon statistics
|Index  |Port  |Owner                          |Status
-------------------------------------------------------
1       4      xmh                            Active
-------------------------------------------------------
The total number: 1
Console(config)#
```

Relative Command

Command	Description
rmon statistics	Setting an Ethernet interface statistics monitoring

12.14 show rmon event

show event table configuration information.

show rmon event

Command mode

global configuration mode

Configuration Example

Here is an example of a show event information table:

```
Console(config)# show rmon event
|Index  |Description                |Event Type     |Event Last Trigger Time        |Owner
|Status
-------------------------------------------------------------------------------------------------------------------------
--
1       BroadcastPkts_too_much        snmptrap        2000-01-01 01:57:39             xmh
Active
-------------------------------------------------------------------------------------------------------------------------
--
The total number: 1
Console(config)#
```

Relative Command

Command	Description
rmon event	Define an event

12.15 show rmon alarm

show alarm entry

show rmon alarm

Command mode global configuration mode

Configuration Example Here is an example of the table show the alarm message:

```
Console(config)# show rmon alarm
|Index  |Interval(Sec) |StaticItem |PortIndex |SampType |CurSampValue
|RisThresh |FalThresh |RisEventIndex |FalEventIndex |Owner     |Status
------------------------------------------------------------------------------------------------------------
--------------------
1      30     (6)BroadcastPkts        1      delta     0           300        10        1      1
xmh                 Active
------------------------------------------------------------------------------------------------------------
--------------------
The total number: 1
Console(config)#
```

Relative Command

Command	Description
Rmon alarm	Adding a Monitoring Alarms

12.16 show rmon history

Show historical information table

show rmon history

Command mode global configuration mode

Configuration Example Here is the history tables show examples of information:

```
Console(config)# show rmon history
|Index  |Port |Buckets Requested   |Buckets Granted     |Interval(Sec)  |Owner
|Status
------------------------------------------------------------------------------------------------------------
------
1      4     10                10                20            xmh                         Active
------------------------------------------------------------------------------------------------------------
------
The total number:
```

Relative Command

Command	Description
rmon history	Recording a history Ethernet interface

13 system status

13.1 ping

Ping specific IP address

ping -t **-ifname** *iface* **-count** *cnt* **-size** *len* **-waittime** *waittime* **-ttl** *ttl* **-pattern** *pattern* **-saddr** *saddr* **-v** *daddr*

Parameter Description

Parameter	Description
iface	Ping Interface name
cnt	The number of Ping packets
len	The length of the Ping packet
waittime	Ping timeout waiting for a response
ttl	Survival time Ping packets
pattern	Ping packet data content
saddr	Source ip address Ping packet
daddr	Ping data packet's destination ip address

Command mode Enable configuration mode

Configuration Example Here is an example of ping:

```
Console#
Console# ping -t -count 5 -size 1024 -waittime 10 192.168.1.111
Console#
```

13.2 traceroute

Discovery packet transmission path experienced by

traceroute -saddr [<*hostname*> | *ipaddr*]

Parameter Description

Parameter	Description
ipaddr	Traceroute dst Ipaddr

Command mode Enable configuration mode

Configuration Example

Here is an example of the password reset:

```
Console#
Console# traceroute 192.168.1.111
Console#
```

13.3 tftp

Get and send files via FTP

tftp [**put** | **get**] [**-a** | **-o**] <*localfilename*> *ipaddr* <*servfilename*>

Parameter Description

Parameter	Description
localfilename	Tftp file to be transferred
ipaddr	Remote host ip tftp needs to be transmitted
servfilename	File tftp needs to receive

Command mode

Enable configuration mode

Usage Guide

Need to use ftp software assisted.

Configuration Example

Here is the ftp to get files example:

```
Console#
Console# tftp get -a 192.168.1.21 switch.conf
Console#
```

13.4 copy running-config startup-config

Save the current configuration

copy running-config startup-config

Parameter Description

Parameter	Description
running-config	Currently running configuration
startup-config	After rebooting saved configuration

Command mode

Enable configuration mode

Configuration Example

Here is to save the configuration examples:

```
Console#
Console# copy running-config startup-config
Console#
```

Relative Command

Command	Description
write	Save Configuration Command
show running-config	show the current configuration

13.5 Copy filename tftp: serveraddress

Export current configuration file, the configuration file must exist in / var / config (usually switch.conf)

Parameter Description

Filename: Profile serveraddress / var / config under: save the host ip export file

Command mode

Enable mode， global mode

Configuration Example

Here is an example of preservation:

```
Console#copy switch.conf tftp: 192.168.2.33
/var/config/switch.conf----------Begin to check file!~
file checksum=[1649282097] [0x624e0c31]

Please wait....
@@@@@ tftpc upload bind socket to interface 'eth0.1' successfully after 1 times.
Transfering image to remote host file named switch.conf...
Send data to remote.

Put image to remote success!
Console#
```

Relative Command

Command	Description
Copy filename tftp: serveraddress	Get files via TFTP

13.6 Copy tftp: server-address configfile

Switch configuration

Parameter Description

Parameter	Description
Serverfile	Import file in the File Name
serveraddress	Host import file saved

Command mode Enable mode and global mode

Configuration Example

```
Console#copy tftp: 192.168.2.33 switch123.conf switch.conf

Please wait....
@@@@@ tftpc download bind socket to interface 'eth0.1' successfully after 1 times.
Request remote file named switch123.conf ...
Receive data...

Done.
Get file from remote success!
Console#
```

Relative Command

Command	Description
Copy tftp:serveraddress serverfile	Inform configuration

13.7 system config backup

Export current configuration

system config backup *ipaddr remotefile*

Parameter Description

Parameter	Description
ipaddr	Save export profile host ip
remotefile	Export configuration file name

Command mode Enable configuration mode

Configuration Example Here is an example of the backup configuration file:

```
Console#
Console# system config backup 192.168.1.11 switch.txt
Console#
```

13.8 system config upgrade

Upgrade your current configuration

system config upgrade *ipaddr* { *remotefile* }

Parameter Description

Parameter	Description
ipaddr	Save the upgrade file host ip
remotefile	Upgrade file filename

Command mode Enable configuration mode

Usage Guide While upgrading a configuration, use the auxiliary software tftp, tftp and set the path for the upgrade path to the configuration file is located.

Configuration Example The following is an upgrade profile examples:

```
Console#
Console# system config upgrade 192.168.1.11 switch.txt
Console#
```

13.9 system upgrade

When you need to upgrade the system, use the system upgradeCommand carried out in the Enable mode.

system upgrade *ipaddr servfilename*

Parameter Description

Parameter	Description
ipaddr	Save the upgrade file host ip
servfilename	Upgrade file filename

Command mode Enable configuration mode

Usage Guide While upgrading a configuration, use the auxiliary software tftp, tftp and set the path for the upgrade path to the configuration file is located.

Configuration Example Here is an example of a software upgrade:

```
Console(config)#
Console(config)# system upgrade 192.168.1.11 switch.bin
Console(config)#
```

13.10 telnet-radius-auth

Authentication telnet set authentication method

telnet-auth-auth [local | **radius** | **radius-loca/**]

Parameter Description

Parameter	Description
local	Local authentication
radius	Using radius authentication
radius-local	First use radius authentication and then local authentication

Command mode global configuration mode

Configuration Example Here is an example of the telnet authentication methods:

```
Console#
Console# config
Console(config)# telnet-auth-auth local
Console(config)#
```

Relative Command

Command	Description
Console(config)# show telnet-radius-auth	Show telnet authentication configuration

13.11 telnet tel_port

Set telnet port authentication

telnet tel_port <0-65535>

no telnet tel_port <0-65535>

Command mode global configuration mode

Configuration Example The following is an example set telnet port 23:

```
Console#
Console# config
Console(config)# telnet tel_port 23
```

13.12 ssh-radius-auth

Set ssh authentication authentication method

ssh-auth-auth [**local** | **radius** | **radius-local**]

Parameter Description

Parameter	Description
local	Local authentication
radius	Using radius authentication
radius-local	First use radius authentication and then local authentication

Command mode global configuration mode

Configuration Example Here is an example to set up ssh authentication methods:

```
Console(config)#
Console(config)# ssh-radius-auth local
Console(config)#
```

14 Basic Configuration Management

14.1 Enable

To Enable the user to enter the mode, perform the normal user configuration CommandEnable.

enalbe

Command mode User mode

Usage Guide --

Configuration Example --

Relative Command

Command	Description

Platform Description --

14.2 Enable password

Use password to enter the configuration under Enable mode, the Command's no form to not use the default password.

Enable password

no Enable password

Parameter Description

Parameter	Description

Default Configuration --

Command mode global configuration mode

Usage Guide --

Configuration Example The following sample configuration to use when entering the Enable mode password:

```
Console(config)# Enable password 12345
Console(config)#
```

14.3 clock set

To manually configure the system time, you can Enable users Commandcock setCommand set.

clock set *hh:mm:ss month day year*

Parameter Description

Parameter	Description
hh:mm:ss	The current time in the format hours (24-hour): minutes: seconds
month	(1-12), months of the year
day	(1-31), the date of the year
year	Year (1990-9999), can not use abbreviations

Default Configuration

--

Command mode

Enable mode

Usage Guide

Use this Command to set the system time, easy management.

Configuration Example

Here is the current time for October 9, 2013 in the afternoon 16:25:30 examples:

```
Console# clock set 16:25:30 10 9 2013
Wed Oct  9 16:25:30 UTC 2013
Console#
```

14.4 Enable service

To open and close the specified service (SSH Server / Telnet Server / Snmp Agent), in global configuration mode, you can use CommandEnable service. The Command's no closed form specified services.

Enable service [**ssh-server** | **telnet-server** | **snmp-agent**]

no Enable service [**ssh-server** | **telnet-server** | **snmp-agent**]

Parameter Description

Parameter	Description
ssh-server	Enable and disable ssh-server
telnet-server	Enable and disable telnet-server
snmp-agent	Enable and disable snmp-agent

Default Configuration

--

Command

global configuration mode

mode

Usage Guide The Command for opening or closing the specified service, use no Enable service shut down the specified service.

Configuration Example Enable telnet-server function of example：

```
Console# config
Console(config)# Enable service telnet-server
Console(config)#
```

Relative Command

Command	Description
show telnet	Show current telnet-server status information
show ssh	Show current ssh-server status information

14.5 hostname

To modify the host name of the device, perform global configuration Commandhostname.

hostname *name*

Parameter Description

Parameter	Description
name	host name of the device, the maximum length of 20 characters.

Default Configuration The default host name is Switch.

Command mode global configuration mode

Usage Guide --

Configuration Example Here is the modified example of the device's host named TW:

```
Console# config
Console(config)# hostname TW
set hostname: TW success !
TW(config)#
```

Relative Command

Command	Description

Platform Description --

14.6 username

To set up a local user name, use the global configuration mode Command username.

username *name*{**nopassword**|**password**{*password* | [**0**|**7**]*encrypted-password* }}

username *name* **privilege** *privilege-level*

no username *name*

Parameter Description

Parameter	Description
name	username
password	User password
0|*7*	Password encryption type, encryption 0-- 7 simple encryption
privilege	Bind user privilege level

Command mode

global configuration mode

Usage Guide

The Command is used to create a local user database for authentication use.
If you specify the type of encryption 7, legitimate ciphertext you enter must be an even number.
Usually - Must specify an encryption type 7. Under normal circumstances, only when the copy and paste has been encrypted passwords, only need to specify the type of encryption is 7.

Configuration Example

The following example configures a user name and password, and bind user level is 15:
Console(config)#username test privilege 15 password 0 pw15

Relative Command

Command	Description
show system users	Show username

14.7 password

Set admin user and the user's password

password [**admin** | **user**] *pwdcode*

Parameter Description

Parameter	Description
pwdcode	The new password set

Default Configuration The default password is admin

Command mode Enable mode

Usage Guide --

Configuration Example Here is an example of the password reset:

```
Console#
Console# password admin
New Password:
Confirm Password:
Change password success!
Console#
```

14.8 reload

Reboot or restart the device to factory configuration

reload

Default Configuration --

Command mode Enable mode

Usage Guide --

Configuration Example Here is an example of the device to restart and restore the factory configuration:

```
Console#
Console# delete switch.conf
Console# reload
Console#
```

Relative Command

Command	Description
delete	Delete file

14.9 write

The system configuration (running-config) to save.

write

Command mode Enable mode

Configuration Example

```
Console#
Console# write
Console# reload
Console#
```

Relative Command

Command	Description
copy	Copy the files on the device

14.10 line-detect

Administrators can be detected by the cable detection Command operating condition of the cable. When the cable is short circuit or other abnormal status, line
Cable tests can help determine the correct working conditions cables.

line-detect { **detail** }

Parameter Description

Parameter	Description
detail	Details show the cable line length

Command mode interface configuration mode

Usage Guide

Note 1. Only electrical cable detection physical eloquence support media, optical media physical port, AP port does not support cable detection.
2. In the implementation of the interface cable detection of normal connection, the connection is temporarily cut off, and then re-establish the connection.

Configuration Example

The following is a diagnostic cable is short circuit or other abnormal length, status of Open or Short length corresponding to the length of the cable is a port on the point of failure.

```
Console(config-if-GigabitEthernet3)#line-detect
The following is a detailed diagnosis of the cable show, based on the length of each cable to transfer time signals to be calculated
Console(config-if-GigabitEthernet3)#line-detect detail
```

14.11 uptime

Update the system time

uptime

Command mode Global configuration mode

Configuration Example

Update the system time

```
Console(config)# uptime
```

Relative Command

Command	Description
show clock	Show current time

14.12 interface vlan

Create, delete management vlan

Interface vlan <1-4094>

No interface vlan <1-4094>

Default Configuration

The default mode is bound vlanid 1

Command mode

global configuration mode

Usage Guide

Add the management vlan, you must first create vlan id, then create vlan vlan id and set binding management IP and subnet mask vlanid bound to take effect by the ipaddress;
Remove vlan, need to remove the management vlan id bound by no ipaddress , then ipaddress delete vlan id.

Configuration Example

The following example, add the management VLAN ID 2, and check the configuration.

```
Console(config)# vlan 2
Console(config-vlan)# exit
Console(config)# interface vlan 2
Console(config-if-vlan3)# show ipaddress vlan list
 ID   common info: [vlanid]       [ipmode]       [dhcp-reqip]    [pri]          [scope]
  1              2              static         0.0.0.0         7              4
        net info: [ip addr]       [netmask]       [gateway]       [major dns]     [backup
dns]
                  ---------------------------------------------------------------------
         current: 192.168.2.12     255.255.255.0   192.168.2.254   0.0.0.0
0.0.0.0
          static: 192.168.2.12     255.255.255.0   192.168.2.254   0.0.0.0
0.0.0.0

        net info: [ip6 addr/mask]
                  ---------------------------------------------------------------------
         current:
          static:
```

Relative Command

command	description
show ipaddress vlan list	View the management vlan information

14.13 ip address dns

Manager vlan dns primary and backup servers

Ip address dns major <A.B.C.D>

Ip address dns backup <A.B.C.D>

Clear dns server

ipaddress dns major clear

ipaddress dns backup clear

Default Configuration The default mode is bound vlanid 1

Command mode global configuration mode

Usage Guide --

Configuration Example 1: The following example, add the primary DNS server 172.16.2.2

```
Console(config-if-vlan2)# ip address dns major 172.16.2.2
```

Relative Command --

Relative Command

Command	Description
Show ipaddress vlan list	Show information management vlan
ifconfig	Show basic information about the switch

14.14 ip address

Setting change management IP

ip address Unicast address <A.B.C.D> mask<A.B.C.D> {static-ip6 <X:X::X:X/M> | gateway<A.B.C.D>}

Default Configuration The default mode is bound vlanid 1

Command mode global configuration mode

Usage Guide Add the management vlan, you must first create vlan id, then create vlan vlan id and set binding management IP and subnet mask vlanid bound to take effect by the ipaddress;
Remove vlan, need to remove the management vlan id bound by no ipaddress, then ipaddress delete vlan id.

Configuration Example 1: In the following example, the management vlan 1 ip administration is set to 192.168.2.12, IPv6 is set to fe80 :: 2e0: 4cff: fe00: 8/64

```
Console(config-if-vlan1)# ip address  192.168.2.12 255.255.255.0 static-ip6 fe80::2e0:4cff:fe00:8/64
```

Relative Command

Command	Description
Show ipaddress vlan list	Show information management vlan
ifconfig	Show basic information about the switch

14.15 ip address mtu

Manager vlan jumbo frames

ipaddress vlan mtu <88-1486>

Parameter Description

-

Default Configuration

The default mode is bound vlanid 1

Command mode

global configuration mode

Usage Guide

--

Configuration Example

1: The following example of setting up giant is 1200

```
Console(config-if-vlan2)# ip address mtu 1200
```

Relative Command

-

Relative Command

Command	Description
Show ipaddress vlan list	Show information management vlan
ifconfig	Show basic information about the switch

14.16 ip address gateway

Manager vlan subnet mask

Ip address gateway <A.B.C.D>

Default Configuration

The default mode is bound vlanid 1

Command mode

global configuration mode

Configuration

1: The following example of setting up the management VLAN subnet mask is

Example

255.255.255.0 1

```
Console(config-if-vlan1)# ip address gateway 255.255.255.0
```

Relative Command

-

Relative Command

Command	Description
Show ipaddress vlan list	Show information management vlan
ifconfig	Show basic information about the switch

14.17 ip address pri

Manager vlan priority

Ip address pri <0-7>

Default Configuration

The default mode is bound vlanid 1

Command mode

global configuration mode

Usage Guide

--

Configuration Example

1: The following example priority, settings management VLAN 1 to 5

```
Console(config-if-vlan1)# ip address pri 5
```

Relative Command

-

Relative Command

Command	Description
Show ipaddress vlan list	Show information management vlan
ifconfig	Show basic information about the switch

14.18 ip address ip-mode

Set the device to obtain dynamic static ip address.

Ip address **ip-mode** [dhcp | static]

Parameter Description

Parameter	Description
ip-mode	Get the ip mode (dynamic or static)

Default Configuration

--

Command mode	global configuration mode
Usage Guide	The Command set ip access way (dynamic or static).
Configuration Example	Console(config-if-vlan1)# ip address ip-mode dhcp Console(config-if-vlan1)#

14.19 ip address ip-mode dhcp

Under Dhcp mode device to retrieve ip address, reboot the device and DHCP to obtain the release of the ip address.

Ip address ip-mode dhcp [*renew* | *release*| *restart*]

Parameter Description

Parameter	Description
dhcp *renew*	Retrieve ip address
dhcp *release*	To obtain the release of the ip address
dhcp *restart*	Get ip address dhcp restart

Default Configuration	--
Command mode	global configuration mode
Usage Guide	Dhcp under acquisition, restart and release ip address (you need to be set to dhcp mode).
Configuration Example	Here is an example :(three Command were to acquire, restart, release) Console(config-if-vlan1)# ip address dhcp renew Console(config-if-vlan1)# ip address dhcp restart Console(config-if-vlan1)# ip address dhcp release

Relative Command

Command	Description
Ifconfig	To view the acquired ip address

14.20 resetfactoryconfig

Restore factory settings

resetfactoryconfig

Command mode	factory mode
Configuration Example	Restore factory settings: Console#factory Console(factory)# resetfactoryconfig

Relative Command	Command	Description
	Ifconfig	To view the acquired ip address

14.21 jumbo-frame

Set all the ports support jumbo-frame.

jumbo-frame num

Parameter Description	Parameter	Description
	num	In the range of 1518-9216

Default Configuration

The default value is 1518.

Command mode

global configuration mode

Usage Guide

-Set the interface supports jumbo-frame (maximum transmission frame length).

Configuration Example

The Jumbo Frame setting is 1600
Console(config)# jumbo-frame 1600

Relative Command	Command	Description
	show interfaces	Show the interface Settings and statistics.

14.22 eee

Setting All ports support the eee.

eee Enable

Default Configuration

By default status is Enable.

Command mode

global configuration mode

Usage Guide

-Set the interface supports EEE.

Configuration Example

Enable eee：
Console(config)# eee Enable

Relative	Command	Description

Command

show eee status	Show eee status

14.23 SNTP Enable

Enables the SNTP server as the network time.

sntp Enable primiry server<A.B.C.D> secondry server<A.B.C.D> thirdly server<A.B.C.D> timeout<0-30> pollint<0-30> retrycnt<0-5> timezone< 0-30> daylight<0-1>

Parameter Description

Parameter	Description
primiry server	primiry IP server
second server	Second IP server
thirdly server	Thirdly ip server
Sntp timeout time	Interval for SNTP clients to send requests to the NTP / SNTP server, in the range 0-30
Sntp pollint	Set SNTP poll interval,range 0-30
Sntp retrycnt	Set SNTP timeout retry time,range 0-5
Sntp timezone	Sntp timezone time: (0: (GMT-12:00) International Date Line West; 1:(GMT-11:00) Midway Island; 2: (GMT-10:00) Hawaii; 3: (GMT-09:00)Alaska; 4: (GMT-08:00) Pacific Time (US, Canada), Tijuana; 5:(GMT-07:00) Arizona; Mountain Time (US, Canada); 6: (GMT-06:00)Central America; Central Time (US, Canada); 7: (GMT-05:00) Eastern Time (US, Canada); 8: (GMT-04:00) Atlantic Time (Canada); 9: (GMT-03:00) Brasilia; Buenos Aires; Greenland; 10: (GMT-02:00)Mid-Atlantic; 11: (GMT-01:00) Cape Vade; 12: (GMT) Greenwhich Mean Time: Dublin, Lisbon, London; Casablanca; 13: (GMT+01:00) Amsterdam,Berlin, Rome, Stockholm, Vienna, Paris; 14: (GMT+02:00) Athens,Istanbul, Cairo, Harare, Jerusalem; 15: (GMT+03:00) Baghdad, Kuwait,Riyadh, Moscow;

	16: (GMT+04:00) Muscat; 17: (GMT+05:00) Islamabad, Karachi; 18: (GMT+05:30) Chennai, Kolkata, Mumbai, New Delhi; 19: (GMT+06:00) Dhaka; 20: (GMT+07:00) Bangkok, Hanoi, Jakarta; 21: (GMT+08:00) Beijing, Hong Kong; 22: (GMT+09:00) Tokyo, Seoul; 23:(GMT+10:00) Brisbane, Sydney; 24: (GMT+11:00) Magadan, Solomon Islands; 25: (GMT+12:00) Auckland, Wellington, Fiji)
Sntp daylight	1 meanings Enable summer time，0 meanings disable

Default Configuration

Default is disable.

Command mode

Global configuration mode

Usage Guide

Since the SNTP protocol is fully compatible with NTP,
the SNTP server can be configured as a common NTP server on the Internet.

Configuration Example

set sntp server is 202.118.1.81,timezone is 6：
Console(config)# sntp Enable 202.118.1.81 0.0.0.0 0.0.0.0 10 2 2 6 0

Relative Command

Command	Description
show sntp	Show sntp configuration

14.24 show interfaces brief

Show all port traffic information.

show interfaces brief

Command mode

global configuration mode

Usage Guide

show all Port basic information and traffic information.

Configuration Example

View port traffic information:
Console(config)# show interfaces brief

Relative Command

Command	Description
show interfaces brief	show port traffic information:

15 System Log

15.1 Logging on

Start the system log function. The Command's no form will shut down the system log.

Logging on

No logging on

Default Configuration

System logs on.

Command mode

global configuration mode.

Usage Guide

The Command is used to Enable system logging.

Configuration Example

Here is the opening system log function:

```
Console#config
Console(config)# logging on
Console(config)#
```

Relative Command

Command	Description
Show logging	show system log configuration information

15.2 show logging

show system log configuration information

Show logging

Command mode Enable mode

Usage Guide show system log configuration information

Configuration Example The following are examples show snmp server configuration information:

```
Console(config)#
Console(config)# show logging
Syslog logging: Enabled
  Consolee logging: level debugging, 301 messages logged
  Monitor logging: level debugging, 0 messages logged
  Buffer logging: level debugging, 301 messages logged
  Timestamp debug messages: datetime
  Timestamp log messages: datetime
  Sequence-number log messages: disable
  Sysname log messages: disable
  Trap logging: level informational, 281 message lines logged,0 fail
    logging to  192.168.1.15
Log Buffer (Total 4096 Bytes):
*Oct 24 18:54:28: %SYS-5-CONFIG_I: Configured from Consolee by
web(172.16.26.59)
*Oct 24 18:54:29: %SYS-5-CONFIG_I: Configured from Consolee by
web(172.16.26.59)
*Oct 24 18:54:35: %SYS-5-CONFIG_I: Configured from Consolee by
web(172.16.26.59)
Console(config)#
```

Relative Command

Command	Description
Logging on	Open the System Log feature

15.3 Logging Consolee

Configure log output to the Consolee. The Command's no form disables log output to the Consolee.

Logging Consolee *loglevel*

no logging Consolee

Parameter Description

Parameter	Description
Loglevel	Output to the Consolee log level

Default Configuration

disable

loglevel: debugging(7)

Command mode

global configuration mode

Usage Guide

Configuring Open log output to the Consolee, and configure output log level, the log level is higher than the average level of log output.
value of the log level, the higher the grade.

Configuration Example

Below is the log output to the Consolee, the log level for the debugging examples:

```
Console(config)#
Console(config)# logging Consolee debugging
Console(config)# show logging
Syslog logging: Enabled
  Consolee logging: level debugging, 301 messages logged
  Monitor logging: level debugging, 0 messages logged
  Buffer logging: level debugging, 301 messages logged
  Timestamp debug messages: datetime
  Timestamp log messages: datetime
  Sequence-number log messages: disable
  Sysname log messages: disable
  Trap logging: level informational, 281 message lines logged,0 fail
    logging to  192.168.1.15
Log Buffer (Total 4096 Bytes):
*Oct 24 18:54:28: %SYS-5-CONFIG_I: Configured from Consolee by
web(172.16.26.59)
*Oct 24 18:54:29: %SYS-5-CONFIG_I: Configured from Consolee by
web(172.16.26.59)
*Oct 24 18:54:35: %SYS-5-CONFIG_I: Configured from Consolee by
web(172.16.26.59)
Console(config)#
```

Relative Command

Command	Description
Logging on	Open the System Log feature

15.4 Logging buffered

Configure log output to the buffer. The Command's no form to ban log output buffer.

Logging buffered *buffersize loglevel*

no snmp-server host *ip-address* **traps version** *ver-type username-string*

Parameter Description

Parameter	Description
Buffersize	Buffer size. Value: 4096-131072
Loglevel	Log level

Default Configuration

Enable

loglevel: debugging(7)

Command mode

global configuration mode

Usage Guide

Configure log output to the buffer, the buffer size, output log level

Configuration Example

Below is the log output to the buffer, the size of 4096, the log level debugging examples:

```
Console#config
Console(config)# logging buffered 4096 debugging
Console(config)# show logging
Syslog logging: Enabled
  Consolee logging: level debugging, 301 messages logged
  Monitor logging: level debugging, 0 messages logged
  Buffer logging: level debugging, 301 messages logged
  Timestamp debug messages: datetime
  Timestamp log messages: datetime
  Sequence-number log messages: disable
  Sysname log messages: disable
  Trap logging: level informational, 281 message lines logged,0 fail
    logging to  192.168.1.15
Log Buffer (Total 4096 Bytes):
*Oct 24 18:54:28: %SYS-5-CONFIG_I: Configured from Consolee by
web(172.16.26.59)
*Oct 24 18:54:29: %SYS-5-CONFIG_I: Configured from Consolee by
web(172.16.26.59)
*Oct 24 18:54:35: %SYS-5-CONFIG_I: Configured from Consolee by
web(172.16.26.59)
Console(config)#
```

Relative Command

Command	Description
Logging on	Open the System Log feature

15.5 Logging monitor

Configure log output to vtp. The Command's no form disables log output to vty.

Logging monitor *loglevel*

No logging monitor

Parameter Description

Parameter	Description
Loglevel	Log level

Default Configuration

Enable

-oglevel: debugging(7)

Command mode

global configuration mode

Usage Guide

Configure log output to tty, log output level

Configuration Example

Below is the log output to tty, log level debugging Liezi:

```
Console#config
Console(config)# logging monitor debugging
Console(config)# show logging
Syslog logging: Enabled
  Consolee logging: level debugging, 301 messages logged
  Monitor logging: level debugging, 0 messages logged
  Buffer logging: level debugging, 301 messages logged
  Timestamp debug messages: datetime
  Timestamp log messages: datetime
  Sequence-number log messages: disable
  Sysname log messages: disable
  Trap logging: level informational, 281 message lines logged,0 fail
    logging to  192.168.1.15
Log Buffer (Total 4096 Bytes):
*Oct 24 18:54:28: %SYS-5-CONFIG_I: Configured from Consolee by
web(172.16.26.59)
*Oct 24 18:54:29: %SYS-5-CONFIG_I: Configured from Consolee by
web(172.16.26.59)
*Oct 24 18:54:35: %SYS-5-CONFIG_I: Configured from Consolee by
web(172.16.26.59)
Console(config)#
```

Relative Command

Command	Description
Logging on	Open the System Log feature

15.6 Logging file

Configure log output to flash. The Command's no form disables log

output to flash.

Logging file *filename maxfilesize loglevel*

No logging file

Parameter Description

Parameter	Description
Filename	The log file name is stored on the flash
Maxfilesize	The maximum size of the log file. Value: 131072-512000 Unit: Byte Default: 131072
Loglevel	Log level

Default Configuration

disable

loglevel: informational(6)

Command mode

global configuration mode

Usage Guide

Configure log output to flash, the log file size, output log level

Configuration Example

Here is an example of the configuration log output to flash, the log file name switch, the size is 131072, the log level informational:

```
Console#config
Console(config)# logging file switch 131072 informational
Console(config)# show logging
Syslog logging: Enabled
  Consolee logging: level debugging, 301 messages logged
  Monitor logging: level debugging, 0 messages logged
  Buffer logging: level debugging, 301 messages logged
    File logging: level informational, 8 messages logged
  File name: switch.txt, size 128 Kbytes, have written 1 file
  Timestamp debug messages: datetime
  Timestamp log messages: datetime
  Sequence-number log messages: disable
  Sysname log messages: disable
  Trap logging: level informational, 281 message lines logged,0 fail
    logging to  192.168.1.15
Log Buffer (Total 4096 Bytes):
*Oct 24 18:54:28: %SYS-5-CONFIG_I: Configured from Consolee by
web(172.16.26.59)
*Oct 24 18:54:29: %SYS-5-CONFIG_I: Configured from Consolee by
web(172.16.26.59)
*Oct 24 18:54:35: %SYS-5-CONFIG_I: Configured from Consolee by
web(172.16.26.59)
Console(config)#
```

Relative Command

Command	Description

Logging on	Open the System Log feature

15.7 Logging server

Configure log server ip. The Command's no form to delete the log server ip.

Logging server *ipaddr*

No logging server *ipaddr*

Logging *ipaddr*

Parameter Description

Parameter	Description
ipaddr	Log server ip address

Default Configuration

-

Command mode

global configuration mode

Usage Guide

Configure log server ip address
log server address number is 1

Configuration Example

Below is the log server address 192.168.1.15 is an example of:

```
Console#config
Console(config)# logging server 192.168.1.15
Console(config)# show logging
Syslog logging: Enabled
  Consolee logging: level debugging, 301 messages logged
  Monitor logging: level debugging, 0 messages logged
  Buffer logging: level debugging, 301 messages logged
  Timestamp debug messages: datetime
  Timestamp log messages: datetime
  Sequence-number log messages: disable
  Sysname log messages: disable
  Trap logging: level informational, 281 message lines logged,0 fail
    logging to  192.168.1.15
Log Buffer (Total 4096 Bytes):
*Oct 24 18:54:28: %SYS-5-CONFIG_I: Configured from Consolee by
web(172.16.26.59)
*Oct 24 18:54:29: %SYS-5-CONFIG_I: Configured from Consolee by
web(172.16.26.59)
*Oct 24 18:54:35: %SYS-5-CONFIG_I: Configured from Consolee by
web(172.16.26.59)
Console(config)#
```

Relative Command

Command	Description

Logging on	Open the System Log feature
Logging *ipaddr*	Command the same role, configure the log server ip address

15.8 Logging trap

Configured to output logs to the log server. The Command's no form disables log output to the log server.

Logging trap *loglevel*

No logging trap

Parameter Description

Parameter	Description
Loglevel	Log level

Default Configuration

Enable

loglevel: informational(6)

Command mode

global configuration mode

Usage Guide

Configured to output logs to the log server, log output level

Configuration Example

Below is the log output to a log server example, the log level informational:

```
Console#config
Console(config)# logging trap informational
Console(config)# show logging
Syslog logging: Enabled
  Consolee logging: level debugging, 301 messages logged
  Monitor logging: level debugging, 0 messages logged
  Buffer logging: level debugging, 301 messages logged
  Timestamp debug messages: datetime
  Timestamp log messages: datetime
  Sequence-number log messages: disable
  Sysname log messages: disable
  Trap logging: level informational, 281 message lines logged,0 fail
    logging to  192.168.1.15
Log Buffer (Total 4096 Bytes):
*Oct 24 18:54:28: %SYS-5-CONFIG_I: Configured from Consolee by
web(172.16.26.59)
*Oct 24 18:54:29: %SYS-5-CONFIG_I: Configured from Consolee by
web(172.16.26.59)
*Oct 24 18:54:35: %SYS-5-CONFIG_I: Configured from Consolee by
web(172.16.26.59)
Console(config)#
```

Relative Command	Command	Description
	Logging on	Open the System Log feature

15.9 Logging source

Configure the log server source ip address. The Command's no form to delete the source ip address.

Logging source ip *ipaddr*

No logging source ip

Parameter Description

Parameter	Description
ipaddr	Source ip address

Default Configuration

-

Command mode

global configuration mode

Usage Guide

Configure the log server source ip address
□ If configured ip address does not exist, the default interface ip address.

Configuration Example

Below is the source log server ip address 192.168.1.2 as an example of:

```
Console#config
Console(config)# logging source ip 192.168.1.2
Console(config)# show logging
Syslog logging: Enabled
  Consolee logging: level debugging, 301 messages logged
  Monitor logging: level debugging, 0 messages logged
  Buffer logging: level debugging, 301 messages logged
  Timestamp debug messages: datetime
  Timestamp log messages: datetime
  Sequence-number log messages: disable
  Sysname log messages: disable
  Trap logging: level informational, 281 message lines logged,0 fail
    logging to  192.168.1.15
Log Buffer (Total 4096 Bytes):
*Oct 24 18:54:28: %SYS-5-CONFIG_I: Configured from Consolee by
web(172.16.26.59)
*Oct 24 18:54:29: %SYS-5-CONFIG_I: Configured from Consolee by
web(172.16.26.59)
*Oct 24 18:54:35: %SYS-5-CONFIG_I: Configured from Consolee by
web(172.16.26.59)
Console(config)#
```

Relative Command

Command	Description
Logging on	Open the System Log feature

15.10 Logging facility

Configure logging equipment value. The Command's no form of the device will use the default value.

Logging facility *facilityvalue*

No logging facility

Parameter Description

Parameter	Description
facilityvalue	Facilities value

Default Configuration

Local 7

Command mode

global configuration mode

Usage Guide

Configuring log generating device value

Configuration Example

Below is the log generating device is local7 examples:

```
Console#config
Console(config)# logging facility local7
Console(config)# show logging
Syslog logging: Enabled
  Consolee logging: level debugging, 301 messages logged
  Monitor logging: level debugging, 0 messages logged
  Buffer logging: level debugging, 301 messages logged
  Timestamp debug messages: datetime
  Timestamp log messages: datetime
  Sequence-number log messages: disable
  Sysname log messages: disable
  Trap logging: level informational, 281 message lines logged,0 fail
    logging to  192.168.1.15
Log Buffer (Total 4096 Bytes):
*Oct 24 18:54:28: %SYS-5-CONFIG_I: Configured from Consolee by
web(172.16.26.59)
*Oct 24 18:54:29: %SYS-5-CONFIG_I: Configured from Consolee by
web(172.16.26.59)
*Oct 24 18:54:35: %SYS-5-CONFIG_I: Configured from Consolee by
web(172.16.26.59)
Console(config)#
```

Relative Command

Command	Description
Logging on	Open the System Log feature

15.11 Service sequence-numbers

Configuring log message contains the serial number. The Command's no form to remove the log message sequence number.

Service sequence-numbers

No service sequence-numbers

Default Configuration disable

Command mode global configuration mode

Usage Guide Configuring log message contains the serial number

Configuration Example Here is an example of the configuration log sequence number contained in the message:

```
Console#config
Console(config)# service sequence-numbers
Console(config)# show logging
Syslog logging: Enabled
  Consolee logging: level debugging, 301 messages logged
  Monitor logging: level debugging, 0 messages logged
  Buffer logging: level debugging, 301 messages logged
  Timestamp debug messages: datetime
  Timestamp log messages: datetime
  Sequence-number log messages: Enable
  Sysname log messages: disable
  Trap logging: level informational, 281 message lines logged,0 fail
    logging to  192.168.1.15
Log Buffer (Total 4096 Bytes):
000033: Oct 24 09:45:30 %PORTMANAGE-5-UPDOWN: Port 3, changed state to
up
Console(config)#
```

Relative Command

Command	Description
Logging on	Open the System Log feature

15.12 Service timestamps

Configuring log message contains a timestamp. The Command's no form to remove the log message timestamp.

Service timestamps *logtype timetype*

No Service timestamps

Parameter Description

Parameter	Description
logtype	Debug: debug infomartion Log: log information
timetype	Time Type Uptime: system uptime Datetime: System time

Default Configuration

Enable

Datetime

Command mode

global configuration mode

Usage Guide

Configuring log message contains a timestamp

Configuration Example

Below is the debug log messages timestamp datetime examples:

```
Console#config
Console(config)# service timestamps debug datetime
Console(config)# show logging
Syslog logging: Enabled
  Consolee logging: level debugging, 301 messages logged
  Monitor logging: level debugging, 0 messages logged
  Buffer logging: level debugging, 301 messages logged
  Timestamp debug messages: datetime
  Timestamp log messages: datetime
  Sequence-number log messages: Enable
  Sysname log messages: Enable
  Trap logging: level informational, 281 message lines logged,0 fail
    logging to  192.168.1.15
Log Buffer (Total 4096 Bytes):
000033: Oct 24 09:45:30 localhost %PORTMANAGE-5-UPDOWN: Port 3,
changed state to up
Console(config)#
```

Relative Command

Command	Description
Logging on	Open the System Log feature

15.13 Service sysname

Configuring log message contains the name of the system. The Command's no form to remove the log message system name.

Service sysname

No service sysname

Default Configuration	Disable
Command mode	global configuration mode
Usage Guide	Configuring log message contains the name of the system
Configuration Example	Here is an example of the configuration log message contains the name of the system:

```
Console#config
Console(config)# service sysname
Console(config)# show logging
Syslog logging: Enabled
  Consolee logging: level debugging, 301 messages logged
  Monitor logging: level debugging, 0 messages logged
  Buffer logging: level debugging, 301 messages logged
  Timestamp debug messages: datetime
  Timestamp log messages: datetime
  Sequence-number log messages: Enable
  Sysname log messages: Enable
  Trap logging: level informational, 281 message lines logged,0 fail
    logging to  192.168.1.15
Log Buffer (Total 4096 Bytes):
000033: Oct 24 09:45:30 localhost %PORTMANAGE-5-UPDOWN: Port 3,
changed state to up
Console(config)#
```

Relative Command

Command	Description
Logging on	Open the System Log feature

15.14 Clear logging

Clear buffer log.

Clear logging

Command mode	Enable mode
Usage Guide	Clear buffer log.
Configuration Example	Here is the clear buffer log examples:

```
Console# clear logging
Console# show logging
Syslog logging: Enabled
  Consolee logging: level debugging, 301 messages logged
  Monitor logging: level debugging, 0 messages logged
  Buffer logging: level debugging, 301 messages logged
  Timestamp debug messages: datetime
  Timestamp log messages: datetime
  Sequence-number log messages: Enable
  Sysname log messages: Enable
  Trap logging: level informational, 281 message lines logged,0 fail
```

```
    logging to  192.168.1.15
Log Buffer (Total 4096 Bytes):
<empty syslog>
Console#
```

Relative Command

Command	Description
Logging on	Open the System Log feature

15.15 Terminal monitor

Configure the log file output to the current vty. The Command's no form to log off the output current vty.

Termilnal monitor

Termilnal no monitor

Default Configuration

Disable

Command mode

Enable mode

Usage Guide

Configure the log file output to the current vty
switch only when the logging monitor and terminal monitor switch are simultaneously turned on, the log will be output to the current vty

Configuration Example

Below is the log file output to the current vty examples:

```
Console# terminal monitor
000033: Oct 24 09:45:30 localhost %PORTMANAGE-5-UPDOWN: Port 3,
changed state to up
Console#
```

Relative Command

Command	Description
Logging on	Open the System Log feature

15.16 Dir

Show flash the file

Dir

Command mode

Enable mode

Usage Guide

Show flash the file

Configuration Example

Here is an example show flash the file:

```
Console# dir
node      user      group          size time              name
-------------------------------------------------------------------------
30        admin     root          58552 2013-10-24 10:53:35  switch.txt
-------------------------------------------------------------------------
Console#
```

Relative Command

Command	Description
Logging on	Open the System Log feature

15.17 Delete

Delete files in flash

Delete *filename*

Parameter Description

Parameter	Description
filename	file name

Default Configuration

-

Command mode

Enable mode

Usage Guide

Delete files in flash

Configuration Example

Here is to delete the files in the flash switch.txt examples:

```
Console# delete switch.txt
Delete "switch.txt",
Are you sure? (Y or y for "yes", N or n for " no") y -->user confirmed
File "switch.txt" is deleted.
Console#
```

Relative Command

Command	Description
Logging on	Open the System Log feature

15.18 More

Show flash content in files

More *filename*

Parameter Description

Parameter	Description
filename	File name

Command mode

Enable mode

Usage Guide

Show flash content in files

Configuration Example

Here is an example of a file switch.txt showflash content:

```
Console# more switch.txt
000229: Oct 22 16:29:14 localhost %PORTMANAGE-5-UPDOWN: Port 3, changed state to
down
000230: Oct 22 16:29:29 localhost %PORTMANAGE-5-UPDOWN: Port 2, changed state to up
Console#
```

Relative Command

Command	Description
Logging on	Open the System Log feature

15.19 Debug

Turn debugging a module

Debug *modname*

Show debugging

Parameter Description

Parameter	Description
modname	modname

Command mode

Enable mode

Usage Guide

Open debugging a module

Configuration Example

The following are open vlan debugging examples:

```
Console# debug vlan
Console#show debugging
vlan debugging is on
Console#
```

Relative Command

Command	Description
Logging on	Open the System Log feature

16 AAA

16.1 aaa new-model

Global Enable AAA security services. The Command's no closed form AAA security services.

aaa new-model

no aaa new-model

Default Configuration

Open AAA Security Services

Command mode

global configuration mode

Usage Guide

The formula is AAA Command Enabled Command, if you want to use the AAA security services, you must use the Command Enable AAA security services. If you do not Enable AAA, then all Command will not be configurable.

Configuration Example

Here is to Enable AAA security services examples:

```
Console(config)# aaa new-model
Console(config)#
```

Relative Command

Command	Description
aaa authentication	Define user authentication method list

16.2 aaa authentication dot1x

Use this Command to configure 802.1x user authentication method list. The Command's no form to delete 802.1x user authentication method list.

aaa authentication dot1x {default | *list-name*} *method1 [method2..]*

no aaa authentication dot1x {default | *list-name*}

Parameter Description

Parameter	Description
default	Methods of using the Parameter, the list defined later as the default method for 802.1x user authentication
list-name	Define a 802.1x user authentication method list, it can be any string

method	It must be one of the keywords listed in "local, none, group", a list of methods up to four methods
local	Use local username authentication data
none	Without certification
group	Using server group for authentication, currently supports RADIUS and TACACS + server group

Command mode

global configuration mode

Usage Guide

If the device is Enabled 802.1x security service, the user must use AAA for 802.1x user authentication negotiation. Use this Command to configure the default or optional list of methods for 802.1x user authentication.
Only the first method does not respond, you can use the latter method for authentication.

Configuration Example

The following example defines the default authentication method list to use RADIUS security server for authentication, if a certain time limit does not receive RADIUS security server response, use the local user database for authentication:

```
Console(config)# aaa authentication dot1x default group radius local
Console(config)#
```

Relative Command

Command	Description
aaa new-model	Use AAA security services
username	Define local user database
dot1x	Open 802.1x authentication device
dot1x port-control auto	802.1x port authentication turned on

Platform Description

-

16.3 aaa authentication Enable

The method of using a list configuration Command Enable authentication. The Command's no form to remove the list of Enable authentication method.

aaa authentication Enable {**default** | *list-name*} *method1 [method2..]*

no aaa authentication Enable {**default** | *list-name*}

Parameter Description

Parameter	Description
default	Methods of using the Parameter, the list defined later as the default authentication method Enable

list-name	Define a Enable authentication method list, it can be any string
method	It must be one of the keywords listed in "local, none, group", a list of methods up to four methods
local	Use local username authentication data
none	Without certification
group	Using server group for authentication, currently supports RADIUS and TACACS + server group

Command mode

global configuration mode

Usage Guide

If the device is Enabled Enable AAA authentication services, the user must use the AAA Enable authentication negotiation. Use this Command to configure the default or optional list of methods for Enable certification.
Only the first method does not respond, you can use the latter method for authentication.

Configuration Example

The following example defines AAA Enable authentication list. This authentication method list to use RADIUS security server for authentication, if a certain time limit does not receive RADIUS security server response, use the local user database for authentication:

```
Console(config)# aaa authentication Enable default group radius local
Console(config)#
```

Relative Command

Command	Description
aaa new-model	Use AAA security services
Enable	Switch the user level
username	Define local user database

16.4 aaa authentication login

Use the Command configuration Login (login) authentication method list. The Command's no form to remove the list of approved methods.

aaa authentication login {**default** | *list-name*} *method1 [method2..]*

no aaa authentication login {**default** | *list-name*}

Parameter Description

Parameter	Description
default	Methods of using the Parameter, the list defined later as the default authentication method Enable
list-name	Login authentication method to define a list can be any string

method	It must be one of the keywords listed in "local, none, group", a list of methods up to four methods
local	Use local username authentication data
none	Without certification
group	Using server group for authentication, currently supports RADIUS and TACACS + server group

Command mode global configuration mode

Usage Guide If the device is Enabled AAA login authentication service, the user must use the AAA Login authentication negotiation. Use this Command to configure the default or optional list of methods used for Login authentication.
Only the first method does not respond, you can use the latter method for authentication.

Configuration Example
The following example defines the default authentication list Login AAA. This authentication method list to use RADIUS security server for authentication, if a certain time limit does not receive RADIUS security server response, use the local user database for authentication:
Console(config)# aaa authentication login default *group radius local*
Console(config)#

Relative Command

Command	Description
aaa new-model	Use AAA security services
username	Define local user database

16.5 aaa group server

The AAA server group configuration mode. The Command's no form to remove the server group.

aaa group server {radius | tacacs+} *name*

no aaa group server {radius | tacacs+} *name*

Parameter Description

Parameter	Description
name	Named server group

Command mode global configuration mode

Usage Guide The Command configure AAA server group, currently supports RADIUS and TACACS + server group.

Configuration Example
Console(config)# aaa group server radius r1
enter radius server group node!
Console(config-sg-radius)#server 192.168.2.99
Console(config-sg-radius)

Relative Command

Command	Description
show aaa group	Show aaa server group

16.6 server

Add Server A group. The Command's no form to delete the corresponding server.

server *ip-addr* [**auth-port** *port*]

no server *ip-addr* [**auth-port** *port*]

Parameter Description

Parameter	Description
ip-addr	Server ip address
port	Server authentication port

Command mode

Server group configuration mode

Usage Guide

Adding a server to the specified server, the default value is not specified port.

Configuration Example

Console(config)# aaa group server radius r1

```
enter radius server group node!
Console(config-sg-radius)#server 192.168.2.99
Console(config-sg-radius)
```

Relative Command

Command	Description
aaa group server	Configuration aaagroup server
show aaa group	Show aaa server group

16.7 aaa domain Enable

AAA-based domain name service switch, default is off status. When this switch is on when the priority domain-based AAA service configuration. The Command's no form to close the switch.

aaa domain Enable

no aaa domain Enable

Default Configuration disable

Command mode global configuration mode

Usage Guide AAA-based domain name service configuration, you need to open the configuration switch.

Configuration Example Here is an example of open name-based AAA services:

```
Console(config)# aaa domain Enable
Console(config)#
```

Relative Command

Command	Description
aaa new model	Open the AAA security services
show aaa domain	Show domain configuration

16.8 aaa domain

The domain configuration mode, configuration properties of the domain. The Command's no form to cancel the Command.

aaa domain {default | *domain-name***}**

no aaa domain {default | *domain-name***}**

Parameter Description

Parameter	Description
default	Use the Command, configure the default domain
domain-name	Specifies the name of the domain

Default Configuration Any domain not configured

Command mode global configuration mode

Usage Guide

Specifies the AAA service domain-based configuration. default is the default domain configuration, that is, if the user does not carry the Method field information, the network equipment used list. domain-name for the specified domain configuration, if the user carries the domain name, specify the list of domains associated with this method. Currently, the system supports up to 32 domains.
The domain configuration is Enabled by default domain-based service.

Configuration Example

The following are examples of configuration setting the domain name:

```
Console(config)# aaa domain example.com
Config AAA domain example.com
Console(config-aaa-domain)#
```

Relative Command

Command	Description
aaa new model	Enable AAA new model
aaa domain Enable	Open AAA domain-based service
show aaa domain	Show domain configuration

16.9 state

Setting domain is valid, the Command's no form to restore the default configuration.

state {block | active}

no state

Parameter Description

Parameter	Description
mac-addr	Mac address authentication can access terminal

Default Configuration

By default, the effective domain

Command mode

Domain configuration mode

Usage Guide

Domain specified configuration is valid.

Configuration Example

Here is to set the specified domain - valid examples:

```
Console(config)# aaa domain example.com
Config AAA domain example.com
Console(config-aaa-domain)#state block
Console(config-aaa-domain)#
```

Relative Command

Command	Description
aaa new model	Enable AAA new model

aaa domain Enable	Open AAA domain-based service
show aaa domain	Show domain configuration

16.10 username-format

In domain configuration mode when configuring the NAS interaction with the server whether they carry the domain information, the Command's no form to restore the default configuration for the user name.

username-format {with-domain | without-domain}

no username-format

Parameter Description

Parameter	Description
with-domain	Without peeling domain information
without-domain	Peeling domain information

Default Configuration

By default, no peeling domain information

Command mode

Domain configuration mode

Usage Guide

In domain configuration mode, configure NFS is specified domain for interaction with the server, user name, whether it carries the domain information.

Configuration Example

Here is an example of setting the release domain information:

```
Console(config)# aaa domain example.com
Config AAA domain example.com
Console(config-aaa-domain)#username-domain without-domain
Console(config-aaa-domain)#
```

Relative Command

Command	Description
aaa new model	Enable AAA new model
aaa domain Enable	Open AAA domain-based service
show aaa domain	Show domain configuration

16.11 aaa local authentication attempts

Configuring login user login attempt failed login attempts, the Command's no form to restore the default configuration.

aaa local authentication attempts *max-attempts*

no aaa local authentication attempts

Parameter Description

Parameter	Description
max-attempts	The maximum number of failed attempts, in the range of 1 to 2147483647

Default Configuration

The default is 3 times

Command mode

global configuration mode

Usage Guide

The Command Configure Login Login User failed login attempts.

Configuration Example

Console(config)# aaa local authentication attempts 5

Console(config)#

Relative Command

Command	Description
show aaa lockout	show current login lock configuration Parameter

16.12 aaa local authentication lockout-time

Configure the login user login attempts exceeds the specified number of logon failures, the length of time locked, the Command's no form to restore the default configuration.

aaa local authentication lockout-time *lockout-time*

no aaa local authentication lockout-time

Parameter Description

Parameter	Description
lockout-time	Lock time (unit: hour), ranging from 1 to 2147483647

Default Configuration

The default is 15 hours

Command mode

global configuration mode

Usage Guide

Configure the login user login attempts exceeds the specified number of logon failures, the length of time locked.

Configuration Example

```
Console(config)# aaa local authentication lockout-time 5
Console(config)#
```

Relative Command

Command	Description
show aaa lockout	show current login lock configuration Parameter

16.13 show aaa method-list

Show AAA all the list of methods.

show aaa method-list

Command mode

Enable mode

Usage Guide

The Command show AAA method list all

Configuration Example

The following are examples show:

```
Console(config)# aaa authentication Enable default local
add method:local
Console(config)# exit
Console#show aaa method-lists
AAA Authentication method
aaa authentication Enable default local
```

17 802.1X

17.1 dot1x

Open 802.1x authentication device. The Command's no closed form 802.1x authentication.

dot1x

no dot1x

Default Configuration By default, 802.1x authentication.

Command mode global configuration mode

Usage Guide The Command globally Enable 802.1x authentication device.

Configuration Example Here is an example of the 802.1x authentication:

```
Console(config)# dot1x
Console(config)#
```

Relative Command

Command	Description
show dot1x	Review the settings of 802.1x
dot1x port-control auto	802.1x port authentication turned on

17.2 dot1x port-control auto

Enable 802.1x authentication on the port. The Command's no closed form 802.1x authentication on the port.

dot1x port-control auto

no dot1x port-control auto

Default Configuration Default off

Command mode interface configuration mode

Usage Guide Global 802.1x must be configured Command.

Configuration Example Here is the 802.1x authentication on the port 4:

```
Console(config-if-GigabitEthernet4)# dot1x port-control auto
```

```
Console(config-if-GigabitEthernet4)
```

Relative Command

Command	Description
show dot1x port-control	Show 802.1x port setting information

17.3 dot1x port-control-mode

Configure port controlled mode. The Command's no form to restore the default configuration port controlled mode

dot1x port-control-mode { mac-based | port-based }

no dot1x port-control-mode

Parameter Description

Parameter	Description
mac-based	MAC-based controlled mode
port-based	Based on Port - controlled mode

Default Configuration

The default is controlled based on mac

Command mode

interface configuration mode

Usage Guide

Controlled port on the requirements of each user based MAC authentication configuration can be controlled mode of communication at the scene;
Controlled port allows a user after authentication, other users can communicate, you can configure a port controlled mode.

Configuration Example

Below is the 4-port port-based controlled examples:

```
Console(config-if-GigabitEthernet4)# dot1x port-control-mode port-based
Console(config-if-GigabitEthernet4)#
```

Relative Command

Command	Description
show dot1x port-control	Show 802.1x port setting information

17.4 dot1x auto-req

Configure the device initiates 802.1x authentication. The Command's no closed form Active Authentication.

dot1x auto-req

no dot1x auto-req

Parameter Description

Parameter	Description

Default Configuration

Default off

Command mode

global configuration mode

Usage Guide

End-use operating system comes with the authentication client can choose to turn this feature.

Configuration Example

The following are open Active Authentication:

```
Console(config)# dot1x auto-req
Console(config)#
```

Relative Command

Command	Description
show dot1x auto-req	show Facilities initiates 802.1x authentication configuration information

17.5 dot1x auto-req packet-num

Configure the device initiates the number of authentication request packets.

dot1x auto-req packet-num *num*

Parameter Description

Parameter	Description
num	Active Authentication of the number of packets sent, the default value is 0, indicating that has been sent, the configuration range 0-65535

Command mode

global configuration mode

Configuration Example

The following is a configuration example of authentication request packets request number:

```
Console(config)# dot1x auto-req packet-num 100
Console(config)#
```

Relative Command

Command	Description
dot1x auto-req	Configure the device initiates 802.1x authentication
show dot1x auto-req	show Facilities initiates 802.1x authentication configuration information

17.6 dot1x auto-req interval

Configure the device initiates an authentication request packet interval.

dot1x auto-req interval *time*

Parameter Description

Parameter	Description
time	Active Authentication transmitted packet interval, the default is 30 seconds, the configuration range 10-3600 seconds

Default Configuration

30 s

Command mode

global configuration mode

Usage Guide

-

Configuration Example

The following is a configuration example of authentication request packets requesting interval:

```
Console(config)# dot1x auto-req interval 20
Console(config)#
```

Relative Command

Command	Description
dot1x auto-req	Configure the device initiates 802.1x authentication
show dot1x auto-req	show Facilities initiates 802.1x authentication configuration information

17.7 dot1x auto-req user-detect

Set the device on a port if the user authentication by the presence of no longer take the initiative to issue an authentication request packet. The Command's no closed form the corresponding function.

dot1x auto-req user-detect

no dot1x auto-req user-detect

Default Configuration Default off

Command mode global configuration mode

Usage Guide Single-user port is recommended to turn the feature to reduce the pressure on the server authentication result.

Configuration Example Below is the active certification testing whether there is a user authentication example:

```
Console(config)# dot1x auto-req user-detect
Console(config)#
```

Relative Command

Command	Description
dot1x auto-req	Configure the device initiates 802.1x authentication
show dot1x auto-req	show Facilities initiates 802.1x authentication configuration information

17.8 dot1x re-auth

Configure re-authentication is required supplicant periodic re-certification. The Command's no closed form re-authentication function.

dot1x re-auth

no dot1x re-auth

Default Configuration Default off

Command mode global configuration mode

Usage Guide Setting the Command, the authentication supplicant authentication is passed, each after a certain time must also be re-certified.

Configuration Example Below is the re-authentication function examples:

```
Console(config)# dot1x re-auth
Console(config)#
```

Relative Command

Command	Description
dot1x timeout re-authperiod	Set the re-authentication interval
show dot1x re-auth	show re-authentication configuration

17.9 dot1x req-max

Dot1x and server interaction in the process, if dot1x within a certain time does noteceive a response from the server, the dot1x will initiate a request to the server again, use the Command setting the maximum number of requests to the server allowed. The Command's no reply form to their default values.

dot1x req-max *count*

no dot1x req-max

Parameter Description

Parameter	Description
count	Request / challenge packet retransmission times

Default Configuration

The default value is 2 times

Command mode

global configuration mode

Configuration Example

Here is to set 802.1x authentication five times the maximum retransmission examples:

```
Console(config)#dot1x req-max 5
Console(config)#
```

Relative Command

Command	Description
show dot1x	show the settings of 802.1x

17.10 dot1x pae-group-addr

Configuring the multicast address for authentication. The Command is no indication in the form of unicast address for authentication.

dot1x pae-group-addr

no dot1x pae-group-addr

Default Configuration

By default, the multicast address

Command mode

global configuration mode

Configuration Example

Here is the unicast address authentication examples:

```
Console(config)# no dot1x pae-group-addr
Console(config)#
```

Relative Command

Command	Description
show dot1x	show the settings of 802.1x

17.11 dot1x timeout re-authperiod

Set the re-authentication interval that the certification period.

dot1x timeout re-authperiod *seconds*

Parameter Description

Parameter	Description
seconds	Certification cycle, which ranges from 1 to 65,535 seconds.

Default Configuration

3600 s

Command mode

global configuration mode

Usage Guide

-

Configuration Example

Here is to set the re-authentication period is 1000 seconds examples:

```
Console(config)# dot1x timeout re-authperiod 1000
Console(config)#
```

Relative Command

Command	Description
show dot1x	show the settings of 802.1x

17.12 dot1x timeout server-timeout

Set the timeout before the device and server authentication interaction.

dot1x timeout server-timeout *seconds*

Parameter Description

Parameter	Description
seconds	Server timeout period in the range 1 to 65535.

Default Configuration

10 s

Command mode

global configuration mode

Configuration Example

Here is to set the server timeout 15 seconds interactive examples:

```
Console(config)# dot1x timeout server-timeout 15
Console(config)#
```

Relative Command

Command	Description
show dot1x	show the settings of 802.1x

17.13 dot1x timeout supp-timeout

Set the timeout before the device and supplicant authentication interaction.

dot1x timeout supp-timeout *seconds*

Parameter Description

Parameter	Description
seconds	request / challenge packet retransmission interval in the range of 1 to 65,535 seconds.

Default Configuration

5 s

Command mode

global configuration mode

Configuration Example

Here is to set the client timeout 10 seconds interactive examples:

```
Console(config)# dot1x timeout supp-timeout 10
Console(config)#
```

Relative Command

Command	Description
show dot1x	show the settings of 802.1x

17.14 dot1x timeout tx-period

Configuration request / id packet retransmission interval. The Command's no option to restore the settings to default values.

dot1x timeout tx-period *seconds*

Parameter Description

Parameter	Description
seconds	Request / id packet retransmission interval in the range of 1 to 65,535 seconds.

Default Configuration 5 S

Command mode global configuration mode

Usage Guide -

Configuration Example Here is the setting request / id retransmission interval is 10 seconds examples:

```
Console(config)# dot1x timeout tx-period 10
Console(config)#
```

Relative Command

Command	Description
show dot1x	show the settings of 802.1x

17.15 dot1x max-users

Based on the following MAC authentication mode, limiting the maximum number of clients allowed to authenticate the port.

dot1x max-users *counts*

Parameter Description

Parameter	Description
counts	The maximum allowable number of clients, ranging from 0-255

Default Configuration 64

Command mode interface configuration mode

Usage Guide -

Configuration Example The following are the maximum allowed under 4 set the port number of the authentication client 10 as an example:

```
Console(config-if-GigabitEthernet4)# dot1x max-users 10
Console(config-if-GigabitEthernet4)
```

Relative Command

Command	Description
show dot1x port-control	Show 802.1x port setting information

17.16 dot1x auth-address-table address

Configuration authentication host list. The Command's no option to delete certifiable address.

dot1x auth-address-table address *mac-addr*

no dot1x auth-address-table address *mac-addr*

Parameter Description

Parameter	Description
mac-addr	Mac address authentication can access terminal

Default Configuration

-

Command mode

interface configuration mode

Usage Guide

Limit specified port only designated terminal mac address can 802.1x authentication.

Configuration Example

Below is the list of hosts certifiable examples:

```
Console(config-if-GigabitEthernet4)# dot1x auth-address-table address
      00:30:ab:0a:c0:c6
Console(config-if-GigabitEthernet4)
```

Relative Command

Command	Description
show dot1x auth-address-table	show a list of hosts certification

17.17 dot1x mac-auth-bypass

Configure a single MAB certification. The Command is no single form of closed MAB certification.

dot1x mac-auth-bypass

no dot1x mac-auth-bypass

Default Configuration

off

Command mode

interface configuration mode

Usage Guide

MAB namely MAC bypass authentication for 802.1x authentication client device access, for a single MAB, the tx-period and within reauth-max time - client response, the 802.1x authentication will monitor this port MAC addresses connected to the MAC address and user name and password to the authentication server initiates an authentication by the authentication server returns the results to

determine the MAC address is allowed to access the network.
MAB single user applies a second line, only for a user initiates an authentication.

Configuration Example

Below is the single MAB authentication examples:

```
Console(config-if-GigabitEthernet4)# dot1x mac-auth-bypass
Console(config-if-GigabitEthernet4)#
```

Relative Command

Command	Description
show dot1x port-control	show 802.1x interface information

17.18 dot1x mac-auth-bypass multi-user

Configure multiple MAB authentication. The Command of no more closed form MAB certification.

dot1x mac-auth-bypass multi-user

no dot1x mac-auth-bypass multi-user

Default Configuration

off

Command mode

interface configuration mode

Usage Guide

Multi MAB applies to the second line multiple users, for different users, after more MAB silence time expires, you can continue to initiate bypass authentication request.

Configuration Example

Here is an example of configuring multiple MAB authentication:

```
Console(config-if-GigabitEthernet4)# dot1x mac-auth-bypass multi-user
Console(config-if-GigabitEthernet4)#
```

Relative Command

Command	Description
dot1x multi-mab quiet-period	Configure multiple MAB silent time authentication failure
show dot1x port-control	show 802.1x interface information

17.19 dot1x mac-auth-bypass timeout-activity

Configure MAC address authentication bypass time online. The Command's no form to restore the default value.

dot1x mac-auth-bypass timeout-activity *time*

no dot1x mac-auth-bypass timeout-activity

Parameter Description

Parameter	Description
time	MAB users online time in seconds, default 0, which means to be online. Configuration range 1-65535

Default Configuration 0 s

Command mode interface configuration mode

Usage Guide Restrict access to network users can bypass the authentication time

Configuration Example Below is the MAB authentication timeout:

```
Console(config-if-GigabitEthernet4)# dot1x mac-auth-bypass timeout-activity 3600
Console(config-if-GigabitEthernet4) #
```

Relative Command

Command	Description
show dot1x port-control	show 802.1x interface information

17.20 dot1x multi-mab quiet-period

Configure multiple MAB silent time authentication failure. The Command's no form to restore the default value.

dot1x multi-mab quiet-period *time*

no dot1x multi-mab quiet-period

Parameter Description

Parameter	Description
time	Quiet time more MAB authentication failure, in seconds, the configuration range 0-65535

Default Configuration 30 s

Command mode global configuration mode

Configuration Example

Below is the example of the latter more MAB authentication fails silence time:

```
Console(config)# dot1x multi-mab quiet-period 5
Console(config)#
```

Relative Command

Command	Description
show dot1x	show the settings of 802.1x

17.21 dot1x guest-vlan

Configuration controlled port guest vlan. The Command's no closed form controlled port guest vlan.

dot1x guest-vlan *vlan-id*

no dot1x guest-vlan

Parameter Description

Parameter	Description
vlan-id	Ports will be guest vlan

Default Configuration

off

Command mode

interface configuration mode

Usage Guide

802.1x user connections controlled port but no authentication client can configure this Command; when the controlled port at a certain time (90s) is not received within the scope of any EAPOL packets will automatically add the port where the guest vlan vlan, vlan and removed from the other.

Configuration Example

Open controlled port 2 guest vlan 10:

```
Console(config-if-GigabitEthernet2)# dot1x guest-vlan 10
Console(config-if-GigabitEthernet2)#
```

Relative Command

Command	Description
show dot1x port-control	show 802.1x interface information

17.22 dot1x auth-fail max-attempt

Configure Authentication failed attempts. The Command's no form to restore the configuration authentication failed attempts.

dot1x auth-fail max-attempt *value*

no dot1x auth-fail max-attempt

Parameter Description

Parameter	Description
value	The number of failed authentication attempts, in the range of 1-3

Default Configuration The default is 3 times

Command mode global configuration mode

Usage Guide FAIL VLAN need to adjust to enter the number of times a user can configure this authentication fails Command.

Configuration Example Configure Authentication failed attempts to 1:

```
Console(config)# dot1x auth-fail max-attempt 1
Console(config)#
```

Relative Command

Command	Description
show dot1x	show the settings of 802.1x

17.23 dot1x auth-fail vlan

Configuration controlled port authentication failure vlan. The Command's no form of authentication failure to close the controlled port vlan.

dot1x auth-fail vlan *vlan-id*

no dot1x auth-fail vlan

Parameter Description

Parameter	Description
vlan-id	Authentication failure to join vlan

Default Configuration off

Command interface configuration mode

mode

Usage Guide But hope after the failure of the user authentication can also access the network situation can configure Command; when the controlled port in the authentication fails, it will automatically add the port FAIL VLAN in vlan located and removed from the other vlan.

Configuration Example Open controlled port authentication failure vlan 2 to 20:

```
Console(config-if-GigabitEthernet2)# dot1x auth-fail vlan 20
Console(config-if-GigabitEthernet2)#
```

Relative Command

Command	Description
show dot1x port-control	show 802.1x interface information

17.24 dot1x dynamic-vlan Enable

Configure dynamic port VLAN hopping. The Command's no closed form dynamic port VLAN hopping.

dot1x dynamic-vlan Enable

no dot1x dynamic-vlan Enable

Parameter Description

Parameter	Description

Default Configuration off

Command mode interface configuration mode

Usage Guide The need for user authentication is added to the radius server issues VLAN can be configured in the case of this Command.

Configuration Example Open Port 2 dynamic VLAN Jump:

```
Console(config-if-GigabitEthernet2)# dot1x dynamic-vlan Enable
Console(config-if-GigabitEthernet2)#
```

Relative Command

Command	Description
show dot1x port-control	show 802.1x interface information

17.25 show dot1x

show 802.1x settings.

show dot1x

Command mode

Enable mode

Configuration Example

```
Console#show dot1x
-------------------Dot1x Config-------------------
dot1x Enable              : Enable
total user number         : 1
authed user number        : 1
pae group addr            : true
reauth Enable             : disable
reauth period             : 300
active req                : disable
server timeout            : 10
supp timeout              : 5
tx timeout                : 5
req-max                   : 2
auth fail vlan attempts   : 3
multi mab quiet period    : 30
Console#
```

Relative Command

Command	Description
dot1x	Open 802.1x authentication device
dot1x re-auth	Configure re-authentication, requiring periodic re-authentication supplicant
dot1x req-max	Configuration Request / challenge packet retransmission times
dot1x pae-group-addr	Configure whether to use multicast address authentication
dot1x timeout re-authperiod	Set the re-authentication interval
dot1x timeout server-timeout	Set the server timeout
dot1x timeout supp-timeout	Timeout authentication exchange between Facilities and setting the supplicant
dot1x timeout tx-period	Configuration request / id packet retransmission interval
dot1x auth-fail max-attempt	Configure Authentication failed attempts

17.26 show dot1x port-control

Show 802.1x port setting information.

show dot1x port-control

Command mode

Enable mode

Configuration Example

```
Console#show dot1x port-control
Interface Mode  Method    Max-users Dynamic-vlan Guest-vlan Failed-vlan   MAB
Mab-timeout
g1        --    mac-based   64      disable      0          0           disable    --
g2        auto  mac-based   64      disable      3          0           disable    --
g3        --    mac-based   64      disable      0          0           disable    --
g4        auto  mac-based   64      disable      0          4           disable    --
g5        auto  mac-based   64      disable      0          0           multi-mab  0
g6        --    mac-based   64      disable      0          0           disable    --
g7        --    mac-based   64      disable      0          0           disable    --
g8        auto  mac-based   64      disable      0          0           single-mab 3600
……
```

Relative Command

Command	Description
dot1x port-control auto	802.1x port authentication turned on
dot1x port-control-mode	Configure port controlled mode
dot1x max-users	Limiting the maximum number of allowed ports to authenticate the client
dot1x guest-vlan	Configuration controlled port guest vlan
dot1x auth-fail vlan	Configuration controlled port authentication failure vlan
dot1x dynamic-vlan Enable	Configure port dynamic VLAN Jump

17.27 show dot1x auto-req

show Facilities initiates 802.1x authentication configuration information

show dot1x auto-req

Command mode

Enable mode

Configuration Example

```
Console#show dot1x auto-req
auto-Req: disable
user-Detect: Enable
packet-Num: 0
req-Interval: 30
```

Relative Command

```
Console#
```

Command	Description
dot1x auto-req	Configure the device initiates 802.1x authentication
dot1x auto-req packet-num	Configure the device initiates the number of authentication request packets
dot1x auto-req interval	Configure the device initiates an authentication request packet interval
dot1x auto-req user-detect	Set the device on a port if the user authentication by the presence of no longer take the initiative to issue an authentication request packet

17.28 show dot1x re-auth

show re-authentication configuration

show dot1x re-auth

Command mode

Enable mode

Configuration Example

```
Console#show dot1x re-auth
reauth Enable: disable

Console#
```

Relative Command

Command	Description
dot1x re-auth	Configure re-authentication

17.29 show dot1x summary

Show user authentication entries

show dot1x summary

Command mode

Enable mode

Configuration Example

```
Console#show dot1x summary
ID        MAC               Interface   VLAN      Auth-state
1         00:21:cc:bf:06:d3   4         2         Authenticated
Console#
```

Relative Command

Command	Description
dot1x	Open device 802.1x authentication function
dot1x port-control auto	802.1x port authentication turned on

17.30 show dot1x auth-address-table

show a list of hosts certification

show dot1x auth-address-table

Command mode

Enable mode

Configuration Example

```
Console#show dot1x auth-address-table
ID          Interface   MAC
1           4           00:30:ab:0a:c0:c6
Console#
```

Relative Command

Command	Description
dot1x auth-address-table address	Authentication configuration Host List

18 RADIUS

18.1 radius-server host

Specifies REDIS security server host address and password to communicate with the server share of the Command's no form to remove the specified host.

radius-server host {*ipv4-address* | *ipv6-address*} [**auth-port** *port-number*] [**test username** *name* [**idle-time** *time*]] [**key** *text-string*]

no radius-server host {*ipv4-address* | *ipv6-address*}

Parameter Description

Parameter	Description
ipv4-address	RADIUS security server host IPv4 address
ipv6-address	RADIUS security server host IPv6 address
auth-port *port-number*	RADIUS authentication and UDP port number
test username *name*	Username for the server is not reachable under the status active probing server is reachable, and to specify the active probe used.
idle-time *time*	Active detection device configured to send packets interval.
key *text-string*	Shared text passwords

Default Configuration

No specific RADIUS host.

Command mode

global configuration mode

Usage Guide

In order to use RADIUS for AAA security services, you must define RADIUS security server. You can use the Command define one or more RADIUS security server.

Configuration Example

```
Console(config)# radius-server host 192.168.2.99 key 1234
Console(config)#
```

Relative Command

Command	Description
aaa authentication	Defined AAA authentication method list
radius-server retransmit	Define RADIUS packet retransmission times
radius-server timeout	Define RADIUS timeout
radius-server dead-criteria	RADIUS security server defined criteria

	unreachable
radius-server deadtime	Defining Device stop time to the RADIUS security server unreachable status of sent packets

18.2 radius-server attribute

Configuration property type value.

radius attribute {sn *num* **| id** *attr-id* **| name** *attr-name* **} value** *attr-value* [**applied** *{authen | none }*]

no radius attribute sn

Parameter Description

Parameter	Description
sn *num*	The serial number of each attribute is assigned a unique serial number
id *attr-id*	Property ID
name *attr-name*	Property name
value *attr-value*	Property details
authen	This attribute applies to authenticated communication
none	The property does not apply to any communication

Command mode global configuration mode

Usage Guide Each attribute corresponding to the ID name specific reference rfc2865

Configuration Example

```
Console(config)# radius-server attribute id 26 value vendor-info applied authen
Console(config)#
```

Relative Command

Command	Description
show radius attribute	Show Attribute Type Value Configuration

18.3 radius-server retransmit

Configure the device that the RADIUS server is not safe frequency response before sending packets. The Command's no form to restore the default configuration

radius-server retransmit *retries*

no radius-server retransmit

Parameter Description

Parameter	Description
retries	RADIUS retransmission attempts times, the range is 1-100

Default Configuration

The default number of retransmissions to 3

Command mode

global configuration mode

Usage Guide

AAA premise to the next method to authenticate the user's current authentication security server does not respond. Analyzing server security device does not respond to standard security server equipment retransmission during a specified number of RADIUS packets did not answer, there is a timeout interval between each retransmission.

Configuration Example

Below is the number of retransmissions of Example 5:

```
Console(config)# radius-server retransmit 5
Console(config)#
```

Relative Command

Command	Description
radius-server host	Host and a shared password defined RADIUS security server
radius-server timeout	Define RADIUS packet timeout timer

18.4 radius-server timeout

Configuring RADIUS packet retransmission device waits secure server response time. The Command's no form to restore the default value.

radius-server timeout *seconds*

no radius-server timeout

Parameter Description

Parameter	Description
seconds	Timeout (in seconds). You can set the range of values from 1 to 1000 seconds.

Default Configuration

2 s

Command mode

global configuration mode

Usage Guide

Use the Command timeout for sending packets to adjust.

Configuration Example

Here is to set the timeout to 5 seconds examples:

```
Console(config)# radius-server timeout 5
```

```
Console(config)#
```

Relative Command

Command	Description
radius-server host	Host and a shared password defined RADIUS security server
radius-server retransmit	Define RADIUS packet retransmission times

18.5 radius-server dead-criteria

Configure the device determines RADIUS security server is unreachable standards. The Command's no form to restore the default value.

radius-server dead-criteria {time *seconds* [**retries** number] | **retries** number [**time** *seconds*]**}**

no radius-server dead-criteria

Parameter Description

Parameter	Description
time *seconds*	Configuration time conditions Parameter. Device does not receive the correct response packet from the RADIUS security server within the specified time, it considers that the RADIUS server security conditions are not satisfied longer reachable. You can set the range of 0 to 120 seconds.
retries number	Configuration request timeouts conditions Parameter. When the device sends a request to a RADIUS security server with the packet timeout times reaches the set number of times, it is considered that the RADIUS security server to meet unreachable timeouts conditions. The setting range is 0-100.

Default Configuration

time seconds The default is 60 seconds.
retries number The default value 10 times.

Command mode

global configuration mode

Usage Guide

If a RADIUS server security while meeting the conditions of time and request timeouts conditions, the device considers that the RADIUS security server is unreachable. Use the Command, the user can request timeout Parameter time conditions and the number of conditions to be adjusted.

Configuration Example

Below is the market is 120 seconds, the timeout is 20 times the number of examples:

```
Console(config)# radius-server dead-criteria time 120 retries 20
Console(config)#
```

Relative Command

Command	Description
radius-server host	Host and a shared password defined RADIUS security server
radius-server deadtime	Defined in the device to stop unreachable status of RADIUS security server sends a request message of the length of time
radius-server timeout	Define RADIUS packet timeout timer

18.6 radius-server deadtime

Configure the device to stop sending a request message to the length of time in the RADIUS server is unreachable status of security. The Command's no form to restore the default values.

radius-server deadtime *minutes*

no radius-server deadtime

Parameter Description

Parameter	Description
minutes	Configure the device to stop time in RADIUS security server unreachable status request is sent in minutes. The setting range is 0-1440 minutes (24 hours).

Default Configuration

The default value is 0 minutes (ie RADIUS security server fails, the device still sends a request to the RADIUS server)

Command mode

global configuration mode

Usage Guide

If the device on a RADIUS security server Active detection is Enabled, then this time Parameter for the RADIUS security server does not work; otherwise, the RADIUS security server in the specified time will be unreachable status for longer than the set time, is the unit automatically reverts to up status.

Configuration Example

Here is the setting stops transmission of 1 minute example:

```
Console(config)# radius-server deadtime 1
Console(config)#
```

Relative Command

Command	Description
radius-server host	Host and a shared password defined RADIUS security server

radius-server dead-criteria	RADIUS security server is unreachable defined criteria

18.7 show radius

Show RADIUS server all the configuration information

show radius

Command mode

global configuration mode

Configuration Example

```
Console(config)# show radius

radius global information:
   radius_retries            :      5
   radius_timeout            :      5
   radius_deadtime           :      0
   dead-criteria retries     :      20
   dead-criteria time        :      120

radius server information:
    Index       Ip address    AuthPort    AcctPort          Key    Status      Deathtime
   ----------------------------------------------------------------------------------------
       1      192.168.2.30       1812        1813      (not set)   Active          <N/A>
       2       192.168.2.5       1812        1813          1234    Active          <N/A>
   ----------------------------------------------------------------------------------------

radius attribute information:
      SN      Id              Name      Type            Value              applied
   ----------------------------------------------------------------------------------------
       1      26     Vendor-Specific    String        vendor-info             Authen
   ----------------------------------------------------------------------------------------

Console(config)#
```

Relative Command

Command	Description
radius-server host	Host and a shared password defined RADIUS security server
radius-server attribute	Configuring Attribute Type Value
radius-server retransmit	Define RADIUS packet retransmission times
radius-server timeout	Define RADIUS timeout
radius-server dead-criteria	RADIUS security server defined criteria unreachable
radius-server deadtime	Defining Device stop time to the RADIUS security server unreachable status of sent packets

18.8 show radius server

Show RADIUS server configuration.

show radius server

Command mode

global configuration mode

Configuration Example

```
Console(config)# show radius server
Server IP:              192.168.2.30
Accounting Port:        1813
Authen  Port:           1812
Test Username:          (not set)
Test Idle Time:         0 Minutes
Test Ports:             Authen and Accounting
Server State:           Active
        Current duration 03:44:06s, previous duration 03:44:06s
        Dead: total time 0s, count 0
        Statistics:
                Authen:         request 7,      timeouts 0
                Account:        request 0,      timeouts 0

Server IP:              192.168.2.5
Accounting Port:        1813
Authen  Port:           1812
Test Username:          (not set)
Test Idle Time:         0 Minutes
Test Ports:             Authen and Accounting
Server State:           Active
        Current duration 03:28:38s, previous duration 03:43:55s
        Dead: total time 0s, count 0
        Statistics:
                Authen:         request 7,      timeouts 21
                Account:        request 0,      timeouts 0

Console(config)#
```

Relative Command

Command	Description
radius-server host	Host and a shared password defined RADIUS security server

18.9 show radius attribute

show attribute type configuration

show radius attribute

Command mode

global configuration mode

Configuration Example

```
Console(config)# show radius attribute
Attribute SN:           1
        ID:             26
```

```
        name:          Vendor-Specific
        value:         vendor-info
        type:          String
        applied:       PAP  CHAP  EAPoL

Console(config)#
```

Relative Command

Command	Description
radius-server attribute	Configuring Attribute Type Value

19 TACACS+

19.1 tacacs-server host

Configuring TACACS server host IP address.

tacacs-server host *ip-address* [port *port-number*] [timeout *time*] [key *string*]

no tacacs-server host *ip-address*

Parameter Description

Parameter	Description
ip-address	TACACS + security server host ip address
port *port-number*	TACACS + TCP port, in the range 1-65535 is used to communicate.
timeout *time*	Timeout TACACS + host, in the range 1-1000, default is 5s.
ignore-auth-port	Close detection of RADIUS server authentication port security, Enabled by default.
key *string*	TACACS + client and server shared key.

Default Configuration

Not specified TACACS + host.

Command mode

global configuration mode

Usage Guide

In order to use TACACS + to achieve ASA security service, you must define the TACACS + security server. You can use the Command define one or more TACACS + security server.

Configuration Example

```
Console(config)# tacacs-server host 192.168.2.99
Console(config)#
```

Relative Command

Command	Description
aaa authentication	Defined AAA authentication method list
tacacs-server key	Sharing passwords globally defined TACACS + security server
tacacs-server timeout	Globally defined TACACS + server response packet timeout timer

19.2 tacacs-server key

Configuring TACACS global key.

tacacs-server key [*0* | *7*] *sting*

no tacacs-server key

Parameter Description

Parameter	Description
string	Shared text passwords

Default Configuration

It does not specify a shared password.

Command mode

global configuration mode

Usage Guide

The password is shared infrastructure and TACACS + security server to communicate properly. To make the device and the TACACS + security server can communicate, you must define the same shared password on the device and TACACS + security server. When we need to specify a different key for each server, we use the tacacs-server hostCommand realization of key options, where you can configure all servers through the global distribution key is not a configuration option key.

Configuration Example

The following is an example of the definition of a shared password TACACS + security server is abc:

```
Console(config)# tacacs-server key abc
Console(config)#
```

Relative Command

Command	Description
tacacs-server host	Host definitions TACACS + security server
tacacs-server timeout	Globally defined TACACS + server response packet timeout timer

19.3 tacacs-server timeout

When configured with the TACACS + server communication, the server waits for a global timeout. The Command's no form to restore the default configuration.

tacacs-server timeout *seconds*

no tacacs-server timeout

Parameter Description

Parameter	Description
seconds	Timeout (in seconds). Settable range 1-1000 seconds.

Default Configuration

5 s

Command mode

global configuration mode

Usage Guide

Use the Command response timeout time to adjust. When we need to specify a timeout for each server, use the tacacs-server hostCommand the timeout options to achieve, where you can configure the global configuration of all outstanding options to configure a server timeout timeout.

Configuration Example

Here is the timeout to 10 seconds examples:

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

Relative Command

Command	Description
tacacs-server host	Host definitions TACACS + security server
tacacs-server key	Sharing passwords globally defined TACACS + security server

19.4 tacacs-server attempts

Configuration and TACACS + server communications, the server attempts to authenticate the server times. The Command's no form to restore the default configuration

tacacs-server attempts numbers

no tacacs-server attempts

Parameter Description

Parameter	Description
numbers	Try certification number. Settable range 1-1000 seconds.

Default Configuration

3 times

Command mode

global configuration mode

Usage Guide

Use the Command attempts to authenticate the server can be configured times.

Configuration Example

Here is the attempt to authenticate to 10 examples:

```
Console(config)# tacacs-server attempts 10
Console(config)#
```

Relative Command

Command	Description
tacacs-server host	Host definitions TACACS + security server
tacacs-server key	Sharing passwords globally defined TACACS + security server

19.5 tacacs-client session-sock

Configuring TACACS + server communication with each share a session, that is, whether to keep the TCP connection. The Command's no form to restore the default value.

tacacs-client session-sock {*multi* **|** *only***}**

no tacacs-client session-sock

Parameter Description

Parameter	Description
multi	Each communication is to establish a new TCP connection
only	All communication uses the same TCP connection

Default Configuration

multi

Command mode

global configuration mode

Configuration Example

Here is an example of setting all communication share a TCP connection:

```
Console(config)# tacacs-client session-sock only
Console(config)#
```

Relative Command

Command	Description
tacacs-server host	Host definitions TACACS + security server

19.6 show tacacs

Interactive operation and show each TACACS + server.

show tacacs

Command mode

global configuration mode

Configuration Example

```
Console(config)# show tacacs
tacacs+ server: 192.168.2.99/49
Timeout: 5
Socket Opens: 0
Socket Closes: 0
Total Packets Sent: 0
Total Packets Recv: 0
Reference Count: 1

tacacs+ server default attempts: 3
tacacs+ server default timeout: 5
tacacs+ session sock num type: multi
Console(config)#
Console(config)#
```

Relative Command

Command	Description
tacacs-server host	Host definitions TACACS + security server
tacacs-server timeout	Globally defined TACACS + server response packet timeout timer
tacacs-client session-sock	Definition and TACACS + server communication shared TCP connection

20 GVRP

20.1 GVRP Enable

The Command Open GVRP function, use the Command's no restore default settings.

gvrp Enable

no gvrp Enable

Default Configuration Disable GVRP.

Command mode Global Mode and interface configuration mode

Usage Guide use show GVRP configurationCommand to view configuration.

Configuration Example

```
Console(config)#gvrp Enable
Console(config)# interface aggregateport 1
Console(config-if-AggregatePort 1)# grvp Enable
```

Relative Command

Command	Description
show gvrp configuration	Show GVRP configuration information

20.2 gvrp timer

The Command set three timer. Unit of time is 10ms.

gvrp timer {join |leave |leaveall}

no gvrp timer {join |leave |leaveall}

Parameter Description

Parameter	Description
join	To ensure reliable transmission of Join messages to other entities, GARP entity sends each Join message two times. The time interval between the two sending control Join timer.

leave	When a GARP entity expects to deregister a piece of attribute information, it sends out a Leave message, the message is received GARP entity starts Leave timer. If not received Join message again before the timer times out, it will deregister the attribute information .
leaveall	Once a GARP entity starts up, it starts LeaveAll timer. When the timer expires, GARP application entity sends a LeaveAll message so that other GARP entities can re-register all the attribute information on this entity. Then, the LeaveAll timer to begin a new cycle.

Default Configuration

the default is join:20; eave:60; leaveall:1000.

Command mode

Global Mode

Usage Guide

Use show GVRP configurationCommand to view configuration.

Configuration Example

```
Console(config)# gvrp timer join 40
```

Relative Command

Command	Description
show grvp configuration	Show GVRP configuration information

21 DHCP CLIENT

21.1 ipaddress vlan 1 ip-mode

Set the device to obtain dynamic static ip address.

ipaddress ip-mode [dhcp **|** static]

Parameter Description

Parameter	Description
ip-mode	Get the ip mode (dynamic or static)

Command mode global configuration mode

Usage Guide The Command set ip access way (dynamic or static).

Configuration Example

```
Console(config-if-vlan1)# ip address ip-mode dhcp
Console(config-if-vlan1)#
```

21.2 ip address dhcp

Under Dhcp mode device to retrieve ip address, reboot the device and DHCP to obtain the release of the ip address.

ipaddress dhcp [*renew* | *release*| *restart*]

Parameter Description

Parameter	Description
dhcp *renew*	Retrieve ip address
dhcp *release*	To obtain the release of the ip address
dhcp *restart*	Get ip address dhcp restart

Command mode global configuration mode

Usage Guide Dhcp under acquisition, restart and release ip address (you need to be set to dhcp mode).

Configuration Example Here is an example :(three Command were to acquire, restart, release)

```
Console(config-if-vlan1)# ip address dhcp  renew
Console(config-if-vlan1)# ip address dhcp  restart
Console(config-if-vlan1)# ip address dhcp  release
```

Relative Command

Command	Description

Ifconfig	To view the acquired ip address

22 FTP Client

22.1 Copy filename ftp: serveraddress

Export current configuration file, the configuration file must exist in / var / config (usually switch.conf)

Parameter Description

Filename: Profile serveraddress / var / config under: save the host ip export file

Command mode

Enable mode， global mode

Configuration Example

Here is an example of preservation:

```
Console#copy switch.conf ftp:192.168.2.59
send cmd TYPE I

ftp response:200 Type set to I.

send cmd PASV

ftp response:227 Entering Passive Mode (192,168,2,59,203,249).

send cmd STOR switch.conf

ftp response:125 Data connection already open; Transfer starting.

begin to write file!
##################################
send data over!size : 17721
download config file successed!
Console#
```

Relative Command

Command	Description
tftp get [-a|-o] <A.B.C.D> <servfilename> <localfilename>	Get files via FTP

22.2 Copy ftp:serveraddress serverfile

Switch configuration or firmware upgrades

Parameter Description

Parameter	Description
serveraddress	Host upgrade file saved

Serverfile Upgrade file in the File Name

Command mode

Enable mode and global mode

Configuration Example

```
Console#copy ftp: 192.168.2.59 vmlinux.bix upgrade.bin
get remote file vmlinux.bix

Please wait....
killall: msntp: no process killed
killall: snmpd: no process killed
Receive data...
########################################
########################################
########################################
########################################
########################################
########################################
########################################
########################################
########################################
########################################
#################
Get file from remote success!

Begin to check image!~
process dd file to mtdblock5
....!
```

Relative Command

Command	Description
system upgrade serveraddress vmlinux	Firmware Upgrade

23 Port Security

23.1 port-security violation

Open port security, port security and set the mishandling of. The Command's no form disable port security.

port-security violation {protect | restrict | shutdown}

no port-security violation

Parameter Description

Parameter	Description
protect	Found violations, it drops the offending packets.
restrict	Found violations, it drops the offending packets and sends the trap.
shutdown	Discovered violation, the packet is discarded, and shut down the interface to send Trap.

Default Configuration

Safety default interface is closed.

Command mode

interface configuration mode

Usage Guide

Use port security this feature, you can limit the maximum number of secure addresses on a port can be included, if the maximum number is set to 1 and the configuration of a security for the port address M, the workstation is connected to the port (its address as a configuration security M address) will be exclusive of all the broadband port.

Configuration Example

Here is the open port security on the interface 4, and set the mishandling of the shutdown:

```
Console(config)# interface GigabitEthernet 4
Console(config-if-GigabitEthernet4)# port-security violation shutdown
Console(config-if-GigabitEthernet4)#
```

Relative Command

Command	Description
show port-security interfaces GigabitEthernet 4	show port security setup information and address security.

23.2 port-security aging-time

Set the aging time for dynamic address learning. The Command's no form to restore the default value.

port-security aging-time *time*

no port-security aging-time

Parameter Description

Parameter	Description
time	Set up a dynamic address learning aging time, the range is 10-1000000, in seconds, if set to 0, then turn off the aging function.

Default Configuration

The default aging time is 300 seconds.

Command mode

interface configuration mode

Configuration Example

The following is a configuration port 4 address aging time to 200 seconds:

```
Console(config)# interface GigabitEthernet 4
Console(config-if-GigabitEthernet4)# port-security aging-time 200
Console(config-if-GigabitEthernet4)#
```

Relative Command

Command	Description
show port-security interfaces GigabitEthernet 4	show port security setup information and address security.

23.3 port-security mac-address

Interface mode manually configure a static secure addresses. Address of the Command's no form to remove the configuration

port-security mac-address *mac-addr* **vlan** *vlan-id*

no port-security mac-address *mac-addr* **vlan** *vlan-id*

Parameter Description

Parameter	Description
mac-address	Static address security
vlan-id	MAC address VID

Command mode interface configuration mode

Configuration Example Below is the interface at 4 to add a static address:

```
Console(config)# interface GigabitEthernet 4
Console(config-if-GigabitEthernet4)# port-security mac-address 00:30:ab:0a:c0:c6 vlan 1
Console(config-if-GigabitEthernet4)#
```

Relative Command

Command	Description
show port-security interfaces GigabitEthernet 4	show port security setup information and address security.

23.4 por-security max-mac-count

Set the port security maximum number of addresses. The Command's no form to restore the default number.

port-security max-mac-count *num*

no port-security max-mac-count

Parameter Description

Parameter	Description
num	Maximum Security number address, in the range 1-8191

Default Configuration The default is 128.

Command interface configuration mode

mode

Usage Guide The number of security address contains static configuration and dynamic learning secure address number of the sum.

Configuration Example Here are 4 set the port security maximum number of addresses is 2:

```
Console(config)# interface GigabitEthernet 4
Console(config-if-GigabitEthernet4)# port-security max-mac-count 2
Console(config-if-GigabitEthernet4)#
```

Relative Command

Command	Description
show port-security interfaces GigabitEthernet 4	show port security setup information and address security.

23.5 port-security mac-address stick

The dynamically learned addresses paste forcibly converted to static address.

port-security mac-address stick

Command mode interface configuration mode

Configuration Example Here is a 4 port is currently under study to address forced paste into static address:

```
Console(config)# interface GigabitEthernet 4
Console(config-if-GigabitEthernet4)# port-security mac-address stick
Console(config-if-GigabitEthernet4)#
```

Relative Command

Command	Description
show port-security interfaces GigabitEthernet 4	show port security setup information and address security.

23.6 port-security block

Configuring Blacklist MAC address. Corresponding unblock Command to remove it from the blacklist.

port-security block {src-mac | dst-mac} *mac-addr* **vlan** *vlan-id*

port-security unblock {src-mac | dst-mac} *mac-addr* **vlan** *vlan-id*

Parameter Description

Parameter	Description
src-mac	Source MAC address blacklist

dst-mac	Destination MAC address blacklist
mac-addr	MAC address
vlan-id	VID MAC address

Command mode

interface configuration mode

Configuration Example

Here is the source MAC address of 00: 30: ab: 0a: c0: c6, vid = 1 Blacklist:

```
Console(config)# interface GigabitEthernet 4
Console(config-if-GigabitEthernet4)# port-security block src-mac
00:30:ab:0a:c0:c6 vlan 1
Console(config-if-GigabitEthernet4)#
```

Relative Command

Command	Description
show port-security interfaces GigabitEthernet 4	show port security setup information and address security.

23.7 port-security clear mac-table unicast

Clear specify the type of unicast address.

port-security clear mac-table unicat {static | dynamic | violation | all}

Parameter Description

Parameter	Description
static	Delete the static address security
dynamic	Remove dynamically learned addresses
violation	Remove illegal status of address
all	Deletes all unicast addresses

Command mode

interface configuration mode

Configuration Example

Below it is safe to delete the static address examples:

```
Console(config)# interface GigabitEthernet 4
Console(config-if-GigabitEthernet4)# port-security clear mac-table unicast static
Console(config-if-GigabitEthernet4)#
```

Relative Command

Command	Description
show port-security	show port security setup information and address security.

23.8 show port-security

show port security setting information and address security

show port-security [interfaces GigabitEthernet port-number**]**

Command mode

interface configuration mode

Configuration Example

```
Console(config-if-GigabitEthernet4)# show port-security
------------ Port security Information-------------
       Violation mode: : restrict
            Age time: : 300
        Max mac count: : 2

Vlan       MAC Address          Type       Interface
---------- ------------------- -------- --------------------
1          02:31:AC:0B:C0:C2    Violation  GigabitEthernet 4
1          02:30:AB:0A:C0:C9    DYNAMIC    GigabitEthernet 4
1          00:30:AB:0A:C0:C6    DYNAMIC    GigabitEthernet 4
Console(config-if-GigabitEthernet4)#
```

Relative Command

Command	Description
port-security violation	Open port security, port security and set violation
port-security aging-time	Set the aging time for dynamic address learning
port-security mac-address	Configure static secure address
port-security max-mac-count	Set the port security maximum number of addresses
port-security mac-address stick	Dynamic address learning compulsory paste into static address
port-security block	MAC address block

24 Trunk & LACP

24.1 aggregateport load-balance

Configuring AP global traffic balancing algorithm, the Command's no form of the global flow balance settings to their default values.

aggregateport load-balance { dst-mac | src-mac | src-dst-mac | dst-ip | src-ip | src-dst-ip}

no aggregateport load-balance

Parameter Description

Parameter	Description
dst-mac	Traffic distribution according to the input packet destination MAC address. Each link in the AP, the same destination address of the packet is sent to the same port, the destination MAC different packets assigned to different ports.
src-mac	Traffic distribution according to the input packets based on source MAC address. AP in each link, packets of different MAC addresses assigned to packets of different ports, the same MAC address use the same port.
src-dst-mac	Traffic distribution according to the source MAC and destination MAC. Different source and destination MAC MAC + flow through different port forwarding, the same source and destination MAC MAC + forwarded through the same link.
dst-ip	Traffic distribution according to the input packet destination IP address. Each link in the AP, the destination IP address of the same packet is sent to the same port, destination IP different packets assigned to different ports.
src-ip	Traffic distribution according to the input packets based on source IP address. AP in each link, packets of different IP address assigned to a different port, the packet the same IP address use the same port.
src-dst-ip	Assign IP traffic based on source and destination IP. Different source IP + destination IP traffic through a different port forwarding, IP + the same source and destination IP forwarding through the same link.

Default Configuration

Traffic distribution according to the input packets based on source MAC address and destination MAC address

Command mode

global configuration mode

Usage Guide -

Configuration Example Configuring AP global traffic balancing algorithm based on the destination MAC address:

```
Console(config)# aggregateport load-balance dst-mac
Console(config)#
```

Relative Command

Command	Description
show aggregateport	show Aggregate Port configuration information

24.2 port-group

A physical Ethernet port is set to AP static member port or LACP dynamic member port, the Command's no form to remove Aggregate Port member property of the port.

port-group *key-number* **mode {static | active | passive}**

no port-group mode {static | active | passive}

Parameter Description

Parameter	Description
key-number	AP member port group number that AP interface number
static	The port is set to AP static member port
active	The polymerization mode indicates the port will initiate LACP aggregation operations.
passive	The polymerization mode indicates that the port will not initiate LACP aggregation operation, but after receiving the neighbor LACP packets LACP passive participation calculations.

Default Configuration Ethernet physical port by default does not belong to any AP

Command mode interface configuration mode and range interface configuration mode

Configuration Example The following example is configured as two Ethernet AP 4 LACP dynamic member, and the polymerization mode to active mode:

```
Console(config)# interface GigabitEthernet 2
Console(config-if-GigabitEthernet2)# port-group 4 mode active
```

Relative Command

Command	Description
show aggregateport	show Aggregate Port configuration information

show lacp	show LACP link aggregation port configuration and status information

24.3 lacp Enable

Global Enabling LACP dynamic link aggregation function. The Command's no form to disable LACP function

lacp Enable

no lacp Enable

Default Configuration The default LACP disabled

Command mode global configuration mode

Configuration Example The following are examples of functions Enable LACP:

```
Console(config)# lacp Enable
Console(config)#
```

Relative Command

Command	Description
show lacp	show LACP link aggregation port configuration and status information

24.4 lacp system-priority

Configuring LACP system priority. The Command's no form to restore the default value.

lacp system-priority *system-priority*

no lacp system-priority

Parameter Description

Parameter	Description
system-priority	LACP system priority can be set to a value in the range 1-65535.

Default Configuration The default is 1

Command mode global configuration mode

Configuration Below is the LACP system priority to Example 10:

Example

```
Console(config)# lacp system-priority 10
Console(config)#
```

Relative Command

Command	Description
show lacp	show LACP link aggregation port configuration and status information

24.5 lacp tick-time

Set tick-time for LACP function. The Command's no form to restore the default value.

lacp tick-time *<mill-sec>*

no lacp tick-time

Parameter Description

Parameter	Description
tick-time *<mill-sec>*	LACP time-time, in milliseconds, in the range of 50 to 5000 ms

Default Configuration

The default value is 500 milliseconds.

Command mode

global configuration mode

Configuration Example

Below is the TCP heartbeat is 1 second example:

```
Console(config)# lacp tick-time 1000
Console(config)#
```

Relative Command

Command	Description
show lacp	show LACP link aggregation port configuration and status information

24.6 lacp port-priority

Configuring LACP AP member interface port priority, the Command's no form to restore the default value.

lacp port-priority *port-priority*

no lacp port-priority

Parameter Description

Parameter	Description
port-priority	LACP port priority of a port, in the range 0-65535

Default Configuration

The default value is 1

Command mode

interface configuration mode and range interface configuration mode

Configuration Example

Below is the port Port Priority 2 for example 222:

```
Console(config)# interface GigabitEthernet 2
Console(config-if-GigabitEthernet2)# lacp port-priority 222
```

Relative Command

Command	Description
radius-server host	Host and a shared password defined RADIUS security server
radius-server dead-criteria	RADIUS security server is unreachable defined criteria

24.7 lacp admin-key

Configuring LACP AP member port management KEY value of the Command's no form to restore the default value.

lacp admin-key *key-value*

no lacp admin-key

Parameter Description

Parameter	Description
key-value	Management KEY value of the port, in the range 0-65535

Default Configuration

The default value is 1

Command mode

interface configuration mode and range interface configuration mode

Usage Guide

-

Configuration Example

The following is a configuration management port 2 KEY 100 is an example:

```
Console(config)# interface GigabitEthernet 2
Console(config-if-GigabitEthernet2)# lacp admin-key 100
```

Relative

Command	Description

Command

show lacp	show LACP link aggregation port configuration and status information

24.8 show aggregateport

show Aggregate Port configuration information

show aggregateport { load-balance | [*aggregate-port-number*] **summary}**

Parameter Description

Parameter	Description
load-balance	show AP traffic balancing algorithm
aggregate-port-number	AP interface number
summary	Show AP summary information in each or all of the links

Command mode

Each mode can be executed

Configuration Example

The following are examples show:

```
Console#show aggregateport summary
|AggregatePort |MaxPorts     |Status |Ports
-----------------------------------------------------
Ag1          8         Enabled     Gi0/6  ,Gi0/7
Console#
Console#show aggregateport load-balance
Load-balance    : Destination MAC
Console#
```

Relative Command

Command	Description
aggregateport load-balance	Configure the global flow of the AP-balancing algorithms
port-group	A physical Ethernet port is set to AP static member ports or dynamic member ports LACP

24.9 show lacp

show LACP link aggregation port configuration and status information.

show lacp [agg**]**

Parameter Description

Parameter	Description
agg	show LACP link aggregation status information

Command mode

global configuration mode

Configuration Example

The following are examples show:

```
Console(config)# show lacp

        lacp status                :disable
        system id                  :-561323774
        system priority             :1
        tick times                 :500 ms


           Port | Link Status    Priority    Admin Key    Agg Id    Agg Mode
         -------- ------------ --------- ---------- ------ --------
           Gi0/1    Down          1          1          0        NULL
           Gi0/2    Up            1          1          1        Active
           Gi0/3    Down          1          1          0        NULL
           Gi0/4    Up            1          1          1        Active
           Gi0/5    Down          1          1          0        NULL
           Gi0/6    Down          1          1          0        NULL
           Gi0/7    Down          1          1          0        NULL
           Gi0/8    Down          1          1          0        NULL
           Gi0/9    Down          1          1          0        NULL
           Gi0/10   Down          1          1          0        NULL
           Gi0/11   Down          1          1          0        NULL
           Gi0/12   Down          1          1          0        NULL
           Gi0/13   Down          1          1          0        NULL
           Gi0/14   Up            1          1          0        NULL
           Gi0/15   Down          1          1          0        NULL
           Gi0/16   Down          1          1          0        NULL
 __More__
Console(config)#
Console(config)# show lacp agg

Flags: S - Device is requesting Slow LACPDUs
        F - Device is requesting Fast LACPDUs.
        A - Device is in active mode.
        P - Device is in passive mode.
Aggregate Id 1:

             Port | Flags    State    Priority    Oper Key    Number    Actor State
Partner State
           Gi0/4    SA       susp     1           3           4         0xcd000000
0x43000000
           Gi0/2    SA       susp     1           3           2         0xcd000000
0x43000000
```

```
Console(config)#
```

Relative Command

Command	Description
lacp Enable	Global Enabling LACP dynamic link aggregation
lacp system-priority	Configuring LACP system priority
lacp tick-time	Setting LACP function heartbeat
lacp port-priority	Configuring LACP AP member interface port priority
lacp admin-key	Configuring LACP AP member port management KEY value

25 Monitor

25.1 monitor session

Configure mirror source and destination ports

monitor session <1-4> source interface <1-26> {both | rx | tx}

monitor session <1-4> destination interface <1-26>

monitor session <1-4> source interface <1-26> acl *name* **[rx]**

no monitor session <1-4> source interface <1-26> {both | rx | tx}

no monitor session <1-4> source interface <1-26> acl *name*

no monitor session <1-4> destination

no monitor session all

no monitor session all

no monitor session <1-4>

Parameter Description

Parameter	Description
both	Two-terminal transmission and reception of packets can be mirrored to
rx	Mirroring receiving port traffic
tx	Send mirror port traffic
acl *name*	ACL policy name or id

Default Configuration

--

Command mode

global configuration mode

Usage Guide

Enable port mirroring, all packets on the source port will be a copy is forwarded to the destination port, usually connected to a packet analyzer analyze source port of the packet destination port on the situation, multiple ports can be mirrored to a destination port .

Configuration Example

Configure port 2 packet traffic mirroring to 6:

```
Console(config)#  monitor session 1 source interface 2
Console(config)# monitor session 1 destination interface 6
```

Relative Command

Command	Description

Console(config)# show monitor	show mirroring setup information

25.2 show monitor

show monitor Port setting information

show monitor

Command mode

Each mode can be executed

Configuration Example

```
Console(config)# show monitor
monitor session: 1

Source ports:
RX port: 3
TX port: 3
Flow monitor source:
ACL Name: 700
RX port: 2
Destination interface: GigabitEthernet 0/1
```

26 ERPS-Ethernet Ring Protection Switching

26.1 erps ring ring-id rplowner

The Command is used to create ERPS ring, and the device is set to ring RPL owner node.

erps ring *ring-id* **rplowner vlan** *vlan-id* **non_rpl interface GigabitEthernet** *port-num* **rpl interface GigabitEthernet** *port-num*

Parameter Description

Parameter	Description
ring-id	ERPS ring ID, in the range 1-239
vlan-id	ERPS ring belongs to VLAN
non_rpl interface GigabitEthernet *port-num*	Non-RPL link the ports
rpl interface GigabitEthernet *port-num*	RPL link the ports

Default Configuration

--

Command mode

global configuration mode

Usage Guide

The Command for creating RPL owner node, each ring and only need to configure a link RPL, RPL both ends of the link are connected RPL owner node and RPL neighbor node.

Configuration Example

Here is an example of the establishment of ERPS ring 1 RPL Owner node, wherein the port 6 to RPL link the ports of:

```
Console(config)# erps ring 1 rplowner vlan 1 non_rpl interface GigabitEthernet 2
rpl interface GigabitEthernet 6
Console(config)#
```

Relative Command

Command	Description
show erps ring	show ERPS ring Parameter and status

26.2 erps ring ring-id rplneighbor

The Command is used to create ERPS ring, and the device is set to ring RPL neighbor node.

erps ring *ring-id* **rplneighbor vlan** *vlan-id* **non_rpl interface GigabitEthernet** *port-num* **rpl interface GigabitEthernet** *port-num*

Parameter Description

Parameter	Description
ring-id	ERPS ring ID, in the range 1-239
vlan-id	ERPS ring belongs to VLAN
non_rpl interface GigabitEthernet *port-num*	Non-RPL link the ports
rpl interface GigabitEthernet *port-num*	RPL link the ports

Command mode

global configuration mode

Usage Guide

The Command for creating RPL neighbor node, and each ring only need to configure a link RPL, RPL both ends of the link are connected RPL owner node and RPL neighbor node.

Configuration Example

Here is an example of the establishment of ERPS ring 1 RPL neighbor node, wherein the port 6 to RPL link the ports of:

```
Console(config)# erps ring 1 rplneighbor vlan 1 non_rpl interface GigabitEthernet 2
rpl interface GigabitEthernet 6
Console(config)#
```

Relative Command

Command	Description
show erps ring	show ERPS ring Parameter and status

26.3 erps ring ring-id common

The Command is used to create ERPS ring, and the device is set to ring in the ordinary nodes.

erps ring *ring-id* **common vlan** *vlan-id* **primary interface GigabitEthernet** *port-num* **secondary interface GigabitEthernet** *port-num*

Parameter Description

Parameter	Description
ring-id	ERPS ring ID, in the range 1-239
vlan-id	ERPS ring belongs to VLAN
primary interface GigabitEthernet *port-num*	A ring port to ERPS
secondary interface GigabitEthernet *port-num*	Join ERPS ring port two

Command mode

global configuration mode

Usage Guide

The Command is used to create RPM common node, ERPS ring node link-Africa RPL should be configured as an ordinary node, in addition to a ring RPL owner and neighbor nodes, the rest are ordinary nodes.

Configuration Example

Here is an example of the establishment of ERPS ring 1 RPL common node:

```
Console(config)# erps ring 1 common vlan 1 primary interface GigabitEthernet 2
secondary interface GigabitEthernet 6
Console(config)#
```

Relative Command

Command	Description
show erps ring	show ERPS ring Parameter and status

26.4 erps ring ring-id Enable

The Command is used to Enable a ERPS ring. The Command's no form to disable the ring.

erps ring *ring-id* **Enable**

no erps ring *ring-id* **Enable**

Parameter Description

Parameter	Description
ring-id	ERPS ring ID, in the range 1-239

Default Configuration

By default, the disabled

Command mode

global configuration mode

Configuration Example

Here is an example of ERPS Enable ring 1:

```
Console(config)# erps ring 1 Enable
Console(config)#
```

Relative Command

Command	Description
show erps ring	show ERPS ring Parameter and status

26.5 erps ring ring-id fs

The Command used to impose a ring is blocking a port blocking status.

erps ring *ring-id* **fs interface GigabitEthernet** *port-num*

Parameter Description

Parameter	Description
ring-id	ERPS ring ID, in the range 1-239
port-num	Forced to block the port status

Command mode

global configuration mode

Usage Guide

After forcibly set blocking status, the port can not be automatically switched to the forwarding status, can only be restored through clearCommand.

Configuration Example

Below are forced ERPS ring 1 port 2 is blocked status examples:

```
Console(config)# erps ring 1 fs interface GigabitEthernet 2
Console(config)#
```

Relative Command

Command	Description
erps ring *ring-id* **clear**	The ring to recover from a manual or forced blocking status of
show erps ring	show ERPS ring Parameter and status

26.6 erps ring ring-id ms

The Command used to manually set up a ring of blocking a port blocking status.

erps ring *ring-id* **ms interface GigabitEthernet** *port-num*

Parameter Description

Parameter	Description
ring-id	ERPS ring ID, in the range 1-239
port-num	Forced to block the port status

Default Configuration

--

Command mode global configuration mode

Usage Guide After manually set to blocking status, the port can then be automatically switched to the forwarding status, you can also clearCommand recovery.

Configuration Example Here is manually set ERPS ring 1 port 2 is blocked status examples:

```
Console(config)# erps ring 1 ms interface GigabitEthernet 2
Console(config)#
```

Relative Command

Command	Description
erps ring *ring-id* **clear**	The ring to recover from a manual or forced blocking status of
show erps ring	show ERPS ring Parameter and status

26.7 erps ring ring-id clear

The Central Command is used to recover from a manual or forced blocking status in.

erps ring *ring-id* **clear**

Parameter Description

Parameter	Description
ring-id	ERPS ring ID, in the range 1-239

Command mode global configuration mode

Configuration Example Here is an example ERPS ring 1 to recover from manual / force in blocking status:

```
Console(config)# erps ring 1 clear
Console(config)#
```

Relative Command

Command	Description
erps ring *ring-id* **fs**	Forced a ring is blocking a port blocking status
erps ring *ring-id* **ms**	Manually set a ring is blocking a port blocking status

26.8 erps ring ring-id subring

The Command for setting the sub-loop of interconnected nodes.

erps ring *ring-id* **subring {rplowner rpl | rplneighbor rpl | common} interface GigabitEthernet** *port-num* **[primary | secondary]**

Parameter Description

Parameter	Description
ring-id	ERPS ring ID, in the range 1-239
rplowner	The switch is set for the sub-ring RPL owner node
rplneighbor	The switch is set for the sub-ring RPL neighbor node
common	The switch is set for the sub-loop ordinary nodes
port-num	Sub-interfaces on the ring of interconnected nodes located
primary	As two interconnected nodes master node is responsible for the sub-loop transmit connectivity check messages
secondary	As Vice node two interconnected nodes, the default is secondary

Command mode

global configuration mode

Usage Guide

Child node on the ring interconnect only one interface, the primary ring and sub-ring must be in the same VLAN inside. Two interconnected nodes, you need to set a primary master node, another deputy to secondary nodes.

Configuration Example

The following are the main ring interconnect to create a sub-ring 2, for example, and set your own sub-ring RPL owner node:

```
Console(config)# erps ring 1 subring 2 rplowner rpl interface GigabitEthernet 8 primary
Console(config)#
```

Relative Command

Command	Description
show erps ring	show ERPS ring Parameter and status

26.9 erps ring ring-id ring_role

The Central Command for setting the role of the main ring or sub-rings.

erps ring *ring-id* **ring_role {master | sub}**

Parameter Description

Parameter	Description
ring-id	ERPS ring ID, in the range 1-239
master	master ring

sub	Sub ring

Default Configuration

The default

Command mode

global configuration mode

Usage Guide

-

Configuration Example

Here is an example of setting ERPS ring 2 sub-ring:

```
Console(config)# erps ring 2 ring_role sub
Console(config)#
```

Relative Command

Command	Description
show erps ring	show ERPS ring Parameter and status

26.10 erps ring ring-id mode

Command mode is used to set the ring is reversible or irreversible.

erps ring *ring-id* **mode {revertive | non_revertive}**

Parameter Description

Parameter	Description
ring-id	ERPS ring ID, in the range 1-239
revertive	Reversible
non_revertive	irreversible

Default Configuration

The default is reversible

Command mode

global configuration mode

Usage Guide

-

Configuration Example

Here is a set ERPS ring irreversible examples:

```
Console(config)# erps ring 1 mode non_revertive
Console(config)#
```

Relative Command

Command	Description

show erps ring	show ERPS ring Parameter and status

26.11 erps ring ring-id mac

Here is a set ERPS ring irreversible examples:

erps ring *ring-id* **mac** *mac-addr*

Parameter Description

Parameter	Description
ring-id	ERPS ring ID, in the range 1-239
mac-addr	MAC address

Default Configuration

The default is reversible

Command mode

global configuration mode

Usage Guide

-

Configuration Example

Here is an example of setting ERPS ring 1 source mac address:

```
Console(config)# erps ring 1 mac 00:00:02:23:32:22
Console(config)#
```

Relative Command

Command	Description
show erps ring	show ERPS ring Parameter and status

26.12 erps delete ring

Command used to delete the ring.

erps delete ring *ring-id*

Parameter Description

Parameter	Description
ring-id	ERPS ring ID, in the range 1-239

Default Configuration

The default is reversible

Command mode global configuration mode

Usage Guide -

Configuration Example Here is an example of deleting the ring:

```
Console(config)# erps delete ring 1
Console(config)#
```

Relative Command

Command	Description
erps ring *ring-id* **rplowner**	Create ERPS ring, and the device is set to ring RPL owner node
erps ring *ring-id* **rplneighbor**	Create ERPS ring, and the device is set to ring RPL neighbor node
erps ring *ring-id* **common**	Create ERPS ring, and the device is set to ring in the ordinary nodes
erps ring *ring-id* **subring**	Set of interconnected nodes ringlet

26.13 erps timeout

The Command is used to configure each ERPS timer. The Command's no form to restore the default value.

erps timeout {wtr_timeout *interval1***| guard_timeout** *interval2***| holdoff_timeout** *interval3***}**

Parameter Description

Parameter	Description
wtr_timeout *interval1*	WTR timer value, in minutes, range 1-12, default is 5 minutes
guard_timeout *interval2*	Guard timer value, in milliseconds, in the range of 10-2000, the default is 500 milliseconds
holdoff_timeout *interval3*	Holdoff timer value, in milliseconds, in the range 0-10000, default is 0

Default Configuration WTL timer default is five minutes; Guard timer default is 500 milliseconds; Holdoff timer default is 0 milliseconds.

Command mode global configuration mode

Usage Guide WTR (Wait-to-restore) timer: This timer is only for RPL owner device, and other devices - effect. This timer is used to prevent RPL owner of the ring network status misjudgment. When the RPL owner detects a fault recovery is not performed immediately switched topology, but after the WTR timer expires and so,

if it is confirmed Ethernet indeed recovered from the fault, only perform topology switching. If the timer expires before the WTR ring again detected a fault, the WTR timer is canceled, no longer perform topology switching.
Guar timer: The timer is used to prevent the device from receiving outdated R-APS message. When the device detects link recovery from a failure, it sends link recovery message packets, and starts the timer guard. Prior to guard timer expires, in addition to indicating sub-ring topology changes flush packets, other packets will be directly discarded without processing.
Holdoff timer: The timer is used to prevent intermittent link failure, causing ERPS constantly switching topology. After configuring the timer when it detects a link fault, ERPS not perform topology switching immediately, but after the timer times out, etc., if it is confirmed a link failure is still only perform topology switching.

Configuration Example

Here is the WRT set a time of 1 minute example:

```
Console(config)# erps timeout wtr_timeout 1
Console(config)#
```

Relative Command

Command	Description
show erps timeout	Show ERPS each timer configuration value

26.14 show erps ring

show ERPS ring Parameter and status

show erps ring

Command mode

global configuration mode

Configuration Example

```
Here is the show ring examples:
Console(config)# show erps ring
############################################################
Ring id          : 1
Raps Channel     : 1
Node Role        : RPLOWNER
Ring Role        : Major
Revertive Mode   : Revertive
Ring Enable      : Enable
Machine State    : PROTECTION
Local Pri        : LOCAL_SF
Local Node Id    : 00:00:22:33:44:55
RPL port         : 4 Link State : link down State : Discard
Non RPL port     : 2 Link State : link down State : Discard
Timer            : Stop
Send Pkt Timer   : Yes
############################################################

Console(config)#
```

Relative

Command	Description

Command

erps ring *ring-id* **rplowner**	Create ERPS ring, and the device is set to ring RPL owner node
erps ring *ring-id* **rplneighbor**	Create ERPS ring, and the device is set to ring RPL neighbor node
erps ring *ring-id* **common**	Create ERPS ring, and the device is set to ring in the ordinary nodes
erps ring *ring-id* **Enable**	Enable ERPS ring
erps ring *ring-id* **fs**	Forced a ring is blocking a port blocking status
erps ring *ring-id* **ms**	Manually set a ring is blocking a port blocking status
erps ring *ring-id* **subring**	Set of interconnected nodes ringlet
erps ring *ring-id* **ring_role**	Set role-based ring or a ring of sub-rings
erps ring *ring-id* **mode**	Setting mode ring is reversible or irreversible
erps ring *ring-id* **mac**	Set the source mac address of the device node in a ring used

26.15 show erps timeout

Show ERPS each timer configuration value

show erps timeout {wtr_timeout | guard_timeout | holdoff_timeout}

Parameter Description

Parameter	Description
wtr_timeout	show WTR timer value
guard_timeout	Show Guard timer value
holdoff_timeout	Show Holdoff timer value

Default Configuration

-

Command mode

global configuration mode

Usage Guide

-

Configuration Example

```
The following are examples show:
Console(config)# show erps timeout wtr_timeout
erps wtr timeout: 5 min
Console(config)#
```

Relative Command

Command	Description
erps timeout	Configuring ERPS each timeout period

27 Loopback

27.1 loopback

Enable loopback test function

loopback

no loopback

Default Configuration By default, it is disabled

Command mode global configuration mode

Usage Guide Use the loopback test to verify that the Ethernet port is working properly.

Configuration Example

```
Configure loop detection to be Enabled:
Console(config)# loopback
```

Relative Command

command	description
show loopback	Show loopback configuration

27.2 loopback action

Set the port loop behavior

Loopback action {shutdown|block |warning}

Parameter Description

command	
shutdown	After the port loop is found, the port is down
block	After the loop is found, the port can only pass BPDU and loop detection packets
warning	The loop is found to send out alarm information

Default Configuration -

Command mode global configuration mode

Usage Guide If a loop is present, the port will not resume the controlled state by default after a

controlled operation.

Configuration Example

Example of Port Blocking When Setting Loop:

Console(config)# loopback action block

Relative Command

command	description
show loopback	Show loopback configuration

27.3 loopback time

Set the loop detection time

Loopback time <10-3600>

Default Configuration

60 s

Command mode

global configuration mode

Usage Guide

If there is a loop, the port is detected once after the set time.

Configuration Example

Set the loop once every 100 seconds.

Console(config)# loopback time 100

Relative Command

command	description
show loopback	Show loopback configuration

27.4 show loopback

Show loopback configuration information

show loopback

Command mode

global configuration mode

Configuration Example

Here's an example:

```
Console(config)# show loopback
loopback info:
-----------------------------------------------------
      global Enable: Yes
            times: 100
           action: block
      debug level: 1
```