



## Command Line Manual

Rev.1.2

Applicable for below models:

BSD-PS2010G, BSD-3430P, BSD-4804P10, BSD-4804P10800

## Preface

The purpose of this document is to provide software engineers with general information about the use of switch source files for chip development by the switch team.

Although every effort has been made to ensure that this document is up-to-date and accurate, more information may have been updated since this guide was prepared.

## Version record

Version	Time	Description
1.0	-	First draft
1.1	2019-08-31	Add Static Routing
1.2	2020-10-20	Add RSTP and IPV6

---

## Contents

### Contents

1. Use the command line .....	14
Local login through the console port.....	Error! Bookmark not defined.
Login via telnet .....	Error! Bookmark not defined.
Login via SSH .....	Error! Bookmark not defined.
Password authentication mode.....	15
Command line mode .....	Error! Bookmark not defined.7
Description .....	17
Command line security level.....	18
Command line format convention .....	Error! Bookmark not defined.
Basic format convention .....	Error! Bookmark not defined.
Special characters .....	Error! Bookmark not defined.
Shortcut list .....	19
Page shortcut table .....	Error! Bookmark not defined.
Various signs .....	Error! Bookmark not defined.
Error message .....	20
2. AAA .....	21
AAA authentication .....	21
login authentication .....	22
ip http login authentication .....	23
enable authentication .....	24
show aaa authentication .....	25
show line lists .....	26
tacacs default-config .....	27
tacacs host .....	28
show tacacs default-config .....	29
show tacacs .....	29
show default-config .....	30
radius host .....	31
show radius default-config .....	32
show radius .....	32
3. ACL .....	34
mac acl .....	34
permit (MAC) .....	34
deny (MAC) .....	35
ip acl .....	36
permit (IP) .....	37
deny (IP) .....	39
ipv6 acl .....	41
permit (IPv6) .....	41
deny (IPv6) .....	43
bind acl .....	45

---

show acl .....	45
show acl utilization .....	46
4. Administration .....	48
configure .....	48
clear arp .....	48
clear service .....	49
enable .....	49
end .....	50
exit .....	51
history .....	51
hostname .....	53
interface .....	54
ip address .....	54
ip default-gateway .....	55
ip dhcp .....	56
ip dns .....	56
ip dns lookup .....	57
ipv6 autoconfig.....	58
ipv6 address .....	59
ipv6 default-gateway.....	60
ipv6 dhcp .....	60
ip service .....	61
ip session-timeout .....	62
ip ssh .....	63
line .....	64
reboot .....	65
enable password .....	66
exec-timeout .....	66
password-thresh .....	68
ping .....	69
traceroute .....	70
silent-time .....	70
ssl .....	71
system name .....	72
system contact .....	72
system location .....	73
terminal length .....	74
username .....	75
show arp .....	76
show cpu utilization .....	76
show history .....	77
show info .....	78
show ip .....	78
show ip dhcp .....	79

---

show ip dns .....	79
show ip http .....	80
show ipv6 .....	80
show ipv6 dhcp .....	81
show line .....	81
show memory statistics .....	82
show privilege .....	83
show username .....	83
show users .....	84
show version .....	85
5. AuthenticationManager .....	86
authentication .....	86
authentication(Interface) .....	86
authentication mac radius .....	87
authentication mac local .....	88
authentication guest-vlan .....	89
authentication guest-vlan (Interface) .....	90
authentication host-mode .....	90
authentication max-hosts .....	91
authentication port-control .....	92
clear authentication sessions .....	93
show authentication .....	94
show authentication sessions .....	96
6. Diagnostic .....	98
show cable-diag .....	98
show fiber-transceiver .....	98
7. DHCP Snooping .....	100
ip dhcp snooping .....	100
ip dhcp snooping vlan .....	100
ip dhcp snooping trust.....	101
ip dhcp snooping verify .....	102
ip dhcp snooping rate-limit .....	102
clear ip dhcp snooping statistics.....	103
show ip dhcp snooping.....	104
8. DOS .....	105
dos .....	105
dos(interface) .....	106
show dos .....	107
9. Dynamic ARP Inspection .....	109
ip arp inspection .....	109
ip arp inspection vlan .....	109
ip arp inspection trust .....	110
ip arp inspection validate .....	111
ip arp inspection rate-limit .....	112

---

clear ip arp inspection statistics .....	112
show ip arp inspection .....	113
show ip arp inspeciton interface .....	113
10. GVRP .....	115
gvrp (Global).....	115
gvrp (Interface) .....	115
gvrp registration-mode .....	116
gvrp vlan-create-forbid .....	117
clear gvrp statistics .....	117
show gvrp statistics .....	118
show gvrp .....	119
show gvrp configuration .....	120
11. IGMP Snooping .....	121
ip igmp snooping .....	121
ip igmp snooping version .....	121
ip igmp snooping querier .....	122
ip igmp snooping vlan .....	122
ip igmp snooping vlan fastleave .....	123
ip igmp snooping vlan query-interval .....	124
ip igmp snooping vlan response-time .....	124
ip igmp snooping vlan router .....	125
ip igmp snooping vlan forbidden-port .....	126
ip igmp snooping vlan static-port .....	126
ip igmp snooping vlan static-router-port .....	127
ip igmp snooping vlan static-group .....	127
ip igmp snooping vlan group .....	128
ip igmp profile .....	129
profile range .....	129
ip igmp filter .....	130
ip igmp max-groups .....	131
ip igmp max-groups action .....	131
clear ip igmp snooping groups .....	132
clear ip igmp snooping statistics .....	133
show ip igmp snooping groups counters .....	134
show ip igmp snooping groups .....	134
show ip igmp snooping router.....	135
show ip igmp snooping querier .....	136
show ip igmp snooping .....	136
show ip igmp snooping vlan .....	137
show ip igmp snooping forward-all .....	138
show ip igmp profile .....	139
show ip igmp filter.....	139
show ip igmp max-group .....	140
show ip igmp max-group action .....	141

---

12. IP SourceGuard .....	142
ip source verify .....	142
ip source binding .....	142
show ip source interfaces .....	143
show ip source binding .....	144
13. LinkAggregation .....	145
lag .....	145
lag load-balance .....	146
lACP port-priority .....	146
lACP system-priority .....	147
show lACP .....	148
show lag .....	148
14. LLDP .....	150
lldp .....	150
lldp tx .....	151
lldp lldpdu .....	152
lldp tlv-select .....	153
lldp tlv-select pvid .....	154
lldp tlv-select vlan-name .....	155
show lldp .....	156
show lldp local-device .....	157
show lldp neighbor .....	158
15. Logging.....	159
logging .....	159
logging host .....	159
logging severity .....	160
show logging .....	161
clear logging .....	162
16. MAC AddressTable .....	164
mac address-table aging-time .....	164
mac address-table static .....	164
clear mac address-table .....	165
show mac address-table .....	165
show mac address-table counters .....	166
show mac address-table aging-time .....	167
17. MAC VLAN .....	168
vlan mac-vlan group (Global) .....	168
vlan mac-vlan group (Interface) .....	168
show vlan mac-vlan groups .....	169
show vlan mac-vlan interfaces .....	169
18. Management ACL .....	171
management access-list .....	171
management access-class .....	171
deny .....	172

---

permit .....	172
no sequence .....	173
show management access-list .....	174
show management access-class .....	174
19. MLD Snooping .....	176
ipv6 mld snooping .....	176
ipv6 mld snooping report-suppression .....	176
ipv6 mld snooping version .....	176
ipv6 mld snooping unknown-multicast action .....	177
ipv6 mld snooping vlan .....	178
ipv6 mld snooping vlan fastleave .....	178
ipv6 mld snooping vlan last-member-query-count .....	179
ipv6 mld snooping vlan last-member-query-interval .....	179
ipv6 mld snooping vlan query-interval .....	180
ipv6 mld snooping vlan response-time .....	180
ipv6 mld snooping vlan router .....	181
ipv6 mld snooping vlan static-port .....	181
ipv6 mld snooping vlan forbidden-router-port .....	182
ipv6 mld snooping vlan static router port .....	182
ipv6 mld snooping vlan static-group .....	183
ipv6 mld snooping vlan group .....	183
ipv6 mld profile .....	184
profile range .....	184
ipv6 mld filter .....	185
ipv6 mld max-groups .....	185
ipv6 mld max-groups action .....	186
clear ipv6 mld snooping groups .....	186
clear ipv6 mld snooping statistics .....	187
show ipv6 mld snooping groups counters .....	187
show ipv6 mld snooping groups .....	187
show ipv6 mld snooping router .....	188
show ipv6 mld snooping .....	189
show ipv6 mld snooping vlan .....	190
show ipv6 mld snooping forward-all .....	191
show ipv6 mld profile .....	191
show ipv6 mld filter .....	192
show ipv6 mld max-group .....	192
show ipv6 mld max-group action .....	193
20. MVR .....	194
mvr .....	194
mvr vlan .....	194
mvr group .....	195
mvr mode .....	195
mvr query-time .....	196



---

mvr port type .....	196
mvr immediate .....	197
mvr vlan group .....	198
clear mvr members .....	198
show mvr members.....	199
show mvr interface .....	199
show mvr .....	199
21. POE .....	201
poe .....	201
poe schedule .....	201
show poe .....	202
22. PortMirror.....	204
mirror session source interface .....	204
mirror session destination interface .....	204
show mirror .....	205
23. Port .....	206
description .....	206
speed .....	206
duplex.....	207
shutdown .....	208
flowcontrol .....	209
jumbo-frame .....	209
protected .....	210
eee .....	Error! Bookmark not defined.
clear interface .....	211
show interface .....	212
24. Port ErrorDisable .....	214
errdisable recovery cause .....	214
errdisable recovery cause uidd .....	214
errdisable recovery interval .....	215
show errdisable recovery .....	215
25. PortSecurity .....	217
port-security (Global) .....	217
port-security (Interface) .....	217
port-security address-limit .....	218
show port-security .....	218
show port-security interface .....	219
26. Protocol VLAN .....	220
vlan protocol-vlan group (Global).....	220
vlan protocol-vlan group (Interface) .....	220
show vlan protocol-vlan .....	221
show vlan protocol-vlan interfaces .....	222
27. QOS .....	223
qos .....	223

---

qos cos .....	223
qos map.....	224
qos queue.....	226
qos remark .....	228
qos trust .....	228
qos trust (Interface) .....	229
show qos .....	230
show qos interface .....	230
show qos map .....	231
show qos queueing .....	232
28. Rate Limit .....	233
rate-limit egress .....	233
rate-limit ingress .....	233
rate limit egress queue.....	234
29. SNMP .....	235
snmp .....	235
snmp view .....	235
snmp group .....	236
snmp community .....	236
snmp user.....	237
snmp engineid .....	238
snmp engineid remote .....	238
snmp trap .....	239
snmp host.....	239
show snmp view .....	240
show snmp group .....	241
show snmp community .....	241
show snmp user .....	242
show snmp engineid .....	242
show snmp trap.....	243
show snmp host .....	243
30. RMON .....	244
rmon event .....	244
rmon alarm .....	244
rmon history.....	246
clear rmon interfaces statistics .....	246
show rmon interfaces statistics .....	247
show rmon event .....	248
show rmon event log.....	249
show rmon alarm .....	249
show rmon history .....	250
show rmon history statistic .....	250
31. SpanningTree .....	252
instance (MST) .....	252

---

name (MST) .....	252
revision (MST) .....	253
spanning-tree mst configuration .....	253
spanning-tree mst cost .....	254
spanning-tree mst port-priority .....	254
spanning-tree mst priority .....	255
spanning-tree .....	255
spanning-tree mode .....	256
spanning-tree bpdu .....	257
spanning-tree bpdu-filter .....	257
spanning-tree bpdu-guard .....	257
spanning-tree cost .....	258
spanning-tree forward-delay .....	259
spanning-tree hello-time .....	259
spanning-tree maximum-age .....	260
spanning-tree edge .....	260
spanning-tree link-type .....	261
spanning-tree max-hops .....	261
spanning-tree mcheck .....	262
spanning-tree pathcost method .....	262
spanning-tree port-priority .....	263
spanning-tree priority .....	263
spanning-tree tx-hold-count .....	264
show spanning-tree .....	264
show spanning-tree interface .....	265
show spanning-tree mst .....	266
show spanning-tree mst interface .....	267
show spanning-tree mst configuration .....	268
32. StaticRouting .....	269
interface vlan (IPv4) .....	269
ip route .....	269
arp .....	270
interface vlan (IPv6) .....	271
ipv6 address .....	271
ipv6 route .....	272
ipv6 neighbors .....	273
show ip interface vlan .....	274
show ipv6 interface vlan .....	274
show ip route .....	275
show ipv6 route .....	275
show arp .....	276
show ipv6 neighbors .....	276
33. StormControl .....	278
storm-control .....	278

---

storm-control action .....	279
storm-control ifg .....	279
storm-control level .....	280
storm-control unit .....	281
show storm-control .....	282
34. System File .....	283
copy .....	283
delete .....	284
restore-defaults .....	284
save .....	285
show config .....	285
show flash .....	287
35. SurveillanceVLAN .....	288
surveillance-vlan (Global) .....	288
surveillance-vlan (Interface) .....	288
surveillance-vlan vlan .....	289
surveillance-vlan oui-table .....	290
surveillance-vlan cos (Global) .....	290
surveillance-vlan cos (Interface) .....	291
surveillance-vlan mode .....	292
surveillance-vlan aging-time .....	293
show surveillance-vlan .....	294
36. Time .....	295
clock set .....	295
clock timezone .....	295
clock source .....	296
clock summer-time .....	296
ntp .....	297
show clock .....	298
show ntp .....	298
37. UDLD .....	300
udld .....	300
udld aggressive .....	300
udld message time .....	301
udld reset .....	301
show udld .....	302
38. VLAN .....	303
vlan .....	303
Name (vlan) .....	303
switchport mode .....	304
switchport hybrid pvid .....	305
switchport hybrid ingress-filtering .....	306
switchport hybrid acceptable-frame-type .....	306
switchport hybrid allowed vlan .....	307

---

switchport access vlan .....	308
switchport tunnel vlan .....	308
switchport trunk native vlan .....	309
switchport trunk allowed vlan .....	309
switchport default-vlan tagged .....	310
switchport forbidden default-vlan .....	310
switchport forbidden vlan .....	311
switchport vlan tpid .....	311
management-vlan .....	312
show vlan .....	312
show vlan interface membership .....	313
show interface switchport .....	314
show management-vlan .....	314
39. VoiceVLAN .....	316
voice-vlan (Global) .....	316
voice-vlan (Interface) .....	316
voice-vlan vlan .....	317
voice-vlan oui-table .....	318
voice-vlan cos (Global) .....	319
voice-vlan cos (Interface) .....	320
voice-vlan mode .....	321
voice-vlan aging-time .....	322
show voice-vlan .....	323

## Command Line UserGuide

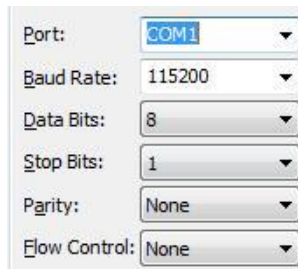
### 1 Use the command line

Users can log in to the switch in three ways to use the command line:

1. Log in locally through the Console port;
2. Use Telnet to log in locally or remotely through the Ethernet port;
3. Use SSH to log in locally or remotely through the Ethernet port.

#### Local login through the console port

1. First, connect the serial port of the computer (or terminal) to the console port of the Ethernet switch through the configuration cable.
2. Open the terminal emulation program (such as HyperTerminal program) of the computer and configure the following parameters:

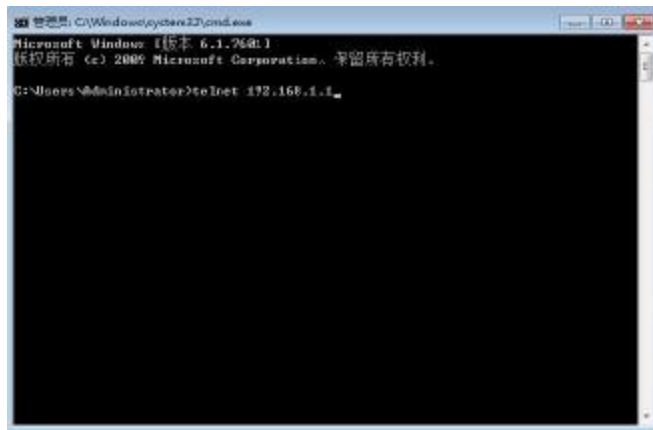


A screenshot of a terminal emulation configuration dialog box. The dialog has several fields with dropdown menus:

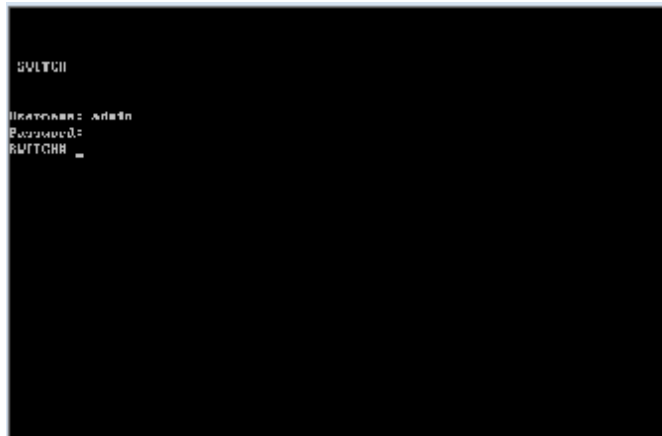
- Port: COM1
- Baud Rate: 115200
- Data Bits: 8
- Stop Bits: 1
- Parity: None
- Flow Control: None

#### Login via telnet

1. Please make sure that the switch and the computer are in the same LAN. Select Start, enter "cmd" in the search box and enter the Enter key to enter the cmd window.
2. A running window as shown in Figure 1-5 pops up, enter telnet 192.168.1.1, and click the OK button to enter the DOS interface.



3. Enter the login user name and password (the default value is "admin"), press Enter to enter the user mode



### Login via SSH

It is recommended to use the third-party client software PuTTY to establish an SSH connection. Please set it up before logging in with SSH for the first time

The password to enter the privileged mode. , SSH login has two authentication modes

Password authentication mode: Need to log in to enter the user name and password, the default value is admin.

Key authentication mode: No need to log in user name and password, but you need to generate a pair of public key and private key through Putty key generator first

Import the public key into the switch, and import the private key into the client software for authentication.

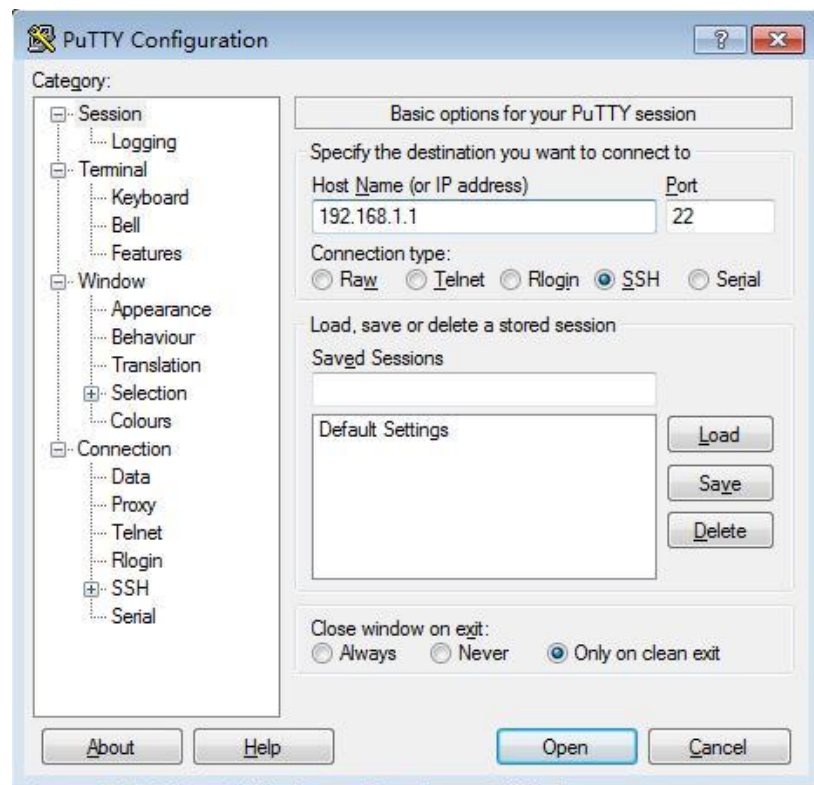
Before SSH login, please follow the steps shown in the figure below to enable the SSH function

of the switch in HyperTerminal

```
Username: admin
Password: *****
*Jan 02 2020 03:14:20: %AAA-5-CONNECT: New console connection for user admin, source async ACCEPTED
Switch# configure
Switch(config)# ip ssh
Switch(config)#
```

### Password authentication mode

1. Open the software and log in to the main interface of PuTTY. Fill in the IP address of the switch in "Host Name"; keep the default 22 for "Port"; select SSH for "Connection type". As shown below



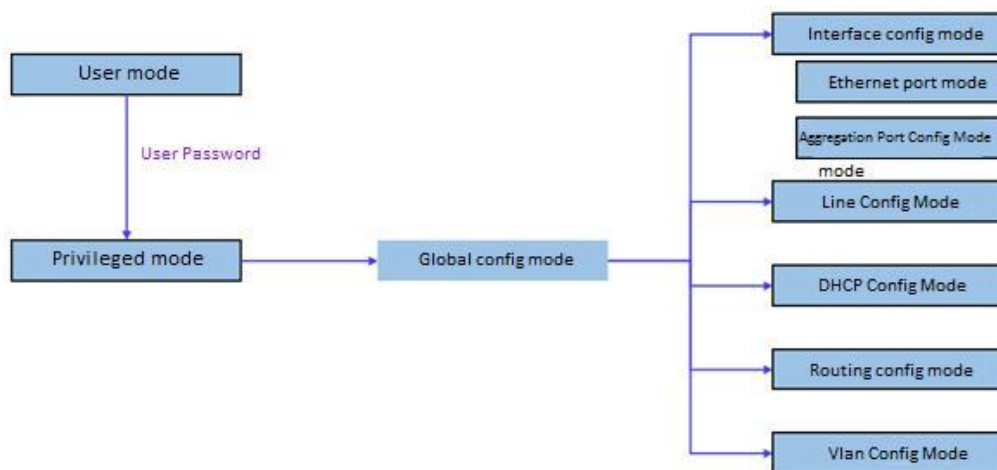
2. Click the <Open> button to log in to the switch. The operation method is the same as Telnet. Enter the login user name and login password to continue the configuration operation. As shown below.



```
Username: admin
Password: ****
Switch#
```

### Command line mode

CLI is divided into the following modes according to functions: user mode, privileged mode, global configuration mode, line configuration mode, VLAN configuration mode, interface configuration mode, routing configuration mode, DHCP configuration mode and MST configuration mode. The interface configuration mode is divided into Ethernet Network port configuration mode and aggregation port configuration mode, etc., as shown below



### Description

1. After establishing a connection with the switch through the Console port or Telnet, it enters the

user mode.

2. Each mode has its own command. To configure the corresponding command, you must first enter the corresponding mode:

- Ø Global configuration mode: provide commands for global configuration, such as spanning tree, queue scheduling mode, etc.;
- Ø Interface configuration mode: Divided into multiple interfaces, each interface has its own corresponding command:
- Ø VLAN configuration mode: Create VLAN, add port to designated VLAN.
- Ø Routing configuration mode: configure the relevant parameters of the three-layer function.

3. Some commands are global and can be executed in all command modes:

- Ø show: Display various information of the switch, such as statistics, port information, VLAN information, etc.
- Ø history: Display history commands.

□

### Command line security level

There are three user levels: Visitor, User and Admin. The default user name is shown in the following table:

User Name	Password	User Level
Guest		Visitor
Manager	123	User
Superuser	123	Admin

The three user levels have different access rights, see Reasonable.

User level	Explanation
Visitor	<p>The following commands can be accessed:</p> <p>clear disable enable exit help ping ----- show (note)</p> <p>Note: The following commands cannot be accessed: show user show snmp community show snmp traps-host</p>

	show snmp user
User	The following commands cannot be accessed: user no user <i>user-name</i> reset configuration tftp <i>server-ip</i> { get <i>source-file</i>   put <i>dest-file</i> } update firmware <i>file-name</i> tftp-server <i>server-ip</i>
Admin	Can execute all commands

### Command line format

Basic format convention

Command line format convention

Convention	Description
<b>Boldface</b>	Command line keywords are in bold type.
<i>italics</i>	Command variables are in italics.
[ ]	Items (keywords or variables) are placed in square brackets [] to indicate optional items.
{ x   y   ... }	Substitute item groups, add parentheses and separate them with vertical bars. Only select one item.
[ x   y   ... ]	Optional grouping of alternative items, enclosed in square brackets and separated by vertical bars. Select an item or no item.
#	Line comment lines beginning with # sign.

### Special characters

If the variable is in the form of a string, please note when inputting:

- ≥ " <> , \ & These six characters are not allowed to be entered.
- ≥ If the string contains spaces, you need to add single quotes ' ' or double quotation marks at the beginning and end of the string, such as hello world'、 "hello world".

At this time, two (or more) words in single/double quotation marks will be input as a string parameter; if single/double quotation marks are not added, they will be parsed into two (or more) characters

### 5.3 Shortcut list


Hot key	Description
<b>【Delete】</b>	Delete the character on the cursor, only applicable to telnet.
<b>【←Backspace】</b> or <b>【Ctrl】 + 【h】</b>	Delete the character to the left of the cursor.
<b>【↑】</b> or <b>【Ctrl】 + 【p】</b>	If there is one in the history command list, execute the previous command.
<b>【↓】</b> or <b>【Ctrl】 + 【n】</b>	If there is one in the history command list, execute the next command.
<b>【←】</b> or <b>【Ctrl】 +</b>	The cursor moves one position to the left.

<b>【b】</b>	
<b>【→】</b> or <b>【Ctrl】</b> + <b>【f】</b>	The cursor moves one position to the right.
<b>【Ctrl】</b> + <b>【z】</b>	Except the system view, exit the current view.
<b>【Ctrl】</b> + <b>【w】</b>	Delete the character to the left of the cursor until a blank separator is encountered.
<b>【Ctrl】</b> + <b>【a】</b>	The cursor moves to the beginning of the line.
<b>【Ctrl】</b> + <b>【e】</b>	The cursor moves to the end of the line.
<b>【Ctrl】</b> + <b>【u】</b>	Starting from the beginning of the line, delete everything until the cursor is.
<b>【Ctrl】</b> + <b>【d】</b>	Delete the character on the cursor.
<b>【Ctrl】</b> + <b>【k】</b>	Delete everything from the cursor to the end of the line.
<b>【Ctrl】</b> + <b>【c】</b>	Skip the current command and go to a new line.

#### Page shortcut table

Hot key	Description
Any key except <b>【Enter】</b> and <b>【q】</b>	Show next page
<b>【q】</b>	Stop display
<b>【Enter】</b>	Show next line

#### Various signs

 Notice	Remind the matters that should be paid attention to during operation, improper operation may cause data loss or equipment damage.
<b>&amp;</b> Description	The description of the operation content shall be supplemented and explained as necessary.

#### 5.6 Error message

If you enter incorrect parameters or the command cannot be executed, the following error message will be displayed on the screen.

1. Incomplete command
2. Type parameter error
3. Wrong parameter value
4. Command is not clear
5. Too many or wrong parameters
6. Invalid parameters
7. Missing parameters
8. Command error

## User Interface

### 2AAA

#### AAA authentication

##### Format

```
aaa authentication (login | enable) (default | LISTNAME) METHODLIST
[METHODLIST] [METHODLIST] [METHODLIST]
```

```
no aaa authentication (login | enable) LISTNAME
```

##### Parameter

login	Add/Edit login authentication list
enable	Add/edit enable authentication list
default	Edit the default authentication list
<i>LISTNAME</i>	Specifies the name of the list of authentication types
<i>METHODLIST</i>	Specify the verification method, including none,local, enable, tacacs+, radius

##### Default

The default authentication list name is "Default" and the default method is "local".

The name of the default authentication list of type enable is "Default", and the default method is "enable"

##### Mode

Global configuration mode

##### Instructions

When a user attempts to log in to the switch, login authentication is used. For example, CLI login dialog box and WEB UI login webpage.

Enable authentication is only used for the CLI of users who are trying to switch from user EXEC mode to privileged EXEC mode.

They all support the following authentication methods

Local: Use a local user account database for authentication. (Enable authentication does not support this method)

Enable: Use the local enable password database for authentication

Tacacs+: Use remote Tacacs+ server for authentication

Radius: Use remote Radius server for authentication

None: Do nothing, just let the user be authenticated.

Each list allows you to combine these methods in a different order. For example, we want to use the remote Tacacs+ server to authenticate the logged-in user, but the server may crash. Therefore, we need a backup plan, such as another Radius server. Therefore, we can configure the list as Tacacs+server as the first authentication method and Radius server as the second authentication method.

Use the no command to delete the existing list. However, it is not allowed to delete the "default" list.  
Instance

How to add login authentication list to use tacacs+, radius, local for authentication.

```
Switch(config)# aaa authentication login test1 tacacs+ radius local
```

Query the existing login authentication list

```
Switch# show aaa authentication login lists
```

```
LoginList Name Authentication MethodList
```

```
-----
```

```
default    local
test1     tacacs+  radius  local
```

Add an Enable authentication list to use the order tacacs+, radius, enable for authentication.

```
Switch(config)# aaa authentication enable test1 tacacs+ radius enable
```

Query the existing login authentication list

```
Switch# show aaa authentication enable lists
```

```
EnableListName Authentication MethodList
```

```
-----
```

```
default    enable
test1     tacacs+  radius  enable
```

### login authentication

#### Format

```
login authentication LISTNAME
```

```
no login authentication
```

#### Parameter

<i>LISTNAME</i>	Specify the name of the login authentication list to use
-----------------	--

#### Default

The default login authentication list is "default".

#### Mode

Line Configuration mode

## Instructions

Allow different access methods to bind different login authentication lists. Use the "login authentication" command to bind the list to a specific line (console, telnet, ssh).

Use the no command to restore the configuration.

## Instance

```

Create a new login authentication list and bind to telnet
Switch(config)# aaa authentication logintest1 tacacs+ radius local
Switch(config)# line telnet
Switch(config-line)# login authentication test1
Query list
Switch# show line lists
  LineType | AAAType | ListName
-----+-----+-----
  console|          | login | default
          |          | enable |
  default telnet| login | test1
          |          | enable | default
          |          | login | default
  ssh|          |          |
          |          | enable | default
  http |          | login | default
  https|          | login | default

```

## ip http login authentication

### Format

```

ip (http | https) login authentication LISTNAME
no ip (http | https) login authentication

```

### Parameter

http	Use the http protocol to bind the login authentication list to the user to access WEBUI
https	Use the https protocol to bind the login authentication list to the user to access the WEBUI
<i>LISTNAME</i>	Specifies the name of the login authentication list to be used.

### Default

The default login authentication list is "default"

### Mode

Global configuration mode

### Instructions

Allow different access methods to bind different login authentication lists. Use the command "ip (http | https) login authentication" to bind the list to WEBUI access from http or https.

Use no to return to the default configuration.

### Instance

Create two new login authentication lists and bind to http and https.

```
Switch(config)# aaa authentication login test1 tacacs+ radius local
```

```
Switch(config)# aaa authentication login test2 radius local
```

```
Switch(config)# ip http login authentication test1
```

```
Switch(config)# ip https login authentication test2
```

Query bound list information

```
Switch# show line lists
```

```
LineType      |  AAAType      |  ListName
```

```
-----+-----+-----
```

```
console | login | default
```

```
| enable | default
```

```
telnet | login | default
```

```
| enable |
```

```
default ssh | login
```

```
| default
```

```
| enable | defaulthttp | login |
```

```
test1 https | login | test2
```

### enable authentication

### Format

```
enable authentication LISTNAME
```

```
no enable authentication
```

### Parameter

<i>LISTNAME</i>	Specify the name of the Enable authentication list to be used
-----------------	---

### Default

The default Enable authentication list is "default"

### Mode

Line Configuration mode



## Instructions

Allow different access methods to bind different lists of enabled

authentication. Use the command "enable

Authentication" binds the list to a specific Line (console, telnet, ssh).

Use no to return to the default configuration

## Instance

Create a new Enable authentication list and bind it to telnet.

```
Switch(config)# aaa authentication enable test1 tacacs+ radius enable
```

```
Switch(config)# line telnet
```

```
Switch(config-line)# enable authentication test1
```

Query binding information

```
Switch# show line lists
```

```
LineType   | AAAType   | ListName
-----+-----+-----
console | login | default
| enable | default
telnet | login | default
| enable | test1
ssh | login | default
| enable | default
http | login | default
https | login | default
```

## show aaa authentication

## Format

show aaa authentication (login | enable) lists

## Parameter

login	Query login authentication list
enable	Query the Enable certification list

## Default

## Mode

Privileged mode

## Instructions

Use the command "show aaa authentication" to query the login authentication list or the list information of Enable authentication

#### Instance

Query the list of logged in authentication  
 Switch# show aaa authentication login lists  
 LoginListName | Authentication MethodList  
 -----+-----  
 default |local  
 test1 |tacacs+radius local

How to query the list of existing Enable authentication  
 Switch# show aaa authentication enable lists  
 Enable List Name | Authentication Method List  
 -----+-----  
 default |enable  
 test2 |tacacs+radius enable

#### show line lists

#### Format

show line lists

#### Parameter

#### Default

#### Mode

Privileged mode

#### Instructions

Use the command "show line lists" to query all the binding list authentication, authorization and accounting functions.

#### Instance

Query all binding lists  
 Switch# show line lists  
 LineType | AAAType | ListName  
 -----+-----  
 console| login |default

```

| enable |
default telnet| login |test1
| enable |default
ssh| login |default
| enable |default
http | login |default
https| login |default

```

## tacacs default-config

### Format

```
tacacs default-config [key TACACSKEY] [timeout <1-30>]
```

### Parameter

key	Specify the key value of the tacacs+ server
timeout	Specify tacacs+ server timeout

### Default

The default tacacs+ key is "".

The default tacacs+ timeout period is 5 seconds

### Mode

Global configuration mode

### Instructions

Use the command "tacacs default-config" to modify the Default value of the tacacs+ server. When a user tries to create a new tacacs+ server without assigning these values, the Default value will be used.

### Instance

```

Modify the configuration of tacacs+
Switch(config)# tacacs default-config timeout 20
Switch(config)# tacacs default-config key tackey

```

```

Query the configuration of tacacs+
Switch# show tacacs default-config
Timeout|    Key
-----+-----
10 |    tackey

```

Use the Default configuration above to create a new tacacs+ server and display the results

```
Switch(config)# tacacs host 192.168.1.111
Switch# show tacacs
Prio |Timeout | IP Address | Port |Key
-----+-----+-----+-----+-----
1 | 10 | 192.168.1.111 | 49 |tackey
```

## tacacs host

### Format

```
tacacs host HOSTNAME [port <0-65535>] [key TACPLUSKEY] [priority<0- 65535>]
[timeout <1-30>]
no tacacs [host HOSTNAME]
```

### Parameter

host	Specify the host name of tacacs+ server, IP address and domain name are available
port	Specify the udp port number of the tacacs+ server
key	Specify the key value of tacacs+ server
priority	Specify the priority of tacacs+ server
timeout	Specify the timeout period of the tacacs+ server

### Default

Default tacacs+ key is "".  
Default tacacs+ timeout time is 5 seconds

### Mode

Global configuration mode

### Instructions

Use the command "tacacs host" to add or edit tacacs+ servers for authentication, authorization or accounting. Use no to delete one or more tacacs servers

### Instance

```
Create a new tacacs+ server
Switch(config)# tacacs host 192.168.1.111 port 12345 key tacacs+ priority 100
timeout 10
```

```
Query tacacs+ server
Switch# show tacacs
```

---

```

Prio |Timeout | IP Address | Port |Key
-----+-----+-----+-----+-----
          192.168.1.111 |          12345 |tacacs+
100 | 10 |

```

### show tacacs default-config

#### Format

```
show tacacs default-config
```

#### Parameter

#### Default

#### Mode

Privilege Mode

#### Instructions

Use the command "show tacacs default-config" to query tacacs+ Default configuration

#### Instance

```

Query tacacs+ configuration
Switch# show tacacs default-config
Timeout| Key
-----+-----
10 | tackey

```

### show tacacs

#### Format

```
show tacacs
```

#### Parameter

#### Default

#### Mode

Privileged mode

#### Instructions

Use the command "show tacacs" to query tacacs+ server configuration

## Instance

```

Query tacacs+ server configuration
Switch# show tacacs
Prio |Timeout |  IP Address  |  Port |Key
-----+-----+-----+-----+-----
          192.168.1.111|          12345 |tacacs+

```

## show default-config

## Format

```
radius default-config [key RADIUSKEY] [retransmit <1-10>] [timeout <1-30>]
```

## Parameter

key	Specify the radius server key value
retransmit	Specify the number of retransmissions by the radius server
timeout	Specify the radius server timeout period

## Default

The keyDefault value of radius is ""  
 The default value of radius retransmission is 3 times  
 The default value of the radius timeout is 3 seconds

## Mode

Global configuration mode

## Instructions

Use the command "radius default-config" to modify the default configuration of radius. When the user tries to create a new radius server without assigning these values, the Default value will be used.

## Instance

```

Modify the configuration of radius
Switch(config)# radius default-config timeout 20
Switch(config)# radius default-config key radiuskey
Switch(config)# radius default-config retransmit 5
Query radius configuration
Switch# show radius default-config
Retries| Timeout|Key
-----+-----+-----
5      | 20 | radiuskey radiushost

```

Create a new radius server using the Default value above  
 Switch(config)# radius host 192.168.1.111  
 Switch# show radius

```

Prio|   IP Address       | Auth-Port| Retries|Timeout|Usage-Type|  Key
-----+-----+-----+-----+-----+-----+-----
---
1   | 192.168.1.111 | 1812   | 5     |20|    All |radiuskey

```

## radius host

### Format

radius host HOSTNAME [auth-port <0-65535>] [key RADIUSKEY] [priority <0-65535>] [retransmit <1-10>] [timeout <1-30>] [type (login|802.1x|all)]  
 no radius [host HOSTNAME]

### Parameter

host	Specify radius server host name, IP address and domain name are available
auth-port	Specify radius server udp port number
key	Specify the radius server key value
priority	Specify radius server priority
retransmit	Specify radius server retransmission times
timeout	Specify radius server timeout
type	Types, including: login, 802.1X authentication, login and 802.1x authentication

### Default

The keyDefault value of radius is ""  
 The default value of radius retransmission is 3 times  
 The default timeout of radius is 3 seconds

### Mode

Global configuration mode

### Instructions

Use the command "radius host" to add or edit a radius server  
 Use no to delete one or more radius servers

### Instance

Add a new radius server  
 Switch(config)# radius host 192.168.1.111 auth-port 12345 key radiuskey priority

100 retransmit 5 timeout 10 type all

Query the radius  
server.

Switch# show radius

Prio	IP Address	Auth-Port	Retries	Timeout	Usage-Type	Key
100	192.168.1.111	12345	5	10	All	radiuskey

**show radius default-config**

#### Format

show radius default-config

#### Parameter

Default

#### Mode

Privileged mode

#### Instructions

Use command "show radius default-config" Query radius configuration

#### Instance

Query radius configuration

Switch# show radius default-config

Retries	Timeout	Key
5	20	radiuskey

**show radius**

#### Formatshow radius

#### Parameter

Mode

Privileged mode

#### Instructions

Use the command "show radius" to query the added radius server



---

**Instance**

Query the added radius server

Switch# show radius

Prio	IP Address	Auth-Port	Retries	Timeout	Usage-Type	Key
-						
100	192.168.1.111	12345	5	10	All	radiuskey

### 3. ACL

#### mac acl

##### Format

```
mac acl NAME
no mac acl NAME
```

##### Parameter

NAME	Specify MAC ACL name
------	----------------------

##### Mode

Global configuration mode

##### Instructions

Use the command `mac acl` to create a MAC access list and enter the MAC acl configuration mode. The name of the ACL must be unique and cannot have the same name as other ACLs or QoS policies. After creating the ACL, create an implicit "deny any" ACE at the end of the ACL. That is, if there is no match, the packet is rejected.

Use `no` to delete the configuration

##### Instance

Create a mac acl. The configuration can be queried through the command `show acl`

```
Switch(config)# mac acl test
Switch(mac-acl)# show acl
MAC access list test
```

#### permit (MAC)

##### Format

```
[sequence <1-2147483647>] permit (A:B:C:D:E:F/A:B:C:D:E:F|any)
(A:B:C:D:E:F/A:B:C:D:E:F|any) [vlan <1-4094>] [cos <0-7><0-7>]
[ethertype <0x0600-0xFFFF>]
no sequence <1-2147483647>
```

##### Parameter

sequence	(Optional) Specify the serial number of the ACE, the serial index represents Priority of ACE in ACL
----------	---

A:B:C:D:E:F/A:B:C:D:E:F any	Specify source or destination MAC address and mask or any
vlan	(Optional) Specify VLAN ID
cos	(Optional) Specify the COS value of 802.1P
ethtype	(Optional) Specify the value of the ether type

## Mode

MAC ACL configuration Mode

## Instructions

Use the command permit to add permission conditions for access to ACE for mac ACE that bypasses these packets. "Sequence" also indicates the priority of the ACL when binding to the interface. If the ACE is not specified

The "sequence" index will specify a sequence index, which is the maximum value of the existing index plus 20. If the message content can match multiple ACEs, the lowest sequence ACE will be hit. If it has the same conditions as the existing ACE, it cannot be added.

## Instance

Add a source MAC address of 22:33:44:55:66:77, VLAN 3 and Ethernet type 1999

ACE of the packet. The settings can be verified by the following show acl command Switch (config)# mac acl test

```
Switch (mac-acl)# sequence 999 permit 22:33:44:55:66:77/FF:FF:FF:FF:FF:FF
```

```
any vlan 3 ethtype 0x2800
```

```
Switch(mac-acl)# show acl
```

```
MAC access list test
```

```
sequence 999 permit 22:33:44:55:66:77/FF:FF:FF:FF:FF:FF any vlan 3 ethtype 0x2800
```

## deny (MAC)

### Format

```
[sequence <1-2147483647>] deny (A:B:C:D:E:F/A:B:C:D:E:F|any)
(A:B:C:D:E:F/A:B:C:D:E:F|any) [vlan <1-4094>] [cos <0-7><0-7>] [ethtype
<0x0600-0xFFFF>]
[shutdown] no sequence <1-2147483647>
```

### Parameter

sequence	(Optional) Specify the serial number of the ACE, the serial index represents Priority of ACE in ACL
----------	--

A:B:C:D:E:F/A:B:C:D:E:F any	Specify source or destination MAC address and mask or any
vlan	(Optional) Specify VLAN ID
cos	(Optional) Specify the COS value of 802.1P
ethtype	(Optional) Specify the value of the ether type
shutdown	(Optional) Close interface when ACE hits

## Default

## Mode

MAC ACL Configuration Mode

## Instructions

Use the deny command to add a deny condition to mac ACE, so that the dropped packets hit the ACE. "Sequence" also indicates the priority of hits when the ACL is bound to the interface. If ACE does not specify a "sequence" index, it will specify a sequence index, which is the maximum value of the existing index plus 20. If the package content can match multiple ACE, hit the lowest sequence ACE. If it has the same conditions as the existing ACE, you cannot add the ACE. Use the command "shutdown" to shut down the interface when the ACE hits.

Add an ACE that rejects packets whose destination MAC address is aa:bb:cc:xx:xx:xx and VLAN 9. The settings can be verified by the following show acl command

```
Switch(config)# mac acl test
```

```
Switch(mac-al)# sequence 30 permit any any
```

```
Switch(mac-al)# deny any aa:bb:cc:00:00:00/FF:FF:FF:00:00:00 vlan 9 shutdown
```

```
Switch(mac-al)# show acl
```

```
MAC access list test
```

```
sequence 30 permit any any
```

```
sequence 50 deny any AA:BB:CC:00:00:00/FF:FF:FF:00:00:00 vlan 9 shutdown
```

## ip acl

## Format

```
ip acl NAME
```

```
no ip acl NAME
```

## Parameter

NAME	Specify the name of the IPv4 ACL
------	----------------------------------

## Default

## Mode

Global configuration mode

## Instructions

Use the command `ip acl` to create an IPv4 access list and enter the `ip acl` configuration mode. The name of the ACL must be unique and cannot have the same name as other ACLs or QoS policies. After creating the ACL, create an implicit "deny any" ACE at the end of the ACL. That is, if there is no match, the packet is rejected.

Use `no` to delete the configuration

Create an IP ACL. You can verify the settings with the `show acl` command `Switch(config)#ip acl iptest`

```
Switch(ip-acl)# show acl
IP access list iptest
```

## permit (IP)

## Format

```
[sequence <1-2147483647>] permit (<0-255>|ipinip|egp|igp|hmp|rdp|ipv6|ipv6:rout|ipv6:frag|rsvp|ipv6:icmp|ospf|pim|l2tp|ip) (A.B.C.D/A.B.C.D|any) (A.B.C.D/A.B.C.D|any) [(dscp|precedence) VALUE]
[sequence <1-2147483647>] permit icmp (A.B.C.D/A.B.C.D|any) (A.B.C.D/A.B.C.D|any) (<0-255>|echo-reply|destination-unreachable|source- quench|echo- request|router-advertisement|router-solicitation|time- exceeded|timestamp| timestamp-reply|traceroute|any) (<0- 255>|any) [(dscp|precedence) VALUE]
[sequence <1-2147483647>] permit tcp (A.B.C.D/A.B.C.D|any) (<0-65535>|echo|discard|daytime|ftp-data|ftp|telnet|smtp|time|hostname|whois|tacacs- ds|domain|www|pop2|pop3|syslog|talk|klogin|kshell|sunrpc|drip|PORT_RANG E|any) (A.B.C.D/A.B.C.D|any) (<0-65535>|echo|discard|daytime|ftp-data|ftp|telnet|smtp|time|hostname|whois| tacacs- ds|domain|www|pop2|pop3|syslog|talk|klogin|kshell|sunrpc|dri p|PORT_RANGE|any)[match-all TCP_FLAG] [(dscp|precedence) VALUE]
[sequence <1-2147483647>] permit udp (A.B.C.D/A.B.C.D|any) (<0-65535>|echo|discard| time|nameserver|tacacs- ds|domain|bootps|bootpc|tftp|sunrpc|ntp|netbios-ns|snmp|snmptrap|who|syslog|talk|rip|PORT_RANGE|any) (A.B.C.D/A.B.C.D|any) (<0- 65535>|echo|discard|time|nameserver|tacacs- ds|domain|bootps|bootpc|tftp|sunrpc|ntp|netbios-ns|snmp|snmptrap|who|syslog|PORT_RANGE|any) [(dscp|precedence)
```

VALUE] no sequence <1-2147483647>

### Parameter

sequence	(Optional) Specify the sequence index of the sequence number to indicate the priority of the ACE in the ACL.
A.B.C.D/A.B.C.D any	Specify the source and destination IPv4 address and mask of the packet or any IPv4 address.
dscp	(Optional) Specify the DSCP of the packet
precedence	(Optional) Specify the ip precedence of the message
icmp-type	Specify the ICMP message type used to filter ICMP packets. Input list Type name or number of ICMP message types.
icmp-code	Specify the ICMP message code used to filter ICMP packets
I4-source-port	Specify the TCP/UDP source port number to filter TCP/UDP data packets
I4-destination-port	Specify the TCP/UDP destination port number to filter TCP/UDP data packets
match-all	Specifies the tag of TCP packets. If you want to set a flag, its prefix is \"+\". If the flag should be unset, the prefix of the flag is \"-\". Available options are +urg, +ack, +psh, +rst, +syn, +fin, -urg, -ack, -psh, -rst, -syn, and -fin. To define multiple targets Please input other signs without spaces (for example, +syn ack).

### Default

### Mode

IP ACL Configuration Mode

### Instructions

Use the permit command to add permission conditions to access the ACE for the IP ACE that bypasses these packets. "Sequence" also indicates the priority of hits when the ACL is bound to the interface. If ACE is not specified

The "sequence" index will specify a sequence index, which is the maximum value of the existing index plus 20. If the message content can match multiple ACEs, the lowest sequence ACE will be hit. If it has the same conditions as an existing ACE, you cannot add an ACE.

### Instance

Add and set an ACE. Use the following command show acl to view the IP subnets allowed by the configuration

```
Switch(ip-al)# permit ip 192.168.1.0/255.255.255.0
```

Allowed ICMP request message

```
Switch(ip-al)# permit icmp any any echo-request any
```

Allow HTTP packets of any IP address through DSCP

```
5Switch(ip-al)# permit tcp any any any www dscp 5
```

Allow any source IP address SNMP packet to connect to the destination IP address

192.168.1.1

```
Switch(ip-al)# permit udp any any 192.168.1.1/255.255.255.255 snmp
```

```
Switch(ip-al)# show acl
```

IP access list iptest

```
sequence 1 permit ip 192.168.1.0/255.255.255.0 any sequence 21
```

```
permit icmp any any echo-request any sequence 41 permit tcp any any any
```

```
www dscp 5
```

```
sequence 61 permit udp any any 192.168.1.1/255.255.255.255 snmp
```

## deny (IP)

### Format

```
[sequence <1-2147483647>] deny (<0-255>|ipinip|egp|igp|hmp|rdp|ipv6|ipv6:rout|ipv6:frag|rsvp|ipv6:icmp|ospf|pim|l2tp|ip)(A.B.C.D/A.B.C.D|any) (A.B.C.D/A.B.C.D|any) [(dscp|precedence) VALUE][sequence <1-2147483647>] deny icmp (A.B.C.D/A.B.C.D|any) (A.B.C.D/A.B.C.D|any) (<0-255>|echo-reply|destination-unreachable|source- quench|echo- request|router-advertisement|router-solicitation|time- exceeded|timestamp| timestamp-reply|traceroute|any) (<0- 255>|any) [(dscp|precedence) VALUE][sequence <1-2147483647>] deny tcp (A.B.C.D/A.B.C.D|any) (<0-65535>|echo|discard|daytime|ftp- data|ftp|telnet|smtp|time|hostname|whois|tacacs- ds|domain|www|pop2|pop3|syslog|talk|klogin|kshell|sunrpc|drip|PORT_RANG E|any) (A.B.C.D/A.B.C.D|any) (<0-65535>|echo|discard|daytime|ftp- data|ftp|telnet|smtp|time|hostname|whois| tacacs- ds|domain|www|pop2|pop3|syslog|talk|klogin|kshell|sunrpc|dri p|PORT_RANGE|any)[match-all TCP_FLAG] [(dscp|precedence) VALUE][sequence <1-2147483647>] deny udp (A.B.C.D/A.B.C.D|any) (<0-65535>|echo|discard| time|nameserver|tacacs- ds|domain|bootps|bootpc|tftp|sunrpc|ntp|netbios-ns|snmp|snmptrap|who|syslog|talk|rip|PORT_RANGE|any) (A.B.C.D/A.B.C.D|any) (<0- 65535>|echo|discard|time|nameserver|tacacs- ds|domain|bootps|bootpc|tftp|sunrpc|ntp|netbios-ns| snmp|snmptrap|who|syslog|PORT_RANGE|any) [(dscp|precedence) VALUE] no sequence <1-2147483647>
```

### Parameter

sequence	(Optional) Specify the sequence index of the sequence number to indicate the priority of the ACE in the ACL.
A.B.C.D/A.B.C.D any	Specify the source and destination IPv4 address and mask of the packet or any IPv4 address.
dscp	(Optional) Specify the DSCP of the packet
precedence	(Optional) Specify the ip precedence of the message
icmp-type	Specify the ICMP message type used to filter ICMP packets. Input list Type name or number of ICMP message types.
icmp-code	Specify the ICMP message code used to filter ICMP packets
I4-source-port	Specify the TCP/UDP source port number to filter TCP/UDP data packets
I4-destination-port	Specify the TCP/UDP destination port number to filter TCP/UDP data packets
match-all	Specifies the tag of TCP packets. If you want to set a flag, its prefix is \'+\'. If the flag should be unset, the prefix of the flag is \'-\'. Available options are +urg, +ack, +psh, +rst, +syn, +fin, -urg, -ack, -psh, -rst, -syn, and -fin. To define multiple targets Please input other signs without spaces (for example, +syn ack).

## Default

## Mode

IP ACL Configuration Mode

## Instructions

Use the command deny to add deny conditions to the IP ACE that discards these packets. "Sequence" also means

The hit priority when the ACL is bound to the interface. If ACE does not specify a "sequence" index, it will specify a sequence index, which is the maximum value of the existing index plus 20. If the message content can match multiple ACEs, the lowest sequence ACE is hit. If it has the same conditions as an existing ACE, you cannot add an ACE.

Make the command "shutdown" shut down the interface when the ACE hits.

## Instance

Add an ACE that rejects packets whose source IP address is 192.168.1.80. The settings can be verified by the following show acl command

```
Switch(config)# ip acl iptest
```

```
Switch(ip-acl)# deny ip 192.168.1.80/255.255.255.255 any
```



```
Switch(ip-al)# show acl
IP access list iptest
sequence 1 deny ip 192.168.1.80/255.255.255.255 any
```

## IPv6 acl

### Format

```
ipv6 acl NAME
no ipv6 acl NAME
```

### Parameter

NAME	Specify the name of the IPv6 ACL
------	----------------------------------

### Default

### Mode

Global configuration mode

### Instructions

Use the command `ipv6 acl` to create an IPv6 access list and enter the `ipv6 acl` configuration mode. The name of the ACL must be unique and cannot have the same name as other ACLs or QoS policies. After creating the ACL, create an implicit "deny any" ACE at the end of the ACL. That is, if there is no match, the packet is rejected.

Use `no` to delete the configuration

### Instance

Create an IPv6 ACL. You can verify the settings with the `show acl` command

```
Switch(config)#ip acl
ipv6test
```

```
Switch(ip-al)# show acl
IPv6 access list ipv6test
```

## permit (IPv6)

### Format

```
[sequence <1-2147483647>] permit (<0-255> | ipv6) (X::X:X/<0-128> | any)
(X::X:X/<0-128> | any)[(dscp | precedence) VALUE]
[sequence <1-2147483647>] permit icmp (X::X:X/<0-128> | any)(X::X:X/<0-128> | any) (<0-255> | destination- unreachable | packet-
too-big | time-exceeded | parameter-problem | echo-request | echo-reply | mld-
```

```

query|mld-report|mldv2-report|mld-done|router-solicitation|router-
advertisement|nd-ns|nd-na|any (<0-255>|any)[(dscp|precedence) VALUE]
[sequence <1-2147483647>] permit tcp (X::X:X/<0-128>|any) (<0-
65535>|echo|discard|daytime|ftp-data|ftp|telnet|smtp|
time|hostname|whois|tacacs-
ds|domain|www|pop2|pop3|syslog|talk|klogin|kshell|sunrpc|drip|PORT_R
ANGE|any) (X::X:X/<0-128>|any) (<0-65535>|echo|discard|daytime|ftp-
data|ftp|telnet|smtp|time|hostname|whois|tacacs-
ds|domain|www|pop2|
pop3|syslog|talk|klogin|kshell|sunrpc|drip|PORT_RANGE|any) [match-all
TCP_FLAG] [(dscp|precedence) VALUE]
[sequence <1-2147483647>] permit udp (X::X:X/<0-128>|any)(<0-
65535>|echo|discard|time|nameserver|tacacs-ds|domain|
bootps|bootpc|tftp|sunrpc|ntp|netbios-
ns|snmp|snmptrap|who|syslog|talk|rip|PORT_RANGE|any)
(X::X:X/<0-128>|any) (<0-
65535>|echo|discard|time|nameserver|tacacs-ds|domain|
bootps|bootpc|tftp|sunrpc|ntp|netbios-ns|
snmp|snmptrap|who|syslog|PORT_RANGE|any) [(dscp|precedence)
VALUE] no sequence <1-2147483647>

```

#### Parameter

sequence	(Optional) Specify the serial number sequence index to indicate the priority of the ACE in the ACL.
(X::X:X/<0-128> any)	Specify the source and destination IP addresses and masks of IPv6 packets or whatever.
dscp	(Optional) Specify the DSCP of the packet
precedence	(Optional) Specify the ip precedence of the message
icmp-type	Specify the ICMP message type used to filter ICMP packets. Type of input list Name or number of ICMP message types.
icmp-code	Specify the ICMP message code used to filter ICMP packets
I4-source-port	Specify the TCP/UDP source port number to filter TCP/UDP data packets
I4-destination-port	Specify the TCP/UDP destination port number to filter TCP/UDP data packets
match-all	Specifies the tag of TCP packets. If you want to set a flag, its prefix is "+" and "\". If the flag should be unset, the prefix of the flag is "-" and "\". Available options are +urg, +ack, +psh, +rst, +syn, +fin, -urg, -ack, -psh, -rst, -syn, and -fin. If you want to define multiple flags, please enter one by one without spaces Other signs (for example, +syn ack).

Default

Mode

## IPv6 ACL Configuration Mode

### Instructions

Use the permit command to add permission conditions to access the ACE for the IPv6 ACE that bypasses these packets. "Sequence" also indicates the priority of hits when the ACL is bound to the interface. If ACE is not specified  
The "sequence" index will specify a sequence index, which is the maximum value of the existing index plus 20. If the message content can match multiple ACEs, the lowest sequence ACE will be hit. If it has the same conditions as the existing ACE, it cannot be added.

### Instance

Add and set up an ACE. The settings can be verified by the following show acl command. Allowed IPv6 subnet  
Switch(ipv6-al)# permit permit ipv6 fe80:1122:3344:5566::1/64 any

```
Switch(ipv6-al)# show acl
IPv6 access list ipv6test
sequence 1 permit ipv6 fe80:1122:3344:5566::1/64 any
```

### deny (IPv6)

### Format

```
[sequence <1-2147483647>] deny (<0-255>|ipv6) (X:X::X/X/<0-128>|any)
(X:X::X/X/<0-128>|any)[(dscp|precedence) VALUE]
[sequence <1-2147483647>] deny icmp (X:X::X/X/<0-128>|any)(X:X::X/X/<0-128>|any) (<0-255>|destination- unreachable|packet-
too-big|time-exceeded|parameter-problem|echo-request|echo-reply| mld-
query|mld-report|mldv2-report|mld-done| router- solicitation|router-
advertisement|nd-ns|nd-na|any) (<0- 255>|any)[(dscp|precedence) VALUE]
[sequence <1-2147483647>] deny tcp (X:X::X/X/<0- 128>|any) (<0-
65535>|echo|discard|daytime|ftp-data|ftp|telnet|smtp|
time|hostname|whois|tacacs-
ds|domain|www|pop2|pop3|syslog|talk|klogin|kshell|sunrpc|drip|PORT_R
ANGE|
any) (X:X::X/X/<0-128>|any) (<0-65535>|echo|discard|daytime|ftp-
data|ftp|telnet|smtp|time|hostname|whois|tacacs-
ds|domain|www|pop2|
pop3|syslog|talk|klogin|kshell|sunrpc|drip|PORT_RANGE|any)
[match-all TCP_FLAG] [(dscp|precedence) VALUE]
[sequence <1-2147483647>] deny udp (X:X::X/X/<0- 128>|any)(<0-
65535>|echo|discard|time|nameserver|tacacs-ds|domain|
bootps|bootpc|tftp|sunrpc|ntp|netbios-
ns|snmp|snmptrap|who|syslog|talk|rip|PORT_RANGE|any)
(X:X::X/X/<0- 128>|any) (<0-
65535>|echo|discard|time|nameserver|tacacs-ds|domain|
bootps|bootpc|tftp|sunrpc|ntp|netbios-ns|
```

```
snmp|snmptrap|who|syslog|PORT_RANGE|any) [(dscp|precedence)
VALUE] [shutdown]
no sequence <1-2147483647>
```

### Parameter

sequence	(Optional) Specify the serial number sequence index to indicate the priority of the ACE in the ACL.
(X:X::X:X/<0	128> any) Specify the source and destination IP addresses and masks of IPv6 packets or whatever.
dscp	(Optional) Specify the DSCP of the packet
precedence	(Optional) Specify the ip precedence of the message
icmp-type	Specify the ICMP message type used to filter ICMP packets. Type of input list Name or number of ICMP message types.
icmp-code	Specify the ICMP message code used to filter ICMP packets
I4-source-port	Specify the TCP/UDP source port number to filter TCP/UDP data packets
I4-destination-port	Specify the TCP/UDP destination port number to filter TCP/UDP data packets
match-all	Specifies the tag of TCP packets. If you want to set a flag, its prefix is "+" . If the flag should be unset, the prefix of the flag is "-" . Available options are +urg, +ack, +psh, +rst, +syn, +fin, -urg, -ack, -psh, -rst, -syn, and -fin. If you want to define multiple flags, please enter one by one without spaces Other signs (for example, +syn ack).
shutdown	(Optional) Close interface when ACE hits

### Default

### Mode

IPv6 ACL Configuration Mode

### Instructions

Use the deny command to add deny conditions to the IPv6 ACE that discards these packets. "Sequence" also means

The hit priority when the ACL is bound to the interface. If the ACE does not specify the "sequence" index, a sequence index will be assigned, which is the largest existing index plus 20. If the package content can match multiple ACEs, the lowest sequence ACE will be hit. If it has the same conditions as an existing ACE, you cannot add an ACE.

### Instance

Add an ACE that rejects packets whose destination IP address is fe80::abcd. The

settings can be verified by the following show acl command

```
Switch(config)# ipv6 acl ipv6test
Switch(ip-al)# deny ipv6 any fe80::abcd/128 Switch(ip-al)# show acl
IPv6 access list ipv6test
sequence 1 deny ipv6 any fe80::abcd/128
```

## bind acl

### Format

```
(mac|ip|ipv6) acl NAME
no (mac|ip|ipv6) acl NAME
```

### Parameter

(mac ip ipv6)	Specify an ACL type binding interface
NAME	Specify the name of the ACL

### Default

### Mode

Interface Configuration Mode

### Instructions

Use the command (mac|ip|ipv6) acl NAME to bind the ACL to the interface. Interface can only be bound to one ACL or QoS Strategy.

Use no to unbind

### Instance

```
Bind ACL to interface
switch(config)# interface ge1
switch(config-if)# mac acltest
switch(config-if)# do show running-config interfaces ge1
interface ge1 mac acl test
```

## show acl

### Format

```
show acl
show (mac|ip|ipv6) acl
show (mac|ip|ipv6) acl NAME
```

### Parameter

(mac ip ipv6)	Specify an ACL type binding interface
NAME	Specify the name of the ACL

### Default

### Mode

Global configuration mode

Privileged mode

### Instructions

Use the show acl command to display the created acl. You can use mac, ip, or ipv6 to display a specific type of ACL, or use a unique name string to display an ACL with that name.

### Instance

```
Query all IP ACLs
Query all IP
ACLsSwitch(config)# show
ip acl IP access list iptest
sequence 1 deny ip 192.168.1.80/255.255.255.255 any
```

### show acl utilization

### Format

```
show acl utilization
```

### Parameter

### Default

### Mode

Global configuration mode

### Instructions

Use the command show acl utilization to display the usage of ASIC's PIE. When an ACL is bound to an interface, it requires ASIC resources to help filter packets. ASIC has limited resources. This command helps you understand AISC's PIE usage.

### Instance

Query usage

Switch(config-if)# do show acl utilization

Type: sys usage: 128

Type: mac ACL usage: 128

Type: IPv4 ACL usage: 128

Type: IPv6 ACL usage: 128

## 4. Administration

### configure

#### Format

configure

#### Parameter

#### Mode

Privilege Configuration Mode

#### Instructions

Make the command "configure" Global configuration mode. In the global configuration mode, the prompt will be displayed as "Switch(config)#"

#### Instance

```
Enter    global
configuration
ModeSwitch#
configure
Switch(config)#
```

### clear arp

#### Format

clear arp [A.B.C.D]

#### Parameter

A.B.C.D	Specify the ARP address to be cleared
---------	---------------------------------------

#### Mode

Privileged mode

#### Instructions

Use the command "clear arp" to clear one or all ARP entries

#### Instance

Clear all ARP entries



---

Switch(config)# clear arp

### clear service

#### Format

clear (telnet | ssh)

#### Parameter

telnet	Cancel all telnet sessions
ssh	Cancel all ssh sessions

#### Default

#### Mode

Privileged mode

#### Instructions

Use the command "clear service" to cancel a certain session service

#### Instance

Cancel telnet session  
Switch# clear telnet

### enable

#### Format

enable [<1-15>]  
disable [<1-14>]

#### Parameter

enable	Specify a privilege level to enable
disable	Specify a certain privilege level to enable

#### Default

If the privilege level is not specified on the enable command, the default privilege level is 15. If the permission level is not specified on the disable command, the default permission level is 1.

## Mode

Privileged mode

## Instructions

Use the command "enable" to enter Privileged mode and perform more operations on the switch. Use the command "disable" command to specify the required permission level. In Privileged mode, the prompt will display "Switch#"

## Instance

In Privileged mode Enable and check the level

```
Switch>enable
Switch# show privilege
CurrentCLIUsername:  admin
Current CLI Privilege:15
```

Disable and set the  
privilege level to 3

```
Switch# disable 3
Switch>show privilege
Current CLI Privilege: 3
```

end

## Format

end

## Parameter

## Default

## Mode

All Mode

## Instructions

Use the command "end" to return to Privileged mode

## Instance

Enter the interface configuration mode, and then use end to fall back to Mode

```
Switch# configure
Switch(config)# interface ge1
Switch(config-if)# end
```

Switch#

## exit

Format

exit

Parameter

Default

Mode

All Mode

Instructions

Use the exit command to close the current CLI session

Instance

Use the command exit to exit the current Mode

Switch>enable

Switch# exit

Switch>

## History

Format

history <1-256>

no history

Parameter

history	Maximum number of CLI history records
---------	---------------------------------------

Default

The maximum number of default history records is 128.

Mode

Line Configuration Mode

Instructions

Use the command "history" to be the largest command history number of the CLI running on the console, telnet, or ssh service. Each command entered will be recorded in the history buffer. If all history commands exceed the configured history number, the old commands will be deleted from the buffer.

Use the command "no history" to cancel the history record function Use the command "show history" to view all history records

### Instance

Configure the serial port command history record to 100, telnet to 150, and ssh to 200

```
Switch(config)# line console
Switch(config-line)# history 100
Switch(config-line)# exit
Switch(config)# line telnet
Switch(config-line)# history 150
Switch(config-line)# exit
Switch(config)# line ssh
Switch(config-line)# history 200
Switch(config-line)# exit
```

Query line type  
informationSwitch  
# show line  
Console

=====

```
Session Timeout : 10 (minutes)
History Count: 100Password Retry   : 3
SilentTime      : 0(seconds)
```

Telnet

=====

```
Telnet Server : disabled Session Timeout : 10 (minutes) History Count : 150
PasswordRetry   :3
SilentTime      : 0 (seconds)
```

SSH

=====

```
SSH Server   : disabled Session Timeout : 10 (minutes) History Count : 200
PasswordRetry   :3
SilentTime      : 0(seconds)
```

View historical command records

```
Switch# show history
Maximun History Count: 100
```

-----

1. enable

2. configure
3. lineconsole
4. exit
5. show history
6. line
7. exit
8. show history
9. configure
10. line
11. lineconsole
12. exit
13. lineconsole
14. history100
15. exit
16. show history
17. exit
18. show history

## hostname

### Format

hostname *WORD*

### Parameter

<i>WORD</i>	Specify the name of the switch
-------------	--------------------------------

### Default

The default name of the switch is "Switch".

### Mode

Global configuration mode

### Instructions

Use the command "hostname" to modify the name of the switch

### Instance

Edit name  
Switch(config)# hostname myname  
myname(config)#

## interface

### Format

```
interface IF_PORTS
interface range IF_PORTS
```

### Parameter

IF_PORTS	Specify the port to be selected. This Parameter allows partial port names and ignores case. For example: fa1, FastEthernet3, Gigabit4 If the port range is specified, the list Format is also available. For example: fa1,3,5,fa2,gi1-3
----------	--

### Default

### Mode

Global configuration mode

### Instructions

Some configurations are port-based. In order to configure these configurations, we need to enter the interface configuration mode to configure them. Use the command "interface" to enter the interface configuration mode and select the port to be configured.

### Instance

```
Enter interface configuration Mode
Switch# configure
Switch(config)# interface fa1
Switch(config-if)#
```

## ip address

### Format

```
ip address A.B.C.D [mask A.B.C.D]
```

### Parameter

address	Specify the switch IPv4 address
mask	Specify IP address mask

### Default

The default IP address of the switch is 192.168.2.1, and the subnet mask is 255.255.255.0.

## Mode

Global configuration mode

## Instructions

Use the command "ip address" to modify the management IPv4 address of the switch. This address is very important. When we try to use telnet, ssh, http, https, snmp... to connect to the switch, we need to use this ip address to access it

## Instance

Configure management address

```
Switch(config)# ip address 192.168.1.200 mask 255.255.255.0
```

Query management address

```
Switch# show ip
```

```
IP Address: 192.168.1.200
```

```
Subnet Netmask: 255.255.255.0
```

```
Default Gateway: 192.168.1.254
```

## ip default-gateway

## Format

```
ip default-gateway A.B.C.D
```

```
no ip default-gateway
```

## Parameter

A.B.C.D	Specify the Default gateway address managed by the switch
---------	---

## Default

The management gateway address of Switch Default is 192.168.2.254.

## Mode

Global configuration mode

Use the command "ip default-gateway" to modify the Default gateway address of the switch management IP address.

## Instance

Modify the Default gateway of the management address  
Switch(config)# ip default-gateway 192.168.1.100

Query management address  
Switch# show ip  
IP Address: 192.168.1.1  
Subnet Netmask: 255.255.255.0  
Default Gateway: 192.168.1.100

## ip dhcp

### Format

ip dhcp  
no ip dhcp

### Parameter

### Default

DefaultDHCP The client is closed.

### Mode

Global configuration mode

### Instructions

Use the command "ip dhcp" to enable the DHCP client function and obtain an IP address from the DHCP server

### Instance

Enable the DHCP  
client function  
Switch(config)# ip  
dhcp

Query DHCP client  
configuration Switch#  
show ip dhcp DHCP  
Status : enabled

## ip dns

### Format



```
ip dns A.B.C.D [A.B.C.D]
no ip dns [A.B.C.D]
```

#### Parameter

A.B.C.D	Specify the IP address of the DNS server
---------	--

#### Default

#### Mode

Global configuration mode

#### Instructions

Use the command "ip dns" to specify the IP address of the DNS server.

#### Instance

```
Configuration DNS
Switch(config)# ip dns 111.111.111.111 222.222.222.222
```

```
Inquire DNS
Switch# show ip dns
DNS lookup is enabled
DNS Server 1 : 111.111.111.111
DNS Server 2 : 222.222.222.222
```

#### ip dns lookup

#### Format

```
ip dns lookup
no ip dns lookup
```

#### Parameter

#### Default

Default Turn on DNS lookup.

#### Mode

Global configuration mode

## Instructions

Use the command "ip dns lookup" to enable the domain name to IP address service

## Instance

Enable DNS

```
Switch(config)# ip dns lookup
```

Inquire DNS

```
Switch# show ip dns
```

```
DNS Server 1 : 111.111.111.111
```

```
DNS Server 2 : 222.222.222.222
```

## ipv6 autoconfig

### Format

```
ipv6 autoconfig
```

```
no ipv6 autoconfig
```

### Parameter

### Default

IPv6 automatic configuration Default is enabled.

### Mode

Global configuration mode

## Instructions

Use command "ipv6 autoconfig" Enable IPv6 automatic configuration.

## Instance

Disable IPv6 automatic configuration

```
Switch(config)# no ipv6 autoconfig
```

Inquire IPv6

```
Switch# show ipv6
```

```
##### Config #####
```

```
State: enabled
```

```
Auto Config: disabled
```

```
DHCPv6: disabled
```

```
Gateway: ::
```

```
##### Status #####
  IP Address:
fe80::1e2a:a3ff:fec4:292/64 Default
Gateway: ::
```

## ipv6 address

### Format

```
ipv6 address X:X::X:X prefix <0-128>
```

### Parameter

address	Specify the switch IPv6 address
prefix	Specify IPv6 address prefix

### Default

### Mode

Global configuration mode

### Instructions

Use the command "ipv6 address" to configure a static IPv6 address

### Instance

```
Configure IPv6 address
Switch(config)# ipv6 address fe80::20e:2eff:fe1:4b3c prefix 128
```

```
Query IPv6 address
Switch# show ipv6
##### Config #####
  State: enabled
  Auto Config: disabled
  DHCPv6: disabled
  Gateway: ::
  IP Address: fe80::20e:2eff:fe1:4b3c/128
```

```
##### Status #####
  IP Address:
fe80::1e2a:a3ff:fec4:292/64 IP
Address:
fe80::20e:2eff:fe1:4b3c/128
```

Default Gateway:

## ipv6 default-gateway

### Format

ipv6 default-gateway X:X::X

### Parameter

default-gateway	DefaultIPv6 Gateway Address
-----------------	-----------------------------

### Default

Use the command "ipv6 default-gateway" to modify the DefaultIPv6 gateway address.

### Mode

Global configuration mode

### Instructions

Configure IPv6 gateway address

```
Switch(config)# ipv6 default-gateway fe80::dcad:beff:feef:103
```

Inquire IPv6

```
Switch# show ipv6
```

```
##### Config #####
```

```
State: enabled
```

```
Auto Config: disabled
```

```
DHCPv6: disabled
```

```
Gateway: fe80::dcad:beff:feef:103
```

```
IP Address: fe80::20e:2eff:fef1:4b3c/128
```

```
##### Status #####
```

```
IP Address: fe80::1e2a:a3ff:fec4:292/64
```

```
IP
```

```
Address: fe80::20e:2eff:fef1:4b3c/128
```

```
Default Gateway:
```

### Instance

How to add a login authentication list to use tacacs+

## ipv6 dhcp

### Format

```
ipv6 dhcp  
no ipv6 dhcp
```

### Parameter

### Default

The DefaultIPv6 DHCP client is disabled.

### Mode

Global configuration mode

### Instructions

Use the command "ipv6 dhcp" to enable the dhcpv6 client to obtain an IP address from the remote dhcpv6 server

### Instance

```
Enable IPv6 DHCP  
Switch(config)# ipv6 dhcp
```

```
Inquire IPv6 DHCP  
Switch# show ipv6 dhcp  
DHCPv6 Status : enabled
```

## ip service

### Format

```
ip (telnet | ssh | http | https)  
no ip (telnet | ssh | http | https)
```

### Parameter

telnet	Enable or disable telnet service
ssh	Enable or disable ssh service
http	Enable or disable http service
https	Enable or disable https service

### Default

```
telnet service Default disabled
ssh service Default disable
http service Default disabled
https service Default disable
```

## Mode

Global configuration mode

## Instructions

Use the command "ip service" to enable various ip services. For example, telnet, ssh, http, and https.

## Instance

```
Enable telnet service and
querySwitch(config)# ip
telnet Telnetd daemon
enabled. Switch(config)#
exit Switch# show line
telnet Telnet
=====
Telnet Server : enabled
Session Timeout : 10 (minutes)
History Count: 128
PasswordRetry   : 3
SilentTime      : 0(seconds)

Enable HTTPS service and
query
Switch(config)# ip https
Switch(config)# exit
Switch# show ip https
HTTPS daemon : enabled
Session Timeout : 10 (minutes)
```

## ip session-timeout

### Format

```
ip (http | https) session-timeout <0-86400>
```

### Parameter

http	Set the timeout period of http service type
https	Set the timeout period of the https service type
session-timeout	Timeout time, in minutes, 0 means never timeout

## Default

The default timeout time for http and https services is 10 minutes

## Mode

Global configuration mode

## Instructions

Use the command "ip session-timeout" to set the timeout period for http and https service types.

## Instance

Configure the timeout period for http and https

```
Switch(config)# ip http session-timeout 15
```

```
Switch(config)# ip https session-timeout 20
```

Query http timeout

```
Switch# show ip http
```

```
HTTPS daemon : enabled
```

```
Session Timeout : 15 (minutes)
```

Query the timeout of

https

```
Switch# show ip https
```

```
HTTPS daemon : disabled
```

```
Session Timeout : 20 (minutes)
```

## ip ssh

### Format

```
ip ssh (v1|v2|all)
```

```
no ip ssh (v1|v2|all)
```

### Parameter

v1	Generate/delete version 1 key file
v2	Generate/delete version 2 key file
all	Generate/delete version 1 and 2 key files

### Default

DefaultSSH version is V2

## Mode

Global configuration mode

## Instructions

Use the command "ip ssh" to generate the key file for the ssh connection.

## Instance

Cancel the SSH version file

```
Switch(config)# no ip ssh v2
```

```
Switch(config)# do show flash
```

```
FileName      File Size Modified
```

```
-----
```

```
startup-config 1913 2000-01-0108:29:10
```

```
rsa1 976 2000-01-05 23:28:38
```

```
ssl_cert 875 2000-01-05 23:03:20
```

```
image0(active) 4856825 2014-04-0215:17:34
```

Configure SSH V2 file

```
Switch(config)# ip ssh v2
```

Generating a SSHv2 default RSA Key.

This may take a few minutes, depending on the key size.

Generating a SSHv2 default DSA Key.

This may take a few minutes, depending on the key size.

Query FLASH files

```
Switch(config)# do show flash
```

```
FileName      File SizeModified
```

```
-----
```

```
startup-config 1913 2000-01-0108:29:10
```

```
rsa1 976 2000-01-05 23:28:38
```

```
rsa21675 2000-01-0523:34:43
```

```
dsa2 668 2000-01-0523:34:58
```

```
ssl_cert 875 2000-01-05 23:03:20
```

```
image0(active) 4856825 2014-04-0215:17:34
```

## line

### Format

line ( console | telnet | ssh )

### Parameter



console	Enter configuration under serial port Mode
telnet	Enter configuration under telnetMode
ssh	Enter sshMode configuration

### Default

### Mode

Global configuration mode

### Instructions

Some configurations are line-based. In order to configure these configurations, we need to enter the line configuration Mode to configure them. Use the command "line" to enter the line configuration mode and select the line to be configured.

### Instance

```
Enter serial port configuration mode
Switch# configure
Switch(config)# line console
Switch(config-line)#
```

### reboot

### Format

reboot

### Parameter

### Default

### Mode

Privileged mode

### Instructions

Use the command "reboot" to warm up the system.

### Instance

```
Restart the system
Switch# reboot
```

## enable password

### Format

```
enable [privilege <1-15>] (password UNENCRYPY-PASSWORD | secret
UNENCRYPY-PASSWORD | secret encrypted ENCRYPT-PASSWORD)
no enable [privilege <0-15>]
```

### Parameter

privilege	Specify permission level
password	Set the password string and make it unencrypted
secret	Set the password string and make it encrypted
secret encrypted	Enter the encryption password. Use this keyword to enter the encrypted password. For example, a password copied from the configuration file of another device

### Default

The Default enable password for all permission levels is ""

### Mode

Global configuration mode

### Instructions

Use the command "enable password" to edit the password of each permission level to enable authentication.

### Instance

```
Password for editing permission level
Switch(config)# enable secret enblpasswd
```

## exec-timeout

### Format

```
exec-timeout<0-65535>
```

### Parameter

<0-65535>	Specify the session timeout time, 0 means never timeout
-----------	---

## Default

Default timeout for all login sessions is 10 minutes

## Mode

Line Configuration Mode

## Instructions

Use the command "exec-timeout" to specify the session timeout value of the CLI running on the serial port, telnet or ssh service. When logging in to the system CLI without doing any operation, the system will log out of the login session after the timeout period expires.

## Instance

```
Modify the serial port timeout time to 15 minutes, telnet to
20 minutes and SSH to 25 minutes Switch(config)# line
console
Switch(config-line)# exec-timeout 15
Switch(config-line)# exit
Switch(config)# line telnet
Switch(config-line)# exec-timeout 20
Switch(config-line)# exit
Switch(config)# line ssh
Switch(config-line)# exec-timeout 25
Switch(config-line)# exit
```

Query configuration

```
Switch# show line
```

Console

```
=====
Session Timeout : 15 (minutes)
History Count: 128
PasswordRetry   : 3
SilentTime      : 0(seconds)
```

Telnet

```
=====
Telnet Server : disabled
Session Timeout : 20 (minutes)
History Count: 128
PasswordRetry   : 3
SilentTime      : 0(seconds)
```

SSH

```
=====
SSH Server : disabled
```

Session Timeout : 25 (minutes)  
 History Count: 128  
 PasswordRetry : 3  
 SilentTime : 0(seconds)

## password-thresh

### Format

password-thresh <0-120>

### Parameter

<0-120>	The number of retries after password verification fails, 0 means no limit
---------	---

### Default

Default number of retries is 3.

### Mode

Line Configuration Mode

### Instructions

Use the command "password-thresh" to set the number of failed password retries for the CLI running on the console, telnet, or ssh service. When the password login authentication fails, the number of failed retries increases by one. After the number of failed retries exceeds the configured number, the CLI will block login during the silent time period configured by the command "silent time"

### Instance

```
Configure password failure retry times
Switch(config)# line console
Switch(config-line)# password-thresh 4
Switch(config-line)# exit Switch(config)#
line telnet Switch(config-line)#
password-thresh 5 Switch(config-line)#
exit Switch(config)# linessh
Switch(config-line)# password-thresh 6
Switch(config-line)# exit
```

```
Check line status
Switch# show line
Console
```

```
=====
Session Timeout : 10 (minutes)
```

```
History Count: 128
PasswordRetry : 4
SilentTime : 0 (seconds)
Telnet
```

```
=====
Telnet Server : disabled
Session Timeout : 10 (minutes)
History Count: 128
PasswordRetry :5
SilentTime : 0 (seconds)
SSH
```

```
=====
SSH Server : disabled
Session Timeout : 10 (minutes)
History Count: 128
PasswordRetry : 6
SilentTime : 0(seconds)
```

## ping

### Format

```
ping HOSTNAME [count <1-999999999>]
```

### Parameter

HOSTNAME	Specify IPv4/IPv6 address or domain name to ping
count	Configure the number of pings

### Default

### Mode

Privileged mode

### Instructions

Use the command "ping" for network diagnosis.

### Instance

```
ping remote host
192.168.1.111. Switch# ping
192.168.1.111
PING 192.168.1.111 (192.168.1.111): 56 data bytes
64 bytes from 192.168.1.111: icmp_seq=0 ttl=128 time=10.0 ms
64 bytes from 192.168.1.111: icmp_seq=1 ttl=128 time=0.0 ms
64 bytes from 192.168.1.111: icmp_seq=2 ttl=128 time=0.0 ms
64 bytes from 192.168.1.111: icmp_seq=3 ttl=128 time=0.0 ms
```

---

```
--- 192.168.1.111 ping statistics ---
4 packets transmitted, 4 packets received, 0% packet
loss round-trip min/avg/max = 0.0/2.5/10.0 ms
```

## traceroute

### Format

```
traceroute A.B.C.D [max_hop <2-255>]
```

### Parameter

A.B.C.D	Specify IPv4 address for traceroute
max_hop	Maximum next hop

### Default

### Mode

Privileged mode

### Instructions

Use the command "traceroute" for network diagnosis.

### Instance

```
Traceroute Remote host 192.168.1.111.
Switch# traceroute 192.168.1.111
traceroute to 192.168.1.111 (192.168.1.111), 30 hops max, 40 byte packets
 192.168.1.111(192.168.1.111)  0ms   10ms   0ms
```

## silent-time

### Format

```
silent-time <0-65535>
```

### Parameter

<0-65535>	Quiet time, in seconds, 0 means never silent.
-----------	---

### Default

Default is 0

## Mode

Line Configuration Mode

## Instructions

Use the command "silent time" to set the silent time for the CLI running on the console, telnet or ssh service. When the user enters a password to log in and fails to verify, the number of failed retries will increase by one. After the number of failed retries exceeds the configured number, the CLI will block login during the silent time period configured by the "silent time" command.

## Instance

```
Configure quiet time
Switch(config)# line console
Switch(config-line)# silent-time 10
```

```
Query line
information
Switch# show line
Console
=====
Session Timeout : 10 (minutes)
History Count: 128
PasswordRetry   :3
SilentTime      : 10(seconds)
```

## ssl

## Format

```
ssl
```

## Parameter

## Default

## Mode

Global configuration mode

## Instructions

Use the command "ssl" to generate a security certificate file, such as RSA, DSA

## Instance

Config SSL

```
Switch(config)# ssl
```

```
Inquire flash file
```

```
Switch# show flash
```

```
FileName      File SizeModified
-----
startup-config 1191 2000-01-0100:00:23
backup-config 1607 2000-01-0108:36:23
rsa1 974 2000-01-01 00:00:18
rsa21675 2000-01-0100:00:18
dsa2 668 2000-01-0100:00:18
ssl_cert 993 2000-01-01 00:00:18
```

### system name

#### Format

```
system name NAME
```

#### Parameter

NAME	Specify system name
------	---------------------

#### Default

Default system name is "Switch"

#### Mode

Global configuration mode

#### Instructions

Use the command "system name" to specify the system name.

#### Instance

Configure system name

```
Switch(config)# system name myname
```

```
myname(config)#
```

### system contact

#### Format

```
system contact CONTACT
```



**Parameter**

CONTACT	Specify contact information
---------	-----------------------------

**Default****Mode**

Global configuration mode

**Instructions**

Use the command "system contact" to specify the system contact information.

**Instance**

Configure contact information and query

```
Switch(config)# system contact callme
```

```
Switch# show info
```

```
System Name: Switch
```

```
SystemLocation : Default Location
```

```
SystemContact :callme
```

```
MAC Address :DE:AD:BE:EF:01:02
```

```
IP Address :192.168.1.1
```

```
Subnet Mask : 255.255.255.0
```

```
LoaderVersion :1.3.0.26225
```

```
Loader Date : Thu May 17 15:19:42 CST 2012
```

```
Firmware Version : 2.5.0-beta.32811
```

```
FirmwareDate : Mon Sep 24 19:33:42 CST 2012
```

```
System Object ID :1.3.6.1.4.1.27282.3.2.10
```

```
SystemUp Time : 0 days, 0 hours, 2 mins, 37secs
```

**system location****Format**

system location LOCATION

**Parameter**

LOCATION	Specify system local information
----------	----------------------------------

**Default****Mode**

---

Global configuration mode

### Instructions

Use the command "system location" to specify system local information.

### Instance

Configure contact information and query

```
Switch(config)# system location home
```

```
Switch# show info
```

```
System Name: Switch
```

```
SystemLocation : home
```

```
SystemContact :
```

```
MAC Address :DE:AD:BE:EF:01:02
```

```
IP Address :192.168.1.1
```

```
Subnet Mask : 255.255.255.0
```

```
LoaderVersion :1.3.0.26225
```

```
Loader Date : Thu May 17 15:19:42 CST 2012
```

```
Firmware Version : 2.5.0-beta.32811
```

```
FirmwareDate : Mon Sep 24 19:33:42 CST 2012
```

```
System Object ID :1.3.6.1.4.1.27282.3.2.10
```

```
SystemUp Time : 0 days, 0 hours, 2 mins, 37secs
```

### terminal length

#### Format

```
terminal length <0-24>
```

length	Set the length of the terminal printing table, 0 means never limit.
--------	---

#### Default

Default is24

#### Mode

Privileged mode

### Instructions

Use the command "terminal length" to set the maximum line number that the terminal can print.

### Instance

Configure the terminal display line number

```
Switch# terminal length 3
Switch# show running-config SYSTEM CONFIG FILE ::= BEGIN
! System Description: RTK RTL8380-24FE-4GEC Switch
! System Version: v3.0.4.46766
--More--
```

## username

### Format

```
username WORD<0-32> [privilege (admin|user|<0-15>)] (nopassword |
password UNENCRYPY-PASSWORD | secret UNENCRYPY-PASSWORD |
secret encrypted ENCRYPT-PASSWORD)
no username WORD<0-32>
```

### Parameter

WORD<0-32>	User name, you can add, delete, modify by name
privilege admin	The permission level is administrator (privilege 15)
privilege user	The permission level is user (privilege 1)
privilege <0-15>	Custom user permission level
nopassword	No password
password	Unencrypted password string
secret	Encrypted password string
secret encrypted	Enter the encrypted password string

### Default

The default user name of the system is admin, the password is admin, and the authority level is 15.

### Mode

Global configuration mode

### Instructions

Use the command "username" to add/modify a user.

### Instance

Add a user

```
Switch(config)# username test secret passwd
```

Query all users of the system

```
Switch# show username
```

Priv	Type	UserName	Password
15	secret	admin	MjEyMzJmMjk3YTU3YTVhNzQzODk0YTBINGE4MDFmYzM=
15	secret	test	NzZhMjE3M2JINjM5Mzl1NGU3MmZmYTRkNmRmMTAzMGE=

### show arp

#### Format

```
show arp
```

#### Parameter

#### Default

#### Mode

Privileged mode

#### Instructions

Use the command "show arp" to query all ARP entries.

#### Instance

```
Query ARP entries
Switch# show arp
AddressHWtypeHWaddress  FlagsMask  Iface
192.168.1.111ether      00:0E:2E:F1:4B:3C  C   eth0
```

### show cpu utilization

#### Format

```
show cpu utilization
```

#### Parameter

#### Default

#### Mode

Privileged mode

#### Instructions

Use the command "show cpu utilization" to query the CPU usage.

#### Instance

Query CPU usage  
Switch# show cpu utilization  
CPU utilization  
-----  
Current: 30%

## show history

### Format

show history

### Parameter

### Default

### Mode

Privileged mode

### Instructions

Use the command "show history" to query the command line history.

### Instance

Query historical information  
Switch# show history  
Maximun History Count: 100  
-----

1. enable
2. configure
3. lineconsole
4. exit
5. show history
6. line
7. exit
8. show history
9. configure
10. line
11. lineconsole
12. exit
13. lineconsole
14. history100

## show info

### Format

```
show info
```

### Parameter

Default

Mode

Privileged mode

### Instructions

Use the command "show info" to query the system summary information.

### Instance

```
Query system
summary information
Switch# show info
System Name: Switch
SystemLocation : Default Location
SystemContact  : DefaultContact
MAC Address :DE:AD:BE:EF:01:02
IP Address   :192.168.1.1
Subnet Mask  : 255.255.255.0
LoaderVersion :1.3.0.26225
Loader Date  : Thu May 17 15:19:42 CST 2012
Firmware Version : 2.5.0-beta.32811
FirmwareDate   : Mon Sep 24 19:33:42 CST 2012
System Object ID :1.3.6.1.4.1.27282.3.2.10
SystemUp Time  : 0 days, 1 hours, 49 mins, 29secs
```

## show ip

### Format

```
show ip
```

### Parameter

Default

Mode

Privileged mode

### Instructions

Use the command "show ip" to query the system management IP address.

## Instance

```
Query IP address
Switch# show ip
IP Address: 192.168.1.200
Subnet Netmask: 255.255.255.0
Default Gateway: 192.168.1.254
```

## show ip dhcp

### Format

```
show ip dhcp
```

### Parameter

#### Default

#### Mode

```
Privileged mode
```

### Instructions

Use the command "show ip dhcp" to query the IPv4 DHCP client enable status.

## Instance

```
Query DHCP client
configuration Switch#
show ip dhcp DHCP
Status : enabled
```

## show ip dns

### Format

```
show ip dns
```

### Parameter

#### Default

#### Mode

```
Privileged mode
```

### Instructions

Use the command "show ip dns" to query the system IPv4 DNS address.

## Instance

```
Query DNS
Switch# show ip dns
DNS lookup is enabled
DNS Server 1 : 111.111.111.111
DNS Server 2 : 222.222.222.222
```

## show ip http

### Format

```
show ip (http|https)
```

### Parameter

#### Default

#### Mode

Privileged mode

### Instructions

Use the command "show ip http" to query http and https service information.

## Instance

```
Switch# show ip http
HTTP daemon : enabled Session
Timeout : 10(minutes)
```

## show ipv6

### Format

```
show ipv6
```

### Parameter

#### Default

#### Mode

Privileged mode

### Instructions

Use the command "show ip" to query the system management IPv6 address.

## Instance



```

Query IPv6 address
Switch# show ipv6
##### Config #####
      State: enabled
      Auto Config: enabled
      DHCPv6: disabled
      Gateway:
##### Status #####
      IP Address:
fe80::1e2a:a3ff:fec4:292/64 Default
Gateway: ::

```

### show ipv6 dhcp

#### Format

```
show ipv6 dhcp
```

#### Parameter

Default

Mode

Privileged mode

#### Instructions

Use the command "show ipv6 dhcp" to query the system IPv6 status.

#### Instance

```

Query IPv6 DHCP
Switch# show ipv6 dhcp
DHCPv6 Status : enabled

```

### show line

#### Format

```
show line[(console | telnet | ssh)]
```

#### Parameter

console	Query the configuration under serial port mode
telnet	Query configuration under telnetMode
ssh	Query the configuration under sshMode

#### Default

## Mode

Privileged mode

## Instructions

Use the command "show line" to display all line configurations, including session timeout, history count, password retries, and silent time. For telnet and ssh, it also displays the service enable/disable status.

## Instance

Query line  
information  
Switch# show line  
Console

```
=====
Session Timeout : 15 (minutes)
History Count: 128
PasswordRetry   : 3
SilentTime      : 0(seconds)
```

Telnet

```
=====
Telnet Server : disabled
Session Timeout : 20 (minutes)
History Count: 128
PasswordRetry   : 3
SilentTime      : 0(seconds)
```

SSH

```
=====
SSH Server   : disabled
Session Timeout : 25(minutes)
History Count: 128
PasswordRetry   : 3
SilentTime      : 0(seconds)
```

## show memory statistics

### Format

```
show memory statistics
```

### Parameter

### Default

**Mode**

Privileged mode

**Instructions**

Use the command "show memory statistics" to query system memory usage information.

**Instance**

Query memory usage information

Switch# show memory statistics

	total(KB)	used(KB)	free(KB)	shared(KB)	buffer(KB)
cache(KB)					
-----+-----+-----+-----+-----					
+-----					
Mem:	126192	70752	55440	0	0
0					
-/+ buffers/cache:		70752	55440		
Swap:	0	0	0		

**show privilege****Format**

show privilege

**Parameter****Default****Mode**

Privileged mode

**Instructions**

Use the command "show privilege" to query the privilege level of the current user.

**Instance**

Query current user authority

level

Switch# show privilege

Current CLI username: admin

Current CLI Privilege: 15

**show username**

**Format**

```
show username
```

**Parameter****Default****Mode**

Privileged mode

**Instructions**

Use the command "show username" to query current usage information.

**Instance**

Query user information

```
Switch# show username
```

```
Priv |Type   | user Name   | Password
```

```
-----+-----+-----+-----
```

```
01 | secret | dnXencJRwflV6
```

```
15 | secret | admin | FzjrGO6vfbERY
```

```
15 | secret | test | 7p57T9yMkViSUS
```

**show users****Format**

```
show users
```

**Parameter****Default****Mode**

Privileged mode

**Instructions**

Use the command "show users" to query the current active user information.

**Instance**

Query active user information

```
Switch# show users
```

```
username   ProtocolLocation
```

```
-----
```

```
admin   console0.0.0.0
```

```
admin   telnet   192.168.1.111
```

admin ssh192.168.1.111

## show version

### Format

show version

### Parameter

Default

Mode

Privileged mode

### Instructions

Use the command "show version" to query the system loader and firmware version information.

### Instance

Query version information

Switch# show version

LoaderVersion :1.3.0.26225

Loader Date : Thu May 17 15:19:42 CST 2012

Firmware Version : 2.5.0-beta.32811

FirmwareDate : Mon Sep 24 19:33:42 CST2012

## 5. AuthenticationManager

### authentication

#### Format

```
authentication (dot1x|mac|web)
no authentication (dot1x|mac|web)
```

#### Parameter

#### Default

Default all authentication is disabled

#### Mode

Global configuration mode

#### Instructions

Use the command "authentication" to enable the global settings of 802.1x/MAC/WEB authentication network access control.

#### Instance

```
Enable 802.1x/MAC/WEB
authentication Switch(config)#
authentication dot1x Switch(config)#
authentication mac Switch(config)#
authentication web

Query certification
Switch# show authentication
Authentication dot1x state : enabled
Authentication mac state : enabled
Authentication web state : enabled
Guest VLAN : enabled (3)
Mac-auth Radius user ID Format: XXXXXXXXXXXXX
.....
```

### authentication(Interface)

#### Format

```
authentication (dot1x|mac|web)
no authentication (dot1x|mac|web)
```

## Parameter

## Default

Default all authentication is disabled

## Mode

Interface configuration Mode

## Instructions

Use the command "authentication" to enable 802.1x/MAC/WEB authentication network access control under the interface.

## Instance

```
Enable interface 802.1x/MAC/WEB
authentication Switch(config)# interface
g1 Switch(config-if)# authentication
dot1x Switch(config-if)# authentication
mac Switch(config-if)# authentication
web
```

```
Query authentication under the interface
Switch# show authentication interface g1
Interface GigabitEthernet11
AdminControl: disable
HostMode    : multi-auth
Type dot1x State : enabled
TypemacState    : enabled
Typeweb State   :enabled
.....
```

## authentication mac radius

## Format

```
authentication mac radius [mac-case (lower|upper)] [mac-
delimiter(colon|dot|hyphen|none) [gap (2|4|6)]]
```

## Parameter

mac-case	Select the radius user ID as uppercase or lowercase upper: uppercase; lower: lowercase
----------	---

mac-delimiter	Select radius user ID separator colon: XX:XX:XX:XX:XX:XX; dot: XX.XX.XX.XX.XX.XX; hyphen: XX-XX-XX-XX-XX-XX; none: XXXXXXXXXXXXX
gap	Select separator spacing 2: XX-XX-XX-XX-XX-XX; 4: XXXX-XXXX-XXXX 6: XXXXXX-XXXXXX

### Default

Default's radius identifier Format is upper, and the separator is none.

### Mode

Global configuration mode

### Instructions

Use the command "authentication mac radius" to configure the format of the radius user ID.

### Instance

Configure User ID Format

```
Switch(config)# authentication mac radius mac-case upper
```

```
Switch(config)# authentication mac radius mac-delimiter colon gap 2
```

Query configuration

```
Switch# show authentication
```

```
Authenticationdot1xstate : enabled
```

```
Authenticationmacstate : disabled
```

```
Authenticationwebstate : disabled
```

```
Guest VLAN :disabled
```

```
Mac-auth Radius user ID Format: XX:XX:XX:XX:XX:XX
```

.....

## authentication mac local

### Format

```
authentication mac local mac-addr control auth [vlan <1-4094>] [reauth-  
period <300-4294967294>] [inactive-timeout <60-65535>] authentication
```

```
mac local mac-addr controlunauth
```

```
no authentication mac local mac-addr
```

### Parameter

mac-addr	Locally authenticated MAC address
control auth	The host using the MAC address needs to be authenticated



control unauth	The host using the MAC address is not authenticated
vlan	VLAN assigned by MAC authentication host
reauth- period	Recertification cycle
inactive-timeout	The inactive timeout period of the authentication host

### Default

System Default does not enable MAC address authentication

### Mode

Global configuration mode

### Instructions

Use the command "authentication mac local" for local MAC authentication to the database. When MAC authentication is "local", the local host database is used, and the MAC authentication module queries and authenticates the local host database MAC address.

### Instance

Add MAC local authentication

```
Switch(config)# authentication mac local 00:11:22:33:00:01 control auth vlan 3
reauth-period 500 inactive-timeout 300
```

Query certification

```
Switch# show authentication
```

.....

Mac-auth Local Entry:

```
Reauth      Inactive MAC Address Control VLAN      Period  Timeout
-----
Authorized          3   500300          00:11:22:33:00:01
.....
```

### authentication guest-vlan

### Format

```
authentication guest-vlan <1-4094>
no authentication guest-vlan
```

### Parameter

guest-vlan	Guest's VLAN ID
------------	-----------------

## Default

## Mode

Global configuration mode

## Instructions

Use the command "authentication guest-vlan" to configure the guest's VLAN ID.

## Instance

Add guest VLAN

```
Switch(config)# authentication guest-vlan 3
```

## authentication guest-vlan (Interface)

## Format

```
authentication guest-vlan  
no authentication guest-vlan
```

## Parameter

## Default

Default is disabled.

## Mode

Interface configuration Mode

## Instructions

Use the command "authentication guest-vlan" to enable the VLAN ID of the interface guest.

## Instance

Enable VLAN for interface

guest

```
Switch(config)# interface gi1
```

```
Switch(config)# authentication guest-vlan
```

## authentication host-mode

## Format

```
authentication host-mode (multi-auth|multi-host|single-host)
```

no authentication host-mode

#### Parameter

multi-auth	Multiple authentication modes. Each client in this mode needs to be individually authenticated
multi-host	Multi-host Mode. Only one client needs to be authenticated in this mode, and other clients End will get the same accessibility
single-host	Single host mode. Only one host is allowed to be authenticated. It is related to multiple authentication mode Same, the maximum number of hosts is configured as 1.

#### Default

Default is multi-auth

#### Mode

Interface configuration Mode

#### Instructions

Use the command "authentication host-mode" to configure the host authentication mode.

#### Instance

```
Configure interface authentication mode
Switch(config)# interface gi1
Switch(config-if)# authentication host-mode multi-host
Query the authentication mode of the interface
Switch# show authentication interface gi1
Interface FastEthernet1
AdminControl: auto
HostMode    : multi-host
Type dot1x State : disabled
TypemacState  : disabled
Typeweb State  : disabled
.....
```

#### authentication max-hosts

#### Format

```
authentication max-hosts<1-
256>no authentication max-hosts
```

## Parameter

max-hosts	The maximum number of hosts available in multiple authentication mode.
-----------	--

## Default

The maximum number of hosts in the system multi-identity authentication mode is 256.

## Mode

Interface configuration Mode

## Instructions

Use the command "authentication max-hosts" to configure the maximum number of hosts on the interface in multi-authentication mode. When the number of hosts exceeds the maximum, the creation of authentication sessions and authentication are not allowed.

## Instance

Configure the maximum number of authentication hosts for the interface

```
Switch(config)# interface g1
Switch(config-if)# authentication max-hosts 100
```

Query authentication under interface

```
Switch# show mac-auth interface g1
Interface GigabitEthernet1
AdminControl : disable
HostMode     : multi-auth
Type dot1x State : disabled
TypemacState : disabled
Typeweb State  :disabled
TypeOrder    : dot1x MAC/WEB
MethodOrder  : radius Guest
VLAN : disabled
Reauthentication : disabled
MaxHosts     :100
.....
```

## authentication port-control

## Format

```
authentication port-control (auto|force-auth|force-unauth)
no authentication port-control
```

## Parameter

auto	Need to go through the authentication process to gain network accessibility
force-auth	The port is authorized by force, and all clients have network accessibility.
force-unauth	The port is forced to be unauthorized, and all clients have no network accessibility.

### Default

Default is disabled.

### Mode

Interface configuration Mode

### Instructions

Use the command "authentication port-control" to enable the mode of port authentication control.

### Instance

```

Configure port authentication control mode
Switch(config)# interface g1
Switch(config-if)# authentication port-control auto
Switch# show authentication interface g1
Interface GigabitEthernet1
AdminControl: auto
HostMode      : multi-auth
Type dot1x State : disabled
TypemacState  : disabled
Typeweb State  :disabled
.....

```

### clear authentication sessions

#### Format

```

clear authentication sessions
clear authentication sessions interfaces IF_PORTS
clear authentication sessions mac mac-addr clear
authentication sessions session-idWORD
clear authentication sessions type (dot1x|mac|web)

```

#### Parameter

interfaces	Clear according to interface
mac	Clear by MAC

session-id	Clear according to session ID
type	Clear according to session authentication type

### Default

### Mode

Privileged mode

### Instructions

Use the command "clear authentication sessions" to delete existing sessions. If you do not specify Parameter, delete all sessions. After the session is deleted, the user needs to re-authenticate.

### Instance

Clear all sessions and query  
 Switch# clear authentication sessions  
 Switch# show authentication sessions No  
 Auth Manager sessions currently exist

### show authentication

### Format

show authentication  
 show authentication interfaces *IF\_PORTS*

### Parameter

interfaces	Query certification information through the specified interface
------------	---

### Default

### Mode

Privileged mode

### Instructions

Use the command "show authentication" to query all authentication configurations. Use the command "show authentication interface" to query the authentication configuration under the interface.

### Instance

```

Check all certifications
Switch# show authentication
Authenticationdot1xstate : enabled
Authenticationmacstate   : disabled
Authenticationwebstate   : disabled
Guest VLAN :disabled
Mac-auth Radius user ID Format: XXXXXXXXXXXXX

```

```

Mac-auth Local Entry:
Reauth      Inactive MAC Address Control VLAN      Period  Timeout
-----
Authorized          3   30000   123          00:11:22:33:44:55

```

```

Web-auth Local Entry :
Reauth  Inactive
user Name  VLAN  Period  Timeout
-----
          12345  333          acct1      5

```

```

Interface Configurations Interface
GigabitEthernet1 AdminControl :disable
HostMode          : multi-auth
Type dot1x State  : disabled
TypemacState     : disabled
Typeweb State    :disabled
TypeOrder        : dot1x MAC/WEB
MethodOrder      : radius Guest
VLAN             : disabled
Reauthentication : disabled
MaxHosts         :256
VLANAssignMode   : static Common Timers
Reauthenticate Period: 3600 Inactive Timeout : 60
Quiet Period : 60 802.1x Parameters
EAP Max Request : 2
EAP TX Period : 30 Supplicant Timeout : 30 Server Timeout : 30
Web-auth Parameters
Login Attempt : 3
.....

```

```

By interface Query certification
Switch# show authentication interface g7
Interface ConfigurationsInterface
GigabitEthernet7 AdminControl :auto
HostMode          :multi-auth
Typedot1x State   : enabled
TypemacState     :disabled
Typeweb State    : disabled
TypeOrder        : dot1x MAC/WEB
Method Order     : radius Guest VLAN

```

```

: disabled
Reauthentication      : disabled
MaxHosts             256
VLANAssignMode       :static
Common Timers Reauthenticate Period: 3600
InactiveTimeout      60
Quiet Period 60
802.1x Parameters
EAP Max Request 2
EAPTXPeriod          30
SupplicantTimeout    30
ServerTimeout        :
65535 Web-
authParameters
Login Attempt

```

### show authentication sessions

#### Format

```

show authentication sessions [detail]
show authentication sessions interface IF_PORTS
show authentication sessions session-id WORD show
authentication session type (dot1x|mac|web)

```

#### Parameter

detail	Query session details
interface	Query session information according to the specified interface
session-id	Query session information based on the specified ID
type	Query session information based on authentication type

#### Default

#### Mode

Privileged mode

#### Instructions

Use the command "show authentication sessions" to query session information.

#### Instance

```

Query session information
Switch# show authentication sessions
Interface MACAddressType      Status  SessionID
-----
----- g7

```



00:01:6C:CB:29:4A dot1x      Authorized      000000010000A028

Query session details

Switch# show authentication sessions detail

Interface : GigabitEthernet7

MAC Address : 00:01:6C:CB:29:4A

SessionID    :000000010000A028

Current Type : dot1x

Status      : Authorized Authorized Information

VLAN        : 5 (fromRADIUS)

Reauthenticate Period: 301 (from RADIUS)

Inactive Timeout : 600 (from RADIUS)

Operational Information VLAN : 5 Session

Time :1143

Inactive Time : 168

QuietTime    :N/A

## 6. Diagnostic

### show cable-diag

#### Format

show cable-diag interfaces *IF\_NMLPORTS*

#### Parameter

Interfaces	Display the interface ID of the copper medium or the cable diagnostic information of the interface ID list.
------------	---

#### Default

#### Mode

Privileged mode

#### Instructions

Use the command "show cable-diag" to display the estimated copper cable length connected to a specific interface. In order to get the correct cable length information, the interface must be active and connected.

#### Instance

Interface G1 and G2 for line diagnosis

Switch# show cable-diag interfaces g1-2

```

Port   | Speed | Local pair | Pair length | Pairstatus
-----+-----+-----+-----+-----
gi1    | auto  | PairA      | 1.00        | Open
        |       | Pair B     | 0.96        | Open
        |       | Pair C     | 0.92        | Open
        |       | Pair D     | 0.88        | Open

gi2    | auto  | PairA      | 2.12        | Open
        |       | Pair B     | 2.11        | Open
        |       | PairC     | 2.03        | Open
        |       | PairD     | 2.06        | Open

```

### show fiber-transceiver

#### Format

show fiber-transceiver interfaces *IF\_NMLPORTS*

## Parameter

Interfaces	Display the interface ID of the fiber optic transceiver or diagnostic information of the interface ID list.
------------	---

## Default

## Mode

Privileged mode

## Instructions

Use the command "show fiber-transceiver" to display the diagnostic information of the fiber optic transceiver.

## Instance

Query optical module DDM information

Switch# showfiber-transceiver interfaces gi1-2

```
Port|Temperature      | Voltage | Current | Output power | Input power|[C] |[Volt]
    |[mA]      | [mWatt]|[mWatt]|
```

```
=====
```

```
=====
```

```
gi1 |N/S      |N/S      |N/S      |N/S      |N/S      |Insert  |gi2|N/S      |N/S
    | N/S|N/S      |N/S      |Insert  |
```

Temp - Internally measured transceiver

temperature Voltage - Internally measured

supplyvoltage

Current - Measured TX bias current

Output Power - Measured TX output power in milliWatts

Input Power - Measured RX received power in milliWatts

OE-Present - SFP Presetn or NotPresent

LOS - Loss of signal

N/A - Not Available, N/S - Not Supported, W - Warning, E - Error

## 7. DHCP Snooping

### ip dhcp snooping

#### Format

```
ip dhcp snooping no  
ip dhcp snooping
```

#### Parameter

#### Default

Default disable

#### Mode

Global configuration mode

#### Instructions

Use the command "ip dhcp snooping" to enable DHCP Snooping.

#### Instance

```
Enable DHCP Snooping function and  
query  
switch(config)# ip dhcp snooping  
switch(config)# ip dhcp snooping vlan 1  
switch(config)# show ip dhcp snooping  
DHCP Snooping: enabled Enable on following Vlans 1  
circuit-id default format: vlan-port  
remote-id : 00:11:22:33:44:55 (Switch Mac in Byte Order)
```

### ip dhcp snooping vlan

#### Format

```
ip dhcp snooping vlan VLAN-LIST
```

#### Parameter

vlan	Specify VLAN ID or range to enable DHCP Snooping
------	--

#### Default

Default disable

## Mode

Global configuration mode

## Instructions

Use the command "ip dhcp snooping vlan" to enable the VLAN-level DHCP Snooping function.

## Instance

```
Enable the VLAN-level DHCP Snooping
function and check
switch(config)# vlan 1-100 switch(config)#
exit
switch(config)# ip dhcp snooping
switch(config)# ip dhcp snooping vlan 1-100
switch(config)# show ip dhcp snooping
DHCP Snooping      :enabled
Enable onfollowingVlans  : 1-100
circuit-id default format :vlan-port
remote-id: 00:11:22:33:44:55 (Switch Mac in Byte Order)
```

## ip dhcp snooping trust

### Format

```
ip dhcp snooping trust no
ip dhcp snoopingtrust
```

### Parameter

#### Default

#### Mode

Interface configuration Mode

## Instructions

Use the command "ip dhcp snooping trust" to set the interface trust switch. The switch does not check the DHCP packet received on the trusted interface; it just forwards it.

## Instance

```
Configure interface G1 as a trusted port
and query
switch(config)# interface gi1
switch(config-if)# ip dhcp snooping trust
switch(config-if)# do show ip dhcp snooping interface gi1
Interfaces | Trust State | Rate (pps) | hwaddr Check | Insert Option82 |
```

```

-----+-----+-----+-----+-----
-----+
      gi1 | Trusted|None |disabled |disabled |

```

### ip dhcp snooping verify

#### Format

```

ip dhcp snooping verify mac-address no
ip dhcp snooping verify mac-address

```

#### Parameter

#### Default

#### Mode

Interface configuration Mode

#### Instructions

Use the command "ip dhcp snooping verify" to enable the MAC address verification function on the interface.

#### Instance

```

Enable MAC authentication of the interface
switch(config)# interface gi1
switch(config-if)# ip dhcp snooping verify mac-address
switch(config-if)# do show ip dhcp snooping interface gi1 Interfaces
| Trust State | Rate (pps) | hwaddr Check | Insert Option82 |
-----+-----+-----+-----+-----
-----+
      gi1 | Untrusted | None|disabled |disabled |

```

### ip dhcp snooping rate-limit

#### Format

```

ip dhcp snooping rate-limit <1-300>
no ip dhcp snooping rate-limit

```

#### Parameter

rate-limit	Set the DHCP packet rate limit from 1 to 300 PPS
------------	--

#### Default

Default unlimited speed

## Mode

Interface configuration Mode

## Instructions

Use the command "ip dhcp snooping rate-limit" to set the rate limit on the interface. The switch discards DHCP packets after receiving more than the configured packet rate per second

## Instance

Configure the interface DHCP message rate  
 switch(config)# interface gi1  
 switch(config-if)# ip dhcp snooping rate-limit 30  
 switch(config-if)# do show ip dhcp snooping interfaces gi1 Interfaces|Trust  
 State|Rate (pps)|hwaddr Check|Insert Option82|  
 -----+-----+-----+-----+-----+  
 gi1 | Untrusted|30 |disabled |disabled |

## clear ip dhcp snooping statistics

### Format

clear ip dhcp snooping interfaces IF\_PORTS statistics

### Parameter

interfaces	Clear the statistics of the specified interface
------------	---

### Default

### Mode

Privileged mode

### Instructions

Use the command "clear ip dhcp snooping interfaces statistics" to clear the statistics under the interface.

### Instance

Clear the statistics of GE1 interface  
 switch# clear ip dhcp snooping interfaces gi1 statistics

```

switch# show ip dhcp snooping interfaces gi1 statistics
Interfaces | Forwarded | Chaddr Check Dropped | Untrust Port Dropped | Untrust
Port With Option82 Dropped | Invalid Drop
-----+-----+-----+-----+-----
-----+-----
gi1 | 0 | 0 | 0 | 0 | 0

```

### show ip dhcp snooping

#### Format

```
show ip dhcp snooping
```

#### Parameter

#### Default

#### Mode

Privileged mode

#### Instructions

Use the command "show ip dhcp snooping" to query the DHCP Snooping configuration.

#### Instance

```

Query DHCP Snooping
switch(config)# show ip dhcp snooping
DHCP Snooping      : enabled
Enable onfollowingVlans  : 1
circuit-id default format:vlan-port
remote-id:         : 00:11:22:33:44:55 (Switch Mac in ByteOrder)

```



## 8. DOS

### dos

#### Format

```
dos (daeqsa-deny|icmp-frag-pkts-deny|icmpv4-ping-max- check|icmpv6-
ping-max-check|ipv6-min-frag-size-check|land- deny|nullscan-deny|pod-
deny|smurf-deny|syn-sport1024-deny|synfin- deny|synrst-deny|tcp-frag-
off-min-check|tcpblat- deny|tcphdr-min- check|udpblat-deny|xmas-deny)
dos icmp-ping-max-length MAX_LEN dos
ipv6-min-frag-size-length MIN_LEN dos
smurf-netmask MASK
dos tcphdr-min-length HDR_MIN_LEN
no dos (tcp-frag-off-min-check|synrst-deny|synfin-deny|xma-
deny|nullscan-deny|syn-sport1024-deny|tcphdr-min-check|smurf-
deny|icmpv6-ping-max-check|icmpv4-ping-max-check|icmp-frag-
pkts- deny|ipv6-min-frag-size-check|pod-deny|tcpblat- deny|udpblat-
deny|land- deny|daeqsa-deny)
```

#### Parameter

daeqsa-deny	If the destination MAC address is equal to the source MAC address, the packet is discarded.
icmp-frag-pkts-deny	Delete fragmented ICMP packets
icmpv4-ping-max-check	Check the maximum size of the ICMP ping packet and delete the one that is larger than the command definition Maximum packet size packet
icmpv6-ping-max-check	Check the maximum size of the ICMPv6 ping packet, and delete the command definition greater than The maximum packet size of the packet
ipv6-min-frag-size-	Check the minimum size of the IPv6 fragment and discard the minimum size less than the command defined
check	data pack
land-deny	Drop packets with the same source and destination IP
nullscan-deny	Delete empty scanned packets
pod-deny	Avoid death attacks
smurf-deny	Avoid man-in-the-middle attacks
syn-sport1024-deny	Discard synchronization packets whose source port is less than 1024
synfin-deny	Discard SYN-FIN packets
synrst-deny	Discard SNY-RST packets
tcp-frag-off-min-check	Discard TCP fragment packets with offset equal to 1
tcpblat-deny	Discard TCP fragment packets with offset equal to 1...
tcphdr-min-check	Check the minimum TCP header and delete the TCP whose header is less than the minimum size defined by the command

	data pack
udpblat-deny	If the UDP source port is equal to the UDP destination port, the packet is discarded
xmas-deny	If the serial number is zero and the FIN, URG and PSH bits are set, the number is discarded According to the package
icmp-ping-max-length	Specify the maximum size of ICMPv4/ICMPv6 ping packets. The valid range is 0 To 65535 bytes, the Default value is 512 bytes.
ipv6-min-frag-size-length	Specify the minimum size of IPv6 fragments. The valid range is from 0 to 65535 bytes, Default Value is 1240 bytes
smurf-netmask	Specify the mask for man-in-the-middle attacks. The length ranges from 0 to 323 bytes, Default length 0 bytes
tcphdr-min-length	Specify the minimum TCP header length. The length ranges from 0 to 31 bytes, and the Default length is 20 byte

### Default

In the default case, all DoS protections are enabled. DefaultParameter is:  
 The maximum size of an ICMP ping packet is 512 bytes  
 The minimum size of the IPv6 fragment is 1240 bytes  
 Smurf netmask length is 0 bytes  
 The minimum length of the TCP header is 20 bytes

### Mode

Global configuration mode

### Instructions

Use the command "dos" to enable specific denial of service (DoS) protection.

### Instance

Configure the minimum length of the IPv6 fragment to be 1024 bytes, and enable checking  
 Switch(config)# dos ipv6-min-frag-size-length 1024  
 Switch(config)# dos ipv6-min-frag-size-check

### dos(interface)

### Format

dos  
no dos

#### Parameter

#### Default

Default disable

#### Mode

Interface configuration Mode

#### Instructions

To enable DoS on a specific interface, please command the DoS command in Interface configuration Mode

#### Instance

Enable interface DOS function  
Switch(config)# interface GigabitEthernet1  
Switch(config-if)# dos

### show dos

#### Format

show dos  
show dos interface IF\_PORTS

#### Parameter

interface	Query DOS configuration based on interface
-----------	--

#### Default

#### Mode

Privileged mode

#### Instructions

Use the command "show dos" to display the DoS protection configuration globally or under the interface.

#### Instance

Query DOS configuration

Switch# show dos

Type	State(Length)
-----+-----	
DMAC equaltoSMAC	
enabled Land (DIP=SIP)	enabled
UDP Blat (DPORT=SPORT)	enabled
TCP Blat (DPORT=SPORT)	enabled
POD (PingofDeath)	enabled
IPv6 MinFragmentSize	enabled (1240 Bytes)
ICMPFragmentPackets	enabled
IPv4 Ping Max Packet Size	enabled (512 Bytes)
IPv6 Ping Max Packet Size	enabled (512 Bytes)
SmurfAttack	enabled (Netmask Length: 0)
TCP MinHeaderLength	enabled (20Bytes)
TCP Syn (SPORT<1024)	enabled
NullScanAttack	enabled
X-MasScanAttack	enabled
TCPSYN-FINAttack	enabled
TCPSYN-RSTAttack	
enabled TCP Fragment (Offset = 1)	enabled

Query the DOS configuration under the interface

Switch# show dos interfaces GigabitEthernet 1

Port	DoSProtection
-----+-----	
gi1	disabled

## 9. Dynamic ARP Inspection

### ip arp inspection

#### Format

```
ip arp inspection
no ip arp inspection
```

#### Parameter

#### Default

Default disable

#### Mode

Global configuration mode

#### Instructions

Use the command "ip arp inspection" to enable dynamic ARP inspection.

#### Instance

```
Enable DAI
switch(config)# ip arp inspection
switch(config)# ip arp inspection vlan 1
switch(config)# show ip arp inspection
DynamicARPInspection      : enabled
EnableonVlans              1
```

### ip arp inspection vlan

#### Format

```
ip arp inspection vlan VLAN-LIST
no ip arp inspection vlan VLAN-LIST
```

#### Parameter

vlan	Specify VLANID or range to enable dynamic ARP inspection
------	--

#### Default

Default disable

## Mode

Global configuration mode

## Instructions

Use the command "ip arp inspection vlan" to enable the VLAN DAI switch.

## Instance

```
Enable DAI function in VLAN
switch(config)# vlan 1-100
switch(config)# exit
switch(config)# ip arp inspection
switch(config)# ip arp inspection vlan 1-100
switch(config)# show ip arp inspection
DynamicARPInspection    :enabled
EnableonVlans           :1-100
```

## ip arp inspection trust

## Format

```
ip arp inspection trust no
ip arp inspectiontrust
```

## Parameter

## Default

Default disable

## Mode

Interface configuration Mode

## Instructions

Use the command "ip arp inspection trust" to set the trusted interface. The switch does not check the ARP packets received on the trusted interface.

## Instance

```
Configure DAI information interface
switch(config)# interface gi1
switch(config)# ip arp inspection trust
```

Query interface DAI information

```

switch(config)# do show ip arp inspection interface gi1
Interfaces | Trust State | Rate (pps) | SMAC Check | DMAC Check | IP Check/Allow Zero
|-----+-----+-----+-----|-----
-----+
gi1 | Trusted|None |disabled |disabled |disabled/disabled

```

## ip arp inspection validate

### Format

```

ip arp inspection validate src-mac
ip arp inspection validate dst-mac
ip arp inspection validate ip [allow-zeros]
no ip arp inspection validate src-mac
no ip arp inspection validate dst-mac
no ip arp inspection validate ip [allow-zeros]

```

### Parameter

#### Default

Default disable all verification

#### Mode

Interface configuration Mode

### Instructions

Use the command "ip arp inspection validate" to enable the interface verification function. "Src-mac" discards the ARP request and replies to packets that do not match the ARP sender mac and the Ethernet source mac. "Dst mac" drops ARP target ARP reply packet with mismatch between mac and Ethernet dstmac. "Ip" discards sending ARP request and response packets with invalid ip, such as broadcast, multicast, all-zero ip address and discard ARP response packets with invalid target ip. "Allow zeros" means that all zero IP addresses will not be deleted.

### Instance

```

Enable interface DAI verification
switch(config)# interface gi1
switch(config-if)# ip arp inspection validate src-mac
switch(config-if)# ip arp inspection validate dst-ma
switch(config-if)# ip arp inspection validate ip allow-zeros
switch(config)# do show ip arp inspection interface gi1
Interfaces | Trust State | Rate (pps) | SMAC Check | DMAC Check | IP Check/Allow Zero
|-----+-----+-----+-----|-----

```

----+-----+  
 gi1 | Untrusted | None | enabled | enabled | enabled/ enabled

### ip arp inspection rate-limit

#### Format

ip arp inspection rate-limit <1-50>  
 no ip arp inspection rate-limit

#### Parameter

<1-50>	Set the limit of ARP packets, 1-50PPS.
--------	--

#### Default

Default does not limit

#### Mode

Interface configuration Mode

#### Instructions

Use the command "ip arp inspection rate-limit" to set the interface limit. The switch discards ARP packets after receiving more than the configured packet rate per second.

#### Instance

Configure interface ARP restriction  
 switch(config)# interface gi1  
 switch(config)# ip arp inspection rate-limit 30

### clear ip arp inspection statistics

#### Format

clear ip arp inspection interfaces IF\_PORTS statistics

#### Parameter

interfaces	Query DAI's specified interface statistics
------------	--

#### Default



**Mode**

Privileged mode

**Instructions**

Use the command "clear ip arp inspection interfaces statistics" to clear the DAI statistics under the interface.

**Instance**

Clear DAI statistics under the interface  
 switch# clear ip arp inspection interfaces gi1 statistics

**show ip arp inspection****Format**

show ip dhcp snooping

**Parameter****Default****Mode**

Privileged mode

**Instructions**

Use the command "show ip arp inspection" to query DAI configuration information.

**Instance**

Query DAI configuration  
 switch(config)# show ip arp inspection  
 DynamicARPInspection : enabled  
 EnableonVlans 1

**show ip arp inspeciton interface****Format**

show ip arp inspection interfaces IF\_PORTS  
 show ip arp inspection interfaces IF\_PORTS statistics

**Parameter**

interfaces	Query the DAI configuration under the interface
------------	---

## Default

## Mode

Privileged mode

## Instructions

Use the command "show ip arp inspection interfaces" to query the DAI configuration and statistics under the specified interface.

## Instance

Query the DAI configuration of interface GE1

```
switch# show ip arp inspection interface gi1
```

Interfaces	Trust State	Rate (pps)	SMAC Check	DMAC Check	IP Check/Allow Zero
gi1	Trusted	None	disabled	disabled	disabled/disabled

Query DAI statistics of interface GE1

```
switch# show ip arp inspection interfaces gi1
```

statistics Port	Forward	Source MAC Failures	Dest MAC Failures	SIP Validation Failures	DIP Validation Failures	IP-MAC Mismatch Failures
gi1	0	0	0	0	0	0

## 10. GVRP

### gvrp (Global)

#### Format

```
gvrp no
gvrp
```

#### Parameter

#### Default

```
GVRPDefault disable
```

#### Mode

```
Global configuration mode
```

#### Instructions

Use the command "gvrp" to enable the GVRP global switch.

#### Instance

```
Configure GVRP
Switch(config)# gvrp
```

```
Quiry GVRP
Switch# show gvrp
```

GVRP	Status
GVRP	:Enabled
Jointime	: 200ms
Leavetime	: 600ms
LeaveAlltime	: 10000ms

### gvrp (Interface)

#### Format

```
gvrp no
gvrp
```

#### Parameter

## Default

GVRPDefault disable

## Mode

Interface configuration Mode

## Instructions

Use the command "gvrp" to enable the interface GVRP function, and GVRP must work on the trunk port.

## Instance

Enable GVRP on the  
interface  
Switch(config)#gvrp

Query GVRP of the interface  
Switch# show gvrp configuration interfaces gi1  
Port | GVRP-Status | Registration | Dynamic VLAN Creation  
-----+-----+-----+-----  
gi1 Enabled Normal Disabled

## gvrp registration-mode

## Format

gvrp registration-mode (normal | fixed | forbidden)

## Parameter

normal	Register dynamic vlan and transfer all vlan attributes
fixed	Do not register dynamic VLANs, only transmit static VLAN attributes
forbidden	Do not register dynamic vlan, only transmit Defaultvlan attributes

## Default

Default works in normal

## Mode

Interface configuration Mode

## Instructions

When the registration mode is set to fixed or prohibited, the port will be removed from the vlan and switched to a dynamic port. do not studyvlan.

## Instance

```
Configure GVRP working mode
Switch(config-if)# gvrp registration-mode fixed

Query interface GVRP configuration
Switch# show gvrp configuration interfaces gi1
Port | GVRP-Status | Registration | Dynamic VLAN Creation
-----+-----+-----+-----
gi1 Enabled Fixed Disabled
```

## gvrp vlan-create-forbid

### Format

```
gvrp vlan-creation-forbid no
gvrpvlan-creation-forbid
```

### Parameter

### Default

Default disable

### Mode

Interface configuration Mode

## Instructions

Using the command "gvrp vlan-creation-forbid" will not delete the dynamic port from the vlan instantly.

## Instance

```
Configure GVRP to delete interfaces instantly
Switch(config)#interface gi1
Switch(config-if)# gvrp vlan-creation-forbid
```

## clear gvrp statistics

**Format**

clear gvrp (error-statistics | statistics) [interfaces IF\_PORTS]

**Parameter**

error-statistics	Incorrect GVRP packet statistics
statistics	GVRP event message
interfaces	Designated interface

**Default****Mode**

Privileged mode

**Instructions**

Use the command "clear gvrp" to clear the GVRP statistics of the interface.

**Instance**

Clear GVRP statistics of the interface

Switch# clear gvrp statistics

Switch# clear gvrp error-statistics

**show gvrp statistics****Format**

show gvrp (error-statistics | statistics) [interfaces IF\_PORTS]

**Parameter**

error-statistics	Incorrect GVRP packet statistics
statistics	GVRP event message
interfaces	Specify an interface, if no interface is specified, query all interfaces

**Default****Mode**

Privileged mode

**Instructions**

Use the command "show gvrp" to query the GVRP statistics of all or connected interfaces.

### Instance

```

Query GVRP statistics
Switch# show gvrp statistics
Portid :gi1
TotalRX: 0
JoinEmptyRX: 0
JoinInRX : 0
Empty RX : 0
LeaveIn RX : 0
LeaveEmptyRX : 0
LeaveAll RX : 0
Total TX : 0
JoinEmpty TX : 0
JoinInTX : 0
EmptyTX : 0
LeaveInTX : 0
LeaveEmptyTX : 0
LeaveAllTX : 0

```

### show gvrp

#### Format

```
show gvrp
```

#### Parameter

#### Default

#### Mode

Privileged mode

#### Instructions

Use the command "show gvrp" to query the global information of GVRP.

### Instance

```

Query GVRP
Switch# show gvrp
GVRP Status
-----

GVRP : Disabled

```

Join time : 200 ms  
 Leavetime : 600ms  
 LeaveAll time : 10000 ms

## show gvrp configuration

### Format

show gvrp configuration [interface IF\_PORTS]

### Parameter

interface	Specify the interface, if not specified, it means all interfaces
-----------	--

### Default

### Mode

Privileged mode

### Instructions

Use the command "show gvrp configuration" to query all interface configuration information.

### Instance

Query GVRP configuration information  
 Switch# show gvrp configuration  
 Port | GVRP-Status | Registration | Dynamic VLAN Creation  
 -----+-----+-----+-----  
 gi1 Disabled Normal Enabled  
 gi 2 Disabled Normal Enabled



## 11. IGMP Snooping

### ip igmp snooping

#### Format

```
ip igmp snooping no
ip igmpsnooping
```

#### Parameter

#### Default

Default enable.

#### Mode

Global configuration mode

#### Instructions

Use the command "ip igmp snooping" to enable igmp snooping.

#### Instance

```
Enable igmp snooping
functionSwitch(config)# ip igmp
snooping
```

### ip igmp snooping version

#### Format

```
ip igmp snooping version (2|3)
```

#### Parameter

(2 3)	IGMP version
-------	--------------

#### Default

Default is V2.

#### Mode

Global configuration mode

#### Instructions

Use the command "ip igmp snooping version" to configure the version of IGMP. v3 only supports basic mode. When the version is changed from v3 to v2, all query program versions will be updated to version 2.

#### Instance

Configure IGMP version  
Switch(config)# ip igmp snooping version 3

#### ip igmp snooping querier

#### Format

ip igmp snooping vlan <VLAN-LIST>querier [version (2|3)]  
no ip igmp snooping [vlan <VLAN-LIST>] querier

#### Parameter

vlan	Specify VLAN ID for setting
(2 3)	Query version number

#### Default

#### Mode

Global configuration mode

#### Instructions

Use the command "ip igmp snooping querier" to add the querier. When the igmp vlan querier is enabled, router selection will be processed, and general and specific queries will be sent after the selection is successful.

#### Instance

Configure IGMP Querier  
Switch(config)# ip igmp snooping vlan 2 querier version 3

#### ip igmp snooping vlan

#### Format

ip igmp snooping vlan VLAN-LIST  
no ip igmp snooping vlan VLAN-LIST

#### Parameter

vlan	Configure IGMP Querier...
------	---------------------------

### Default

Default all VLANs are disabled.

### Mode

Global configuration mode

### Instructions

Disabling will clear all IPigmp snooping dynamic groups and dynamic router ports, and enable all static IPigmp groups  
 The VLAN is invalid. No longer will learn dynamic groups and router ports through igmp messages. Use the command "ip igmp snooping vlan" to enable the VLAN-level IGMP function.

### Instance

Enable IGMP multicast VLAN function  
 Switch(config)# ip igmp snooping  
 Switch(config)# ip igmp snooping vlan 2

### ip igmp snooping vlan fastleave

### Format

ip igmp snooping vlan <VLAN-LIST>fastleave  
 no ip igmp snooping vlan <VLAN-LIST>fastleave

### Parameter

vlan	Specify VLAN list
------	-------------------

### Default

Default disable

### Mode

Global configuration mode

### Instructions

Use the command "ip igmp snooping vlan fastleave" to enable the fast leave function. When a leave packet is received, the group will immediately remove the

port.

#### Instance

Enable quick leave  
Switch(config)# ip igmp snooping vlan 1 fastleave

#### ip igmp snooping vlan query-interval

#### Format

ip igmp snooping vlan <VLAN-LIST>query-interval <30-18000>  
no ip igmp snooping vlan <VLAN-LIST>query-interval

#### Parameter

vlan	Specify VLAN
query-interval	Query interval setting

#### Default

Default 125 seconds.

#### Mode

Global configuration mode

#### Instructions

Use the command "ip igmp snooping vlan query-interval" to set the general query interval.

#### Instance

Set general query interval  
Switch(config)# ip igmp snooping vlan 1 query-interval 100

#### ip igmp snooping vlan response-time

#### Format

ip igmp snooping vlan <VLAN-LIST>response-time <5-20>  
no ip igmp snooping vlan <VLAN-LIST>response-time

#### Parameter

vlan	Specify VLAN
response-time	Response time setting

## Default

Default is 10.

## Mode

Global configuration mode

## Instructions

Use the command "ip igmp snooping vlan response-time" to set the response time.

## Instance

Set response time

Switch(config)# ip igmp snooping vlan 1 response-time 12

## ip igmp snooping vlan router

## Format

ip igmp snooping vlan VLAN-LIST router learn pim-dvmrp no ip  
igmp snooping vlan VLAN-LIST router learnpim-dvmrp

## Parameter

vlan	Set response time...
------	----------------------

## Default

Default is enabled.

## Mode

Global configuration mode

## Instructions

Use the command "ip igmp snooping vlan router" to pass routing protocol packets (such as PIM/PIMv2, DVMRP, MOSPF) enable learning router ports.

## Instance

Configure routing

Switch(config)# ip igmp snooping vlan 99 router

## ip igmp snooping vlan forbidden-port

### Format

```
ip igmp snooping vlan <VLAN-LIST>forbidden-port IF_PORTS
no ip igmp snooping vlan <VLAN-LIST>forbidden-port IF_PORTS
```

### Parameter

vlan	Specify VLAN
forbidden-port	Designated port

### Default

### Mode

Global configuration mode

### Instructions

ip igmp listens to vlan 1 static port gi1-2 will add static port gi1-2 to vlan 1. All known vlan 1

The ipv4 group will add a static port.

ip igmp listens to vlan 1 disabled port gi3-4 will add disabled port gi3-4 to vlan 1. All known vlan 1

The ipv4 group will delete the disabled port.

Use the command "ip igmp snooping vlan forbidden-port" to add static non-forwarding ports, and all known vlan 1 ipv4 groups will delete the disabled ports.

### Instance

Configure disable interface

```
Switch(config)# ip igmp snooping vlan 1 forbidden -port gi3-4
```

## ip igmp snooping vlan static-port

### Format

```
ip igmp snooping vlan <VLAN-LIST>static-port IF_PORTS
no ip igmp snooping vlan <VLAN-LIST>static-port IF_PORTS
```

### Parameter

vlan	Specify VLAN
static -port	Designated port

## Default

## Mode

Global configuration mode

## Instructions

Use the command "ip igmp snooping vlan static-port" to add static forwarding ports.  
All known vlan 1 ipv4 groups will add static ports.

## Instance

Configure static forwarding port

```
Switch(config)# ip igmp snooping vlan 1 static -port gi1-2
```

## ip igmp snooping vlan static-router-port

## Format

```
ip igmp snooping vlan <VLAN-LIST>static-router-port IF_PORTS
```

```
no ip igmp snooping vlan <VLAN-LIST>static-router-port IF_PORTS
```

## Parameter

vlan	Specify VLAN
static-router-port	(Specify)Designated port

## Default

## Mode

Global configuration mode

## Instructions

Use the command "ip igmp snooping vlan static-router-port" to add a static route port.  
All query packets will be forwarded to this port.

## Instance

Configure static routing port

```
Switch(config)# ip igmp snooping vlan 1 static-router-port gi1-2
```

## ip igmp snooping vlan static-group

## Format

```
ip igmp snooping vlan <VLAN-LIST>static-group [<ip-addr>] interfaces
IF_PORTS
no ip igmp snooping vlan <VLAN-LIST>static-group [<ip-addr>]
interfaces IF_PORTS
```

#### Parameter

vlan	Specify VLAN
static-group	Static IPv4 multicast address
interfaces	(Specify)Designated port

#### Default

#### Mode

Global configuration mode

#### Instructions

Use the command "ip igmp snooping vlan static-group" to add a static group. The static group will not learn other dynamic ports. If the dynamic group exists, the static group will overlap with the dynamic group. The configuration of the static group is valid unless igmp snooping global and vlan are enabled.

#### Instance

Configure static groups

```
Switch(config)# ip igmp snooping vlan 1 static-group 224.1.1.1 interfaces gi1-2
```

### ip igmp snooping vlan group

#### Format

```
no ip igmp snooping vlan <VLAN-LIST>group <ip-addr>
```

#### Parameter

vlan	Specify VLAN
group	Static IPv4 multicast address

#### Default

#### Mode

Global configuration mode



## Instructions

Use the command "no ip igmp snooping vlan group" to delete a dynamic or static multicast group.

## Instance

Delete multicast group  
Switch(config)# no ip igmp snooping vlan 1 group 224.1.1.1

## ip igmp profile

### Format

```
ip igmp profile <1-128>
no ip igmp profile <1-128>
```

### Parameter

<1-128>	Specify the ID of the generated template
---------	--

### Default

### Mode

Global configuration mode

## Instructions

Use the command "ip igmp profile" to enter the IGMP template configuration Mode.

## Instance

Enter IGMP template configuration  
Switch(config)# ip igmp profile 1

## profile range

### Format

```
profile range ip <ip-addr> [ip-addr] action (permit | deny)
```

### Parameter

ip	Set the start and end IPv4 addresses of multicast
----	---

permit	Allow address learning within the multicast address range
deny	Prohibit address learning in the multicast address range

## Default

### Mode

igmp profile configuration mode

### Instructions

Use the command "profile range" to generate an IGMP template.

### Instance

Configure IGMP template

```
Switch(config)# ip igmp profile 1
```

```
Switch(config-igmp-profile)# profile range ip 224.1.1.1 224.1.1.8 action permit
```

## ip igmp filter

### Format

```
ip igmp filter <1-128>
```

```
no ip igmp filter
```

### Parameter

<1-128>	Configure the ID of the IGMP filter template
---------	--

## Default

### Mode

Interface configuration Mode

### Instructions

Use the command "ip igmp filter" to bind a template to the interface. When the port is bound to the template, the port learning group will be updated. If the group does not match the filtering template rules, it will delete the port from the group. Static groups are excluded.

### Instance

Bind filter template

```
Switch(config)# interface gi1
```

```
Switch(config-if)#ip igmp filter 1
```

## ip igmp max-groups

### Format

```
ip igmp max-groups <0-1024>  
no ip igmp max-groups
```

### Parameter

max-groups	Largest multicast group
------------	-------------------------

### Default

Default is 1024.

### Mode

Interface configuration Mode

### Instructions

Use the command "ip igmp max-groups" to configure the maximum number of learned multicast groups on the interface.

### Instance

Configure the maximum number of learned multicast groups on the interface  
Switch(config-if)#ip igmp max-groups 10

## ip igmp max-groups action

### Format

```
ip igmp max-groups action (deny | replace)
```

### Parameter

deny	When the interface reaches the maximum number of multicast groups, discard new groups
replace	When the interface reaches the maximum number of multicast groups, replace the old group

### Default

Default is deny

## Mode

Interface configuration Mode

## Instructions

Use the command "ip igmp max-groups action" to configure the operation processing when the interface reaches the maximum multicast group.

## Instance

Configuration replacement operation  
Switch(config-if)#ip igmp max-groups action replace

## clear ip igmp snooping groups

## Format

clear ip igmp snooping groups [(dynamic | static)]

## Parameter

none	When dynamic or static is not specified, clear all groups
dynamic	Clear dynamic group
static	Clear static group

## Default

## Mode

Privileged mode

## Instructions

Use the command "clear ip igmp snooping groups" to clear the system's extended groups.

## Instance

Clear multicast group  
Switch# clear ip igmp snooping groups

Query multicast group  
Switch# show ip igmp snooping groups  
VLAN | Group IP Address | Type | Life(Sec) | Port  
-----+-----+-----+-----+-----

Total Number of Entry = 0

### clear ip igmp snooping statistics

#### Format

```
clear ip igmp snooping statistics
```

#### Parameter

#### Default

#### Mode

Privileged mode

#### Instructions

Use the command "show ip igmp snooping statistics" to clear IGMP statistics.

#### Instance

Clear IGMP statistics

```
Switch# clear ip igmp snooping statistics
```

Query IGMP information

```
Switch# show ip igmp snooping
```

IGMP Snooping Status

-----

```
Snooping      : EnabledReportSuppression      : Enabled
Operation Version :v2
Forward Method  : mac Unknown IPMulticast Action  :Flood
```

Packet Statistics

```
TotalRX: 0
```

```
ValidRX: 0
```

```
InvalidRX 0
```

```
Other RX: 0
```

```
Leave RX : 0
```

```
ReportRX : 0
```

```
GeneralQueryRX 0
```

```
Specail GroupQueryRX 0
```

```
Specail Group & SourceQueryRX 0
```

```
Leave TX : 0
```

```
ReportTX : 0
```

```
GeneralQueryTX 0
```

```
Specail GroupQueryTX 0
```

```
Specail Group & SourceQueryTX 0
```

## show ip igmp snooping groups counters

### Format

```
show ip igmp snooping groups counters
```

### Parameter

#### Default

#### Mode

Privileged mode

### Instructions

Use the command "show ip igmp snooping groups counters" to query the multicast group count, including static and dynamic.

### Instance

```
Query multicast group count
Switch# show ip igmp snooping group counters
Total ip igmp snooping group number: 2
Total ip igmp snooping static mac number: 0
```

## show ip igmp snooping groups

### Format

```
show ip igmp snooping groups [(dynamic | static)]
```

### Parameter

none	When dynamic or static is not specified, query all groups
dynamic	Query dynamic group
static	Query static group

### Mode

Privileged mode

### Instructions

Use the command "show ip igmp snooping groups" to query the multicast group of the system.

### Instance

Query multicast group

Switch# show ip igmp snooping groups

VLAN | Group IP Address | Type | Life(Sec) | Port

```
-----+-----+-----+-----+-----
1 | 224.1.2.3|Static| -- | gi9
1 | 224.1.2.4|Static| -- | gi10
```

Total Number of Entry =2

### show ip igmp snooping router

Format

show ip igmp snooping router [(dynamic | forbidden |static)]

Parameter

none	If not specified, query all groups
dynamic	Query dynamic group
forbidden	Query dynamic group...
static	Query dynamic group...

Mode

Privileged mode

Instructions

Use the command "show ip igmp snooping router" to query IGMP routing information.

Instance

Query routing

Switch# show ip igmp snooping router

Dynamic Router Table

VID | Port | Expiry Time(Sec)

```
-----+-----+-----
```

Total Entry 0

Static Router Table VID | Port Mask

```
-----+-----
```

```
1 | gi4
```

Total Entry 1

---

Forbidden Router Table VID | Port Mask

-----+-----

1 | gi8

Total Entry 1

**show ip igmp snooping querier**

**Format**

show ip igmp snooping querier

**Parameter**

**Default**

**Mode**

Privileged mode

**Instructions**

Use the command "show ip igmp snooping querier" to query all IGMP querier information.

**Instance**

Show querier information

Switch# show ip igmp snooping querier

VID | State | Status | Version | QuerierIP

-----+-----+-----+-----+-----

1 | Disabled | Non-Querier | No | -----

Total Entry 1

**show ip igmp snooping**

**Format**

show ip igmp snooping

**Parameter**

**Default**

**Mode**

Privileged mode

**Instructions**

Use the command "show ip igmp snooping" to query the IGMP global configuration



information.

## Instance

Query IGMP information

Switch# show ip igmp snooping

IGMP Snooping Status

-----

Snooping : Enabled ReportSuppression : Enabled  
 Operation Version :v2  
 Forward Method : mac Unknown IP Multicast Action :Flood

Packet Statistics

TotalRX: 0

ValidRX: 0

InvalidRX 0

Other RX: 0

Leave RX : 0

ReportRX : 0

GeneralQueryRX 0

Specail GroupQueryRX 0

Specail Group & SourceQueryRX 0

Leave TX : 0

ReportTX : 0

GeneralQueryTX 0

Specail GroupQueryTX 0

Specail Group & SourceQueryTX 0

## show ip igmp snooping vlan

### Format

show ip igmp snooping vlan [VLAN-LIST]

### Parameter

none	If not specified, query all VLANs
vlan	Specify VLAN query

### Default

### Mode

Privileged mode

### Instructions

Use the command "show ip igmp snooping vlan" to query the IGMP multicast VLAN configuration information.

#### Instance

Query IGMP multicast VLAN information  
 Switch# show ip igmp snooping vlan 1  
 IGMP Snooping is globally enabled  
 IGMP Snooping VLAN 1 admin : disabled  
 IGMP Snooping operation mode : disabled  
 IGMP Snooping robustness: admin 2 oper 2  
 IGMP Snooping query interval: admin 125 sec oper 125 sec  
 IGMP Snooping query max response : admin 10 sec oper 10 sec  
 IGMP Snooping last member query counter: admin 2 oper 2  
 IGMP Snooping last member query interval: admin 1 sec oper 1 sec  
 IGMP Snooping last immediate leave: disabled  
 IGMP Snooping automatic learning of multicast router ports: enabled

#### show ip igmp snooping forward-all

#### Format

show ip igmp snooping forward-all [vlan VLAN-LIST]

#### Parameter

none	If not specified, query all forwarding information
vlan	Specify VLAN query

#### Default

#### Mode

Privileged mode

#### Instructions

Use the command "show ip igmp snooping forward-all" to query all forwarding information.

#### Instance

Query forwarding information  
 Switch# show ip igmp snooping forward-all 1  
 IGMP Snooping VLAN1  
 IGMP Snooping static port : None  
 IGMP Snooping forbidden port : None

## show ip igmp profile

### Format

show ip igmp profile [<1-128>]

### Parameter

none	Not specified, means all templates
<1-128>	Specify the ID of the template

### Default

### Mode

Privileged mode

### Instructions

Use the command "show ip igmp profile" to query the IGMP profile configuration information.

### Instance

Query IGMP template information

Switch# show ip igmp profile

IP igmp profile index: 1

IP igmp profile action: permit

Range low ip: 224.1.1.1 Range high ip: 224.1.1.8

IP igmp profile index: 2

IP igmp profile action: deny

Range low ip: 225.1.1.0 Range high ip: 225.1.2.1

## show ip igmp filter

### Format

show ip igmp filter [interfaces IF\_PORTS]

### Parameter

none	Not specified, which means all ports
interfaces	According to the specified interface

### Default

### Mode

Privileged mode

### Instructions

Use the command "show ip igmp filter" to query the IGMP filter template information.

### Instance

```
Query filter template
Switch# show ip igmp filter
Port ID | Profile ID
-----+-----
gi1 : 1
gi2 : None
gi3 : None
gi4 : None
gi5 : None
--More--
```

### show ip igmp max-group

### Format

```
show ip igmp max-group [interfaces IF_PORTS]
```

### Parameter

none	Not specified, which means all ports
interfaces	According to the specified interface

### Default

### Mode

Privileged mode

### Instructions

Use the command "show ip igmp max-group" to query the maximum learning number of the interface multicast group.

### Instance

```
Query the maximum learning number of the interface multicast group
Switch# show ip igmp max-group
Port ID | Max Group
-----+-----
gi1 : 50
```

```

gi2 : 256
gi3 : 256
gi4 : 256
gi5 : 256
--More--

```

### show ip igmp max-group action

#### Format

```
show ip igmp max-group action [interfaces IF_PORTS]
```

#### Parameter

none	Not specified, which means all ports
interfaces	According to the specified interface

#### Default

Default is deny

#### Mode

Privileged mode

#### Instructions

Use the command "show ip igmp max-group action" to query the operation processing.

#### Instance

```

Query operation
Switch# show ip igmp max-group action
Port ID | Max-groups Action
-----+-----
gi1 : replace
gi2 : deny
gi3 : deny
gi4 : deny
gi5 : deny
--More--

```

## 12. IP SourceGuard

### ip source verify

#### Format

```
ip source verify [mac-and-ip]
no ip source verify
```

#### Parameter

verify	Verify the MAC and IP binding entries
--------	---------------------------------------

#### Default

The IPSG function under the interface is disabled and only the IP is verified in the Default condition.

#### Mode

Interface configuration Mode

#### Instructions

Use the command "ip source verify" to enable the IP source protection function. In the case of Default, IPSG will filter the source IP address. Selecting "mac-and-ip" will filter not only IP but also MAC.

#### Instance

```
Enable the IPSG function of the
interfaceSwitch(config)# interface
gi1 switch(config-if)# ip source
verify
Switch(config)# do show ip source interfaces gi1
  Port |      Status      | Max Entry | CurrentEntry
-----+-----+-----+-----
  gi1 | disabled | NoLimit   | 0
```

### ip source binding

#### Format

```
ip source binding A:B:C:D:E:F vlan <1-4094> A.B.C.D interface IF_PORT
no ip source binding A:B:C:D:E:F vlan <1-4094> A.B.C.D interface IF_PORT
```

#### Parameter

A:B:C:D:E:F	Specify the MAC address of a binding table entry
vlan	Specify the VLAN ID of a binding entry
A.B.C.D	Specify the IP address of a binding entry
interface	Specify a binding table entry interface

### Default

### Mode

Global configuration mode

### Instructions

Use the command "ip source binding" to create a static IP source binding entry with an IP address and its associated MAC address, VLAN ID, interface

### Instance

```
Configure static binding entries
Switch(config)# ip source binding 00:11:22:33:44:55 vlan 1 192.168.1.55 interface
g1
switch(config)# do show ip source binding
Bind Table: Maximun Binding Entry Number 192
Port | VID | MAC Address | IP | Type |
LeaseTime
-----+-----+-----+-----+-----+-----
+-----+-----+-----+-----+-----+-----
g1 | 1 | 00:11:22:33:44:55 | 192.168.1.55(255.255.255.255) | Static | NA
```

### show ip source interfaces

### Format

show ip source interfaces IF\_PORTS

### Parameter

interfaces	Query the IPSG configuration under the specified interface
------------	--

### Default

### Mode

Privileged mode

## Instructions

Use the command "show ip source interface" to query the IPSG configuration under the specified interface.

## Instance

Query the IPSG configuration under the interface

```
Switch# show ip source interfaces gi1
```

```
Port | Status | Max Entry | CurrentEntry
-----+-----+-----+-----
gi1 | disabled | NoLimit | 0
```

## show ip source binding

## Format

```
show ip source binding [(dynamic|static)]
```

dynamic	Query entries learned dynamically
static	Query entries learned through static methods

## Default

## Mode

Privileged mode

## Instructions

Use the command "show ip source binding" to query all dynamic or static entries.

## Instance

Query binding entries

```
switch# show ip source binding
```

```
Bind Table: Maximun Binding Entry Number 192
```

```
Port | VID | MAC Address | IP | Type |
LeaseTime
```

```
-----+-----+-----+-----+-----+-----
+-----+-----+
g1 | 1 | 00:11:22:33:44:55 | 192.168.1.55(255.255.255.255) | Static | NA
```



## 13. LinkAggregation

### lag

#### Format

```
lag <1-8>mode (static | active | passive)
no lag
```

<1-8>	Aggregation group ID
static	Specify a static aggregation group and add the interface to the aggregation group
active	Specify a dynamic aggregation group, and add the interface as an activation port to the LACP aggregation group
passive	Specify a dynamic aggregation group and add the interface as a passive port to the LACP aggregation group

#### Default

#### Mode

Interface configuration Mode

#### Instructions

The link aggregation group function allows you to aggregate multiple physical ports into one logical port to increase bandwidth. This command makes the normal port connect to the specific hysteresis logic port in static or dynamic mode.

#### Instance

```
Configure aggregation group
Switch(config)# interface range g1-3
Switch(config-if)# lag 1 mode active
```

```
Query aggregation group
Switch# show lag
Load Balancing: src-dst-mac-ip
```

```
Group ID | Type | Ports
-----+-----
1 | LACP | Inactive:gi1-32 | ----- |
3 | -----|
4 | -----|
5 | -----|
6 | -----|
7 | -----|
```

8 | -----|

### lag load-balance

#### Format

```
lag load-balance (src-dst-mac | src-dst-mac-ip) no
lag load-balance
```

#### Parameter

src-dst-mac	Use the source and destination MAC address load balancing strategy of all packets
src-dst-mac-ip	Use the source and destination MAC and IP address load balancing strategies of all packets

#### Default

The default load balancing policy is src-dst-mac

#### Mode

Global configuration mode

#### Instructions

The port of the link aggregation group should transmit data packets to all ports to balance the traffic load. Two algorithms are supported. This command allows you to select an algorithm.

#### Instance

```
Configure load balancing
Switch(config)# lag load-balance src-dst-mac-ip
```

### lacp port-priority

#### Format

```
lacp port-priority <1-65535>
no lacp port-priority
```

#### Parameter

<1-65535>	Port priority
-----------	---------------

## Default

Default port priority is 1

## Mode

Interface configuration Mode

## Instructions

Use the command "lACP port-priority" to configure the port priority of LACP aggregation group members.

## Instance

The configuration interface  
priority is 100  
Switch(config)# interface g1  
Switch(config-if)# lACP port-priority 100

## lACP system-priority

## Format

lACP system-priority <1-65535>  
no lACP system-priority

## Parameter

<1-65535>	System priority
-----------	-----------------

## Default

Default system priority is 32768

## Mode

Global configuration mode

## Instructions

Use the command "lACP port-priority" to configure the system priority of the LACP aggregation group.

## Instance

Configure the system priority to 1000  
Switch(config)# lACP system-priority 1000

## show lacp

### Format

```
show lacp sys-id
show lacp [<1-8>] counters
show lacp [<1-8>] (internal | neighbor) [detail]
```

### Parameter

#### Default

#### Mode

Privileged mode

### Instructions

Use the command "show lacp sys-id" to display the system identifier specified by the LACP command. The system identifier is determined by

The LACP system priority is composed of the MAC address of the switch. Use the command "show lacp counter" to query LACP statistics. Use the command "show lacp internal" to query local information. Use the command "show lacp neighbor" queries remote information.

### Instance

Query LACP

```
Switch# show lacp sys-id
32768, 1c2a.a3c4.0292
```

```
Switch# show lacp counters
          LACPDU      LACPDU
Port      Sent  Recv   PktsErr
-----
```

## show lag

### Format

```
show lag
```

### Parameter

#### Default

#### Mode

Privileged mode

## Instructions

Use the command "show lag" to query the configuration information of the aggregation group.

## Instance

Query aggregation group  
Switch# show lag  
Load Balancing: src-dst-mac-ip.

Group ID	Type	Ports
1	LACP	Inactive:gi1-3
2	-----	
3	-----	
4	-----	
5	-----	
6	-----	
7	-----	
8	-----	

## 14. LLDP

### lldp

#### Format

```
lldp
no lldp
```

#### Parameter

##### Default

Default enable

#### Mode

Global configuration mode

#### Instructions

Use the command "lldp" to enable the neighbor discovery protocol.

#### Instance

```
Enable LLDP
Switch (config)# lldp
```

```
Query LLDP
Switch# show lldp
State: Enabled
Timer: 30 Seconds
Hold multiplier: 4
Reinit delay: 2 Seconds
Tx delay: 2Seconds
LLDP packet handling: Flooding
```

Port	State	OptionalTLVs	Address
gi1	RX,TX		192.168.2.100
gi2	RX,TX		192.168.2.100
gi3	RX,TX		192.168.2.100
gi4	RX,TX		192.168.2.100
gi5	RX,TX		192.168.2.100
gi6	RX,TX		192.168.2.100
gi7	RX,TX		192.168.2.100

## lldp rx

### Format

```
lldp rx  
no lldp rx
```

### Parameter

### Default

Default enable

### Mode

Interface configuration Mode

### Instructions

Use the command "lldp rx" to enable the LLDP receiving function on the interface.

### Instance

```
Enable LLDP reception on the  
interface  
Switch(config)# interface gi1  
Switch(config-if)# lldp rx
```

## lldp tx

### Format

```
lldp tx no  
lldptx
```

### Parameter

### Default

Default enable

### Mode

Interface configuration Mode

### Instructions

Use the command "lldp rx" to enable the LLDP transmission function on the interface.

#### Instance

```
Enable interface LLDP
transmission
Switch(config)# interface gi1
Switch(config-if)# lldp tx
```

### lldp lldpdu

#### Format

```
lldp lldpdu (filtering|flooding|bridging)
```

#### Parameter

filtering	When LLDP is globally disabled, LLDP packets are filtered (deleted)
flooding	When LLDP is globally disabled, LLDP packets are flooded (forwarded to all interfaces)
bridging	When LLDP is globally disabled, LLDP packets are being bridged (Bridge LLDP PDUs to VLAN member port)

#### Default

The Default LLDP PDU processing behavior when LLDP is disabled is flooding

#### Mode

Global configuration mode

#### Instructions

Use the command "lldp lldpdu" to configure the LLDP PDU processing behavior when LLDP is globally disabled. It should be noted that if LLDP is globally enabled and the LLDP RX status of each port is configured to be disabled, then the received LLDP PDU will be discarded instead of globally disabled.

#### Instance

```
Config LLDPDU
Switch(config)# lldp lldpdu bridging
```

```
Query LLDP
Switch# show lldp
State: Enabled Timer: 30 Seconds
Hold multiplier: 4
```



Reinit delay: 2 Seconds  
 Tx delay: 2 Seconds  
 LLDP packet handling: Bridging

## Ildp tlv-select

### Format

```
ldp tlv-select TLV [TLV] [TLV] [TLV] [TLV] [TLV] [TLV] [TLV]
no ldp tlv-select
```

### Parameter

TLV	Optional TLV field
sys-name	system name
sys-desc	System specification
sys-cap	System functions
mac-phy	802.3 mac Address
lag	802.3 link aggregation
max- frame-size	Maximum frame
management-addr	Management address

### Default

### Mode

Interface Mode

### Instructions

Use the command "ldp tlv-select" to append the selected TLV to the PDU.

### Instance

#### Configure TLV

```
Switch(config)# interface range gi 1,3
Switch(config-if-range)# ldp tlv-select port-desc sys-name sys-desc sys-cap mac- phy
lag max-frame-size management-addr
```

#### Query TLV configuration

```
Switch# show ldp interfaces gi1,3
State: Enabled
Timer: 30 Seconds
Hold multiplier: 4
Reinit delay: 2 Seconds
Tx delay: 2Seconds
```



## Query interface LLDP configuration

```
Switch# show lldp interfaces gi1
```

```
State: Enabled
Timer: 30 Seconds
Hold multiplier: 4
Reinit delay: 2 Seconds
Tx delay: 2Seconds
LLDP packet handling: Flooding
```

```
Port      | State | OptionalTLVs | Address
-----+-----+-----+----- gi1 | RX,TX |
          |       | PD, SN, SD, SC | 192.168.2.100
```

```
Port ID: gi1
802.3 optional TLVs: 802.3-mac-phy, 802.3-lag, 802.3-max-frame-size, management-
addr
802.1 optional TLVs
PVID: Disabled
```

**lldp tlv-select vlan-name****Format**

```
lldp tlv-select vlan-name (add|remove) VLAN-LIST
```

**Parameter**

add	Add the name of the VLAN
remove	Delete the name of the VLAN

**Default**

Default without VLAN name

**Mode**

Interface configuration Mode

**Instructions**

Use the command "lldp tlv-select vlan-name" to configure the VLAN name in the LLDPDU packet.

**Instance**

Configuration optional TLV

```
PVID
Switch(config)# interface gi1
Switch(config-if)# lldp tlv-select vlan-name add 1
```

```
Query interface LLDP configuration
Switch# show lldp interfaces gi1
```

```
State: Enabled
Timer: 30 Seconds
Hold multiplier: 4
Reinit delay: 2 Seconds
Tx delay: 2Seconds
LLDP packet handling: Flooding
```

```
Port      | State |OptionalTLVs  |Address
-----+-----+-----+----- gi1 | RX,TX |
          PD, SN, SD, SC|192.168.2.100
```

```
Port ID: gi1
802.3 optional TLVs: 802.3-mac-phy, 802.3-lag, 802.3-max-frame-size, management-
addr
802.1 optional TLVs
PVID: Disabled
VLANs: 1
```

## show lldp

### Format

```
show lldp
show lldp interface IF_NMLPORTS
```

### Parameter

interface	Query LLDP configuration by interface
-----------	---------------------------------------

### Default

### Mode

Privileged mode

### Instructions

Use the command "show lldp" to query the system's LLDP configuration.

### Instance

```
Switch# show lldp
```

```
State: Enabled
Timer: 30 Seconds
Hold multiplier: 4
Reinit delay: 2 Seconds
Tx delay: 2Seconds
LLDP packet handling: Flooding
```

Port	State	OptionalTLVs	Address
gi1	RX,TX		192.168.2.100
gi2	RX,TX		192.168.2.100
gi3	RX,TX		192.168.2.100
gi4	RX,TX		192.168.2.100
gi5	RX,TX		192.168.2.100
gi6	RX,TX		192.168.2.100
gi7	RX,TX		192.168.2.100

**show lldp local-device**

**Format**

```
show lldp local-device
show lldp interfaces IF_NMLPORTS local-device
```

**Parameter**

interfaces	Query LLDP local device information by interface
------------	--

**Default**

**Mode**

Privileged mode

**Instructions**

Use the command "show lldp local-device" to query the local device information in the LLDP PDU packet.

**Instance**

```
Query local information
Switch# show lldp local-device
```

LLDP Local Device Information:

```

Chassis Type : Mac Address
ChassisID    :1C:2A:A3:C4:02:92
SystemName   :Switch
SystemDescription : Switch
System Capabilities Support : Bridge,Router
SystemCapabilitiesEnable : Bridge, Router
Management Address : 192.168.2.100(IPv4)
Management Address :fe80::1e2a:a3ff:fec4:292(IPv6)

```

## show lldp neighbor

### Format

```

show lldp neighbor
show lldp interfaces IF_NMLPORTS neighbor

```

### Parameter

interfaces	Query LLDP neighbor information by interface
------------	--

### Default

### Mode

Privileged mode

### Instructions

Use the command "show lldp neighbor" to query the received LLDP neighbor information.

### Instance

Query LLDP neighbor information

```
Switch# show lldp neighbor
```

```

Port | DeviceID          | PortID          | SysName          | Capabilities
| TTL
----+-----+-----+-----+-----
----+----
gi25 | 00:E0:4C:00:53:35|00:E0:4C:00:53:35|                |
                                           | 3380
gi25 | F0:76:1C:F5:DF:F1|F0:76:1C:F5:DF:F1|                |
                                           | 3385

```

## 15. Logging

### logging

#### Format

```
logging
no logging
```

#### Parameter

#### Default

Default enable

#### Mode

Global configuration mode

#### Instructions

Use the command "logging" to enable the logging function on the switch.

#### Instance

```
Enable log
Switch(config)# logging
```

### logging host

#### Format

```
logging host (ip-addr | hostname) [facility facility] [port port] [severity sev]
no logging host (ip-addr | hostname)
```

#### Parameter

ip-addr	IP address of the remote log server
hostname	Host name of the remote log server
facility	Specify the level of log information, it can use the following values: local0, local1, local2, local3, local4, local5, local6, local7, Defaultislocal7
port	The port number of the remote log server. The range is 0~65535, and the Default is 512.
severity	Specify the minimum severity level of log information. The Default value of the lowest severity level is 5
emerg	0 emergency

alert	1 alert
critical	2 critical
error	3 error
warning	4 warning
notice	5 notice
info	6 information
debug	7 debug

## Default

## Mode

Global configuration mode

## Instructions

Use the command "logging host" to define the log server.

## Instance

Configure log server  
Switch(config)# logging host 1.2.3.4  
Switch(config)# logging host SYSLOG

## logging severity

## Format

logging (buffered|console|file) [severity sev]  
no logging (buffered|console|file)

## Parameter

buffered	Log information is recorded to RAM
console	Log information to the serial port
file	Log information is recorded to flash
severity	Specify the minimum severity level of log information. The Default value of the lowest severity level is 5
emerg	0 emergency
alert	1 alert
critical	2 critical
error	3 error
warning	4 warning
notice	5 notice
info	6 information



debug	7 debug
-------	---------

### Default

Default enables buffered and console, the default value of the lowest severity level is 5.

### Mode

Global configuration mode

### Instructions

Use the command "logging severity" to set the minimum severity level of the log and specify the log to be stored in RAM, serial port, flash.

### Instance

Configuration log  
Switch(config)# logging buffered 7  
Switch(config)# logging flash 7

## show logging

### Format

show logging [buffered|file]

### Parameter

buffered	Query log information recorded by RAM
file	Query log information recorded by flash

### Default

### Mode

Privileged mode

### Instructions

Use the command "show logging" to query the system log information.

### Instance

```
Switch# show logging
```

```
Logging service is enabled
```

```
Aggregation: enabled
Aggregation aging time: 300 sec
```

```
Console Logging: level notice
Buffer Logging : level notice
FileLogging      :disabled
```

```
Buffer Logging
```

```
-----
```

```
*Mar 20 2020 18:27:26: AAA-5-CONNECT: New console connection for user admin,
source async ACCEPTED
```

```
*Mar 20 2020 18:27:24: AAA-4-REJECT: New console connection, source async
REJECTED
```

```
*Mar 20 2020 18:16:08: AAA-5-DISCONNECT: console connection for user admin,
source async TERMINATED
```

```
*Mar 20 2020 18:12:21: PORT-5-LINK_DOWN: Interface GigabitEthernet19 link down
```

```
*Mar 20 2020 17:58:23: PORT-5-LINK_UP: Interface GigabitEthernet19 link up,
aggregated (2)
```

```
*Mar 20 2020 17:58:22: PORT-5-LINK_DOWN: Interface GigabitEthernet19 link down,
aggregated (2)
```

### clear logging

#### Format

```
clear logging (buffered | file)
```

#### Parameter

buffered	Clear RAM log information
file	Clear flash log information

#### Default

#### Mode

```
Privileged mode
```

#### Instructions

Use the command "clear logging" to delete the logs recorded by RAM and Flash.

**Instance**

Clear log records

Switch# clear logging buffered

Switch# clear logging file

## 16. MAC AddressTable

### mac address-table aging-time

#### Format

```
mac access-table aging-time seconds
```

#### Parameter

seconds	Set the MAC address aging time, Default300 seconds.
---------	---

#### Default

Default 300 seconds

#### Mode

Global configuration mode

#### Instructions

Use the command "mac address-table aging-time" to specify the aging time of dynamic MAC address table entries.

#### Instance

Configure the aging time  
Switch(config)# mac address-table aging-time 500

### mac address-table static

#### Format

```
mac address-table static mac-addr vlan vlan-id interfaces IF_PORTS
mac address-table static mac-addr vlan vlan-id drop
no mac address-table static mac-addr vlan vlan-id
```

#### Parameter

mac-addr	Designated MAC address
vlan-id	Designated VLAN
IF_PORTS	Designated interface
drop	Drop the packet when the MAC of the packet is matched

#### Default

## Mode

Global configuration mode

## Instructions

Use the command "mac address-table static" to add static MAC table entries.

## Instance

Add a static MAC entry

```
Switch# mac address-table static 00:11:22:33:44:55 vlan 1 interfaces g5
```

**clear mac address-table**

## Format

```
clear mac address-table dynamic [interfaces IF_PORTS|vlan vlan-id]
```

## Parameter

interfaces	Clearing of designated interfaces
vlan	Clear of designated VLAN

## Default

## Mode

Privileged mode

## Instructions

Use the command "clear mac address-table" to clear the MAC address of the system or specify the interface and VLAN

Make a specific deletion.

## Instance

Clear the MAC in the interface

```
Switch# clear mac address-table dynamic interfaces gi1
```

**show mac address-table**

## Format

```
show mac address-table [dynamic|static] [interface IF_PORTS] [vlan vlan-id]
```

```
show mac address-table [mac-addr] [vlan vlan-id]
```

## Parameter

dynamic	Query all dynamically learned MAC addresses of the system
static	Query all statically configured MAC addresses of the system
interface	Query system MAC address by interface
vlan	Query system MAC address by VLAN

## Default Mode

Privileged mode

## Instructions

Use the command "show mac address-table" to query system MAC address table entries.

## Instance

Query the MAC address table

Switch# show mac address-table

VID	MACAddress	Type	Ports
1	1C:2A:A3:C4:02:92	Management	CPU
1	00:0B:0E:0F:00:ED	Dynamic	gi25
1	00:E0:4C:2E:2C:DD	Dynamic	gi15
1	00:E0:70:68:35:7F	Dynamic	gi25

## show mac address-table counters

## Format

show mac address-table counters

## Parameter

## Default

## Mode

Privileged mode

## Instructions

Use the command "show mac address-table counters" to query the total number of system MAC address tables.

### Instance

Query the total number of MAC tables  
Switch# show mac address-table counters  
Total number of entries: 5

### show mac address-table aging-time

### Format

show mac address-table aging-time

### Parameter

#### Default

#### Mode

Privileged mode

### Instructions

Use the command "show mac address-table aging-time" to query the MAC address aging time.

### Instance

Query MAC aging time  
Switch# show mac address-table aging-time  
Mac Address Table aging time: 300 sec

## 17. MAC VLAN

### vlan mac-vlan group (Global)

#### Format

```
vlan mac-vlan group <1-2147483647> mac-address mask <9-48>
no vlan mac-vlan group mac-address mask <9-48>
```

#### Parameter

<1-2147483647>	MAC VLAN group ID
mac-address	Designated MAC address
mask	Specified MAC address mask

#### Default

#### Mode

Global configuration mode

#### Instructions

Use the command "vlan mac-vlan group" to specify the MAC group.

#### Instance

```
Configure MAC VLAN group
Switch(config)# vlan mac-vlan group 333 22:33:44:55:66:77 mask 48
```

### vlan mac-vlan group (Interface)

#### Format

```
vlan mac-vlan group <1-2147483647>vlan <1-4094>
no vlan mac-vlan group <1-2147483647>
```

#### Parameter

none	Not specified, which means all groups
<1-2147483647>	MAC VLAN group ID
vlan	Designated VLAN

#### Default

#### Mode



Interface configuration Mode

### Instructions

Use the command "vlan mac-vlan group" to map the MAC group and VLAN on the interface.

### Instance

```
Configure MAC VLAN group
Switch(config)# interface gi1
Switch(config-if)# vlan mac-vlan group 333 VLAN 100
```

### show vlan mac-vlan groups

### Format

```
show vlan mac-vlan groups
```

### Parameter

Default

Mode

Privileged mode

### Instructions

Use the command "show vlan mac-vlan groups" to query the MAC group configuration.

### Instance

```
Query MAC group
Switch# show vlan mac-vlan groups
MacAddressMask      Group Id
-----
22:33:44:55:66:7  48  222
      7
44:55:66:77:88:9  48  333
      9
88:99:00:aa:bb:cc 40  444
88:99:00:ab:bb:1  48  111
      0
```

### show vlan mac-vlan interfaces

### Format

```
show vlan mac-vlan [interfaces IF_PORTS]
```

**Parameter**

interfaces	Designated interface
------------	----------------------

**Default****Mode**

Privileged mode

**Instructions**

Use the command "show vlan mac-vlan interface" to query the MAC VLAN interface configuration.

Configure MAC VLAN interface configuration

```
Switch# show vlan mac-vlan interfaces gi1
```

```
Port gi1 :
```

```
Mac based VLANs: Group ID Vlan ID
```

```
-----
```

```
333444
```

```
444 1
```

## 18. Management ACL

### management access-list

#### Format

```
management access-list NAME  
no management access-list NAME
```

#### Parameter

NAME	The name of the management ACL
------	--------------------------------

#### Default

#### Mode

Global configuration mode

#### Instructions

Use the command "management access-list" to create a management ACL and enter the management ACL configuration mode. The name of the ACL must be unique and cannot be the same name as other management ACLs.

```
Configure management ACL  
Switch(config)# management access-list test
```

### management access-class

#### Format

```
management access-class NAME  
no management access-class
```

#### Parameter

NAME	The name of the management ACL
------	--------------------------------

#### Default

#### Mode

Global configuration mode

#### Instructions

Use the command "management access-class" to activate a management ACL.

#### Instance

Activate management ACL  
Switch(config)# management access-list test

### deny

#### Format

```
[sequence <1-65535>] deny interfaces IF_PORTS service
(all|http|https|snmp|ssh|telnet)
[sequence <1-65535>] deny ip A.B.C.D/A.B.C.D interfaces IF_PORTS service
(all|http|https|snmp|ssh|telnet)
[sequence <1-65535>] deny ipv6 X:X::X:X/<0-128>interfaces IF_PORTS
service (all|http|https|snmp|ssh|telnet)
```

#### Parameter

sequence	(Optional) Specify the sequence number of the ACE, the sequence index indicates the ACL ACE priority
interfaces	Specify interface
ip	Specify IP address and mask
ipv6	Specify IPv6 address and prefix length
service	Specify related service types

#### Default

#### Mode

Management ACL configuration mode

#### Instructions

Use the command "deny" to reject the rule of discarding packets that conform to the rule.

#### Instance

Add drop rule  
Switch(config)# management access-list test  
Switch(config-macl)# sequence 1 deny ip 1.1.1.1/255.255.255.255 interfaces gi1  
service all

### permit

#### Format

```
[sequence <1-65535>] permit interfaces IF_PORTS service
(all|http|https|snmp|ssh|telnet)
[sequence <1-65535>] permit ip A.B.C.D/A.B.C.D interfaces IF_PORTS
service (all|http|https|snmp|ssh|telnet)
[sequence <1-65535>] permit ipv6 X:X::X:/<0-128>interfaces IF_PORTS
service (all|http|https|snmp|ssh|telnet)
```

#### Parameter

sequence	(Optional) Specify the sequence number of the ACE, the sequence index indicates the ACLACE priority
interfaces	Specify interface
ip	Specify IP address and mask
ipv6	Specify IPv6 address and prefix length
service	Specify related service types

#### Default

#### Mode

Management ACL configuration mode

#### Instructions

Use the command "permit" to add permission rules that allow packets that meet the rules to pass.

#### Instance

```
Add allow rules
Switch(config)# management access-list test
Switch(config-macl)# sequence 2 permit ip 2.2.2.2/255.255.255.255 interfaces gi1
service http
```

#### no sequence

#### Format

```
no sequence <1-65535>
```

#### Parameter

sequence	Specify the serial number of the ACE
----------	--------------------------------------

#### Default

## Mode

Management ACL configuration mode

## Instructions

Use the command "no sequence" to delete the management ACL rules.

## Instance

```
Delete rule
Switch(config)# management access-list test
Switch(config-macl)# no sequence 10
```

## show management access-list

## Format

```
show management access-list NAME
```

## Parameter

NAME	The name of the management ACL
------	--------------------------------

## Default

## Mode

Privileged mode

## Instructions

Use the command "show management access-list" to query management ACL information.

## Instance

```
Query management ACL
Switch#Switch# show management access-list 1
management access-list is created test
----
sequence 1 deny ip 1.1.1.1/255.255.255.255 interfaces gi1 service all
! (Note: all other access implicitly denied)
```

## show management access-class

## Format

show management access-class

**Parameter**

**Default**

**Mode**

Privileged mode

**Instructions**

Use the command "show management access-class" to query the activated management ACL.

**Instance**

Query activation management ACL

Switch# show management access-class

Management access-class is enabled, using access-list test

## 19. MLDSnooping

### ipv6 mld snooping

#### Format

ipv6 mld snooping  
no ipv6 mld snooping

#### Parameter

#### Default

Disabled by default

#### Mode

Global configuration mode

#### Instructions

Use the command "ipv6 mld snooping" to enable the IPv6 MLD snooping function. Disabling will clear all ipv6 mld listening dynamic groups and dynamic router ports, and invalidate static ipv6 mld groups. Will no longer learn dynamic groups and router ports generated by mld messages.

#### Instance

Enable ipv6 mld snooping Function  
Switch(config)# ipv6 mld snooping

### ipv6 mld snooping report-suppression

#### Format

ipv6 mld snooping report-suppression  
no ipv6 mld snooping report-suppression

#### Parameter

#### Default

Disabled by default

#### Mode

Global configuration mode

#### Instructions

Use the command "ipv6 mld snooping report-suppression" to enable the MLD snooping report suppression function

#### Instance

Enable MLD monitoring report suppression function  
Switch(config)# no ipv6 mld snooping report-suppression

### ipv6 mld snooping version



**Format**

ipv6 mld snooping version (1|2)

**Parameter**

(1 2)	IPv6 MLD Version
-------	------------------

**Default**

Default is V1

**Mode**

Global configuration mode

**Instructions**

Use the command "ipv6 mld snooping version" to configure the MLD version. If you select version 1, then version 2 packets will not be processed.

**Instance**

Configure MLD version

Switch(config)# ipv6 mld snooping version 2

**ipv6 mld snooping unknown-multicast action****Format**

ipv6 mld snooping unknown-multicast action (drop | flood | router-port)  
no ipv6 mld snooping unknown-multicast action

**Parameter**

drop	Unknown multicast packet drop
flood	Unknown multicast packet flooding
router-port	Unknown multicast packets are forwarded to the routing port

**Default**

The default is flood

**Mode**

Interface configuration mode

**Instructions**

When igmp and mld monitoring is disabled, it cannot set the action router port.

When igmp snooping and mld snooping are disabled, it sets the flood of unknown multicast operations. When the action is the router port to flood or drop, it will delete the unknown multicast group entry.

Use the command "ipv6 mld snooping unknown-multicast action" to configure the IPv6 MLD unknown multicast policy.

**Instance**

Configure unknown multicast policy

Switch(config)# ipv6 mld snooping unknown-multicast action router-port

### ipv6 mld snooping vlan

#### Format

ipv6 mld snooping vlan VLAN-LIST

no ipv6 mld snooping vlan VLAN-LIST

#### Parameter

vlan	Specify VLAN ID
------	-----------------

#### Default

All VLANs are disabled by default.

#### Mode

Global configuration mode

#### Instructions

Disabling will clear all ipv6 mld listening dynamic groups and dynamic router ports, and make all static ips of this vlan

The igmp group is invalid. Will no longer learn dynamic groups and router ports through igmp messages. Use the command "ipv6 mld snooping vlan" to enable the VLAN-level MLD function.

#### Instance

Enable IPv6 multicast VLAN function

Switch(config)# ipv6 mld snooping vlan 1

### ipv6 mld snooping vlan fastleave

#### Format

ipv6 mld snooping vlan <VLAN-LIST>fastleave

no ipv6 mld snooping vlan <VLAN-LIST>fastleave

#### Parameter

vlan	vlan specifies the VLAN list
------	------------------------------

#### Default

Disabled by default

#### Mode

Global configuration mode

#### Instructions

Use the command "ipv6 mld snooping vlan fastleave" to enable the fast leave function. When a leave packet is received, the group will immediately remove the port.

**Instance**

Enable quick leave

Switch(config)# ipv6 mld snooping vlan 1 fastleave

**ipv6 mld snooping vlan last-member-query-count****Format**

ipv6 mld snooping vlan <VLAN-LIST>last-member-query-count <1-7>

no ipv6 mld snooping vlan <VLAN-LIST>last-member-query-count

**Parameter**

vlan	Specify VLAN list
<1-7>	Specify the last member query count to be set

**Default**

The default is 2

**Mode**

Global configuration mode

**Instructions**

Use the command "ipv6 mld snooping vlan last-member-query-count" to configure how many packets are sent.

**Instance**

Configure the number of sent member query messages

Switch(config)# ipv6 mld snooping vlan 1 last-member-query-count 5

**pv6 mld snooping vlan last-member-query-interval****Format**

ipv6 mld snooping vlan <VLAN-LIST>last-member-query-interval <1- 60>

no ipv6 mld snooping vlan <VLAN-LIST>last-member-query-interval

**Parameter**

vlan	Specify VLAN list
<1-7>	Specify the last member query interval to be set

**Default**

The default is 2

**Mode**

Global configuration mode

**Instructions**

Use the command " ipv6 mld snooping vlan last-member-query-interval" to configure how many packets are sent.

**Instance**

Configure the number of sent member query messages  
 Switch(config)# ipv6 mld snooping vlan 1 last-member-query-interval 3

**ipv6 mld snooping vlan query-interval****Format**

ipv6 mld snooping vlan <VLAN-LIST>query-interval <30-18000>  
 no ipv6 mld snooping vlan <VLAN-LIST>query-interval

**Parameter**

vlan	Specify VLAN
query-interval	Query interval setting

**Default**

The default is 125 seconds.

**Mode**

Global configuration mode

**Instructions**

Use the command "ipv6 mld snooping vlan query-interval" to set the general query interval.

**Instance**

Set general query interval  
 Switch(config)# ipv6 mld snooping vlan 1 query-interval 100

**ipv6 mld snooping vlan response-time****Format**

ipv6 mld snooping vlan <VLAN-LIST>response-time <5-20>  
 no ipv6 mld snooping vlan <VLAN-LIST>response-time

**Parameter**

vlan	Specify VLAN
response-time	Response time setting

**Default**

The default is 10

**Mode**

Global configuration mode

**Instructions**

Use the command "ipv6 mld snooping vlan response-time" to set the Response time.

**Instance**

Set response time

Switch(config)# ipv6 mld snooping vlan 1 response-time 12

**ipv6 mld snooping vlan router****Format**

ipv6 mld snooping vlan VLAN-LIST router learn pim-dvmrp no

ipv6 mld snooping vlan VLAN-LIST router learnpim-dvmrp

**Parameter**

vlan	Specify VLAN
------	--------------

**Default**

Enable Default

**Mode**

Global configuration mode

**Instructions**

Use the command "ipv6 mld snooping vlan router" to enable the learning router port through routing protocol packets (such as PIM/PIMv2, DVMRP, MOSPF).

**Instance**

Configure router

Switch(config)# ipv6 mld snooping vlan 99 router

**ipv6 mld snooping vlan static-port****Format**

ipv6 mld snooping vlan &lt;VLAN-LIST&gt;static-port IF\_PORTS

no ipv6 mld snooping vlan &lt;VLAN-LIST&gt;static-port IF\_PORTS

**Parameter**

vlan	Specify VLAN
static -port	Specify Port

**Default****Mode**

Global configuration mode

**Instructions**

Use the command "ipv6 mld snooping vlan static-port" to add static forwarding ports, and all known vlan 1 ipv6 groups will add static ports.

**Instance**

Configure static forwarding port

```
Switch(config)# ipv6 mld snooping vlan 1 static -port gi1-2
```

### ipv6 mld snooping vlan forbidden-router-port

#### Format

```
ipv6 mld snooping vlan <VLAN-LIST>forbidden-router-port IF_PORTS
```

```
no ipv6 mld snooping vlan <VLAN-LIST>forbidden-router-port IF_PORTS
```

#### Parameter

Vlan	Specify VLAN
IF_PORTS	Speicfy Port

#### Default

#### Mode

Global configuration mode

#### Instructions

Use the command "ipv6 mld snooping vlan forbidden-router-port" to add static forbidden routing ports. This will also remove the port from the static routed port. Prohibited routing ports will not forward received query packets.

#### Instance

Configure to disable router

```
Switch(config)# ipv6 mld snooping vlan 1 forbidden-router-port gi2
```

### ipv6 mld snooping vlan static router port

#### Format

```
ipv6 mld snooping vlan <VLAN-LIST>static-router-port IF_PORTS
```

```
no ipv6 mld snooping vlan <VLAN-LIST>static -router-port IF_PORTS
```

#### Parameter

Vlan	Specify VLAN
IF_PORTS	Speicfy Port

#### Default

#### Mode

Global configuration mode

#### Instructions

Use the command "ipv6 mld snooping vlan static-router-port" to add a static route port. This port will forward all query messages.

#### Instance

Configure router port

```
Switch(config)# ipv6 mld snooping vlan 1 static-router-port gi1-2
```

### ipv6 mld snooping vlan static-group

#### Format

```
ipv6 mld snooping vlan <VLAN-LIST>static-group [<ipv6-addr>]
interfaces IF_PORTS
no ipv6 mld snooping vlan <VLAN-LIST>static-group [<ipv6-addr>]
interfaces IF_PORTS
```

#### Parameter

vlan	Specify VLAN
static-group	Static IPv6 multicast address
interfaces	Specify Port

#### Default

#### Mode

Global configuration mode

#### Instructions

Use the command "ipv6 mld snooping vlan static-group" to add a static group. The static group will not learn other dynamic ports. If the dynamic group exists, the static group will overlap with the dynamic group. The static group configuration is valid unless igmp snooping global and vlan are enabled.

#### Instance

Configure static groups

```
Switch(config)# ipv6 mld snooping vlan 1 static-group ff13::1 interfaces gi1-2
```

### ipv6 mld snooping vlan group

#### Format

```
no ipv6 mld snooping vlan <VLAN-LIST>group <ipv6-addr>
```

#### Parameter

vlan	Specify VLAN
group	Static IPv6 multicast address

#### Default

#### Mode

Global configuration mode

#### Instructions

Use the command "no ipv6 mld snooping vlan group" to delete a dynamic or static multicast

group.

#### Instance

Delete multicast group

Switch(config)# no ipv6 mld snooping vlan 1 group ff13::1

### ipv6 mld profile

#### Format

ipv6 mld profile <1-128>

no ipv6 mld profile <1-128>

#### Parameter

<1-128>	Specify the ID of the generated template
---------	--

#### Default

#### Mode

Global configuration mode

#### Instructions

Use the command "ipv6 mld profile" to enter the MLD template configuration Default.

#### Instance

Enter MLD template configuration

Switch(config)# ipv6 mld profile 1

### profile range

#### Format

profile range ipv6 <ipv6-addr> [ipv6-addr] action (permit | deny)

#### Parameter

ipv6	Set the start and end IPv6 addresses of multicast
permit	Allow address learning within the multicast address range
deny	Prohibit address learning in the multicast address range

#### Default

#### Mode

mld profile config mode

#### Instructions

Use the command "profile range" to generate an MLD template.

#### Instance

Configure the IGMP template.

Switch(config)# ipv6 mld profile 1



---

```
Switch(config-igmp-profile)# profile range ip v6 ff13::1 ff13::10 action permit
```

### ipv6 mld filter

#### Format

```
ipv6 mld filter <1-128>
no ipv6 mld filter
```

#### Parameter

<1-128>	Configure the ID of the MLD filter template
---------	---

#### Default

#### Mode

Port Configuration mode

#### Instructions

Use the command "ipv6 mld filter" to bind a template to the interface. When the port is bound to the template, the port learning group will be updated. If the group does not match the filtering template rules, it will delete the port from the group. Static groups are excluded.

#### Instance

```
Bind filter template
Switch(config)# interface gi1
Switch(config-if)#ipv6 mld filter 1
```

### ipv6 mld max-groups

#### Format

```
ipv6 mld max-groups <0-1024>
no ipv6 mld max-groups
```

#### Parameter

max-groups	Largest multicast group
------------	-------------------------

#### Default

Default is 1024

#### Mode

Port Configuration mode

#### Instructions

Use the command "ipv6 mld max-groups" to configure the maximum number of learned multicast groups on the interface.

#### Instance

```
onfigure the maximum number of learned multicast groups
```

---

Switch(config-if)#ipv6 mld max-groups 10

### ipv6 mld max-groups action

#### Format

ipv6 mld max-groups action (deny | replace)

#### Parameter

deny	When the interface reaches the maximum number of multicast groups, discard new groups
replace	When the interface reaches the maximum number of multicast groups, replace the old group

#### Default

Default is deny

#### Mode

Port Configuration mode

#### Instructions

Use the command "ipv6 mld max-groups action" to configure the action processing when the interface reaches the maximum multicast group.

#### Instance

Configuration replacement operation

Switch(config-if)#ipv6 mld max-groups action replace

### clear ipv6 mld snooping groups

#### Format

clear ipv6 mld snooping groups [(dynamic | static)]

#### Parameter

none	When dynamic or static is not specified, clear all groups
dynamic	Clear dynamic group
static	Clear static group

#### Default

#### Mode

Privilege Mode

#### Instructions

Use the command "clear ipv6 mld snooping groups" to clear the multicast groups of the system.

**Instance**

Clear multicast group

Switch# clear ipv6 mld snooping groups

**clear ipv6 mld snooping statistics****Format**

clear ipv6 mld snooping statistics

**Parameter****Default****Mode**

Privilege Mode

**Instructions**

Use the command "show ipv6 mld snooping statistics" to clear MLD statistics.

**Instance**

Clear IGMP statistics

Switch# clear ipv6 mld snooping statistics

**show ipv6 mld snooping groups counters****Format**

show ipv6 mld snooping groups counters

**Parameter****Default****Mode**

Privilege Mode

**Instructions**

Use the command "show ipv6 mld snooping groups counters" to query the multicast group count, including static and dynamic.

**Instance**

Query multicast group count

Switch# show ipv6 mld snooping group counters

Total ipv6 mld snooping group number: 2

**show ipv6 mld snooping groups****Format**



**Instance**

Query router

Switch# show ipv6 mld snooping router

Dynamic Router Table

VID | Port | Expiry Time(Sec)

-----+-----+-----

Total Entry 0

Static Router Table VID | Port Mask

-----+-----

1 | gi4

Total Entry 1

Forbidden Router Table VID | Port Mask

-----+-----

1 | gi8

Total Entry 1

**show ipv6 mld snooping****Format**

show ipv6 mld snooping

**Parameter****Default****Mode**

Privilege Mode

**Instructions**

Use the command "show ipv6 mld snooping" to query MLD global configuration information.

**Instance**

Query IGMP information

Switch# show ipv6 mld snooping

MLD Snooping Status

-----

Snooping :Enabled

ReportSuppression : Enabled

Operation Version :v1

Forward Method : mac  
 Unknown IPMulticastAction :Flood

#### Packet Statistics

TotalRX: 0  
 ValidRX: 0  
 InvalidRX 0  
 Other RX: 0  
 Leave RX : 0  
 ReportRX : 0  
 GeneralQueryRX 0  
 Specail GroupQueryRX 0  
 Specail Group & SourceQueryRX 0  
 Leave TX : 0  
 ReportTX : 0  
 GeneralQueryTX 0  
 Specail GroupQueryTX 0  
 Specail Group & SourceQueryTX 0

### show ipv6 mld snooping vlan

#### Format

show ipv6 mld snooping vlan [VLAN-LIST]

#### Parameter

none	If not specified, query all VLANs
vlan	Specify VLAN query

#### Default

#### Mode

Privilege Mode

#### Instructions

Use the command "show ipv6 mld snooping vlan" to query the MLD multicast VLAN configuration information

#### Instance

Query MLD multicast VLAN information  
 Switch# show ipv6 mld snooping vlan 1  
 MLD Snooping is globally enabled  
 MLD Snooping VLAN 1 admin : disabled  
 MLD Snooping operation mode : disabled  
 MLD Snooping robustness: admin 2 oper 2  
 MLD Snooping query interval: admin 125 sec oper 125 sec MLD  
 Snooping query max response : admin 10 sec oper 10 sec MLD  
 Snooping last member query counter: admin 2 oper2

MLD Snooping last member query interval: admin 1 sec oper 1 sec  
 MLD Snooping last immediate leave: disabled  
 MLD Snooping automatic learning of multicast router ports: enabled

### show ipv6 mld snooping forward-all

#### Format

show ipv6 mld snooping forward-all [vlan VLAN-LIST]

#### Parameter

none	If not specified, query all forwarding information
vlan	Specify VLAN query

#### Default

#### Mode

Privilege Mode

#### Instructions

Use the command "show ipv6 mld snooping forward-all" to query all forwarding information.

#### Instance

Query forwarding information  
 Switch# show ipv6 mld snooping forward-all 1  
 MLD Snooping VLAN 1  
 MLD Snoopingstaticport: None MLD  
 Snooping forbidden port : None

### show ipv6 mld profile

#### Format

show ipv6 mld profile [<1-128>]

#### Parameter

none	Not specified, means all templates
<1-128>	Specify the ID of the template

#### Default

#### Mode

Privilege Mode

#### Instructions

Use the command "show ipv6 mld profile" to query the IGMP profile configuration information.

#### Instance

Query IGMP template information

```
Switch# show ipv6 mld profile
IPv6 mldprofile index: 1
IPv6 mld profile action: permit
Range low ip: ff13::1
Range high ip: ff13::10
```

### show ipv6 mld filter

#### Format

```
show ipv6 mld filter [interfaces IF_PORTS]
```

#### Parameter

none	Not specified, which means all ports
interfaces	According to the specified interface

#### Default

#### Mode

Privilege Mode

#### Instructions

Use the command "show ipv6 mld filter" to query MLD filter template information.

#### Instance

```
Query filter template
Switch# show ipv6 mld filter
Port ID | Profile ID
-----+-----
gi1 : 1
gi2 : None
gi3 : None
gi4 : None
gi5 : None
--More--
```

### show ipv6 mld max-group

#### Format

```
show ipv6 mld max-group [interfaces IF_PORTS]
```

#### Parameter

none	Not specified, which means all ports
interfaces	According to the specified interface

#### Default

#### Mode



## Privilege Mode

### Instructions

Use the command "show ipv6 mld max-group" to query the maximum learning number of the interface multicast group.

### Instance

Query the maximum learning number of the interface multicast group

```
Switch# show ipv6 mld max-group
```

```
Port ID | Max Group
```

```
-----+-----
```

```
gi1 : 50
```

```
gi2 : 256
```

```
gi3 : 256
```

```
gi4 : 256
```

```
gi5 : 256
```

```
--More--
```

## show ipv6 mld max-group action

### Format

```
show ipv6 mld max-group action [interfaces IF_PORTS]
```

### Parameter

none	Not specified, which means all ports
interfaces	According to the specified interface

### Default

Default is deny

### Mode

Privilege Mode

### Instructions

Use the command "show ipv6 mld max-group action" to query the operation processing.

### Instance

Query operation

```
Switch# show ipv6 mld max-group action
```

```
Port ID | Max-groups Action
```

```
-----+-----
```

```
gi1 : replace
```

```
gi2 : deny
```

```
gi3 : deny
```

```
gi4 : deny
```

```
gi5 : deny
```

```
--More--
```

---

## 20. MVR

### mvr

#### Format

```
mvr
no mvr
```

#### Parameter

#### Default

Disable Default

#### Mode

Global configuration mode

#### Instructions

Use the command "mvr" to enable the MVR function.

#### Instance

```
Configure MVR
Switch(config)# mvr
Switch(config)# no
mvr
```

```
Query MVR
Switch# show mvr MVR
Running : Disabled MVR
Multicast VLAN :1
MVR Group Range : None
MVR Max Multicast Groups : 128
MVR Current Multicast Groups : 0
MVR Global query response time : 1 sec
MVR Mode : compatible
```

---

### mvr vlan

#### Format

```
mvr vlan [VLAN-LIST]
```

#### Parameter

Vlan	Specify the VLAN of the MVR, which must be created first
------	--

#### Default

Default is 1

#### Mode

Global configuration mode

## Instructions

Use the command "mvr vlan" to configure the MVR VLAN. Changing the mvr vlan id will delete the old mvr vlan and the new mvr vlan group. If there is a configured source or sink port, it will check that the source must only be in the mvr vlan, and the sink port cannot be in the mvr vlan member.

## Instance

Configure VLAN for MVR  
 Switch(config)# mvr vlan 2  
 The operation will delete the old and new MVR VLAN groups include static MVR groups.Continue? [yes/no]:y

## mvr group

### Format

mvr group <ip-address> [<1-128>]

### Parameter

<ip-address>	MVR multicast address
[<1-128>]	Consecutive IP address sequence

### Default

### Mode

Global configuration mode

### Instructions

Use the command "mvr group" to configure the sequence of MVR multicast group addresses.

### Instance

Configure MVR group  
 Switch(config)# mvr group 224.1.1.1 8  
 The operation will delete the MVR VLAN groups include static MVR groups.Continue? [yes/no]:y

## mvr mode

### Format

mvr mode (dynamic | compatible)

### Parameter

Dynamic	Allow dynamic MVR membership on the source port
compatible	Not support IGMP dynamic connection on the source port

### Default

Default is compatible

### Mode

Global configuration mode

**Instructions**

Use the command "mvr mode" to configure and modify the MVR Default.

**Instance**

Configure MVR Default  
Switch(config)#mvr mode dynamic

**mvr query-time****Format**

mvr query-time <1-10>  
no mvr query-time

**Parameter**

<1-10>	Specify query or response time
--------	--------------------------------

**Default**

Default is 1

**Mode**

Global configuration mode

**Instructions**

Use the command "mvr query-time" to configure the MVR query time.

**Instance**

Configure MVR query time  
Switch(config)# mvr query-time 10

**mvr port type****Format**

mvr type (source | receiver)  
no mvr type

**Parameter**

Source	Configure the upstream port that receives and sends multicast data as the source port. Subscribers cannot connect directly Connect to the source port. All source ports on the switch belong to a single multicast VLAN.
Receiver	If the port is a subscriber port and should only receive multicast data, configure it as a receiver port. It will not receive data unless it becomes a member of a multicast group (statically or by using IGMP leave and join messages). The receiver port cannot belong to the multicast VLAN.

**Default****Mode**

Interface configuration Mode

**Instructions**

Use the command "mvr port type" to configure the MVR port type.

**Instance**

```
Configure MVR port type
Switch(config)# interface gi1
Switch(config-if)# switchport trunk allowed vlan 2
Switch(config-if)# mvr type source
Switch(config-if)#exit
Switch(config)# interface gi2
Switch(config-if)# switchport mode access
```

---

```
Switch(config-if)#mvr type receiver
```

Query interface MVR configuration

```
Switch# show mvr interface
Port | Type | Immediate Leave
-----+-----+-----
gi1 | Source | Disabled
gi2 | Receiver | Disabled
```

**mvr immediate****Format**

```
mvr immediate no
mvr immediate
```

**Parameter****Default****Mode**

Interface configuration Mode

**Instructions**

Use the command "mvr immediate" to configure the MVR to leave immediately.

Note: This command is only applicable to the receiver port, and should only be enabled on the receiver port connected to a single receiver device.

**Instance**

```
Configure MVR to leave
immediatelySwitch(config)#
interface gi1 Switch(config-
if)#mvr immediate
```

## mvr vlan group

### Format

```
mvr vlan <VLAN-ID>group <ip-addr>interfaces IF_PORTS
no mvr vlan <VLAN-ID>group <ip-addr>interfaces IF_PORTS
```

### Parameter

Vlan	MVR static multicast group VLAN
Group	MVR static multicast address
interfaces	Specify Port

### Default

### Mode

Global configuration mode

### Instructions

Use the command "mvr vlan group" to configure a static MVR multicast group and multicast member ports.

Note: Under Compatible Default, this command is only applicable to the receiver port. Under dynamic Default, it is applicable to receiver port and source port. When deleting the static mvr group, all ports will be deleted.

### Instance

```
Configure MVR static multicast group
Switch(config)# mvr vlan 2 group 224.1.1.1 interfaces gi2
```

## clear mvr members

### Format

```
clear mvr members [dynamic|static]
```

### Parameter

Dynamic	MVR dynamic multicast group
Static	MVR static multicast group
None	Not specified, which means all static and dynamic members

### Default

### Mode

Privilege Mode

### Instructions

Use the command "clear mvr members" to clear the MVR multicast group members.

### Instance

```
Clear MVR multicast group members
```

Switch# clear mvr members  
**show mvr members**

Format

show mvr members

Parameter

Default

Mode

Privilege Mode

Instructions

Use the command "show mvr members" to query the MVR multicast group members.

Instance

Query MVR multicast group members  
 Switch# show mvr members

**show mvr interface**

Format

show mvr interface [IF\_PORTS]

Parameter

None	Not specified, which means all ports
interfaces	According to the specified interface

Default

Mode

Privilege Mode

Instructions

Use the command "show mvr interface" to query the interface MVR configuration.

Instance

Query interface MVR configuration  
 Switch# show mvr interface  
 Port | Type | Immediate Leave

```
-----+-----+-----
gi1| Source| Disabled
gi2|Receiver| Disabled
```

**show mvr**

Format

show mvr

Parameter

Default

Mode

Privilege Mode

Instructions

Use the command "show mvr" to query MVR information.

Instance

Query MVR

Switch# show mvr MVR

Running : Disabled MVR

Multicast VLAN :1

MVR Group Range : None

MVR Max Multicast Groups : 128

MVR Current Multicast Groups : 0

MVR Global query response time : 1 sec

MVR Mode : compatible



## 21. POE

### poe

#### Format

```
poe
no poe
```

#### Parameter

#### Default

Default POE is enabled on all ports.

#### Mode

Interface configuration Mode

#### Instructions

Use the command "poe" to enable the port's POE function.

#### Instance

```
Enable POE port
Switch(config)# interface GigabitEthernet 1
Switch(config-if)# poe
```

#### Query POE configuration

```
Switch# show poe
Get poe power:
```

Port	Enable	State	type	level	actual- power(mW)	volatge(V)	current(mA)	
gi1	enable	on	AT	4	676	52	13	
gi2	enable	off	AF	0	N/A	N/A	N/A	
gi3	enable	off	AF	0	N/A	N/A	N/A	
gi4	enable	off	AF	0	N/A	N/A	N/A	
gi5	enable	off	AF	0	N/A	N/A	N/A	
gi6	enable	off	AF	0	N/A	N/A	N/A	
gi7	enable	off	AF	0	N/A	N/A	N/A	
gi8	enable	off	AF	0	N/A	N/A	N/A	

Total used power: 676 (mW)

Current Temperature: 65 (C)

### poe schedule

#### Format

```
poe schedule week days hour hours
```

no poe schedule week days hour hours

#### Parameter

days	Port poe power supply days
hours	Port poe power supply hours

#### Default

Default all dates and times enable POE power supply

#### Mode

Interface Configuration Mode

#### Instructions

Use the command "poe schedule" to set the port poe power supply time.

#### Instance

Set POE interface time  
 Switch(config)# interface GigabitEthernet 1  
 Switch(config-if)# poe schedule week mon hour 1

Note: The configured time has a deviation of about 0~10 minutes.

#### show poe

#### Format

show poe

#### Parameter

#### Default

#### Mode

Privilege Mode

#### Instructions

Use the command "show poe" to query the POE function of the system

#### Instance

Query POE configuration  
 Switch# show poe  
 Get poe power:

```

Port | Enable | State | type | level|actual- | volatge(V) | current(mA)
      |        |       |      |      |power(mW)|             |
-----+-----+-----+-----+-----+-----+-----+-----
-----

```

---

gi1	enable	on	AT	4	676	52	13
gi2	enable	off	AF	0	N/A	N/A	N/A
gi3	enable	off	AF	0	N/A	N/A	N/A
gi4	enable	off	AF	0	N/A	N/A	N/A
gi5	enable	off	AF	0	N/A	N/A	N/A
gi6	enable	off	AF	0	N/A	N/A	N/A
gi7	enable	off	AF	0	N/A	N/A	N/A
gi8	enable	off	AF	0	N/A	N/A	N/A

Total used power: 676 (mW)

Current Temperature: 65 (C)

## 22. Port Mirror

### mirror session source interface

#### Format

```
mirror session <1-4>source interfaces IF_PORTS (both | rx | tx) no
mirror session<1-4>source interfaces IF_PORTS (both | rx | tx) no
mirror session (<1-4> |all)
```

#### Parameter

<1-4>	Configurable mirroring session
interfaces	Source port of mirrored packets
both	The direction of the mirror message is bidirectional
Rx	The direction of the mirrored message is the receiving direction
Tx	The direction of the mirrored message is the sending direction

#### Default

#### Mode

Global configuration mode

#### Instructions

Use the command "mirror session source interface" to configure port mirroring and specify the source port and packet direction.

#### Instance

```
Configure the mirror source port
Switch(config)# mirror session 1 source interface gi2-5 both
Switch(config)# mirror session 1 destination interface gi1
Switch(config)# do show mirror session 1
Session 1 Configuration Source
RX Port : gi2-5
SourceTXPort : gi2-5
Destinationport : gi1
Ingress State:disabled
```

### mirror session destination interface

#### Format

```
mirror session <1-4>destination interface IF_NMLPORT [allow-ingress]
no mirror session <1-4>destination interface IF_NMLPORT
no mirror session (<1-4> | all)
```

#### Parameter

<1-4>	Configurable mirroring session
interfaces	Destination port of mirrored packets
allow-ingress	Enable ingress traffic forwarding

**Default****Mode**

Global configuration mode

**Instructions**

Use the command "mirror session destination interface" to configure port mirroring and specify the destination port.

**Instance**

```
Switch(config)# mirror session 1 destination interface gi1
Switch(config)# do show mirror session 1
Session 1 Configuration Source
RX Port : gi2-5
SourceTXPort      : gi2-5
Destinationport   : gi1
Ingress State:disabled
```

**show mirror****Format**

show mirror [session &lt;1-4&gt;]

**Parameter**

<1-4>	Configurable mirroring session

**Default****Mode**

Privilege Mode

**Instructions**

Use the command "show mirror" to query the mirroring session configured by the system.

**Instance**

```
Switch#show mirror session 1
Session 1 Configuration Source
RX Port : gi2-5
SourceTXPort      : gi2-5
Destinationport   : gi1
Ingress State:disabled
```

## 23. Port

### description

#### Format

```
description WORD<1-32>
no description
```

#### Parameter

description	Interface description information
-------------	-----------------------------------

#### Default

#### Mode

Interface Mode

#### Instructions

Use the command "description" to easily configure the name information for the interface.

#### Instance

```
Configuration interface description
Switch(config)# interface gi1
Switch(config-if)# description "uplink port"
```

#### Query interface status

```
Switch# show interfaces gi1 status
Port Name Status Vlan Duplex Speed Type
gi1 uplinkport connected 1 a-full a-10M Copper
```

### speed

#### Format

```
speed (10 | 100 | 1000)
speed auto [(10 | 100 | 1000 | 10/100)]
speed nonegiate
no speed nonegiate
```

#### Parameter

10	The rate of the specified interface is mandatory 10Mbit/s or auto-negotiation 10Mbit/s
100	The rate of the designated interface is mandatory 100Mbit/s or auto-negotiation 100Mbit/s
1000	The rate of the designated interface is forced 1000Mbit/s or auto-negotiation 1000Mbit/s
10/100	The rate of the designated interface is auto-negotiation 10Mbit/s and 100Mbit/s

**Default**

Default port rate is auto-negotiation

**Mode**

Interface Configuration Mode

**Instructions**

Use the command "speed" to modify the port rate, but it cannot be configured to exceed the maximum supported rate of the port.

**Instance**

```
Configure interface
rateSwitch(config)# interface
gi1 Switch(config-if)# speed
100 Switch(config-if)# exit
Switch(config)# interface gi2
Switch(config-if)# speed auto 10/100
Query interface configuration
Switch# show running-config interfaces gi1-2
interface gi1
  speed 100!
interface gi2
  speed auto 10/100!
```

**Query port status**

```
Switch# show interfaces gi1-2 status
```

Port	Name	Status	Vlan	Duplex	Speed	Type
gi1		notconnect	1	auto	100M	Copper
gi2		notconnect	1	auto	auto	Copper

**Duplex****Format**

duplex (auto | full | half)

**Parameter**

auto	The duplex of the specified interface Default is auto-negotiation
full	The duplex of the specified interface Default is full duplex
half	The duplex of the specified interface Default is half duplex

**Default**

The Default duplex of the interface is auto-negotiation

**Mode**

Interface Configuration Mode

### Instructions

Use the command "duplex" to modify the duplex Default of the interface.

### Instance

Configure interface  
duplexSwitch(config)#

interface gi1 Switch(config-  
if)# duplex full

Query interface configuration

Switch# show running-config interfaces gi1

interface gi1  
duplex full

Query interface status

Switch# show interfaces gi1 status

Port	Name	Status	Vlan	Duplex	Speed	Type
gi1		connected	1	full	a-10M	Copper

## shutdown

### Format

```
shutdown no  
shutdown
```

### Parameter

### Default

Default configuration is no shutdown

### Mode

Interface Configuration Mode

### Instructions

Use the command "shutdown" to shut down the interface. Use the command "no shutdown" to open the interface.

### Instance

Configure the interface as  
closed

Switch(config)# interface gi1  
Switch(config-if)# shutdown

Query interface configuration

Switch# show running-config interfaces gi1

interface gi1  
shutdown

Query interface status

Switch# show interfaces gi1 status



Port	Name	Status	Vlan	Duplex	Speed	Type
gi1		disable	1	full	auto	Copper

**flowcontrol**

**Format**

```
flowcontrol (auto | off | on)
no flowcontrol
```

**Parameter**

auto	The flow control of the designated interface is auto-negotiation
off	The flow control of the specified interface is closed
On	The flow control of the specified interface is open

**Default**

The flow control of the Default interface is closed

**Mode**

Interface Configuration Mode

**Instructions**

Use the command "flowcontrol" to modify the flow control configuration of the interface.

**Instance**

```
Configure interface flow control
Switch(config)# interface gi1
Switch(config-if)# flowcontrol on
```

**Query interface**

```
Switch# show interfaces gi1
GigabitEthernet1 is up
  Hardware is Gigabit Ethernet
  Full-duplex, Auto-speed, media type is Copper
  flow-control is enable, status is off
  back-pressure is enabled
    151 packets input, 9920 bytes, 0 throttles
  Received 0 broadcasts (151 multicasts)
  0 runs, 0 giants, 0 throttles
  0 input errors, 0 CRC, 0 frame
  151 multicast, 0 pause input
  0 input packets with dribble condition detected
  25358 packets output, 2250933 bytes, 0 underrun
  0 output errors, 0 collisions
  0 babbles, 0 late collision, 0 deferred
  0 PAUSE output
```

**jumbo-frame**

**Format**

jumbo-frame <1518-10000>

**Parameter**

jumbo-frame	Support jumbo frames
-------------	----------------------

**Default**

The Default interface of jumbo frame is 1522.

**Mode**

Global configuration mode

**Instructions**

Use the command "jumbo-frame" to configure the maximum jumbo frame of the interface.

**Instance**

Configure interface jumbo frames  
Switch(config)# jumbo-frame 9216

Query configuration  
Switch# show running-config  
jumbo-frame 9216

**protected****Format**

protected  
no protected

**Parameter****Default**

Default is not isolated

**Mode**

Interface configuration Mode

**Instructions**

Use the command "protected" to enable the port isolation function. Isolated ports are only allowed to communicate with unisolated ports. In other words, the isolated port is not allowed to communicate with another isolated port.

**Instance**

Configure interface isolation  
Switch(config)# interface range gi1-2  
Switch(config-if-range)# protected  
Query interface isolation  
Switch# show interfaces gi1-2 protected  
Port | Protected State

```

-----+-----
      gi1
      |enabled
      gi2
      |enabled

```

### EEE

#### Format

```

eee
no eee

```

#### Parameter

#### Default

Default is to disable

#### Mode

Interface configuration mode

#### Instructions

Use the command "eee" to start the energy-efficient Ethernet function of the interface.

#### Instance

Configure EEE

```
Switch(config)# interface gi1
```

```
Switch(config-if)# eee
```

Query configuration

```
Switch# show running-config interface gi1
```

```
interface gi1
```

```
eee
```

### clear interface

#### Format

```
clear interfaces IF_PORTS counters
```

#### Parameter

interfaces	Specify Port
------------	--------------

#### Default

#### Mode

Privilege Mode

#### Instructions

Use the command "clear interface" to clear the statistics of the specified interface.

### Instance

Clear interface statistics  
Switch(config)# clear interfaces gi1 counters

Query interface  
Switch# show interfaces gi1  
GigabitEthernet1 is up  
Hardware is Gigabit Ethernet  
Full-duplex, Auto-speed, media type is Copper  
back-pressure is enabled  
0 packets input, 0 bytes, 0 throttles  
Received 0 broadcasts (0 multicasts)  
0 runs, 0 giants, 0 throttles  
0 input errors, 0 CRC, 0 frame  
0 multicast, 0 pause input  
0 input packets with dribble condition detected  
6 packets output, 488 bytes, 0 underrun  
0 output errors, 0 collisions  
0 babbles, 0 late collision, 0 deferred  
0 PAUSE output

### show interface

#### Format

show interfaces *IF\_PORTS*  
show interfaces *IF\_PORTS* status  
show interfaces *IF\_PORTS* protected

#### Parameter

interfaces	Specify port
------------	--------------

#### Default

#### Mode

Privilege Mode

#### Instructions

Use the command "show interface" to query detailed statistics and status information of the interface. Use the command "show interface status" to query the interface status information. Use the command "show interface protected" to query interface isolation information.

### Instance

Query Interface  
Switch# show interfaces gi1  
GigabitEthernet1 is up

Hardware is Gigabit Ethernet  
Full-duplex, Auto-speed, media type is Copper  
back-pressure is enabled  
0 packets input, 0 bytes, 0 throttles  
Received 0 broadcasts (0 multicasts)  
0 runts, 0 giants, 0 throttles  
0 input errors, 0 CRC, 0 frame  
0 multicast, 0 pause input  
0 input packets with dribble condition detected  
6 packets output, 488 bytes, 0 underrun  
0 output errors, 0 collisions  
0 babbles, 0 late collision, 0 deferred  
0 PAUSE output

## 24. Port Error Disable

### errdisable recovery cause

#### Format

```
errdisable recovery cause (all|acl|arp-inspection|bpdu-guard|broadcast-
flood|dhcp-rate-limit|psecure-violation|selfloop|unicast-flood|unknown-
multicastflood)
no errdisable recovery cause (all|acl|arp-inspection|bpdu-guard|broadcast-
flood|dhcp-rate-limit|psecure-violation|selfloop|unicast-flood|unknown-
multicastflood)
```

#### Parameter

all	Enable automatic recovery for port errors disabled for all reasons
acl	Enable automatic recovery for port errors disabled by acl
arp-inspection	Enable automatic recovery for port errors disabled for DAI reasons
bpdu-guard	Enable automatic recovery for port errors disabled for bpdu protection reasons
broadcast-flood	Enable automatic recovery for port errors disabled for broadcast flooding reasons
dhcp-rate-limit	Enable automatic recovery for port errors disabled for DHCP rate limiting reasons
psecure-violation	Enable automatic recovery of port errors disabled for security violation reasons
selfloop	Enable automatic recovery for port errors disabled for loop reasons
unicast-flood	Enable automatic recovery for port errors disabled for unknown unicast flooding reasons
unknown-multicastflood	Enable automatic recovery for port errors disabled for unknown multicast reasons

#### Default

Default disable

#### Mode

Global configuration mode

#### Instructions

Use the command "errdisable recovery cause" when the port will be disabled because the protocol detects an invalid operation. To enable port errors, disable recovery from specific causes.

#### Instance

```
Enable errdisable function
Switch(config)# errdisable recovery cause bpdu-guard
Switch(config)# errdisable recovery cause selfloop
```

### errdisable recovery cause udid

#### Format

```
errdisable recovery cause udld
no errdisable recovery cause udld
```

#### Parameter

#### Default

Default disable

#### Mode

Global configuration mode

#### Instructions

Use the command "errdisable recovery cause udld" to enable automatic recovery of unidirectional link detection (UDLD).

#### Instance

```
Configure the errdisable function of UDLD
switch(config)# errdisable recovery cause udld
switch# show errdisable recovery
ErrDisable Reason Timer Status
-----+-----
bpduguard |
disabled udld|enabled
...
```

#### errdisable recovery interval

#### Format

```
errdisable recovery interval seconds
```

#### Parameter

interval	Error disable recovery time interval, Default 300 seconds
----------	---

#### Default

Default is 300 Seconds

#### Mode

Global configuration mode

#### Instructions

Use the command "errdisable recovery interval" to set the recovery interval for the port that disables errors.

#### Instance

```
Set errdisable interval time
Switch(config)# errdisable recovery interval 60
```

#### show errdisable recovery

**Format**

```
show errdisable recovery
```

**Parameter****Default****Mode**

```
Privilege Mode
```

**Instructions**

Use the command "show errdisable recovery" to query the error disable configuration and interface error disable status.

**Instance**

Query error disable configuration

```
Switch# show errdisable recovery
```

```
ErrDisableReason      | TimerStatus
```

```
-----+-----
          bpduguard | disabled
            udld | disabled
            selfloop |
disabled broadcast-flood |
disabled
unknown-multicast-flood | disabled
          unicast-flood | disabled
                acl |
disabled psecure-violation |
disabled
          dhcp-rate-limit | disabled
          arp-inspection | disabled
```

```
Timer Interval : 300 seconds
```

Interfaces that will be enabled at the next timeout:

```
Port | ErrorDisableReason      | TimeLeft
```

```
-----+-----
```



## 25. Port Security

### port-security (Global)

#### Format

```
port-security
noport-security
```

#### Parameter

#### Default

Default disable

#### Mode

Global configuration mode

#### Instructions

Use the command "port-security" to enable the port security global switch.

#### Instance

```
Enable port security
switch(config)#port-security
switch# show port-security
port-security is: Enabled
```

### port-security (Interface)

#### Format

```
port-security
noport-security
```

#### Parameter

#### Default

Default disable

#### Mode

Interface configuration mode

#### Instructions

Use the command "port-security" to enable the port security interface switch.

#### Instance

```
Enable port security under the
interface
switch(config)# interface gi1
switch(config-if)# port-security
switch(config)# show port-security interfaces gi1
Port | Security |CurrentAddr | Action
```

```
gi1 | Enabled(1) | 0 | Discard
```

### port-security address-limit

#### Format

```
port-security address-limit <1-256>
port-security violation (protect | restrict | shutdown)
no port-security address-limit
no port-security violation
```

#### Parameter

<1-256>	The number of MAC addresses learned under the specified interface
protect	When MAC learning exceeds the limit, discard new MAC data frames
restrict	When MAC learning exceeds the limit, forward new MAC data frames and count
shutdown	Shut down the interface when MAC learning exceeds the limit

#### Default

The default MAC address learning number is 1, and packets are discarded when the threshold is exceeded.

#### Default

Interface configuration mode

#### Instructions

Use the command "port-security address-limit" to set the MAC learning limit, and use the command "port-security violation" to set the violation operation after the threshold is exceeded.

#### Instance

```
Configure port security
switch(config)# interface gi1
switch(config-if)# port-security address-limit 10
switch(config-if)# port-security violation protect
switch(config-if)# port-security
```

Query the port security configuration of the interface

```
Switch# show port-security interfaces gi1
```

Port	Status	MaxAddr	TotalAddr	ConfigAddr	Violation	Action
gi1	Up	10	0	0	0	Protect

### show port-security

#### Format

```
show port-security
```

## Parameter

## Default

## Mode

Privilege Mode

## Instructions

Use the command "show port-security" to query the system port security Global configuration.

## Instance

```
Query port security
Global configuration switch#
show port-security port-
security is: Enabled
```

**show port-security interface**

## Format

```
show port-security interface IF_PORTS
```

## Parameter

interface	Specify the interface for query
-----------	---------------------------------

## Default

## Mode

Privilege Mode

## Instructions

Use the command "show port-security interfaces" to query the security configuration information of the specified port.

## Instance

Query the port security configuration of the interface

```
Switch# show port-security interfaces gi1
```

Port	Status	MaxAddr	TotalAddr	ConfigAddr	Violation	Action
-----	-----	-----	-----	-----	-----	-----
gi1	Up	10	0	0	0	Protect

## 26. Protocol VLAN

### vlan protocol-vlan group (Global)

#### Format

```
vlan protocol-vlan group <1-8>frame-type
(ethernet_ii|llc_other|snap_1042) protocol-value VALUE
no vlan protocol-vlan group <1-8>
```

#### Parameter

group	Protocol VLAN group ID
frame-type	Specify frame type
protocol-value	Specified protocol value

#### Default

#### Mode

Global configuration mode

#### Instructions

Use the command "vlan protocol-vlan group" to specify the protocol type to add a protocol VLAN group

#### Instance

Add protocol VLAN group

```
Switch(config)# vlan protocol-vlan group 1 frame-type ethernet_ii protocol-value
0x806
```

```
Switch(config)# vlan protocol-vlan group 2 frame-type llc_other protocol- value
0x800
```

Query protocol VLAN group

```
Switch# show vlan protocol-vlan
```

```
Group ID | Status | Type | value
```

```
-----+-----+-----+-----
```

```
---
```

```
a) |Enabled| Ethernet |0x0806
b) |Enabled| LLC other |0x0800
c) |Disabled| -- | --
d) |Disabled| -- | --
e) |Disabled| -- | --
f) |Disabled| -- | --
g) |Disabled| -- | --
h) |Disabled| -- | --
```

### vlan protocol-vlan group (Interface)

#### Format

```
vlan protocol-vlan group <1-8>vlan <1-4094>
```

```
no vlan protocol-vlan group <1-8>
```

#### Parameter

none	Not specified, which means all groups
<1-8>	Protocol VLAN group ID
vlan	Specify VLAN

#### Default

#### Mode

Interface configuration mode

#### Instructions

Use the command "vlan protocol-vlan group" to map the protocol group and VLAN on the interface.

#### Instance

Configure Protocol VLAN Group

```
Switch(config)# interface gi1
```

```
Switch(config-if)# vlan protocol-vlan group 1 vlan 2
```

### show vlan protocol-vlan

#### Format

```
show vlan mac-vlan [group <1-8>]
```

#### Parameter

group	Protocol VLAN group ID
-------	------------------------

#### Default

Privilege Mode

#### Instructions

Use the command "show vlan protocol-vlan" to query the protocol VLAN group configuration.

#### Instance

Query protocol VLAN group

```
Switch# show vlan protocol-vlan
```

```
Group ID | Status | Type | value
```

```
-----+-----+-----+-----
```

```
---
```

```
1 |Enabled| Ethernet |0x0806
```

```
2 |Enabled| LLC other |0x0800
```

```
3 |Disabled| -- | --
```

```
4 |Disabled| -- | --
```

---

```

5 |Disabled | -- | --
6 |Disabled | -- | --
7 |Disabled | -- | --
8 |Disabled | -- | --

```

### show vlan protocol-vlan interfaces

#### Format

```
show vlan protocol-vlan interfaces IF_PORTS
```

#### Parameter

interfaces	Specify Port
------------	--------------

#### Default

Privilege Mode

#### Instructions

Use the command "show vlan protocol-vlan interface" to query the interface configuration of the protocol VLAN.

#### Instance

Configure protocol VLAN interface configuration

```
Switch# show vlan protocol-vlan interfaces gi1
```

```
Port gi1 : Group 1
```

```
Status : Enabled
```

```
VLAN ID : 2
```

```
Group 2
```

```
Status : Enabled
```

```
VLAN ID :3
```

```
Group 3
```

```
Status : Disabled Group 4
```

```
Status : Disabled Group 5
```

```
Status : Disabled Group 6
```

```
Status : Disabled Group 7
```

```
Status : Disabled Group 8
```

```
Status : Disabled
```

## 27. QOS

### qos

#### Format

qos  
no qos

#### Parameter

#### Default

Default is not enabled

#### Mode

Global configuration mode

#### Instructions

Use the command "qos" to assign the quality of service to the packet queue according to the basic trust type, and the higher priority packets can be sent first.

#### Instance

Enable QOS  
Switch(config)# qos

Query QOS  
configurationSwit  
ch# show qos QoS  
Mode: basic Basic  
trust: cos

### qos cos

#### Format

qos cos <0-7>

#### Parameter

cos	Cos value of the interface
-----	----------------------------

#### Default

Default interface COS value is 0

#### Default

Interface configuration mode

#### Instructions

Sometimes, there is no qos information in the packet, such as CoS, DSCP, IP priority, etc. But we can still assign priority to the packet by configuring the interface Defaultcos value. If there is no qos information in the packet, the device will use this Defaultcos value and find the cos queue mapping to obtain the final target queue. Use the command "qos" to specify the priority of the port.

**Instance**

Configure the COS value of the interface

```
Switch(config)# interface GigabitEthernet 1
```

```
Switch(config-if)# qos cos 7
```

Query the QOS configuration of the interface

```
Switch# show qos interface GigabitEthernet 1
```

```
Port | CoS | Trust State | Remark Cos | Remark DSCP | Remark IP Prec
```

```
-----+-----+-----+-----+-----+-----
```

```
gi1 | 7 | enabled | disabled | disabled | disabled |
```

**qos map****Format**

```
qos map (cos-queue | dscp-queue | precedence-queue) SEQUENCE to <1- 8>
```

```
qos map (queue-cos | queue-precedence) SEQUENCE to <0-7>
```

```
qos map queue-dscp SEQUENCE to <0-63>
```

**Parameter**

cos-queue	Configure and query the mapping relationship between COS and queue
dscp-queue	Configure and query the mapping relationship between DSCP and queue
precedence-queue	Configure and query the mapping relationship between TOS and queue
queue-cos	Configure and query the mapping relationship between queues and COS
queue-precedence	Configure and query the mapping relationship between queues and TOS
queue-dscp	Configure and query the mapping relationship between queues and DSCP
SEQUENCE	Cos, dscp, priority or queue with one or more values
<1-8>	Queue ID
<0-7>	COS or TOS value
<0-63>	DSCP value

**Default****Default COS to queue mapping**

CoS	Queue ID
0	1
1	2
2	3
3	4
4	5
5	6
6	7
7	8

**Default DSCP to queue mapping**



DSCP	Queue ID
0-7	1
8-15	2
16-23	3
24-31	4
32-39	5
40-47	6
48-55	7
56-63	8

## Default TOS to queue mapping

IP Precedence	Queue ID
0	1
1	2
2	3
3	4
4	5
5	6
6	7
7	8

## Default queue to COS mapping

Queue ID	CoS
1	0
2	1
3	2
4	3
5	4
6	5
7	6
8	7

## Default queue to DSCP mapping

Queue ID	DSCP
1	0
2	8
3	16
4	24
5	32
6	40
7	48
8	56

## Default queue to TOS mapping

Queue ID	IP Precedence
1	0
2	1

3	2
4	3
5	4
6	5
7	6
8	7

**Mode**

Global configuration mode

**Instructions**

According to different trust types, data packets are assigned to different queues according to specific qos mapping. For example, if the trust type is trust cos, the device will obtain the cos value in the data packet and refer to the cos queue mapping to allocate the correct queue.

The queue to cos, dscp, or priority mapping is used by the remarking function. If the port marking function is enabled, the marking function will reference these 3 tables to mark the data packet.

**Instance**

Configure COS to queue mapping  
Switch(config)# qos map cos-queue 6 7 to 1

Query COS to queue mapping  
Switch# show qos map cos-queue  
CoS to Queue mappings  
COS 0 1 2 3 4 5 6 7  
-----  
Queue 2 1 3 4 5 6 1 1

Configure queue to COS mapping  
Switch(config)# qos map queue-cos 4 5 to 7

Query queue to COS mapping  
Switch# show qos map queue-cos  
Queue to CoS mappings  
Queue 1 2 3 4 5 6 7 8  
-----  
CoS 1 0 2 7 7 5 6 7

**qos queue****Format**

qos queue strict-priority-num <0-8>  
qos queue weight SEQUENCE

**Parameter**

strict-priority-num	Specify strict priority scheduling policy
weight	Specify WRR weight strategy and specify weight distribution

#### Default

When the value of strict-priority-num is 8, it means that strict priority scheduling is adopted.  
WRR weight scheduling Default weight

Queue ID	Queue Weight
1	1
2	2
3	3
4	4
5	5
6	9
7	13
8	15

#### Mode

Global configuration mode

#### Instructions

The device supports a total of 8 QoS queues. It can set the queue as a strict priority queue or a weighted queue to prevent starvation. The higher the id value, the higher the priority of the queue.

First, you need to decide how many strict priority queues you need. The strict priority queue will always occupy the higher priority queue. For example, if the strict priority number is set to 2, then queues 7 and 8 will be strict priority queues, and the other queues will be weighted queues.

After setting the number of strict priority queues, you need to use the "qos queue" command to set the weight of the weighted queue. The bandwidth will be shared by the weights you configure between these weighted queues.

#### Instance

Configure QOS scheduling strategy

```
Switch(config)# qos queue strict-priority-num 3
```

```
Switch(config)# qos queue weight 5 10 15 20 25
```

Query QOS queue scheduling

```
Switch# show qos queueing
```

```
qid-weights Ef - Priority
```

```
1 - 5 dis- N/A 2
```

```
- 10 dis- N/A 3 -
```

```
15 dis- N/A 4 - 20
```

```
dis- N/A 5 - 25 dis-N/A
```

```
6 - N/A ena-6
```

```
7 - N/A ena-7
```

```
8 - N/A ena-8
```

## qos remark

### Format

```
qos remark (cos | dscp | precedence)
no qos remark (cos | dscp | precedence)
```

### Parameter

cos	Enable or disable COS re-marking
dscp	Enable or disable DSCP remarking
precedence	Enable or disable TOS re-marking

### Default

DefaultCOS/DSCP/TOS is re-marked as disabled.

### Default

Interface configuration mode

### Instructions

The QoS marking function allows you to change the priority information in the packet according to the egress queue. For example, if you want all packets from queue 1 of interface gi1 to mark the cos value as 5 in the next layer of the device, you can enable the cos marking function on gi1 and configure the cos mapping of queue 1 to cos 5.

Use the command "qos remark" to enable the marking function on a specific type.

### Instance

```
Configure priority re-marking
Switch(config)# interface GigabitEthernet 1
Switch(config-if)# qos remark cos
Switch(config-if)# qos remark dscp
Switch(config-if)# qos remark precedence
```

Query interface QOS configuration

```
Switch# show qos interface GigabitEthernet 1
Port |CoS    | Trust State | Remark Cos | Remark DSCP | Remark IPPrec
-----+-----+-----+-----+-----+-----
gi1|0      |  enabled | enabled | enabled | enabled |
```

## qos trust

### Format

```
qos trust (cos | cos-dscp | dscp | precedence)
```

### Parameter

cos	Specify the device trust COS priority
cos-dscp	Specify the device to trust the DSCP of IP packets or the COS priority of non-IP packets

dscp	Specifies that the device trusts the DSCP of IP packets
precedence	Specifies that the device trusts the TOS of IP packets

**Default**

Default trusts COS.

**Mode**

Global configuration mode

**Instructions**

Under the QoS basic Default, there are 4 trust types for the device to determine the appropriate queue for the packet. This command can switch between these trust types.

**COS:**

IEEE 802.1p defines a 3-bit priority value in the vlan tag. Trust this value in the data packet and allocate queues according to the cos queue mapping.

**DSCP:**

IETF RFC2474 defines a 6-bit priority value (the highest 6 bits in the ToS field) in the IP packet. Trust this value in the data packet and allocate queues according to the dscp queue mapping.

**IP priority:**

The highest 3-bit priority value in the ToS field of an IP packet. Trust this value in the data packet and assign queues based on priority queue mapping.

**CoS-DSCP:**

Trust DSCP for IP packets and allocate queues based on DSCP queue mapping. Trust the CoS of non-IP packets, and according to the CoS team Column mapping allocation queue.

**Instance**

Configure device trust type

```
Switch(config)# qos trust precedence
```

Query QOS

configuration

```
Switch# show qos
```

QoS Mode: basic

Basic trust: ip-precedence

**qos trust (Interface)****Format**

```
qos trust
```

```
no qos trust
```

**Parameter****Default**

Default interface trust is enabled.

**Default**

Interface configuration mode

**Instructions**

After the QoS function is enabled under the basic Default, the device also supports the enable/disable QoS function for each interface. If the trust status on the interface is enabled, all ingress packets of this interface will be remapped according to the trust type and qos mapping. Otherwise, all ingress packets will be allocated to queue 1. Use the command "qos trust" to enable the interface trust switch.

**Instance**

```
Configure interface trust
Switch(config)# interface GigabitEthernet 1
Switch(config-if)# no qos trust
```

```
Query interface QOS configuration
Switch# show qos interface GigabitEthernet 1
Port |CoS    | Trust State | Remark Cos | Remark DSCP | Remark IPPrec
-----+-----+-----+-----+-----+-----
gi1|0    | disabled | disabled | disabled | disabled|
```

**show qos****Format**

```
show qos
```

**Parameter****Default****Mode**

```
Privilege Mode
```

**Instructions**

Use the command "show qos" to query the QOS configuration including status and trust type.

**Instance**

```
Query QOS
configuration
Switch# show qos
QoS Mode: basic
Basic trust: cos
```

**show qos interface****Format**

```
show qos interface IF_PORTS
```

**Parameter**

interface	Specify interface to query QOS configuration
-----------	--

**Default****Mode**

Privilege Mode

**Instructions**

Use the command "show qos interface" to query the QOS configuration under the interface, including DefaultCOS, priority marking, status and remarking type.

**Instance**

Query the QOS configuration of the interface

```
Switch# show qos interface GigabitEthernet 1
```

```
Port |CoS    | Trust State | Remark Cos | Remark DSCP | Remark IPPrec
```

```
-----+-----+-----+-----+-----+-----
gi1|7    |   enabled |disabled |   disabled |disabled|
```

**show qos map****Format**

```
show qos map [(cos-queue | dscp-queue | precedence-queue | queue-cos
| queue-dscp | queue-precedence)]
```

cos-queue	Query the mapping relationship between COS and queue
dscp-queue	Query the mapping relationship between DSCP and queue
precedence-queue	Query the mapping relationship between TOS and queue
queue-cos	Query the mapping relationship between queue and COS
queue-precedence	Query the mapping relationship between the queue and TOS
queue-dscp	Query the mapping relationship between queue and DSCP

**Default****Mode**

Privilege Mode

**Instructions**

Use the command "show qos map" to query various types of mapping relationships in QOS.

**Instance**

Query queue to COS mapping

```
Switch# show qos map queue-cos
```

Queue to CoS mappings

```
Queue 1    2    3    4    5    6    7    8
```

```
-----
CoS      1    0    2    7    7    5    6    7
```

## show qos queueing

### Format

show qos queueing

### Default

### Mode

Privilege Mode

### Instructions

Use the command "show qos queueing" to query QOS queue information

### Instance

Query QOS queue scheduling

Switch# show qos queueing

qid-weights Ef - Priority

1 - 5 dis- N/A 2

- 10 dis- N/A 3 -

15 dis- N/A 4 - 20

dis- N/A 5 - 25 dis-N/A

6 - N/A ena-6

7 - N/A ena-7

8 - N/A ena-8



## 28. Rate Limit

### rate-limit egress

#### Format

```
rate-limit egress <16-1000000>  
no rate-limit egress
```

#### Parameter

egress	Specify the rate limit in the sending direction of the interface
--------	--

#### Default

Default is to disable

#### Mode

Interface configuration mode

#### Instructions

Use the command "rate-limit egress" to configure the rate limit in the next sending direction.

#### Instance

```
Configure interface rate limit  
Switch(config)# interfaces gi1  
Switch(config-if)# rate-limit egress 2048
```

```
Query interface speed limit  
Switch# show running-config interfaces gi1  
interface gi1  
rate-limit egress 2048
```

### rate-limit ingress

#### Format

```
rate-limit ingress <16-1000000>  
no rate-limit ingress
```

#### Parameter

ingress	Specify the rate limit in the receiving direction of the interface
---------	--

#### Default

Default is to disable

#### Mode

Interface configuration mode

#### Instructions

Use the command "rate-limit egress" to configure the rate limit in the receiving direction.

**Instance**

```
Configure interface rate limit
Switch(config)# interfaces gi1
Switch(config-if)# rate-limit ingress 128
```

```
Query interface speed limit
Switch# show running-config interfaces gi1
interface gi1
rate-limit ingress 128
```

**rate limit egress queue****Format**

```
rate-limit egress queue <1-8><16-1000000>
no rate-limit egress queue <1-8>
```

**Parameter**

<1-8>	Specifies the queue of the interface
<16-1000000>	Specify the rate limit value of the interface

**Default**

Default disable

**Mode**

Interface configuration mode

**Instructions**

Use the command "rate-limit egress queue" to configure the rate limit of the queue in the sending direction of the interface.

**Instance**

```
Configure egress queue rate limit
Switch(config)# interfaces gi1
Switch(config-if)# rate-limit egress queue 3 2048
Switch# show running-config interfaces gi1 interface gi1
rate-limit egress queue 3 2048
```

## 29. SNMP

### snmp

#### Format

snmp

#### Parameter

#### Default

Default disable

#### Mode

Global configuration mode

#### Instructions

Use the command "snmp" to open the SNMP service of the device.

#### Instance

Enable SNMP service  
Switch(config)# snmp

### snmp view

#### Format

snmp view view-name subtree oid-tree oid-mask (all|oid-mask) viewtype  
(included|excluded)  
no snmp view view-name subtree (all|oid-tree)

#### Parameter

view-name	SNMP view name, up to 30 characters
oid-tree	Specify the ASN.1 subtree object identifier to be included or excluded from the SNMP view(OID)
oid-mask	Specify the OID family mask. It is used to define the view subtree family. For example, OID mask FA.80 is 11111010.10000000. The length of the OID mask must be less than the subtreeThe length of the OID.
iewtype	Include or exclude selected MIBs in the view

#### Default

#### Mode

Global configuration mode

#### Instructions

Use the command "snmp view" to configure the SNMP view.

#### Instance

Configure SNMP view

```
Switch(config)# snmp view private subtree 1.3.3.1 oid-mask all viewtype included
```

### snmp group

#### Format

```
snmp group group-name (1|2c|3) (noauth|auth|priv) read-view read-view
write-view write-view [notify-view notify-view]
no snmp group group-name security-mode version (1|2c|3)
```

#### Parameter

group-name	SNMP group name, maximum support 30 characters
1 2c 3	SNMP version
noauth	Do not perform packet authentication
auth	Perform packet authentication. It only applies to SNMPv3 security Default
priv	Perform packet authentication. It only applies to SNMPv3 security Default
read-view	Configure the view that allows read permissions
write-view	Configure the view that allows write permissions
notify-view	Set the view name to send only TRAP, the content of TRAP is included in the selected SNMP view to be notified

#### Default

#### Mode

Global configuration mode

#### Instructions

To define an SNMP group, use the command "snmp group" to configure it under the global Default.

SNMP group configuration is used to map SNMP V3 users to SNMP groups. These users will be mapped to the group's view. The security level of SNMP v1 or v2 is always noauth.

#### Instance

Configure SNMP group

```
Switch(config)# snmp group v3 version 3 auth read-view all write-view all notify-
view all
```

### snmp community

#### Format

```
snmp community community-name [view view-name] (ro|rw)
snmp community community-name group group-name
no snmp community community-name
```

#### Parameter

community-name	Configure SNMP community name, up to 20 characters
view	Specify the related view name
ro	Read-only access
rw	Read and write permissions
group	Configure the relationship between SNMP groups

**Default**

The system default read-only community name is public

**Mode**

Global configuration mode

**Instructions**

Use the command "snmp community" to configure the read/write community name of SNMP V1/V2C.

**Instance**

Configure community name  
Switch(config)# snmp community private ro

**snmp user****Format**

```
snmp user username group-name [auth (md5|sha) AUTHPASSWD]
snmp user username group-name auth (md5|sha) AUTHPASSWD priv
PRIVPASSWD
no snmp user username
```

**Parameter**

username	Configure the name of the V3 user
group-name	Configure the name of the SNMP group to which V3 belongs
md5	Specify HMAC-MD5-96 authentication protocol as user authentication
sha	Specify HMAC-SHA-96 authentication protocol as user authentication
AUTHPASSWD	Password used for authentication, ranging from 8 to 32 characters
priv	The dedicated password for the private key, the length range is 8 to 64 characters

**Default****Mode**

Global configuration mode

**Instructions**

Use the command "snmp user" to configure SNMP V3 users.

**Instance**

Configure SNMP users

Switch(config)# snmp Use the command r v3 v3 auth md5 12345678

### snmp engineid

#### Format

snmp engineid (default | ENGINEID)

#### Parameter

Default	Default engine ID generated based on the MAC address of the switch
ENGINEID	Specify the SNMP engine ID. Engine ID is 10 to 64 hexadecimal characters, hexadecimal The system number must be divided by 2

#### Default

The DefaultSNMP engine ID on the switch is based on the switch MAC address

#### Mode

Global configuration mode

#### Instructions

Use the command "snmp engineid" to define the engine ID of the switch

#### Instance

Configuration engine

Switch(config)# snmp engineid 00036D001122

### snmp engineid remote

#### Format

snmp engineid remote (ip-addr | ipv6-addr) ENGINEID

no snmp engineid remote (ip-addr | ipv6-addr)

#### Parameter

ip-addr	IPv4 address of the remote host
ipv6-addr	IPv6 address of the remote host
ENGINEID	Specify the SNMP engine ID. Engine ID is 10 to 64 hexadecimal characters, hexadecimalThe system number must be divided by 2

#### Default

#### Mode

Global configuration mode

#### Instructions

Use the command "snmp engineid remote" to define the engine ID of the remote host.

#### Instance

Configure remote engine

```
Switch(config)# snmp engineid remote 192.168.1.11 00036D10000A
```

### snmp trap

#### Format

```
snmp trap (auth|cold-start|linkUpDown|warm-start)
no snmp trap (auth|cold-start|linkUpDown|warm-start)
```

#### Parameter

auth	Failed TRAP
cold-start	TRAP for system cold start
linkUpDown	TRAP for link UP/DOWN status changes
warm-start	TRAP for system hot start

#### Default

Default all TRAP functions are enabled

#### Mode

Global configuration mode

#### Instructions

When you need to report system messages to the TRAP host, use the command "snmp trap" to enable the TRAP reporting function.

#### Instance

```
Enable TRAP
Switch(config)# snmp trap linkUpDown
```

### snmp host

#### Format

```
snmp host (ip-addr|ipv6-addr|hostmane) [traps|informs] [version (1|2c)]
community-name [udp-port udp-port] [timeout timeout] [retries retries]
snmp host (ip-addr|ipv6-addr|hostmane) [traps|informs] version
3[(auth|noauth|priv)] community-name [udp-port udp-port] [timeout
timeout] [retries retries]
no snmp host (ip-addr|ipv6-addr|hostmane) [traps|informs] [version
(1|2c|3)]
```

#### Parameter

ip-addr	The IPv4 address of the TRAP receiving host
ipv6-addr	The IPv6 address of the TRAP receiving host
hostname	The host name of the TRAP receiving host
traps	Report TRAP to the host, this is the Default configuration
informs	Report messages to the host
version (1 2c 3)	Report the SNMP version number of TRAP

noauth	Specifies not to perform packet authentication. It only applies to SNMPv3 security Default
auth	Specifies not to perform packet authentication without encryption. It only applies toSNMPv3 Security Default
priv	Specifies not to use encryption to perform packet authentication. It only applies toSNMPv3 Security Default
community-name	Community name carried in TRAP message
udp-port udp-port	Specify UDP port number
timeout timeout	Specify the timeout period of SNMP messages
retries retries	Specify SNMP notification retry timer

#### Default

#### Mode

Global configuration mode

#### Instructions

When the host is required to receive system TRAP notification, use the command "snmp host" to configure the host.

#### Instance

Configure TRAP host  
Switch(config)# snmp host 192.168.1.11 private

#### show snmp view

#### Format

show snmp view

#### Default

#### Mode

Privilege Mode

#### Instructions

Use the command "show snmp view" to query the system configuration SNMP view.

#### Instance

Query system SNMP view  
Switch# show snmp view

View Name	SubtreeOID
-----------	------------

OID Mask	View Type
----------	-----------

-----	-----	
all	.1	all
included		
Total Entries: 1		



**show snmp group****Format**

show snmp group

**Default****Mode**

Privilege Mode

**Instructions**

Use the command "show snmp group" to query the SNMP group configured by the system

**Instance**

Query configuration SNMP group

Switch# show snmp group

Group Name	Model	Level	ReadView
WriteView	NotifyView		
-----			
ikuaigroup	v3	priv	all
all	all		

Total Entries: 1

**show snmp community****Format**

show snmp community

**Default****Mode**

Privilege Mode

**Instructions**

Use the command "show snmp community" to query the read/write community name configuration of the system SNMP V1/V2C version.

**Instance**

Query group name

Switch# show snmp community

CommunityName	Group Name	View Access
public		all
ro		

Total Entries: 1

## show snmp user

### Format

show snmp user

### Default

### Mode

Privilege Mode

### Instructions

Use the command "show snmp user" to query SNMP V3 users.

### Instance

Query SNMP users

Switch# show snmp user

Username: test

Password: \*\*\*\*\*

PrivilegeMode: rw

AccessGroupName: test

Authentication Protocol: md5

EncryptionProtocol: des

AccessSecLevel: priv

Total Entries: 1

## show snmp engineid

### Format

show snmp engineid

### Default

### Mode

Privilege Mode

### Instructions

Use the command "show snmp engineid" to query the engine configuration of the switch, including the local and remote engines.

### Instance

Query engine configuration

Switch# show snmp engineid

Local SNMPV3 Engine id: 80006a92031c2aa3c40292

IPAddress

Remote SNMPengineID

-----  
Total Entries: 0

## show snmp trap

### Format

```
show snmp trap
```

### Default

### Mode

Privilege Mode

### Instructions

Use the command "show snmp trap" to query the system's TRAP configuration.

### Instance

Query TRAP configuration

```
Switch# show snmp trap
```

```
SNMP authfailedtrap : Enable
```

```
SNMPlinkUpDowntrap : Enable
```

```
SNMPcold-starttrap : Enable
```

```
SNMPwarm-starttrap :Enable
```

## show snmp host

### Format

```
show snmp host
```

### Parameter

### Default

### Mode

Privilege Mode

### Instructions

Use the command "show snmp host" to query the system's TRAP host configuration items.

### Instance

Query TRAP host

```
Switch# show snmp host
```

Server	Community/UserName	NotificationVersion	Notification
Type	UDP Port	Retries	Timeout
192.168.2.20	test	v3	
	trap 162	--	--

-----

```
192.168.2.20      test      v3
```

```
trap 162      --      --
```

```
Total Entries: 1
```

## 30. RMON

### rmon event

#### Format

```
rmon event <1-65535> [log] [trap COMMUNITY] [description
DESCRIPTION] [owner NAME]
no rmon event <1-65535>
```

#### Parameter

<1-65535>	Configure RMON event index
log	(Optional) Specify to display in the system log
trap	(Optional) Specify to be displayed in the SNMP TRAP message
description	(Optional) Description of the event
owner	(Optional) Owner of the event

#### Default

#### Mode

Global configuration mode

#### Instructions

Use the command "rmon event" to add or modify an RMON event.

#### Instance

```
Configure RMON events
switch(config)# rmon event 1 log trap public description test owner admin
Query RMON events
switch# show rmon event 1
Rmon Event Index 1
Rmon Event Type : Log and Trap Rmon Event Community : public Rmon Event
Description : test
Rmon Event Last Sent :
RmonEventOwner      :admin
```

### rmon alarm

#### Format

```
rmon alarm <1-65535>interface IF_PORT (drop-
events|octets|pkts|broadcast-pkts| multicast-pkts|crc-align-
errors|undersize-pkts|oversize-
pkts|fragments|jabbers|collisions|pkts64octets|pkts65to127octets|pkts128
t o255octets|pkts256to511octets|pkts512to1023octets|pkts1024to1518octe
ts) <1-2147483647> (absolute|delta) rising <0-2147483647><0-65535>
falling <0-2147483647><0-65535>startup (rising|rising-falling|falling)
[owner NAME]
no rmon alarm <1-65535>
```

## Parameter

<1-65535>	Configure a RMON alarm index
interface	Specify a RMON sample interface
(variable)	Specify a MIB object to be collected
<0-2147483647>	Specify the time (seconds) for the alarm to monitor MIB variables
(absolute delta)	absolute: absolute comparison sample counter; delta: incremental comparison sample counter
rising <0-2147483647>	The specified event rises and triggers the alarm threshold
rising <0-65535>	Index of the RMON event that triggered the rising threshold alarm
falling <0-2147483647>	The specified event falls and triggers the alarm threshold
falling <0-65535>	Index of the RMON event that triggered the falling threshold alarm
startup	Specifies to send an alarm when rising or falling or both take effect
owner	Specify the owner of the alarm

## Default

## Mode

Global configuration mode

## Instructions

Use the command "rmon alarm" to configure or modify RMON alarm items.

## Instance

Configure RMON events and alarms

```
switch(config)# rmon event 1 log
```

```
switch(config)# rmon event 2 log
```

```
Switch(config)# rmon alarm 1 interface gi1 pkts 300 delta rising 10000 1 falling 100 1 startup rising-falling owner admin
```

## Query RMON alarms

```
Switch# show rmon alarm 1
```

```
Rmon Alarm Index1
```

```
Rmon AlarmSampleInterval    300
```

```
Rmon Alarm Sample Interface : gi1
```

```
Rmon Alarm Sample Variable : Pkts
```

```
Rmon Alarm Sample Type : delta
```

```
Rmon Alarm Type : Rising or Falling
```

```
Rmon Alarm Rising Threshold : 10000
```

```
Rmon AlarmRising Event    1
```

```
Rmon AlarmFalling Threshold  100
```

```
Rmon AlarmFalling Event    1
```

```
RmonAlarmOwner      :admin
```

## rmon history

### Format

```
rmon history <1-65535>interface IF_PORT [buckets <1-65535>] [interval
<1-3600>] [owner NAME]
no rmon history <1-65535>
```

### Parameter

<1-65535>	Configure RMON historical index
interface	Specify a RMON sample interface
buckets	Specify the maximum depth of RMON history
interval	Specify the interval between each sample collection
owner	Specify the owner of RMON history

### Default

### Mode

Global configuration mode

### Instructions

Use the command "rmon history" to add or modify the history configuration of RMON.

### Instance

```
Configure RMON history
switch(config)# rmon history 1 interface gi1 interval 60 owner admin
Query RMON history
switch(config)# show rmon history 1
RmonHistoryIndex    1
Rmon Collection Interface: gi1
RmonHistoryBucket   50
Rmon history Interval 60
RmonHistoryOwner    :admin
```

## clear rmon interfaces statistics

### Format

```
clear rmon interfaces IF_PORTS statistics
```

### Parameter

interfaces	Clear RMON statistics of the specified interface
------------	--

### Default

### Mode

Privilege Mode

### Instructions

Use the command "clear rmon interfaces statistics" to clear the RMON counts under the interface.

#### Instance

Clear RMON interface statistics

```
switch# clear rmon interfaces gi1 statistics
```

Query RMON interface statistics

```
switch# show rmon interfaces gi1 statistics
```

```
==== Port gi1 =====
```

```
etherStatsDropEvents 0
etherStatsOctets 0
etherStatsPkts 0
etherStatsBroadcastPkts 0
etherStatsMulticastPkts 0
etherStatsCRCAlignErrors 0
etherStatsUnderSizePkts 0
etherStatsOverSizePkts 0
etherStatsFragments 0
etherStatsJabbers 0
etherStatsCollisions 0
etherStatsPkts64Octets 0
etherStatsPkts65to127Octets 0
etherStatsPkts128to255Octets 0
etherStatsPkts256to511Octets 0
etherStatsPkts512to1023Octets 0
etherStatsPkts1024to1518Octets0
```

#### show rmon interfaces statistics

#### Format

```
show rmon interfaces IF_PORTS statistics
```

#### Parameter

interfaces	Query RMON statistics of a specified interface
------------	--

#### Default

#### Mode

Privilege Mode

#### Instructions

Use the command "show rmon interface statistics" to query the RMON count statistics on the interface.

#### Instance

Query RMON interface statistics

```

switch# show rmon interfaces gi1 statistics
===== Port gi1 =====

etherStatsDropEvents 0
etherStatsOctets 0
etherStatsPkts 0
etherStatsBroadcastPkts 0
etherStatsMulticastPkts 0
etherStatsCRCAlignErrors 0
etherStatsUnderSizePkts 0
etherStatsOverSizePkts 0
etherStatsFragments 0
etherStatsJabbers 0
etherStatsCollisions 0
etherStatsPkts64Octets 0
etherStatsPkts65to127Octets 0
etherStatsPkts128to255Octets 0
etherStatsPkts256to511Octets 0
etherStatsPkts512to1023Octets 0
etherStatsPkts1024to1518Octets0

```

### show rmon event

#### Format

```
show rmon event (<1-65535> | all)
```

#### Parameter

<1-65535>	Query the event index of the specified RMON
all	Query all RMON events

#### Default

#### Mode

Global configuration mode

#### Instructions

Use the command "show rmon event" to query the RMON events of the system.

#### Instance

Query RMON events

```
switch# show rmon event 1
```

Rmon Event Index 1

Rmon Event Type : Log and Trap Rmon Event Community : public Rmon Event

Description : test

Rmon Event Last Sent :

RmonEventOwner :admin



**show rmon event log****Format**

```
show rmon event <1-65535>log
```

**Parameter**

<1-65535>	Query the log of the specified RMON event
-----------	---

**Default****Mode**

Privilege Mode

**Instructions**

Use the command "show rmon event log" to query the log triggered by the RMON alarm.

**Instance**

Query RMON event log

```
switch(config)# show rmon event 1 log
```

```
=====
```

```
Index      1
```

```
Alarm Index 1
```

```
Action   : StartupFalling
```

```
Time     : (32918334) 3 days,19:26:23.34
```

```
Description : gi1.Pkts=0 <= 100
```

**show rmon alarm****Format**

```
show rmon alarm (<1-65535> | all)
```

**Parameter**

<1-65535>	Query the alarm index of the specified RMON
all	Query all RMON alarms

**Default****Mode**

Privilege Mode

**Instructions**

Use the command "show rmon alarm" to query the alarm items of the system RMON.

**Instance**

Query RMON alarms

```
Switch# show rmon alarm 1
```

```
Rmon Alarm Index1
```

```

Rmon AlarmSampleInterval 300
Rmon Alarm Sample Interface : gi1
Rmon Alarm Sample Variable : Pkts
Rmon Alarm Sample Type : delta
Rmon Alarm Type : Rising or Falling
Rmon Alarm Rising Threshold : 10000
Rmon AlarmRising Event 1
Rmon AlarmFalling Threshold 100
Rmon AlarmFalling Event 1
RmonAlarmOwner :admin

```

### show rmon history

#### Format

```
show rmon history (<1-65535> | all)
```

#### Parameter

<1-65535>	Query the historical index of the specified RMON
all	Query all RMON history

#### Default

#### Mode

Privilege Mode

#### Instructions

Use the command "show rmon history" to query the historical information of the system RMON.

#### Instance

```

Query the history of RMON
switch(config)# show rmon history 1
RmonHistoryIndex 1
Rmon Collection Interface: gi1
RmonHistoryBucket 50
Rmon history Interval 60
RmonHistoryOwner :admin

```

### show rmon history statistic

#### Format

```
show rmon history <1-65535>statistics
```

#### Parameter

<1-65535>	Query the index of the historical statistics of the specified RMON
-----------	--

#### Default

**Mode**

Privilege Mode

**Instructions**

Use the command "show rmon history statistic" to query the historical statistics of the system RMON.

**Instance**

Query RMON historical statistics

switch(config)# show rmon history 1 statistic

=====

Sample Index 2

Interval Start : (32940466) 3 days, 19:30:04.66

DropEvents 0

Octets :117226

Pkts 763

BroadcastPkts9

MulticastPkts 0

CRCAlignErrors 0

UnderSizePkts 0

OverSizePkts 0

Fragments 0

Jabbers 0

Collisions 0

Utilization 1

=====

Sample Index 1

Interval Start : (32939462) 3 days, 19:29:54.62

DropEvents 0

Octets 220

Pkts 3

BroadcastPkts1

MulticastPkts 0

CRCAlignErrors 0

UnderSizePkts 0

OverSizePkts 0

Fragments 0

Jabbers 0

Collisions 0

Utilization 1

## 31. SpanningTree

### instance (MST)

#### Format

```
instance instance-id vlan vlan-list
no instance instance-id vlan vlan-list
```

#### Parameter

instance-id	InstanceID of MSTP, range 0~15
vlan	VLAN of MSTPInstance

#### Default

All VLANs are mapped to public and internal spanning tree (CIST), Instance is 0

#### Mode

MS configuration Mode

#### Instructions

To map a VLAN to a multiple spanning tree (MSTP) instance, use the command Instance in the MST configuration Default. All VLANs that are not explicitly configured as MSTPInstance are mapped to CISTInstance (Instance0). For two or more switches in the same MSTP area, their VLAN mapping, name and revision number configuration must be the same.

#### Instance

```
Configure Multiple Spanning Tree
Switch(config)# spanning-tree mst configuration
Switch(config-mst)# instance 1 vlan 10-20
Switch(config-mst)# instance 2 vlan 100
```

### name (MST)

#### Format

```
name name-str
no name
```

#### Parameter

name	The name of MSTP, the maximum support is 32 characters
------	--

#### Default

The name of MSTP Default is the system bridge MAC

#### Mode

MST Configuration Mode

#### Instructions

Use the command "name" to define the MSTP name.

**Instance**

Configure multiple spanning tree name  
Switch(config)# spanning-tree mst configuration  
Switch(config-mst)# name Valkyrie

**revision (MST)****Format**

revision rev  
no revision

**Parameter**

revision	MSTP version number, the range is from 0 to 65535
----------	---

**Default**

Default version is 0

**Mode**

MST Configuration Mode

**Instructions**

Use the command "revision" to define the version number of MSTP.

**Instance**

Configure the version number of the multiple spanning tree  
Switch(config)# spanning-tree mst configuration  
Switch(config-mst)# revision 1

**spanning-tree mst configuration****Format**

spanning-tree mst configuration

**Parameter****Default****Mode**

Global configuration mode

**Instructions**

Use the command "spanning-tree mst configuration" to enter the MST configuration  
Default to modify the MSTP configuration.

**Instance**

Enter MST configuration Default

Switch(config)# spanning-tree mst configuration

Switch(config-mst)# instance 1 vlan 10-20

### spanning-tree mst cost

#### Format

spanning-tree mst instance-id cost cost

no spanning-tree mst instance-id cost cost

#### Parameter

instance-id	Instance ID of MSTP
cost	The path cost of the interface on a specific MSTP Instance. For the long path cost method, the effective range is 0 to 200000000; for the short path cost method, the effective range is 0 to 65535. A value of 0 means automatic, and the port path cost is determined by the port speed and path cost method

#### Default

Default port path cost is 0, determined by port speed and path cost method (long or short)

Interface	Long	Short
Gigabit Ethernet (1000Mbps)	20000	4
Fast Ethernet (100Mbps)	200000	19
Ethernet (10Mbps)	2000000	100

#### Mode

Interface configuration mode

#### Instructions

Use the command "spanning-tree mst cost" to configure the cost of the interface. If a loop occurs, MSTP will consider the path cost when selecting the interface to enter the forwarding state.

#### Instance

MST Instance cost value of the enabled interface

Switch(config)# interface gi1

Switch(config-if)# spanning-tree mst 1 cost 30000

### spanning-tree mst port-priority

#### Format

spanning-tree mst instance-id port-priority priority

no spanning-tree mst instance-id port-priority

#### Parameter

instance-id	Instance ID of MSTP
port-priority	Specify the port priority of the instance

#### Default

The port priority of Default Instance is 128.

#### Mode

Interface configuration mode

#### Instructions

Use the command "spanning-tree mst port-priority" to configure the interface priority on a specific instance. The priority value must be a multiple of 16. When configuring the port priority on CIST (Instance0), it is equivalent to using the command "spanning-tree port-priority" in Interface configuration mode

#### Instance

Configure MSTP Instance interface priority

```
Switch(config)# interface gi1
```

```
Switch(config-if)# spanning-tree mst 1 port-priority 144
```

```
Switch(config-if)# spanning-tree mst 0 port-priority 96
```

### spanning-tree mst priority

#### Format

```
spanning-tree mst instance instance-id priority priority
```

```
no spanning-tree mst instance instance-id priority
```

#### Parameter

instance-id	Instance ID of MSTP
priority	Specify the priority of the instance, the range is 0-61440. It guarantees the possibility of selecting the switch as the root bridge, and a lower value has a higher priority for selecting the switch as the root bridge.

#### Default

Default Instance priority is 32768.

#### Mode

Global configuration mode

#### Instructions

Use the command "spanning-tree mst priority" to configure the bridge priority on a specific instance. The bridge priority value must be a multiple of 4096. The switch with the lowest priority is the root of the STP topology. For the bridge priority configuration on CIST (Instance0), it is equivalent to using the command "spanning-tree priority" under the global Default

#### Instance

Configure MSTP Instance priority

```
Switch(config)# spanning-tree mst 1 priority 4096
```

```
Switch(config)# spanning-tree mst 0 priority 4096
```

### spanning-tree

**Format**

spanning-tree  
 nospanning-tree

**Parameter****Default**

Disable Default

**Mode**

Global configuration mode

**Instructions**

Use the command "spanning-tree" to enable the STP spanning tree ring function of the system.

**Instance**

Enable STP spanning tree  
 Switch(config)# spanning-tree

**spanning-tree mode****Format**

spanning-tree mode (mstp|rstp|stp)  
 no spanning-tree force-version

**Parameter**

mstp	Enable multiple spanning tree protocol
rstp	Enable Rapid Spanning Tree Protocol
stp	Enable Spanning Tree Protocol

**Default**

Default is rstp

**Mode**

Global configuration mode

**Instructions**

Use the command "spanning-tree mode" to configure the Default of STP spanning tree. When the switch is configured as MSTPDefault, STP and RSTP can be used to be backward compatible with switches that work under STP and RSTPDefault respectively. For RSTP configuration, the switch can also use STP for the switch working in STP operation.

**Instance**

Configure MSTP Spanning Tree  
 Switch(config)# spanning-tree mode mstp



### spanning-tree bpdud

#### Format

spanning-tree bpdud (filtering|flooding)  
no spanning-tree bpdud

#### Parameter

filtering	Filter BPDU packets when STP is disabled
flooding	STP is disabled and BPDU packets are flooded

#### Default

Default is flooding

#### Mode

Global configuration mode

#### Instructions

Use the command "spanning-tree bpdud" to configure the operation of bridge protocol data unit (BPDU) processing when STP is disabled.

#### Instance

Configure BPDU packet processing  
Switch(config)# spanning-tree bpdud filtering

### spanning-tree bpdud-filter

#### Format

spanning-tree bpdud-filter no  
spanning-tree bpdud-filter

#### Parameter

#### Default

Default disable

#### Mode

Interface configuration mode

#### Instructions

Use the command "spanning-tree bpdud-filter" to enable the BPDU filtering function on the interface.

#### Instance

Enable interface BPDU filtering  
Switch(config)# interface gi1  
Switch(config-if)# spanning-tree bpdud-filter

### spanning-tree bpdud-guard

**Format**

```
spanning-tree bpduguard
no spanning-tree bpduguard
```

**Parameter****Default**

Default disable

**Mode**

Interface configuration mode

**Instructions**

Use the command "spanning-tree bpduguard" to enable the BPDUGuard function of the interface.

**Instance**

```
Enable interface BPDUGuard
Switch(config)# interface gi1
Switch(config-if)# spanning-tree bpduguard
```

**spanning-tree cost****Format**

```
spanning-tree cost cost
no spanning-tree cost
```

**Parameter**

cost	STP spanning tree cost value. For the long path cost method, the effective range is 0 to 200000000; for the short path cost method, the effective range is 0 to 65535. A value of 0 means automatic, and the port path cost is determined by the port speed and path cost method.
------	---

**Default**

Default port path cost is 0, determined by port speed and path cost method (long or short)

Interface	Long	Short
Gigabit Ethernet (1000Mbps)	20000	4
Fast Ethernet (100Mbps)	200000	19
Ethernet (10Mbps)	2000000	100

**Mode**

Interface configuration mode

**Instructions**

Use the command "spanning-tree cost" to configure the cost of the interface.

**Instance**

```

Enable interface cost value
Switch(config)# interface gi1
Switch(config-if)# spanning-tree cost 30000

```

### spanning-tree forward-delay

#### Format

```

spanning-tree forward-delay seconds
no spanning-tree forward-delay

```

#### Parameter

forward-time	STP forwarding delay, the range is 4-30 seconds
--------------	---

#### Default

Default forwarding delay is 15 seconds.

#### Mode

Global configuration mode

#### Instructions

To configure the STP bridge forwarding delay time, that is, the amount of time the port stays in the listening and learning state before entering the forwarding state, use the command "spanning-tree forward-delay" to specify the forwarding delay time.

When configuring the forward delay time, the following relationship should be maintained:  
 $2 * (\text{forward-time} - 1) \geq \text{Max-Age}$

#### Instance

```

Configure STP forwarding delay
Switch(config)# spanning-tree forward-time 25

```

### spanning-tree hello-time

#### Format

```

spanning-tree hello-time seconds
no spanning-tree hello-time

```

#### Parameter

hello-time	STP hello message sending time, the range is 1-10 seconds
------------	---

#### Default

Default hello message time is 2 seconds

#### Mode

Global configuration mode

#### Instructions

STP hello time is the time interval for broadcasting its hello message to other bridges. Use the

command "spanning-tree hello-time" to configure the STP hello time.

When configuring the hello time, the following relationships should be maintained:

Max-Age  $\geq 2 * (\text{hello-time} + 1)$

#### Instance

Configure STP Hello Time

Switch(config)# spanning-tree hello-time 4

### spanning-tree maximum-age

#### Format

spanning-tree maximum-age seconds

no spanning-tree maximum-age

#### Parameter

maximum	Maximum aging time of STP messages.
---------	-------------------------------------

#### Default

Default maximum aging time is 20 seconds

#### Mode

Global configuration mode

#### Instructions

To set the time interval (in seconds) that the switch can wait without receiving configuration messages before attempting to redefine its own configuration, use the command "spanning-tree hello-time" to configure the maximum aging time. When configuring the maximum aging time, the following relationships should be maintained:

$2 * (\text{forward-time} - 1) \geq \text{Max-Age} \geq 2 * (\text{hello-time} + 1)$

#### Instance

Configure the maximum aging time of STP

Switch(config)# spanning-tree maximum-age 10

### spanning-tree edge

#### Format

spanning-tree edge

no spanning-tree edge

#### Parameter

#### Default

Default disable

#### Mode

Interface configuration mode

**Instructions**

Use the command "spanning-tree edge" to specify the port as an edge port. Under the edge Default, the interface enters the forwarding state immediately after connection. If the edge Default is enabled for the interface and a BPDU is received on the interface, a loop may occur in a short time

**Instance**

Configure edge ports  
 Switch(config)# interface gi1  
 Switch(config-if)# spanning-tree edge

spanning-tree link-type

**Format**

spanning-tree link-type (point-to-point | shared)  
 no spanning-tree link-type

**Parameter**

point-to-point	Port connection is a point-to-point network
shared	Port connection is shared broadcast network

**Default**

For ports with full-duplex configuration, the Default configuration link type is point-to-point, and for ports with half-duplex settings, the Default configuration link type is shared

**Mode**

Interface configuration mode

**Instructions**

Use the command "spanning-tree link-type" to set the RSTP link type of the interface.

**Instance**

Configure the port connection type.  
 Switch(config)# interface gi1  
 Switch(config-if)# spanning-tree link-type point-to-point

spanning-tree max-hops

**Format**

spanning-tree max-hops counts  
 no spanning-tree max-hops

**Parameter**

max-hops	Specifies the number of hops in the MSTP area before discarding BPDUs. The range is 1~40
----------	--

**Default**

Default is 20.

**Mode**

Global configuration mode

**Instructions**

Use the command "spanning-tree max-hops" to specify the number of hops of BPDUs to be forwarded in the MSTP area.

**Instance**

Configure the maximum number of hops  
Switch(config)# spanning-tree max-hops 10

**spanning-tree mcheck****Format**

spanning-tree mcheck

**Parameter****Default****Mode**

Interface configuration mode

**Instructions**

Use the command "spanning-tree mcheck" to restart the Spanning Tree Protocol (STP) migration process on a specific interface (mandatory negotiation with its neighbors)

**Instance**

Configure STP protocol negotiation  
Switch(config)# interface gi1  
Switch(config-if)# spanning-tree mcheck

**spanning-tree pathcost method****Format**

spanning-tree pathcost method (long|short)

**Parameter**

long	The range of path cost is 1-200000000
short	The range of path cost is 1-65535

**Default**

Default is long

**Mode**

Global configuration mode

#### Instructions

Use the command "spanning-tree pathcost method" to specify the spanning tree protocol path cost Default

#### Instance

Configure path cost Default  
Switch(config)# spanning-tree pathcost method short

### spanning-tree port-priority

#### Format

spanning-tree port-priority priority  
no spanning-tree port-priority

#### Parameter

port-priority	Specify the interface priority, the range is 0-240.
---------------	---

#### Default

The default port priority is 128.

#### Mode

Interface configuration mode

#### Instructions

Use the command "spanning-tree port-priority" to specify the priority of the interface. The priority value must be a multiple of 16.

#### Instance

Configure interface priority  
Switch(config)# interface gi1  
Switch(config-if)# spanning-tree port-priority 96

### spanning-tree priority

#### Format

spanning-tree priority priority  
no spanning-tree priority

#### Parameter

priority	Set the bridge STP priority. The range is 0-61440. It guarantees the possibility of selecting the switch as the root bridge of the STP topology. A lower value has a higher priority for selecting the switch as the root bridge of the STP topology.
----------	---

#### Default

Default priority is 32768.

#### Mode

## Global configuration mode

### Instructions

Use the command "spanning-tree priority" to configure the bridge priority. The bridge priority value must be a multiple of 4096. The switch with the lowest priority is the root of the STP topology. When there are switches with the same priority configuration in the environment, the switch with the lowest MAC address will be selected as the root bridge.

### Instance

Configuration priority  
Switch(config)# spanning-tree priority 4096

## spanning-tree tx-hold-count

### Format

spanning-tree tx-hold-count count  
no spanning-tree tx-hold-count

### Parameter

count	Specifies the tx hold count that limits the maximum number of packets transmitted per second. Range is 1-10
-------	---

### Default

Default is 6

### Mode

Global configuration mode

### Instructions

Use the command "spanning-tree tx-hold-count" to limit the maximum number of data packets transmitted per second.

### Instance

Configure the maximum limit for sending  
Switch(config)# spanning-tree tx-hold-count 4

## show spanning-tree

### Format

show spanning-tree

### Parameter

### Default

### Mode

Privilege Mode



**Instructions**

Use the command "show spanning-tree" to query the system spanning tree information.

**Instance**

Query spanning tree information

Switch# show spanning-tree

Spanning tree enabled mode RSTP

Default portcostmethod: long

```

RootID      Priority   32768
Address
              1c:2a:a3:c4:02:9
2 This switch is theroot
HelloTime   2sec    Max Age20sec    Forward Delay 15sec

```

Number of topology changes 3 last change occurred 00:00:03 ago

Times: hold 0, topology change 0, notification0

hello 2, max age 20, forward delay 15

**Interfaces**

Name	State	Prio.Nbr	Cost	Sts	RoleEdgePort	Type
gi1	enabled	128.1	20000	Frw	Desg	No P2P (RSTP)
gi15	enabled	128.15	200000	Frw	Desg	No P2P (RSTP)
gi25	enabled	128.25	200000	Frw	Desg	No P2P (RSTP)

**show spanning-tree interface****Format**

show spanning-tree interface *IF\_PORTS* [statistic]

**Parameter**

interface	Query interface spanning tree configuration
statistic	Query interface spanning tree statistics

**Default****Mode**

Privilege Mode

**Instructions**

Use the command "show spanning-tree interface" to query interface spanning tree information and statistics.

**Instance**

Query interface spanning tree information

```
Switch# show spanning-tree interfaces gi1
```

```
Port gi1 enabled
State:forwarding                               Role:designated
Portid:128.1                                   Port cost:20000
Type:P2P (RSTP)                                Edge Port:No
Designated bridge Priority:32768               Address:1c:2a:a3:c4:02:92
Designated portid:128.1                       Designated path cost:0
BPDUFilter:Disabled                            BPDUGuard: Disabled
BPDU: sent 90, received0
```

```
Query interface spanning tree statistics
```

```
Switch# show spanning-tree interfaces gi1 statistics
```

```
STP Port Statistics
```

```
=====
Port                               :gi1
ConfigurationBDPUsReceived         0
TCNBDPUsReceived                   0
MSTPBDPUsReceived                  0
ConfigurationBDPUsTransmitted      0
TCNBDPUsTransmitted                0
MSTP BDPUsTransmitted              119
=====
```

**show spanning-tree mst**

Format

```
show spanning-tree mst instace-id
```

Parameter

instance-id	MSTP的InstanceID
-------------	-----------------

Default

Mode

Privilege Mode

Instructions

Use the command "show spanning-tree mst" to query the MSTP information of the specified instance.

Instance

Query spanning tree information of Instance  
Switch# show spanning-tree mst 0

#### MST Instance Information

```
=====
=====
```

```
Instance Type : CIST (0)
Bridge Identifier : 32768/ 0/1C:2A:A3:C4:02:92
```

```
-----
Designated Root Bridge : 32768/ 0/1C:2A:A3:C4:02:92
External Root Path Cost : 0
Regional Root Bridge : 32768/ 0/1C:2A:A3:C4:02:92
Internal Root Path Cost : 0
Designated Bridge : 32768/ 0/1C:2A:A3:C4:02:92
Root Port : 0/0
Max Age : 20
Forward Delay : 15
Topology changes : 3
Last Topology Change : 374
```

```
-----
VLANs mapped: 1-4094
```

```
=====
=====
```

Interface	RoleStsCost	Prio.NbrType
gi1	Desg FWD 20000	128.1 P2P (RSTP)
gi15	Desg FWD 200000	128.15 P2P (RSTP)
gi25	Desg FWD 200000	128.25 P2P (RSTP)

#### show spanning-tree mst interface

##### Format

```
show spanning-tree mst instance-id interface IF_PORTS
```

##### Parameter

instance-id	Instance ID of MSTP
interface	Query interface spanning tree instance configuration

##### Default

##### Mode

Privilege Mode

##### Instructions

Use the command "show spanning-tree mst interface" to query the spanning tree instance information of the interface.

##### Instance

Query interface spanning tree instance information  
 Switch# show spanning-tree mst 0 interfaces g1

MST Port Information

```

=====
=====
Instance Type : CIST (0)
-----
      Port Identifier : 128/1
      External Path-Cost:0          /20000
      Internal Path-Cost:0          /20000
-----
      Designated Root Bridge : 32768/1C:2A:A3:C4:02:92
      External Root Cost : 0
      Regional Root Bridge : 32768/1C:2A:A3:C4:02:92
      Internal Root Cost : 0
      Designated Bridge : 32768/1C:2A:A3:C4:02:92
      Internal Port Path Cost : 20000
      Port Role : Designated
      Port State : Forwarding
-----
  
```

show spanning-tree mst configuration

Format

show spanning-tree mst configuration

Parameter

Default

Mode

Privilege Mode

Instructions

Use the command "show spanning-tree mst configuration" to query MSTP configuration information.

Instance

```

Query MSTP configuration information
Switch# show spanning-tree mst configuration
Name      [1C:2A:A3:C4:02:92]
Revision  0      Instances configured1
Instance  Vlansmapped
-----
0         1-4094
  
```

## 32. StaticRouting

### interface vlan (IPv4)

#### Format

```
interface vlan vlanid
ip address ipaddr mask
no interface vlan vlanid
no ip address
```

#### Parameter

ipaddr	IPv4 address of the interface
mask	Subnet mask of the interface IPv4 address

#### Default

#### Mode

```
Global configuration mode
VLANInterface configuration mode
```

#### Instructions

Use the command "interface vlan" to configure the Layer 3 interface of the VLAN. Use the command "ip address" to configure the IP address of the VLAN interface.

#### Instance

```
Configure Layer 3 VLAN interface
Switch(config)# interface vlan 2
Switch(config-if)# ip address 192.168.3.1 255.255.255.0
```

#### Query VLAN interface information

```
Switch# show ip interface vlan 2
```

IP Address	I/F	I/FStatusadmin/oper	Type	Status
192.168.3.1/24	VLAN2	UP/DOWN	Static	Valid

### ip route

#### Format

```
ip route dest-ipaddr mask router-ipaddr
no ip route dest-ipaddr mask router-ipaddr
```

#### Parameter

dest-ipaddr	The prefix of the destination IP address
mask	The mask of the destination IP address prefix
router-ipaddr	The next hop address of the forwarding route

**Default****Mode**

Global configuration mode

**Instructions**

Use the command "ip route" to add system static routing table entries.

**Instance**

Configure static routing

Switch(config)# ip route 1.1.1.1 255.0.0.0 192.168.3.11

Query routing information

Switch# show ip route

Codes: &gt; - best, C - connected, S - static

S&gt; 1.0.0.0/8 [1/1] via 192.168.3.11, VLAN2

C&gt; 192.168.0.0/24 is directly connected, MGMT

VLAN C&gt; 192.168.3.0/24 is directly connected, VLAN2

**arp****Format**

arp ip-addr mac-addr vlan vlanid

no arp ip-addr mac-addr vlan vlanid

**Parameter**

ip-addr	IP address of ARP entry
mac-addr	MAC address of ARP entry
vlan	VLAN to which the ARP entry belongs

**Default****Mode**

Global configuration mode

**Instructions**

Use the command "arp" to add static ARP entries.

**Instance**

Add static ARP

Switch(config)# arp 192.168.3.22 00:00:11:11:11:11 vlan 2

Query ARP entries

Switch# show arp

VLAN	Interface	IP address	HWaddress	Status
-----	-----	-----	-----	-----
vlan 1		192.168.0.112	00:D0:00:00:00:01	Dynamic

---

```
vlan 2          192.168.3.22    00:00:11:11:11:11  Static
```

### Interface vlan (IPv6)

#### Format

```
interface vlan vlanid
ipv6 enable
no interface vlan vlanid
no ipv6 enable
```

#### Parameter

vlanid	VLAN ID of the VLAN interface
--------	-------------------------------

#### Default

#### Mode

```
Global configuration mode
VLANInterface configuration mode
```

#### Instructions

Use the command "interface vlan" to configure the Layer 3 interface of the VLAN. Use the command "ipv6 enable" to enable the IPv6 function of the interface.

#### Instance

```
Configure IPv6 Layer 3
interfaceSwitch(config)#
interface vlan 2 Switch(config-
if)# ipv6 enable
```

```
Query IPv6 of the interface
Switch# show ipv6 interface vlan 2
```

```
VLAN 2 is up/up
IPv6 is enabled, link-local address is
fe80::2e0:4cff:fe00:0 IPv6 Forwarding is enabled
No global unicast address is configured
Joined group address(es):
ff02::1:ff00:
0 ff02::1
ff01::1
ND DAD is enabled, number of DAD attempts: 1
Stateless autoconfiguration is enabled
```

### ipv6 address

#### Format

```
ipv6 address ipv6-addr
no ipv6 address
```

## Parameter

ipv6-addr	Configure IPv6 address
-----------	------------------------

## Default

## Mode

Global configuration mode  
VLANInterface configuration mode

## Instructions

Use the command "ipv6 address" to configure the IPv6 address of the Layer 3 VLAN interface.

## Instance

Configure IPv6 address  
Switch(config)# interface vlan 2  
Switch(config-if)# ipv6 address 2001:01::01:01/64

## Query interface IPv6

```
Switch# show ipv6 interface vlan 2
VLAN 2 is up/up
IPv6 is enabled, link-local address is
fe80::2e0:4cff:fe00:0 IPv6 Forwarding is enabled
Global unicast address(es):
IPv6GlobalAddress                Type
2001:1::1:1/64                    Manual
Joined group address(es):
ff02::1:ff01:1
ff02::1:ff00:
0 ff02::1
ff01::1
ND DAD is enabled, number of DAD attempts: 1
Stateless autoconfiguration is enabled Stateless autoconfiguration is enabled
```

## ipv6 route

## Format

ipv6 route ipv6-addr/length route-ipv6-addr  
no ipv6 route ipv6-addr/length

## Parameter

ipv6-addr/length	The prefix of the destination IPv6 address
route-ipv6-addr	Next hop address for forwarding IPv6 routes

## Default

## Mode



Global configuration mode

#### Instructions

Use the command "ipv6 route" to add system static IPv6 routing table entries.

#### Instance

Configure IPv6 static routing

```
Switch(config)# ipv6 route 2002:01::01:01/96 2001:01::01:02
```

Query IPv6 static routing

```
Switch# show ipv6 route static
```

Codes: A - active, I - inactive

```
I   2002:1::/96 [1/1] via 2001:1::1:2,inactive
```

### ipv6 neighbors

#### Format

```
ipv6 neighbor ipv6-addr vlan vlanid macaddr
```

```
no ipv6 neighbor
```

#### Parameter

ipv6-addr	Neighbor IPv6 address
vlan	ID of the VLAN interface
macaddr	MAC address of neighbor IPv6 address

#### Default

#### Mode

Global configuration mode

#### Instructions

Use the command "ipv6 neighbor" to add static IPv6 neighbor entries.

#### Instance

Configure IPv6 neighbors

```
Switch(config)# ipv6 neighbor 2001:01::01:11 vlan 2 00:00:00:11:11:12
```

Query IPv6 neighbors

```
Switch# show ipv6 neighbors
```

```
VLANInterface          IPv6address          HW address
```

```
Status   Router State
```

```
-----
```

```
-----
```

```
vlan2          2001:1::1:11          00:00:00:11:11:12
```

```
Static        No
```

Total number of entries: 1

### show ip interface vlan

#### Format

show ip interface vlan vlanid

#### Parameter

vlan	VLAN ID of the Layer 3 interface
------	----------------------------------

#### Default

#### Mode

Privilege Mode

#### Instructions

Use the command "show ip interface vlan" to query the interface information.

#### Instance

Query VLAN interface information

Switch# show ip interface vlan 2

IP Address	I/F	I/FStatusadmin/oper	Type	Status
-----				
192.168.3.1/24	VLAN2	UP/DOWN	Static	Valid

### show ipv6 interface vlan

#### Format

show ipv6 interface vlan vlanid

#### Parameter

vlanid	VLAN ID of the VLAN interface
--------	-------------------------------

#### Default

#### Default

Privilege Mode

#### Instructions

Use the command "show ipv6 interface vlan" to query the IPv6 information of the interface

#### Instance

Query IPv6 of the interface

Switch# show ipv6 interface vlan 2

VLAN 2 is up/up

IPv6 is enabled, link-local address is

```
fe80::2e0:4cff:fe00:0 IPv6 Forwarding is enabled
No global unicast address is configured
Joined group address(es):
ff02::1:ff00:
0 ff02::1
ff01::1
ND DAD is enabled, number of DAD attempts: 1
Stateless autoconfiguration is enabled
```

### show ip route

#### Format

```
show ip route
```

#### Parameter

##### Default

##### Mode

```
Privilege Mode
```

#### Instructions

Use the command "show ip route" to query system IP routing table entries.

#### Instance

Query routing information

```
Switch# show ip route
```

Codes: > - best, C - connected, S - static

```
S> 1.0.0.0/8 [1/1] via 192.168.3.11, VLAN2
```

```
C> 192.168.0.0/24 is directly connected, MGMT
```

```
VLAN C> 192.168.3.0/24 is directly connected, VLAN2
```

### show ipv6 route

#### Format

```
show ipv6 route
```

#### Parameter

##### Default

##### Mode

```
Privilege Mode
```

#### Instructions

Use the command "show ipv6 route" to query the system static IPv6 routing table entries.

#### Instance

Query IPv6 static routes

```
Switch# show ipv6 route static
```

Codes: A - active, I - inactive  
 I 2002:1::/96 [1/1] via 2001:1::1:2,inactive

### show arp

#### Format

show arp

#### Parameter

#### Default

#### Mode

Privilege Mode

#### Instructions

Use the command "show arp" to query static ARP entries.

#### Instance

Query ARP entries

Switch# show arp

VLANInterface	IP address	HWaddress	Status
vlan 1	192.168.0.112	00:D0:00:00:00:01	Dynamic
vlan 2	192.168.3.22	00:00:11:11:11:11	Static

### show ipv6 neighbors

#### Format

show ipv6 neighbor

#### Parameter

#### Default

#### Mode

Privilege Mode

#### Instructions

Use the command "show ipv6 neighbor" to query the system's IPv6 neighbor entries.

#### Instance

Query IPv6 neighbors

Switch# show ipv6 neighbors

VLANInterface	Status	Router State	IPv6address	HW address
-----				

-----

vlan2                    2001:1::1:11

00:00:00:11:11:12

Static        No

Total number of entries: 1



## Drop storm-control action

### Format

storm-control action (drop | shutdown)  
no storm-control action

### Parameter

drop	After the storm exceeds the threshold, the operation is processed as discard
shutdown	After the storm exceeds the threshold, the operation is processed as closing the interface

### Default

Default is drop

### Default

Interface configuration mode

### Instructions

Use the command "storm-control action" to set the operation when the received storm control data packet exceeds the maximum rate on the interface

### Instance

Configure storm suppression operations beyond the threshold

```
Switch(config)# interface gi1
```

```
Switch(config-if)# storm-control action shutdown
```

Query storm suppression configuration

```
Switch# show storm-control interfaces gi1
```

```

  Port   |State| Broadcast | Unkown-Multicast | Unknown-Unicast
  | Action
  |      |          |                |                 |
  |      |          | kbps          | kbps            | kbps          |
  -----+-----+-----+-----+-----+
  gi1    enable  10000         Off( 10000)      Off( 10000)
  shutdown

```

## storm-control ifg

### Format

storm-control ifg (include | exclude)

### Parameter

include	When including preamble and IFG (20 bytes), count the ingress storm control rate
exclude	Exclude the preamble and IFG (20 bytes), when the count enters the storm

	control rate
--	--------------

**Default**

Default storm control frame gap is exclude

**Mode**

Global configuration mode

**Instructions**

The storm control mechanism will try to calculate whether the ingress packet exceeds the configured rate and perform corresponding operations. Use the command "storm-control ifg" to include/exclude the preamble and inter-frame gaps in the calculation.

**Instance**

Configuration includes interframe gap  
Switch(config)# storm-control ifg include

Query and calculate IFG  
Switch# show storm-control  
Storm control preamble and IFG: Included  
Storm control unit: pps

.....

**storm-control level****Format**

storm-control (broadcast | unknown-unicast | unknown-multicast) level  
<1-1000000>  
no storm-control (broadcast | unknown-unicast | unknown-multicast)  
level

**Parameter**

broadcast	Broadcast storm type
unknown-unicast	Unknown unicast type
unknown-multicast	Unknown multicast type
level	Set the storm control rate of the selected type. For bps, the range is 16-1000000
	For pps, the range is 1-262143

**Default**

Default broadcast storm  
suppression rate is 10000  
Default unknown unicast storm  
suppression rate is 10000  
Default unknown multicast storm  
suppression rate is 10000



**Mode**

Interface configuration mode

**Instructions**

Use the command "storm-control (broadcast | unknown-unicast | unknown-multicast) level" to allow different storm control rates for each storm type.

**Instance**

Configure interface storm suppression  
 Switch(config)# interface gi1  
 Switch(config-if)# storm-control broadcast  
 Switch(config-if)# storm-control broadcast level 200

Query storm suppression configuration  
 Switch# show storm-control interfaces gi1

Port	State	Broadcast		Unkown-Multicast		Unknown-Unicast
Action		kbps		kbps		kbps
gi1	enable	200		Off( 10000)		Off( 10000)
shutdown						

**storm-control unit****Format**

storm-control unit (bps | pps)

**Parameter**

bps	Bit-based storm control rate calculation
pps	Packet-based storm control rate calculation

**Default**

Default storm suppression calculation unit is bps

**Mode**

Global configuration mode

**Instructions**

The storm control mechanism will try to calculate whether the ingress packet exceeds the configured rate and perform corresponding operations. Use the command "storm-control unit" to change the unit of the calculation method.

**Instance**

Configure the unit of storm calculation  
 Switch(config)# storm-control unit pps

```

Query storm suppression
Switch# show storm-control
Storm control preamble and IFG: Excluded
Storm control unit: pps

```

### show storm-control

#### Format

```

show storm-control
show storm-control interface IF_PORTS

```

#### Parameter

interface	Query storm suppression by interface
-----------	--------------------------------------

#### Default

#### Mode

Privilege Mode

#### Instructions

Use the command "show storm-control" to display all storm control-related configurations, including Global configuration and each port configuration.

Use the command "show storm-control interface" to query the storm suppression configuration of the specified interface.

#### Instance

```

Query storm suppression
Switch# show storm-control
Storm control preamble and IFG: Excluded
Storm control unit: pps

```

```

Query storm suppression configuration
Switch# show storm-control interfaces gi1

```

Port	State	Broadcast		Unkown-Multicast		Unknown-Unicast
Action		kbps		kbps		kbps
-----						
gi1	enable	200		Off( 10000)		Off( 10000)
shutdown						

## 34. System File

### copy

#### Format

```
copy (flash:// | tftp://) (flash:// | tftp://)
copy tftp:// (backup-config | running-config | startup-config)
copy (backup-config | running-config | startup-config) tftp://
copy (backup-config | startup-config) running-config
copy (backup-config | running-config) startup-config
copy (running-config | startup-config) backup-config
```

#### Parameter

tftp://	Specify the remote server and file name, Format is "Tftp://192.168.1.111/remote_file_name"
running-config	Run configuration file
startup-config	Startup configuration file
backup-config	Backup configuration file

#### Default

#### Mode

Privilege Mode

#### Instructions

There are many types of files in the system. These files are very important for the administrator to manage the switch. The most common file operation is copying. By using these copy commands, we can upgrade and backup the following types of files.

- Y FirmwareImage
- Y ConfigurationFiles
- Y SyslogFiles
- Y LanguageFiles
- Y SecurityCertificate

#### Instance

Copy running configuration to startup configuration

```
Switch# copy running-config startupst-config
```

Upload running file to remote host

```
Switch# copy running-config tftp://192.168.1.111/test1.cfg
```

Uploading file...Please Wait... Uploading Done

Download the configuration file to the startup configuration

```
Switch# copy tftp://192.168.1.111/test2.cfg startup-config
```

Downloading file...Please Wait... Downloading Done

Upgrade config success.  
Do you want to reboot now? (y/n)n

Upload FLASH file to remote host  
Switch# copy flash://dsa2 tftp://192.168.1.111/dsa2  
Uploading file...Please Wait... Uploading Done

## delete

### Format

delete (startup-config | backup-config | flash://)

### Parameter

flash://	Set the configuration file stored in the flash to delete. Available documents include: flash://startup-config flash://backup-config
startup-config	Delete startup configuration file
backup-config	Delete the backup configuration file

### Default

### Mode

Privilege Mode

### Instructions

Use the command "delete" to delete the system configuration file.

### Instance

Delete backup files  
Switch# delete backup-config

### Query FLASH files

Switch# show flash

FileName	FileSize	Modified
-----	-----	-----
startup-config	1485	2020-01-01 00:24:52
rsa2	1679	2020-01-01 00:00:35
dsa2	668	2020-01-01 00:00:58
ssl_cert	1245	2020-01-01 00:01:07
image	8620992	2020-03-22 13:41:58

## restore-defaults

### Format

restore-defaults [interfaces IF\_PORTS]

## Parameter

interfaces	Reset the running configuration under the interface
------------	---

## Default

## Mode

Privilege Mode

## Instructions

Use the command "restore-defaults" to restore the factory configuration of the system.

## Instance

```
Restore system factory
configurationSwitch#
restore-defaults Restore
Default Success.
Do you want to reboot now? (y/n)n
```

**save**

## Format

Save

## Parameter

## Default

## Mode

Privilege Mode

## Instructions

Use the command "save" to save the system running configuration to the startup configuration.

## Instance

```
Save
Switch# save
Success
```

**show config**

## Format

```
show (running-config | startup-config)
show running-config interfaces IF_PORTS
```

## Parameter

running-config	Query running configuration file
startup-config	Query startup configuration file
interfaces	Query the running configuration under the interface

## Default

### Mode

Privilege Mode

### Instructions

Our configuration file is text based. Therefore, we can display the configuration on the terminal and read it with this command. Use the command "show (running-config|startup-config)" to query the required configuration.

### Instance

Query startup configuration

```
Switch# show startup-config
```

```
! System Description: RTK RTL8328-24FE-4GE Switch
```

```
! System Version: v2.5.0-beta.32811
```

```
! System Name: SwitchEF0102
```

```
! System Up Time: 0 days, 4 hours, 31 mins, 43 secs
```

```
!
```

```
!
```

```
!
```

```
!
```

```
username "" privilege user secret "dnXencJRwflV6" username "admin"
```

```
secret "FzjrGO6vfbERY"
```

```
voice-vlan vpt 0
```

```
voice-vlan dscp 0
```

```
.....
```

Query running configuration

```
Switch# show running-config
```

```
! System Description: RTK RTL8328-24FE-4GE Switch
```

```
! System Version: v2.5.0-beta.32811
```

```
! System Name: SwitchEF0102
```

```
! System Up Time: 0 days, 5 hours, 23 mins, 42 secs
```

```
!
```

```
!
```

```
!
```

```
!
```

```
username "" privilege user secret "dnXencJRwflV6" username "admin"
```

```
secret "FzjrGO6vfbERY"
```

```
voice-vlan vpt 0
```

```
voice-vlan dscp 0
```

```
.....
```

Query the running configuration under the interface

```
Switch# show running-config interfaces gi1
```

```
interface gi1
```

```
rate-limit ingress 128
```

## show flash

### Format

show flash

### Parameter

Default

### Mode

Privilege Mode

### Instructions

Use the command "show flash" to query all files saved in flash.

### Instance

Query FLASH files

Switch# show flash

FileName	FileSize	Modified
-----		
startup-config	1485	2020-01-01 00:24:52
rsa2	1679	2020-01-01 00:00:35
dsa2	668	2020-01-01 00:00:58
ssl_cert	1245	2020-01-01 00:01:07
image	8620992	2020-03-22 13:41:58

## 35. SurveillanceVLAN

### surveillance-vlan (Global)

#### Format

surveillance-vlan  
nosurveillance-vlan

#### Parameter

#### Default

Default disable

#### Mode

Global configuration mode

#### Instructions

Use the command "surveillance-vlan" to enable the video VLAN global switch.

#### Instance

Enable video VLAN  
Switch(config)# surveillance-vlan

Query video VLAN configuration  
Switch# show surveillance -vlan  
Administrate Surveillance VLAN state : disabled  
SurveillanceVLANID : none (disable)  
SurveillanceVLANAging : 1440 minutes  
SurveillanceVLANCoS 6  
Surveillance VLAN 1p Remark: disabled

### surveillance-vlan (Interface)

#### Format

surveillance-vlan  
nosurveillance-vlan

#### Parameter

#### Default

#### Mode

Interface configuration mode

#### Instructions

Use the command "surveillance-vlan" to enable OUI video VLAN configuration on the



interface.

#### Instance

Enable the video VLAN of the interface  
 Switch(config)#interface  
 range gi1-3 Switch(config-  
 if)#surveillance-vlan

Query the video VLAN configuration of the interface  
 Switch# show surveillance-vlan interfaces gi1-3  
 SurveillanceVLANAging : 1440 minutes  
 SurveillanceVLANCoS 7  
 Surveillance VLAN 1p Remark: enabled

#### OUI table

OUI MAC | Description

-----+-----

00:01:02 | Test

Port | State | Port Mode | CosMode

-----+-----+-----+-----

gi1 | Disabled | Auto | Src

gi2 | Disabled | Auto | Src

gi3 | Disabled | Auto | Src

### surveillance-vlan vlan

#### Format

surveillance-vlan vlan <1-4094>

no surveillance-vlan vlan

#### Parameter

vlan	Specify VLAN to enable video VLAN function
------	--

#### Default

#### Mode

Global configuration mode

#### Instructions

Use the command "surveillance-vlan vlan" to statically configure the VLAN identifier of the video VLAN.

#### Instance

Configure video VLAN

Switch(config)# surveillance-vlan vlan 128

Query video VLAN

```
Switch# show surveillance-vlan
Administrate Surveillance VLAN state : enabled
SurveillanceVLANID 128
SurveillanceVLANAging : 1440
minutes SurveillanceVLANCoS
6
Surveillance VLAN 1p Remark: disabled
```

### surveillance-vlan oui-table

#### Format

```
surveillance-vlan oui-table A:B:C [DESCRIPTION]
no surveillance-vlan oui-table [A:B:C]
```

#### Parameter

A:B:C	Add or delete OUI MAC
DESCRIPTION	Set the description of the specified MAC address as the video VLAN OUI table

#### Default

#### Mode

Global configuration mode

#### Instructions

Use the command "surveillance-vlan oui-table" to configure the OUI table entry of the MAC address.

#### Instance

```
Configure OUI entries
Switch(config)# surveillance-vlan oui-table 00:01:02 "Test"
```

```
Query interface video VLAN configuration
Switch# show surveillance-vlan interfaces all
SurveillanceVLANAging : 1440 minutes
SurveillanceVLANCoS 7
Surveillance VLAN 1p Remark: enabled
```

#### OUI table

```
OUI MAC | Description
```

```
-----+-----
00:01:02 | Test
Port   | State | Port Mode | CosMode
-----+-----+-----+-----
gi1   | Disabled | Auto   | Src
gi2   | Disabled | Auto   | Src
```

```
gi3 | Disabled | Auto | Src
.....
```

### surveillance-vlan cos (Global)

#### Format

```
surveillance-vlan cos <0-7> [remark]
no surveillance-vlan cos
```

#### Parameter

cos	Set the COS value of video VLAN packets
remark	Enable re-marking COS value

#### Default

The Default COS value is 6, which is re-marked as disabled.

#### Mode

Global configuration mode

#### Instructions

Use the command "surveillance vlan cos" to configure the priority and remark switch of the video VLAN packet.

#### Instance

```
Configure the COS value of the video VLAN
Switch(config)# surveillance-vlan cos 7 remark
```

#### Query video VLAN

```
Switch# show surveillance-vlan
Administrate Surveillance VLAN state : disabled
SurveillanceVLANID    128
SurveillanceVLANAging : 1440
minutes SurveillanceVLANCoS
                        7
Surveillance VLAN 1p Remark: enabled
```

### surveillance-vlan cos (Interface)

#### Format

```
surveillance-vlan cos ( src | all )
no surveillance-vlan cos
```

#### Parameter

src	Set QoS attributes to be applied to packets with OUIs in the source MAC address
all	Set QoS attributes to be applied to packets classified into the video VLAN.

**Default**

Default is src.

**Mode**

Interface configuration mode

**Instructions**

Use the command "surveillance vlan cos" to configure the OUI video VLAN cosDefault configuration on the interface.

**Instance**

Configure the COS value of the video VLAN under the interfaceSwitch(config)#interface range gi1-3 Switch(config-if)# surveillance-vlan cos all

Query interface video VLAN configuration  
Switch# show surveillance-vlan interfaces gi1-3  
SurveillanceVLANAging : 1440 minutes  
SurveillanceVLANCoS 7  
Surveillance VLAN 1p Remark: enabled

**OUI table**

OUI MAC | Description

```
-----+-----
00:01:02 | Test
```

Port | State | Port Mode | CosMode

```
-----+-----+-----+-----
gi1 | Disabled | Auto | Src
gi2 | Disabled | Auto | Src
gi3 | Disabled | Auto | Src
```

**surveillance-vlan mode****Format**

surveillance-vlan mode (auto|manual)  
no surveillance-vlan mode

**Parameter**

auto	The designated port is identified as a candidate port for joining the video VLAN. When a data packet with a source OUI MAC address identifying the remote device as a video device is seen on the port, the port connects the video VLAN as a tagged port
manual	Specify to manually assign the port to the video VLAN

**Default**

Default is auto

**Mode**

Interface configuration mode

**Instructions**

Use the command "surveillance-vlan mode" to configure the video VLAN Default of the interface.

**Instance**

Configure the video VLAN under the interface  
 DefaultSwitch(config)#interface range gi1-3  
 Switch(config-if)# surveillance-vlan mode manual

Query interface video VLAN configuration  
 Switch# show surveillance-vlan interfaces gi1-3  
 SurveillanceVLANAging : 1440 minutes  
 SurveillanceVLANCoS 7  
 Surveillance VLAN 1p Remark: enabled

**OUI table**

OUI MAC | Description

```
-----+-----
00:01:02 | Test
```

Port | State | Port Mode | CosMode

```
-----+-----+-----+-----
gi1 | Disabled | Auto | Src
gi2 | Disabled | Auto | Src
gi3 | Disabled | Auto | Src
```

**surveillance-vlan aging-time****Format**

surveillance-vlan aing-time <30-65536>  
 no surveillance-vlan aing-time

**Parameter**

aing-time	Video VLAN aging time interval, in minutes
-----------	--

**Default**

The default aging time is 1440 minutes.

**Mode**

Global configuration mode

**Instructions**

Use the command "surveillance vlan aging-time" to configure the aging interval of the video VLAN.

**Instance**

Configure the video VLAN aging interval  
 Switch(config)# surveillance-vlan aging-time 720

Query video VLAN configuration  
 Switch# show surveillance-vlan  
 Administrate Surveillance VLAN state : disabled  
 SurveillanceVLANID 1  
 SurveillanceVLANAging : 720  
 minutes SurveillanceVLANCoS  
 5  
 Surveillance VLAN 1p Remark: enabled

**show surveillance-vlan****Format**

show surveillance-vlan  
 show surveillance-vlan interfaces [IF\_PORTS]

**Parameter**

interfaces	Query video VLAN configuration by interface
------------	---

**Default****Mode**

Privilege Mode

**Instructions**

Use the command "show surveillance-vlan" to query the video VLAN Global configuration. Use the command "show surveillance-vlan interface" to query the video VLAN interface configuration.

**Instance**

Query video VLAN configuration  
 Switch# show surveillance-vlan  
 Administrate Surveillance VLAN state : disabled  
 SurveillanceVLANID 1  
 SurveillanceVLANAging : 720  
 minutes SurveillanceVLANCoS  
 5  
 Surveillance VLAN 1p Remark: enabled

## 36. Time

### clock set

#### Format

```
clock set HH:MM:SS (jan|feb|mar|apr|may|jun|jul|aug|sep|oct|nov|dec)
<1-31><2000-2035>
```

#### Parameter

set	The system default startup time is 2000/01/01 08:00:00
-----	--

#### Default

The system default startup time is 2000/01/01 08:00:00

#### Mode

Privilege Mode

#### Instruction

Use the command "clock set" to device system static time. The static time will not be saved to the configuration file.

#### Instance

```
Configure system time
switch# clock set 11:03:00 sep 21 2012
11:03:00 DFL(UTC+8) Sep 21 2012
```

```
Query system time
switch# show clock
11:03:21 DFL(UTC+8) Sep 21 2012
No time source
```

### clock timezone

#### Format

```
clock timezone ACRONYM HOUR-OFFSET [minutes <0-59>]
no clock timezone
```

#### Parameter

ACRONYM	Specify the abbreviated name of the time zone
HOUR-OFFSET	Specify time zone hour offset
minutes	Specify time zone minute offset

#### Default

Default time zone is UTC+8

**Mode**

Global configuration mode

**Instructions**

Use the command "clock timezone" to set the system time zone.

**Instance**

```
Set the system time zone
switch(config)# clock timezone test +5
switch(config)# show clock detail
10:13:27 test(UTC+5)
Sep 21 2012
No time source
```

Time zone: Acronym is test Offset is UTC+5

**clock source****Format**

clock source (local | sntp)

**Parameter**

local	Use local static clock
sntp	Enable remote SNTP clock synchronization

**Default**

The system default clock source is local

**Mode**

Global configuration mode

**Instructions**

Use the command "clock source" to configure the system clock source.

**Instance**

```
Configure the system clock source
switch(config)# clock source sntp
switch(config)# show clock detail
08:32:12 test(UTC+5) Sep 21 2012
Time source is sntp
```

Time zone: Acronym is DFL Offset is UTC+8

**clock summer-time****Format**

clock summer-time ACRONYM date



(jan|feb|mar|apr|may|jun|jul|aug|sep|oct|nov|dec) <1-31><2000-2037>HH:MM (jan|feb|mar|apr|may|jun|jul|aug|sep|oct|nov|dec) <1-31><2000-2037> HH:MM [<1-1440>]  
 clock summer-time ACRONYM recurring (usa|eu) [<1-1440>] clock summer-time ACRONYM recurring (<1-5>|first|last) (sun|mon|tue|wed|thu|fri|sat) (jan|feb|mar|apr|may|jun|jul|aug|sep|oct|nov|dec) HH:MM (<1-5>|first|last) (sun|mon|tue|wed|thu|fri|sat)  
 (jan|feb|mar|apr|may|jun|jul|aug|sep|oct|nov|dec)HH:MM [<1-1440>]  
 no clock summer-time

#### Parameter

ACRONYM	Abbreviated name of time zone
date	Non-recurring daylight saving time duration
<1-1440>	Adjust the daylight saving time offset
usa	Use daylight saving time in the United States, starting on the second Sunday in March and ending on the first Sunday in November
eu	Use daylight saving time in Europe, starting on the last Sunday in March and ending on the last Sunday in October
recurring	Duration of summer-time

#### Mode

Global configuration mode

#### Instructions

Use the command "clock summer-time" to set the summer time of the system time.

#### Instance

```
Set system summer-time
switch(config)# clock summer-time test recurring usa
switch(config)# show clock detail
08:32:12 test(UTC+5) Sep 21 2012
No time source
```

Time zone: Acronym is DFL Offset is UTC+8

Summertime: Acronym is test Recurring every year. Begins at 2 0 3 2:0

Ends at 1 0 11 2:0

Offset is 60 minutes.

## sntp

#### Format

```
sntp host HOSTNAME [port <1-65535>]
no sntp
```

#### Parameter

HOSTNAME	The IP address or host name of the SNTP server
----------	--

port	SNTP server port number
------	-------------------------

**Mode**

Global configuration mode

**Instructions**

Use the command "sntp" to configure the remote SNTP synchronization clock server.

**Instance**

```

Configure SNTP server
switch(config)# clock source sntp
switch(config)# sntp host 192.168.1.100
switch(config)# show sntp
SNTP is Enabled
SNTP Server address: 192.168.1.100
SNTP Server port: 123

```

**show clock****Format**

show clock [detail]

**Parameter**

detail	Query detailed clock information
--------	----------------------------------

**Default****Mode**

Privilege Mode

**Instructions**

Use the command "show clock" to query the system clock information.

**Instance**

```

Query system clock
switch# show clock
11:03:21 DFL(UTC+8) Sep 21 2012
No time source

```

**show sntp****Format**

show sntp

**Parameter****Default****Mode**

### Privilege Mode

#### Instructions

Use the command "show sntp" to query the remote SNTP server information.

#### Instance

```
Query SNTP server
informationswitch(config)
# show sntp SNTP is
Enabled
SNTP Server address: 192.168.1.100
SNTP Server port: 123
```

## 37. UDLD

### udld

#### Format

```
udld
no udld
```

#### Parameter

#### Default

Default disable

#### Mode

Interface configuration mode

#### Instructions

Use the command "udld" to enable unidirectional link detection (UDLD) of the interface.  
Default.

#### Instance

```
UDLD with interface enabled
switch(config)# interface gi1
switch(config-if)# udld
```

#### UDLD query interface

```
switch# show udld interfaces gi1
Port enable administrative configuration setting: Enabled
Port enable operational state: Enabled
Current bidirectional state: Bidirectional
Current operational state: Advertisement - SINGLE NEIGHBOR DETECTED
```

### udld aggressive

#### Format

```
udld aggressive
no udld aggressive
```

#### Parameter

#### Default

Default disable

#### Mode

## Interface configuration mode

### Instructions

Use the command "udld ggressive" to enable unidirectional link detection (UDLD) attacks on the interface Default

### Instance

```
Configure the interface as UDLD
attackDefaultswitch(config)#
interface gi1 switch(config-if)#
udld aggressive
```

### UDLD query interface

```
Switch# show udld interfaces gi1
```

### Interface gi1

---

```
Port enable administrative configuration setting: Enabled / in aggressive mode
Port enable operational state: Enabled / in aggressive mode
Current bidirectional state: Unknown
Current operational state:
Advertisement Message interval: 7
Time out interval: 5
No neighbor cache information stored
```

## udld message time

### Format

```
udld message time message-time-interval
```

### Parameter

time	Specify the interval for sending messages. The range is 1-90 seconds
------	--

### Default

Default is 15 seconds.

### Mode

Global configuration mode

### Instructions

Use the command "udld message time" to set the interval of unidirectional link detection (UDLD) sending messages.

### Instance

```
Configure UDLD message interval
switch(config)# udld message time 30
```

## udld reset

**Format**

udld reset

**Parameter**

Default

**Mode**

Privilege Mode

**Instructions**

Use the command "udld reset" to reset all interfaces disabled by unidirectional link detection (UDLD) and allow communication traffic to start passing through them again. If the interface configuration is still enabled for UDLD, these ports will run UDLD again, if the problem is not corrected, these ports will be disabled for the same reason.

**Instance**

Reset UDLD

Switch# udld reset

1 ports shutdown by UDLD were reset.

**show udld****Format**

show udld

show udld interfaces IF\_NMLPORTS

**Parameter**

interfaces	Query the UDLD configuration of the specified interface
------------	---

**Default****Mode**

Privilege Mode

**Instructions**

Use the command "show udld" to display the unidirectional link detection (UDLD) management and operation status of all ports or designated ports.

**Instance**

UDLD query interface

Switch# show udld interfaces g1

Interface gi1

---

Port enable administrative configuration setting: Enabled / in aggressive mode

Port enable operational state: Enabled / in aggressive mode

Current bidirectional state: Unknown

Current operational state:  
 Advertisement Message interval: 7  
 Time out interval: 5  
 No neighbor cache information stored

## 38. VLAN

### vlan

#### Format

vlan  
 no vlan

#### Parameter

#### Default

System Default has VLAN 1

#### Mode

Global configuration mode

#### Instructions

Use command "vlan" to add system VLAN

#### Instance

Configure  
 VLANSwitch#  
 configure  
 Switch (config)# vlan 100

#### Query VLAN configuration

```
Switch# show vlan
VID | VLAN Name | Untagged Ports | Tagged Ports | Type
-----+-----+-----+-----+-----
-----+-----
1 | default | gi1-48,gi1-4,lag1-8 | --- | Default 100|
  | VLAN0100 | --- | --- |Static
```

### Name (vlan)

#### Format

name NAME

#### Parameter

name	Configure VLAN alias
------	----------------------

The Default name of the new vlan is VLANxxxx. xxxx is a 4-digit vlan number

#### Default

VLAN configuration Default

**Instructions**

Use the command "name" to configure or modify the VLAN alias.

**Instance**

```
Configure VLAN name
Switch(config)# vlan 100
Switch(config-vlan)# name VLAN-one-hundred
```

Query VLAN configuration

```
Switch# show vlan
VID | VLAN Name | Untagged Ports | Tagged Ports | Type
-----+-----+-----+-----+-----
1 | default | gi1-48,gi1-4,lag1-8 | --- | Default
100 | VLAN-one-hundred | --- | --- | Static
```

**switchport mode****Format**

switchport mode ( access | hybrid | trunk [uplink] | tunnel )

**Parameter**

access	VLANDefault is AccessPort
hybrid	VLANDefault is hybridPort
trunk	VLANDefault is trunk Port
uplink	Set the upstream attributes of the trunk port
tunnel	VLAN Default is Q-in-QDefault

**Default**

System default all interfaces are trunk

**Mode**

Interface configuration mode

**Instructions**

Use the command "switchport mode" to configure port VLAN attributes for different port roles.

Access: Only accept untagged frames and join untagged VLANs.

Hybrid: Supports all functions defined in the IEEE 802.1Q specification.

Trunk: An untagged member of at most one VLAN, and is a tagged member of zero or more VLANs. If it is an uplink port, it can identify the double-tagged on this port

Tunnel: Port-based Q-in-QDefault

**Instance**

```
Configure VLAN attributes of the interface
Switch(config)# interface gi12
```



```
Switch(config-if)# switchport mode access
Switch# show interfaces switchport gi12
Port : gi12
Port Mode : Access
Ingress Filtering : enabled
Acceptable Frame Type : untagged-only
Ingress UnTagged VLAN ( NATIVE ) : 1
Trunking VLANs Enabled:
```

Port is member in:

Vlan	Name	Egressrule
1	default	Untagged

Forbidden VLANs:

Vlan	Name
-----	-----

### switchport hybrid pvid

#### Format

```
switchport hybrid pvid <1-4094>
```

#### Parameter

pvid	Default VLAN of the port
------	--------------------------

#### Default

Default is 1

#### Mode

Port configuration Mode

#### Instructions

Use the command "switch hybrid pvid" to configure the default VLAN of the hybrid port.

#### Instance

```
Configure the default VLAN for the hybrid
port
Switch(config)# interface gi10
Switch(config-if)# switchport mode hybrid
Switch(config-if)# switchport hybrid pvid 100
```

```
Switch# show interfaces switchport gi10
Port : gi10
Port Mode : Hybrid Ingress Filtering : enabled
Acceptable Frame Type : all
Ingress UnTagged VLAN ( NATIVE ) : 100 Trunking VLANs Enabled:
```

Port is member in:

Vlan	Name	Egressrule
1	default	Untagged

Forbidden VLANs:

Vlan	Name
-----	-----

### switchport hybrid ingress-filtering

Format

```
switchport hybrid ingress-filtering no
switchport hybridingress-filtering
```

Parameter

Default

Default enable

Mode

Interface configuration mode

Instructions

Use the command "switchport hybrid ingress-filtering" to enable VLAN filtering in the ingress direction of the interface.

Instance

```
Enable VLAN filtering on the interface
Switch(config)# interface gi10
Switch(config-if)# switchport mode hybrid
Switch(config-if)#no switchport hybrid ingress-filtering
```

### switchport hybrid acceptable-frame-type

Format

```
switchport hybrid acceptable-frame-type ( all | tagged-only | untagged-
only )
```

Parameter

all	Receive all frame types
tagged-only	Only receive frame type with TAG
untagged-only	Only receive frame types with UNTAG

Default

Default is all

**Mode**

Interface configuration mode

**Instructions**

Use the command "switchport hybrid accept-frame-type" to configure which type of frame the interface can receive.

**Instance**

Configure the interface receiving frame type

Switch(config)# interface gi10

Switch(config-if)# switchport mode hybrid

Switch(config-if)# switchport hybrid acceptable-frame-type tagged-only

**switchport hybrid allowed vlan****Format**

switchport hybrid allowed vlan add VLAN-LIST [(tagged|untagged)]

switchport hybrid allowed vlan remove VLAN-LIST

**Parameter**

VLAN-LIST	Specify VLAN list to add or delete
tagged untagged	Specify member type is TAG or UNTAG

**Default**

In the default case, only vlan 1 is a member of UNTAG. Default is a TAG member when added.

**Default**

Interface configuration mode

**Instructions**

Use the command "switchport hybrid allow vlan add" to add the VLAN list allowed by the interface

**Instance**

Configure the list of allowed VLANs

Switch(config)# interface gi10

Switch(config-if)# switchport hybrid allowed vlan add 100-105

Switch(config-if)# switchport hybrid allowed vlan remove 105

Query the configuration of the interface

Switch# show interfaces switchport gi10

Port : gi10

Port Mode : Hybrid

Ingress Filtering : disabled

Acceptable Frame Type : tagged-only

Ingress UnTagged VLAN ( NATIVE ) : 100

Trunking VLANs Enabled:

Port is member in:

VlanName Egressrule

```
-----
1   default  Untagged
100 VLAN-one-hundredTagged
101 VLAN0101  Tagged
102 VLAN0102  Tagged
103 VLAN0103  Tagged
104 VLAN0104  Tagged
```

Forbidden VLANs:

Vlan Name

-----

### switchport access vlan

#### Format

```
switchport access vlan <1-4094>
no switchport access vlan
```

#### Parameter

vlan	Specify the VLAN ID of Access
------	-------------------------------

#### Default

Default is 1

#### Default

Interface configuration mode

#### Instructions

Use the command "switchport access vlan" to configure the default VLAN of the Access port.

#### Instance

```
Configure the default VLAN of
the access port
Switch(config)# interface gi10
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 100
```

### switchport tunnel vlan

#### Format

```
switchport tunnel vlan <1-4094>
no switchport tunnel vlan
```

#### Parameter

vlan	Specify the VLAN ID of the tunnel
------	-----------------------------------

#### Default

Default is 1

#### Mode

Interface configuration mode

#### Instructions

Use the command "switchport tunnel vlan" to set the dot1q tunnel vlan on the interface.

#### Instance

Configure the tunnel vlan of  
the interface  
Switch(config)# interface gi10  
Switch(config-if)# switchport mode tunnel  
Switch(config-if)# switchport tunnel vlan 100

### switchport trunk native vlan

#### Format

switchport trunk native vlan <1-4094>  
no switchport trunk native vlan

#### Parameter

vlan	Specify the VLAN ID of the trunk
------	----------------------------------

#### Default

Default is 1

#### Mode

Interface configuration mode

#### Instructions

Use the command "switchport trunk native vlan" to configure the default VLAN of the trunk port.

#### Instance

Configure the default VLAN of  
the Trunk port  
Switch(config)# interface gi10  
Switch(config-if)# switchport mode trunk  
Switch(config-if)# switchport trunk native vlan 100

### switchport trunk allowed vlan

#### Format

switchport trunk allowed vlan ( add | remove ) ( VLAN-LIST | all )

#### Parameter

( add   remove )	Add or delete VLAN of Trunk port
------------------	----------------------------------

( VLAN-LIST   all )	Specify VLAN or all VLANs
---------------------	---------------------------

**Default**

Default is 1

**Mode**

Interface configuration mode

**Instructions**

Use the command "switchport trunk allow vlan add" to configure the VLAN allowed through the trunk port.

Use the command "switchport trunk allow vlan remote" to delete the VLAN of the trunk port.

**Instance**

Configure the VLAN that the Trunk port allows to pass

Switch(config)# interface gi10

Switch(config-if)# switchport mode trunk

Switch(config-if)# switchport trunk allowed vlan add 100

**switchport default-vlan tagged****Format**

switchport default-vlan tagged

no switchport default-vlan tagged

**Parameter****Default**

Default is untagged

**Mode**

Interface configuration mode

**Instructions**

Use the command "switchport default vlan tagged" to become a member of the Default vlan tagged.

**Instance**

Configure Default VLAN tag members

Switch(config)# interface gi10

Switch(config-if)# switchport default-vlan tagged

**switchport forbidden default-vlan****Format**

switchport forbidden default-vlan no

switchport forbiddendefault-vlan

**Parameter****Default**

Default is allowed

**Mode**

Interface configuration mode

**Instructions**

Use the command "switchport forbidden default-vlan" to prohibit the use of Defaultvlan on the interface.

**Instance**

Configuration prohibits use under the interfaceDefaultVLAN  
Switch(config)# interface gi10  
Switch(config-if)# switchport forbidden default-vlan

**switchport forbidden vlan****Format**

switchport forbidden vlan ( add | remove ) VLAN-LIST

**Parameter**

( add   remove )	Add or remove disabled members operation
VLAN-LIST	VLAN ID of the disabled member

**Default****Mode**

Interface configuration mode

**Instructions**

Use the command "switchport forbidden vlan add" to configure a forbidden VLAN on the interface.

Use the command "switchport forbidden vlan remove" to configure the unbanned VLAN on the interface.

**Instance**

Configure VLANs disabled on the interface Switch(config)# interface gi10  
Switch(config-if)# switchport forbidden vlan add 100

**switchport vlan tpid****Format**

switchport vlan tpid (0x8100|0x88a8|0x9100|0x9200)

**Parameter**

tpid	Choose and set a TPID
------	-----------------------

**Default**

Default is 0x8100

**Mode**

Interface configuration mode

**Instructions**

Use the command "switchport vlan tpid" to configure the TPID of the interface.

**Instance**

Configure the TPID of the interface

Switch(config)# interface gi10

Switch(config-if)# switchport vlan tpid 0x9100

**management-vlan****Format**

management-vlan vlan <1-4094>

no management-vlan

**Parameter**

vlan	Specify a VLAN as the management VLAN
------	---------------------------------------

**Default**

Default is 1

**Mode**

Global configuration mode

**Instructions**

Use the command "management vlan" to configure or modify the management VLAN. You must create a VLAN before configuring the management VLAN.

**Instance**

Configure VLAN

Switch(config)#vlan 2

Configure Management VLAN

Switch(config)# management-vlan vlan 2

**show vlan****Format**

show vlan [(VLAN-LIST | dynamic | static)]



## Parameter

vlan	Query all VLAN or specified VLAN information
dynamic	Query all dynamic VLAN information
static	Query all static VLAN information

## Default

## Mode

Privilege Mode

## Instructions

Use the command "show vlan" to query the VLAN information of the system.

## Instance

Query VLAN configuration

Switch# show vlan

VID | VLAN Name | Untagged Ports | Tagged Ports | Type

```
-----+-----+-----+-----+-----
-----+-----
1 | default   |gi1-48,gi1-4,lag1-8| --- | Default 100|
   | VLAN0100 | --- |             | --- |Static
```

**show vlan interface membership**

## Format

show vlan VLAN-LIST interfaces IF\_PORTS membership

## Parameter

vlan	Query by VLAN
interfaces	Query by interface

## Default

## Mode

Privilege Mode

## Instructions

Use the command "show vlan interface membership" to query the member information of the interface VLAN.

## Instance

Query VLAN member information under the interface

Switch# show vlan 1 interfaces gi1 membership

```
----- VLANID
      :1
VLAN Type : Default
```

```

-----+-----
Port   | Membership
-----+-----
gi1    |   Untagged
-----+-----

```

### show interface switchport

#### Format

```
show interface switchport IF_PORTS
```

#### Parameter

IF_PORTS	Query by interface
----------	--------------------

#### Default

#### Mode

Privilege Mode

#### Instructions

Use the command "show interface switchport" to query the information about DefaultVLAN by interface.

#### Instance

Configure interface DefaultVLAN information

```
Switch# show interfaces switchport g1
```

Port : gi1

Port Mode : Trunk

Gvrp Status : disabled

Ingress Filtering : enabled

Acceptable Frame Type : all

Ingress UnTagged VLAN ( NATIVE ) : 1

Trunking VLANs Enabled:

Port is member in:

Vlan	Name	Egressrule
1	default	Untagged

Forbidden VLANs:

Vlan	Name
-----	-----

### show management-vlan

#### Format

```
show management-vlan
```

Parameter

Default

Mode

Privilege Mode

Instructions

Use the command "show management-vlan" to query the management VLAN information.

Query the management VLAN

Switch# show management-vlan

Management VLAN-ID : default(1)

## 39. VoiceVLAN

### voice-vlan (Global)

#### Format

```
voice-vlan  
novoice-vlan
```

#### Parameter

#### Default

Default disable

#### Mode

Global configuration Mode

#### Instructions

Use the command "voice-vlan" to enable the voice VLAN global switch.

#### Instance

```
Enable VOICE VLAN  
Switch(config)# voice-vlan
```

```
Query VOICE VLAN  
configuration  
Switch# show voice-vlan  
Administrate Voice VLAN state : disabled  
VoiceVLANID      : none(disable)  
Voice VLAN Aging: 1440 minutes VoiceVLANCoS      6  
Voice VLAN 1p Remark: disabled
```

### voice-vlan (Interface)

#### Format

```
voice-vlan  
novoice-vlan
```

#### Parameter

#### Default

Default disable

#### Mode

Interface configuration Mode

## Instructions

Use the command "voice-vlan" to enable OUI voice VLAN configuration on the interface.

## Instance

```
Enable VOICE-VLAN of the interface
Switch(config)#interface range gi1-3
Switch(config-if)#voice-vlan
```

Query the VOICE VLAN configuration of the interface

```
Switch# show voice-vlan interfaces gi1-8
VoiceVLANAging      : 1440 minutes
VoiceVLANCoS        6
Voice VLAN 1p Remark: disabled
```

## OUI table

OUI	MAC	Description
00:03:6B		3COM
00:03:6B		Cisco
00:E0:75		Veritel
00:D0:1E		Pingtel
00:01:E3		Siemens
00:60:B9		
00:0F:E2		NEC/Philips
		H3C
00:09:6E		Avaya

Port	State	PortMode	CosMode
gi1	Disabled	Auto	Src
gi2	Disabled	Auto	Src
gi3	Disabled	Auto	Src
gi4	Disabled	Auto	Src
gi5	Disabled	Auto	Src
gi6	Disabled	Auto	Src
gi7	Disabled	Auto	Src
gi8	Disabled	Auto	Src

## voice-vlan vlan

### Format

```
voice-vlan vlan <1-4094>
no voice-vlan vlan
```

### Parameter

vlan	Specify VLAN to enable VOICE VLAN function
------	--

**Default****Mode**

Global configuration Mode

**Instruction**

Use the command "voice-vlan vlan" to statically configure the VLAN identifier of the voice VLAN.

**Instance**

Configure voice VLAN  
Switch(config)# voice-vlan vlan 128

Query voice VLAN  
Switch# show voice-vlan  
Administrate Voice VLAN state : enabled  
VoiceVLANID 128  
Voice VLAN Aging: 1440 minutes  
VoiceVLANCoS 6  
Voice VLAN 1p Remark: disabled

**voice-vlan oui-table****Format**

voice-vlan oui-table A:B:C [DESCRIPTION]  
no voice-vlan oui-table [A:B:C]

**Parameter**

A:B:C	Add or delete OUI MAC
DESCRIPTION	Set the description of the specified MAC address as the voice VLAN OUI table

**Default**

The Default system creates 8 groups of OUI MAC addresses.

**Mode**

Global configuration Mode  
Use the command "voice-vlan oui-table" to configure the OUI entry of the MAC address.

**Instance**

Configure OUI entries  
Switch(config)# voice-vlan oui-table 00:01:02 "Test"

Query interface voice VLAN configuration  
Switch# show voice-vlan interfaces all

Voice VLAN Aging: 1440 minutes VoiceVLANCoS 6  
 Voice VLAN 1p Remark: disabled

#### OUI table

OUI MAC	Description
00:E0:BB	3COM
00:03:6B	Cisco
00:E0:75	Veritel
00:D0:1E	Pingtel
00:01:E3	Siemens
00:60:B9	NEC/Philips
00:0F:E2	H3C
00:09:6E	Avaya
00:01:02	Test

Port	State	Port Mode	CosMode
gi1	Disabled	Auto	Src fa2   Disabled   Auto   Src fa3   Disabled   Auto
.....			

### voice-vlan cos (Global)

#### Format

```
voice-vlan cos <0-7> [remark]
no voice-vlan cos
```

#### Parameter

cos	Set the COS value of voice VLAN packets
remark	Enable re-marking COS value

#### Default

The Default COS value is 6, and it is re-marked as disabled.

#### Mode

Global configuration Mode

#### Instructions

Use the command "voice vlan cos" to configure the priority and remark switch of voice VLAN packets.

#### Instance

```
Configure the COS value of the voice VLAN
Switch(config)# voice-vlan cos 7 remark
```

```

Query voice VLAN
Switch# show voice-vlan
Administrate Voice VLAN state : disabled
VoiceVLANID      128
Voice VLAN Aging: 1440 minutes
VoiceVLANCoS     7
Voice VLAN 1p Remark: enabled

```

### voice-vlan cos (Interface)

#### Format

```

voice-vlan cos ( src | all )
no voice-vlan cos

```

#### Parameter

src	Set QoS attributes to be applied to packets with OUIs in the source MAC address
all	Set QoS attributes to be applied to packets classified into the voice VLAN.

#### Default

Default is src.

#### Mode

Interface configuration Mode

#### Instructions

Use the command "voice vlan cos" to configure the OUI voice VLAN cosMode configuration on the interface.

#### Instance

```

Configure the COS value of the voice
VLAN under the interface
Switch(config)#interface range gi1-3
Switch(config-if)# voice-vlan cos all

```

```

Query interface voice VLAN configuration
Switch# show voice-vlan interfaces gi1-8
VoiceVLANAging      : 1440 minutes
VoiceVLANCoS        6
Voice VLAN 1p Remark: disabled

```

#### OUI table

```

OUI MAC      | Description
-----+-----
00:03:6B     | 3COM
00:03:6B     | Cisco

```



```

00:E0:75 | Veritel
00:D0:1E | Pingtel
00:01:E3 | Siemens
00:60:B9 |
NEC/Philips 00:0F:E2
|H3C
00:09:6E |Avaya

```

Port	State	PortMode	CosMode
gi1	Disabled	Auto	All
gi2	Disabled	Auto	All
gi3	Disabled	Auto	All
gi4	Disabled	Auto	Src
gi5	Disabled	Auto	Src
gi6	Disabled	Auto	Src
gi7	Disabled	Auto	Src
gi8	Disabled	Auto	Src

### voice-vlan mode

#### Format

```

voice-vlan mode (auto | manual)
no voice-vlan mode

```

#### Parameter

auto	The designated port is identified as a candidate port for joining the voice VLAN. When a data packet with the source OUI MAC address identifying the remote device as a voice device is seen on the port, the port connects the voice VLAN Marked port
manual	Specify to manually assign the port to the voice VLAN

#### Default

Default is auto

#### Mode

Interface configuration Mode

#### Instructions

Use the command "voice-vlan mode" to configure the voice VLAN Mode of the interface.

#### Instance

```

Configure the voice VLAN under the
interface
ModeSwitch(config)#interface range gi1-3
Switch(config-if)# voice-vlan mode manual

```

```

Query interface voice VLAN configuration
Switch# show voice-vlan interfaces gi1-8
VoiceVLANAging      : 1440 minutes
VoiceVLANCoS        6
Voice VLAN 1p Remark: disabled

```

#### OUI table

OUI	MAC	Description
00:03:6B		Cisco
00:E0:75		Veritel
00:D0:1E		Pingtel
00:01:E3		Siemens
00:60:B9		
00:0F:E2		NEC/Philips
		H3C
00:09:6E		Avaya

Port	State	PortMode	CosMode
gi1	Disabled	manual	All
gi2	Disabled	manual	All
gi3	Disabled	manual	All
gi4	Disabled	Auto	Src
gi5	Disabled	Auto	Src
gi6	Disabled	Auto	Src
gi7	Disabled	Auto	Src
gi8	Disabled	Auto	Src

### voice-vlan aging-time

#### Format

```

voice-vlan aing-time <30-65536>
no voice-vlan aing-time

```

#### Parameter

aing-time	Voice VLAN aging interval, in minutes
-----------	---------------------------------------

#### Default

The default aging time is 1440 minutes.

#### Mode

Global configuration Mode

#### Instructions

Use the command "voice vlan aging-time" to configure the voice VLAN aging interval.

**Instance**

Configure the voice VLAN aging interval  
 Switch(config)# voice-vlan aging-time 720

Query voice VLAN configuration  
 Switch# show voice-vlan  
 Administrate Voice VLAN state : disabled  
 VoiceVLANID 1  
 Voice VLAN Aging: 720 minutes  
 VoiceVLANCoS 5  
 Voice VLAN 1p Remark: enabled

**show voice-vlan****Format**

show voice-vlan  
 show voice-vlan interfaces [IF\_PORTS]

**Parameter**

interfaces	Query voice VLAN configuration by interface
------------	---

**Default****Mode**

Privileged mode

**Instructions**

Use the command "show voice-vlan" to query the voice VLAN global configuration.  
 Use the command "show voice-vlan interface" to query the voice VLAN interface configuration.

**Instance**

Query voice VLAN configuration  
 Switch# show voice-vlan  
 Administrate Voice VLAN state : disabled  
 VoiceVLANID 1  
 Voice VLAN Aging: 720 minutes  
 VoiceVLANCoS 5  
 Voice VLAN 1p Remark: enabled

Query interface voice VLAN configuration  
 Switch# show voice-vlan interfaces gi1-8  
 VoiceVLANAging : 1440 minutes  
 VoiceVLANCoS 6  
 Voice VLAN 1p Remark: disabled

## OUI table

OUI	MAC	Description
00:03:6B		Cisco
00:E0:75		Veritel
00:D0:1E		Pingtel
00:01:E3		Siemens
00:60:B9		NEC/Philips
00:0F:E2		H3C
00:09:6E		Avaya

Port	State	PortMode	CosMode
gi1	Disabled	manual	All
gi2	Disabled	manual	All
gi3	Disabled	manual	All
gi4	Disabled	Auto	Src
gi5	Disabled	Auto	Src
gi6	Disabled	Auto	Src
gi7	Disabled	Auto	Src
gi8	Disabled	Auto	Src