FIBERROAD

# Ethernet Switch
# Command Line Interface
# User Manual

## About This Manual

Introduction
This chapter describes how to use the command line to configure Fiberroad's managed Ethernet switches. Besides the web interface configuration, the command line interface helps system administrators easily and quickly manage, monitor, and configure Fiberroad's managed Ethernet switch.

Conventions
This document contains notices, figures, screen captures, and certain text conventions.

Figures and Screen Captures
This document provides figures and screen captures as examples. These examples contain sample data. This data may vary from the actual data on an installed system.

Units of Measurement
Units of measurement in this publication conform to SI standards and practices.

Jan 01, 2022
Version number: 1.0

# CONTENT

# 1
# About Command Line Interface

This chapter helps users to understand the command line interface, and demonstrates a general ideal on the command line operation.

The following topics are covered in this chapter:

## 1.1 Accessing the Switch

Users can connect to the switch using one of two method: by console or by Telnet

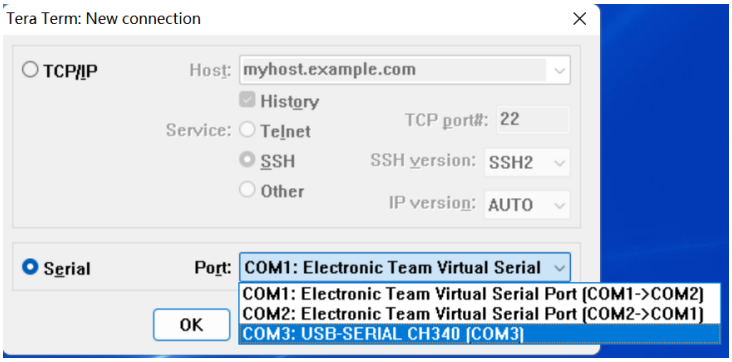
### 1.1.1 Logging in using the RS-232 Console

1, Prepare the included RS-232 serial cable with RJ45 interface

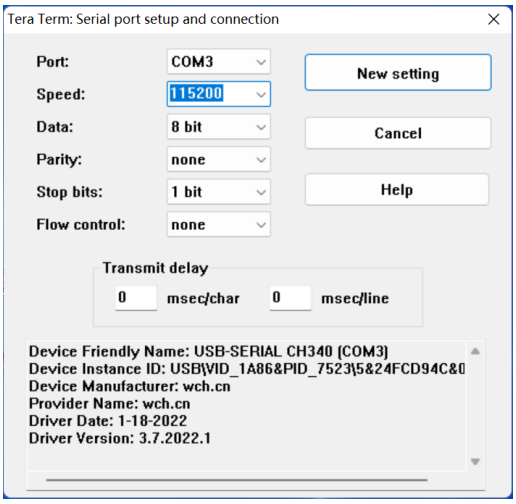
2, Connect the RJ45 interface end to the console port on the switch, and the other end to the computer.

3, Select one of the Serial Terminal Emulator. As to this manual, We utilized “Tera Term” as an example.

4, Select Serial and Connected Com Port



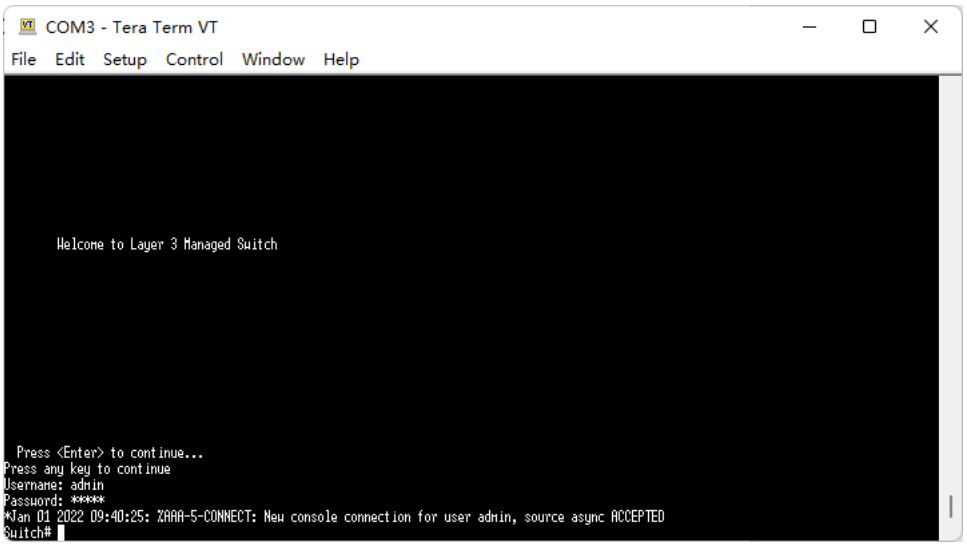

5, Click **Setup**>**Serial Port** to establish a new connection




6, On the **Serial Port Setup and connection parameter** tab, select the COM port will be used for the console connection. Configure the field as follow: **115200** for **Speed(Baud rate)**, **8 bit** for **Data**, **None** for **Parity**, and **1** for **Stop bits**.

7, Click **New setting** to return to interface

8, Log in the console using the default login name **admin** and password **admin.** This password will be required to access any of the consoles (web, serial, telnet)




9, When successfully connected to the switch, you can start configuring the switch parameters by using command line instructions.

**NOTE:** By default, the password assigned to the Fiberroad Switch is admin. We recommended changing the default password after logging in for the first time to help keep your system secure.

### 1.1.2 Logging in using Telnet

Opening the web console over a network requires that the PC host and Fiberroad switch are on the same logical subnet. You may need to adjust your PC host's IP address and subnet mask. By default, the Fiberroad switch's IP address is **192.168.1.6** and subnet mask is **255.255.255.0**. Your PC's IP address must be configured with an IP in the 192.168.1.xxx and a subnet mask 255.255.255.0.

**NOTE:** When connecting to the Fiberroad switch through Telnet or the web console, first connect one of the Fiberroad switch's Ethernet ports to your Ethernet LAN, or directly to your PC's Ethernet port. You may use either a straight-through or cross-over Ethernet cable.

After making sure that the Fiberroad switch is connected to the same LAN and logical subnet as your PC, open the Fiberroad switch's Telnet console as follows:
1, In Windows, Click Start > Run
2, In the Windows Run window, enter telnet followed by the Fiberroad Switch's IP address (192.168.1.6), You can also issue the Telnet command from a DOS prompt.

3. Log in to the Telnet console using the default login name admin and password admin. This pass will be required to access any of the console(Web, serial, telnet).

4. When success fully connected to the switch, you can start configuring the switch parameters by using command line instruction.

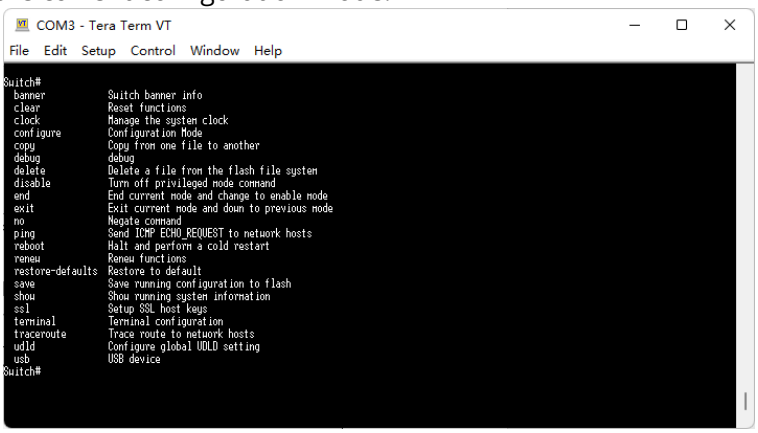
**NOTE:** By default, the password assigned to the Fiberroad Switch is admin. We recommended changing the default password after logging in for the first time to help keep your system secure.

## 1.2 Command Modes

### 1.2.1 Basic Configuration

The Command Line Interface(CLI) for Fiberroad's Managed switched can be accessed through either the serial console or the Telnet console. For either type of connection, access to the CLI is generally referred to as an EXEC session.

The CLI is organized using different configuration levels. When you first enter the CLI, type "?" to view a list of basic commands and a description of each function. Type any of commands shown on the screen to access the next configuration level. The help panel can be accessed from any configuration level by typing "?". The switch will show all the command for the current configuration mode.




### 1.2.2 Understanding All Command Modes

The Fiberroad switch's CLI supports multiple types of configuration levels for performing different functions. Refer to the following table for an overview of all available modes.

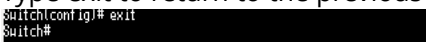
| Mode | Access Method | Prompt | Exit Method | About This Mode |
|---|---|---|---|---|
| User EXEC | Begin a new session And login as user | Switch> | Enter the exit command. This will return you to the previous configuration mode. | Use this mode to display system information. |
| Privileged EXEC | Begin a session and login as admin. | switch # | Enter the exit command. This will return you to the previous login interface. | Use this mode to verify commands that you have entered. |
| Global | Enter the configure | switch (config)# | Enter the exit | Use this mode to |

| | | | | |
|---|---|---|---|---|
| Configuration | command while in Privileged EXEC mode | | command. This will return you to the previous configuration mode. | configure parameters that will apply to the entire switch. |
| Interface Configuration | While in global configuration mode, enter the interface command, followed by an interface identification. | switch (config-if)# | Enter the exit command. This will return you to the previous configuration mode. | Use this mode to configure parameters for the specified interface. |

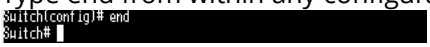
Refer to the following example of changing configuration modes below.

Type config at the command prompt to enter configuration mode.


Type exit to return to the previous configuration mode.




Type end from within any configuration level to return to privileged mode.




## 1.3 Help Messages

The CLI support several types of interactive commands. The Help commands are listed in the following table

| **Command** | **Purpose** |
|---|---|
| ? | Shows a brief description of the Help feature in any command level. |
| Partial command? | Shows a list of commands that begin with the entered character string. There should be no space between the command and the question mark. |
| Partial command<Tab> | Completes a partially entered command name. There should be no space between the command and <Tab>. |
| Command ? | Shows the keywords, arguments, or both associated with the command. There should be a space between the command and the question mark. |
| Command keyword ? | Shows the arguments that are associated with the keyword There should be a space between the command and the keyword, and between the keyword and the question mark. |

## 1.4 Special Usage and Limitations

1. If the command contains any special characters, such as *, #, and %, you need to use the quotation marks (“ ”) to cover these special characters. Refer to the

following figure for an example.

2. You may use a semicolon mark(;) to separate several commands. Refer to the figure below for an example.

## 1.5 Abbreviated Commands

1. The exclamation mark " ! " can be used to enter the global configuration mode , as shown in the example below

2. You can input one or more letters to quickly see all commands starting with these letters. For example, type c?, all commands starting with c will be shown.

3. When press tab after typing the prefix letter, the syntax of the command starting with that letter will be shown.

## 1.6 No and Default Forms of Commands

A " no " command can used to perform the "delete", "disable", or "reset to default" functions. Type "no ?" to check how parameters can be used.


## 1.7 CLI Error Messages

You may encounter some error messages while configuring Fiberroad's Ethenet switch. Refer the following table for an overview of error messages and solutions.

| Error Message | Meaning | Solution |
|---|---|---|
| % Ambiguous command | The characters you enter | Re-enter the command |

| | | |
|---|---|---|
| | insufficient for ed are the switch to recognize the command | with a space between the command and the question mark (?) . The possible keywords with the command will appear. |
| % Incomplete command | The keywords or values you enter are incomplete. | Re-enter the command with a space between the command and the question mark (?) . The possible keywords with the command will appear. |
| % Invalid input detected at '^' marker. | The command you entered is incorrect. The point of invalid input will be indicated by a caret ( ^). | Enter a question mark (?) to display all the available commands in this command mode. The possible keywords with the command will appear. |

## 1.8 Command History

Use the Up arrow and Down arrow keys to show cycle through the history of previously entered commands. Pressing the Up arrow will display the previously entered command. Pressing the Down arrow will display the next command in the history.

# 2
# Commands

## 2.1. AAA

### 2.1.1. AAA Authentication

| | | |
|---|---|---|
| **Syntax** | **aaa authentication** (**login** \| **enable**) (**default** \| *LISTNAME*) *METHODLIST* [*METHODLIST*] [*METHODLIST*] [*METHODLIST*]<br>**no aaa authentication** (**login** \| **enable**) *LISTNAME* | |
| **Parameter** | **login** | Add/Edit login authentication list |
| | **enable** | Add/Edit enable authentication list |
| | **default** | Edit default authentication list |
| | *LISTNAME* | Specify the list name for authentication type |
| | *METHODLIST* | Specify the authenticate method, including none, local, enable, tacacs+, radius. |
| **Default** | Default authentication list name for type login is “default” and default method is “local”.<br>Default authentication list name for type enable is “default” and default method is “enable” | |
| **Mode** | Global Configuration | |
| **Usage** | Login authentication is used when user try to login into the switch. Such as CLI login dialog and WEBUI login web page.<br>Enable authentication is used only on CLI for user trying to switch from User EXEC mode to Privileged EXEC mode.<br><br>Both of them support following authenticate methods.<br>**Local:** Use local user account database to authenticate. (This method is not supported for enable authentication)<br>**Enable:** Use local enable password database to authenticate.<br>**Tacacs+:** Use remote Tacas+ server to authenticate.<br>**Radius:** Use remote Radius server to authenticate.<br>**None:** Do nothing and just make user to be authenticated. | |

| | |
|---|---|
| **Usage** | Each list allows you to combine these methods with different orders. For example, we want to authenticate login user with remote Tacacs+ server, but server may be crashed. Therefore, we need a backup plan, such as another Radius server. So we can configure the list with Tacacs+ server as first authentication method and Radius server as second one.<br><br>Use no form to delete the existing list. However, "default" list is not allowed to remove. |
| **Example** | This example shows how to add a login authentication list to authenticate with order tacacs+, radius, local.<br>Switch(config)# **aaa authentication login test1 tacacs+ radius local**<br><br>This example shows how to show existing login authentication lists<br>Switch# **show aaa authentication login lists**<br>Login List Name \| Authentication Method List<br>----------+----------<br>default \| local<br>test1 \| tacacs+ radius local<br><br>This example shows how to add an enable authentication list to authenticate with order tacacs+, radius, enable.<br>Switch(config)# **aaa authentication enable test1 tacacs+ radius enable**<br><br>This example shows how to show existing enable authentication lists<br>Switch# **show aaa authentication login lists**<br>Enable List Name \| Authentication Method List<br>----------+----------<br>default \| enable<br>test2 \| tacacs+ radius enable |

### 2.1.2 login authentication

| | | |
|---|---|---|
| **Syntax** | **login authentication** *LISTNAME*<br>**no login authentication** | |
| **Parameter** | *LISTNAME* | Specify the login authentication list name to use. |
| **Default** | Default login authentication list for each line is "default". | |
| **Mode** | Line Configuration | |

| | |
|---|---|
| **Usage** | Different access methods are allowed to bind different login authentication lists. Use “login authentication” command to bind the list to specific line (console, telnet, ssh).<br>Use no form to bind the “default” list back. |
| **Example** | This example shows how to create a new login authentication list and bind to telnet line.<br>Switch(config)# **aaa authentication login test1** |

**tacacs+ radius local**
Switch(config)# **line telnet**
Switch(config-line)# **login authentication test1**

This example shows how to show line binding lists.
Switch# **show line lists**

```
Line Type    |     AAA Type       |     List Name
-------------+------------------+-----------------
console      |     login         | default
             |     enable        | default
telnet       |     login         | test1
             |     enable        | default
ssh          |     login         | default
             |     enable        | default http
             |     login         | default
https        |     login         | default
```

### 2.1.3 ip http login authentication

| | | |
|---|---|---|
| **Syntax** | **ip** (**http** \| **https**) **login authentication** *LISTNAME*<br>**no ip** (**http** \| **https**) **login authentication** | |
| | **http** | Bind login authentication list to user access WEBUI with http protocol |
| | **https** | Bind login authentication list to user access WEBUI with https protocol |
| | *LISTNAME* | Specify the login authentication list name to use. |
| **Default** | Default login authentication list for each line is “default”. | |
| **Mode** | Global Configuration | |

| | |
|---|---|
| **Usage** | Different access methods are allowed to bind different login authentication lists. Use "**ip** (**http** \| **https**) **login authentication**" command to bind the list to WEBUI access from http or https.<br><br>Use no form to bind the "default" list back. |
| **Example** | This example shows how to create two new login authentication lists and bind to http and https.<br>Switch(config)# **aaa authentication login test1 tacacs+ radius local**<br>Switch(config)# **aaa authentication login test2 radius local**<br>Switch(config)# **ip http login authentication test1**<br>Switch(config)# **ip https login authentication test2**<br><br>This example shows how to show line binding lists.<br>Switch# **show line lists**<br>Line Type \| AAA Type \| List Name<br>----------+----------+----------<br>console \| login \| default<br>\| enable \| default<br>telnet \| login \| default<br>\| enable \| default<br>ssh \| login \| default<br>\| enable \| default<br>http \| login \| test1<br>https \| login \| test2 |

### 2.1.4 enable authentication

| | |
|---|---|
| **Syntax** | **enable authentication** LISTNAME<br>**no enable authentication** |
| **Parameter** | LISTNAME Specify the enable authentication list name to use. |
| **Mode** | Line Configuration |
| **Usage** | Different access methods are allowed to bind different enable authentication lists. Use "**enable authentication**" command to bind the list to specific line (console, telnet, ssh).<br><br>Use no form to bind the "default" list back. |

**Example** This example shows how to create a new enable authentication list and bind to telnet line.

Switch(config)# **aaa authentication enable test1 tacacs+ radius enable**
Switch(config)# **line telnet**
Switch(config-line)# **enable authentication test1**

This example shows how to show line binding lists.

Switch# **show line lists**

| Line Type | AAA Type | List Name |
|---|---|---|
| console | login | default |
| | enable | default |
| telnet | login | default |
| | enable | test1 |
| ssh | login | default |
| | enable | default |
| http | login | default |
| https | login | default |

### 2.1.5 show aaa authentication

**Syntax** show aaa authentication (login | enable) lists

**Parameter** **login** Show login authentication list
**enable** Show enable authentication list

**Default** No default value for this command

**Mode** Privileged EXEC

**Usage** Use "**show aaa authentication**" command to show login authentication or enable authentication method lists.

**Example** This example shows how to show existing login authentication lists

Switch# **show aaa authentication login lists**

```
Login List Name   | Authentication Method List
------------------------+------------------------------
        default   | local
        test1     | tacacs+      radius    local
```

This example shows how to show existing enable authentication lists

Switch# **show aaa authentication login lists**

```
Enable List Name | Authentication Method List
------------------------+------------------------------
        default   | enable
        test2     | tacacs+      radius    enable
```

### 2.1.6 show line lists

| | |
|---|---|
| **Syntax** | show line lists |
| **Parameter** | |
| **Default** | No default value for this command |
| **Mode** | Privileged EXEC |
| **Usage** | Use "**show line lists**" command to show all lines' binding list of all authentication, authorization, and accounting function. |
| **Example** | This example shows how to show line binding lists.<br>Switch# **show line lists**<br>Line Type \| AAA Type \| List Name<br>----------+----------+----------<br>Console \| login \| default<br>\| enable \| default<br>\| exec \| default<br>\| commands \| default<br>\| accounting-exec \| default<br>telnet \| login \| default<br>\| enable \| default<br>\| exec \| default<br>\| commands \| default<br>\| accounting-exec \| default<br>ssh \| login \| default<br>\| enable \| default<br>\| exec \| default<br>\| commands \| default<br>\| accounting-exec \| default<br>http \| login \| default<br>https \| login \| default |

### 2.1.7 tacacs default-config

| | |
|---|---|
| **Syntax** | tacacs default-config [key TACACSKEY] [timeout <1-30>] |
| **Parameter** | **key** TACACSKEY Specify default tacacs+ server key string<br>**timeout** <1-30> Specify default tacacs+ server timeout value |
| **Default** | Default tacacs+ key is "".<br>Default tacacs+ timeout is 5 seconds. |

| | |
|---|---|
| **Mode** | Global Configuration |
| **Usage** | Use "**tacacs default-config**" command to modify default values of tacacs+ server. These default values will be used when user try to create a new tacacs+ server and not assigned these values. |
| **Example** | This example shows how modify default tacacs+ configuration<br>Switch(config)# **tacacs default-config timeout 20**<br>Switch(config)# **tacacs default-config key tackey** |

This example shows how to show default tacacs+ configurations.

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

This example shows how to create a new tacacs+ server with above default config and show 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
```

### 2.1.8 tacacs host

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

| **Parameter** | | |
|---|---|---|
| | **host** HOSTNAME | Specify tacacs+ server host name, both IP address and domain name are available. |
| | **port** <0-65535> | Specify tacacs+ server udp port |
| | **key** TACPLUSKEY | Specify tacacs+ server key string |
| | **priority** <0-65535> | Specify tacacs+ server priority |
| | **timeout** <1-30> | Specify tacacs+ server timeout value |

| | |
|---|---|
| **Default** | Default tacacs+ key is "".<br>Default tacacs+ timeout is 5 seconds. |
| **Mode** | Global Configuration |
| **Usage** | Use "tacacs host" command to add or edit tacacs+ server for authentication, authorization or accounting. |

Use no form to delete one or all tacacs+ servers from database.

**Example** This example shows how to create a new tacacs+ server
Switch(config)# **tacacs host 192.168.1.111 port 12345 key tacacs+ priority 100 timeout 10**

This example shows how to show existing tacacs+ server.
Switch# **show tacacs**

```
< 192.168,1,111 port 12345 key tacacs+ priority 100 timeout 10
IPv6 address and gateway must in the same subnet
< 192.168.1.111 port 12345 key tacacs+ priority 100 timeout 10
Switch(config)# show tacacs
 Prio | Timeout |     IP Address     | Port  |   Key
------+---------+--------------------+-------+---------
  100 |     10  |     192.168.1.111  | 12345 | tacacs+
Switch(config)#
```

### 2.1.9 show tacacs default-config

**Syntax** show tacacs default-config

**Parameter**

**Default** No default value for this command

**Usage** Use "**show tacacs default-config**" command to show tacacs+ default configurations**.**

**Example** This example shows how to show default tacacs+ configurations.
Switch# **show tacacs default-config**

```
Switch# show tacacs default-config
 Timeout |   Key
---------+--------
     5   |
```

### 2.1.10 show tacacs

**Syntax** show tacacs

**Parameter**

**Default** No default value for this command

**Mode** Privileged EXEC

**Usage** Use "**show tacacs**" command to show existing tacacs+ servers.

**Example** This example shows how to show existing tacacs+ server.

Switch# **show tacacs**

```
Switch# show tacacs
 Prio | Timeout |     IP Address     | Port  |   Key
------+---------+--------------------+-------+---------
  100 |    10   |    192.168.1.111   | 12345 | tacacs+
```

## 2.1.11 show default-config

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

**Parameter** **key** RADIUSKEY Specify default radius server key string
**retransmit** <1-10> Specify default radius server retransmit value
**timeout** <1-30> Specify default radius server timeout value

**Default** Default radius key is “”.
Default radius retransmit is 3 times.
Default radius timeout is 3 second

**Mode** Global Configuration

**Usage** Use “radius default-config” command to modify default values of radius server. These default values will be used when user try to create a new radius server and not assigned these values.

**Example** This example shows how modify default radius configuration
Switch(config)# **radius default-config timeout 20**
Switch(config)# **radius default-config key radiuskey**
Switch(config)# **radius default-config retransmit 5**

This example shows how to show default radius configurations.
**Switch# show radius default-config**

```
Switch# show radius default-config
 Retries| Timeout|   Key
--------+--------+---------
    5   |   20   | radiuskey
```

This example shows how to create a new radius server with above default config and show results.

Switch(config)# **radius host 192.168.1.111**
Switch# **show radius**

```
Switch(config)# radius host 192.168.1.111
Switch(config)# show radius
 Prio |   IP Address    | Auth-Port| Retries| Timeout|    Type   |   Key
------+-----------------+----------+--------+--------+-----------+---------
   1  | 192.168.1.111   |   1812   |   5    |   20   |    All    | radiuskey
```

## 2.1.12 radius host

**Syntax**

**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** HOSTNAME | Specify radius server host name, both IP address and domain name are available. |
| **auth-port** <0-65535> | Specify radius server udp port |
| **key** RADIUSKEY | Specify radius server key string |
| **Priority** <0-65535> | Specify radius server priority |
| **retransmit** <1-10> | Specify radius server retransmit times |
| **timeout** <1-30> | Specify radius server timeout value |
| **type login 802.1X all** | Usage type of this server Use for login Use for 802.1X authentication Use for both login and 802.1X authentication |

**Default**

Default radius key is “”.
Default radius timeout is 3 seconds.

**Mode**

Global Configuration

**Usage**

Use “radius host” command to add or edit an existing radius server.

Use no form to delete one or all radius servers from database.

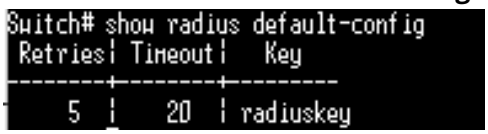
**Example**

This example shows how to create 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**

This example shows how to show existing radius server.
**Switch# show radius**

```
Switch# configure
th-port 12345 key radiuskey priority 100 retransmit 5 timeout 10 type all
Switch(config)# exit
Switch# show radius
 Prio |   IP Address    | Auth-Port| Retries| Timeout|   Type   |   Key
------+-----------------+----------+--------+--------+----------+---------
  100 |  192.168.1.111 |  12345   |   5    |   10   |    All   | radiuskey
```

### 2.1.13 show radius default-config

| | |
|---|---|
| **Syntax** | show radius default-config |
| **Parameter** | |
| **Default** | No default value for this command |
| **Usage** | Use "**show radius default-config**" command to show radius default configurations. |
| **Example** | This example shows how to show default radius configurations.<br>Switch# **show radius default-config**<br>  |

```
Switch# show radius default-config
 Retries| Timeout|   Key
--------+--------+--------
     5  |    20  | radiuskey
```

### 2.1.14 show radius

| | |
|---|---|
| **Syntax** | **show radius** |
| **Parameter** | |
| **Default** | No default value for this command |
| **Mode** | Privileged EXEC |
| **Usage** | Use "show radius" command to show existing radius servers. |
| **Example** | This example shows how to show existing radius server.<br>Switch# **show radius**<br>  |

```
Switch# show radius
 Prio |   IP Address    | Auth-Port| Retries| Timeout|   Type   |   Key
------+-----------------+----------+--------+--------+----------+--------
  100 |  192.168.1.111  |  12345   |   5    |   10   |   All    | radiuskey
```

## 2.2 ACL

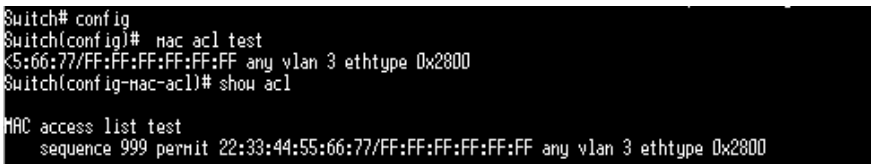
### 2.2.1 mac acl

| | |
|---|---|
| **Syntax** | **mac acl NAME no mac acl NAME** |
| **Parameter** | NAME Specify the name of MAC ACL |
| **Default** | No default value for this command |
| **Mode** | Global Configuration |
| **Usage** | Use the **mac acl** command to create a MAC access list and to enter mac-acl configuration mode. The name of ACL must be unique that can not have same name with other ACL or QoS policy. Once an ACL is created, an implicit “deny any” ACE created at the end of the ACL. That is, if there are no matches, the packets are denied. Use the no form of this command to delete. |
| **Example** | The example shows how to create a mac acl. You can verify settings by the following show acl command<br><br>Switch334455(config)# **mac acl test**<br>Switch334455(mac-al)# **show acl**<br>Switch(config-mac-acl)# show acl<br><br>MAC access list test |

### 2.2.2 permit (MAC)

| | | |
|---|---|---|
| **Syntax** | [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>] [ethtype <0x0600-0xFFFF>] no sequence <1-2147483647> | |
| **Parameter** | **<1-2147483647>** | (Optional) Specify sequence index of ACE, the sequence index represent the priority of an ACE in ACL. |
| | **(A:B:C:D:E:F/A:B:C:D:E:F\|any)** | Specify the source MAC address and mask of packet or any MAC address. |
| | **(A:B:C:D:E:F/A:B:C:D:E:F\|any)** | Specify the destination MAC address and mask of packet or any MAC address |
| | **[vlan <1-4094>]** | (Optional) Specify the vlan ID of packet. |
| | **[cos <0-7> <0-7>]** | (Optional) Specify the Class of Service value and mask of packet. |
| | **[ethtype <0x0600-0xFFFF>]** | (Optional) Specify Ethernet protocol number of packet |
| **Default** | No default value for this command | |
| **Mode** | MAC ACL Configuration | |
| **Usage** | Use the permit command to add permit conditions for a mac ACE that bypass those packets hit the ACE. The "**sequence**" also represents hit priority when ACL bind to an interface. An ACE not specifies "sequence" index would assign a sequence index which is the largest existed index plus 20. If packet content can match more than one ACE, the lowest sequence ACE is hit. An ACE can not be added if has the same conditions as existed ACE. | |
| **Example** | The example shows how to add an ACE that permit packets with source MAC address 22:33:44:55:66:77 、 VLAN 3 and Ethernet type 1999. You can verify settings by the following **show acl** command<br><br>Switch3(config)# **mac acl test**<br>Switch(mac-al)# **sequence 999 permit** | |

**22:33:44:55:66:77/FF:FF:FF:FF:FF:FF any vlan 3 ethtype 0x2800**
Switch(mac-al)# **show acl**



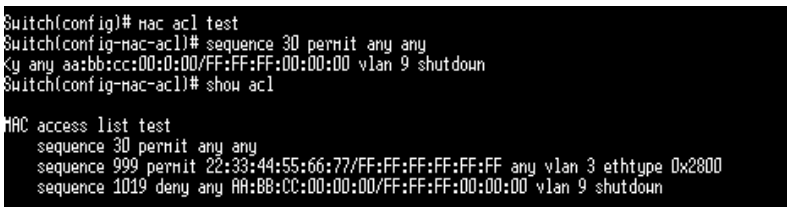

### 2.2.3 deny(MAC)

| | |
|---|---|
| **Syntax** | [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**

| | |
|---|---|
| **<1-2147483647>** | (Optional) Specify sequence index of ACE, the sequence index represent the priority of an ACE in ACL. |
| **(A:B:C:D:E:F/A:B:C:D:E:F\|any)** | Specify the source MAC address and mask of packet or any MAC address. |
| **(A:B:C:D:E:F/A:B:C:D:E:F\|any)** | Specify the destination MAC address and mask of packet or any MAC address. |
| **[vlan <1-4094>]** | (Optional) Specify the vlan ID of packet. |
| **[cos <0-7> <0-7>]** | (Optional) Specify the Class of Service value and mask of packet. |
| **[ethtype <0x0600-0xFFFF>]** | (Optional) Specify Ethernet protocol number of packet |
| **[shutdown]** | (Optional) Shutdown interface while ACE hit |

| | |
|---|---|
| **Default** | No default value for this command |
| **Mode** | MAC ACL Configuration |
| **Usage** | Use the deny command to add deny conditions for a mac ACE that drop those packets hit the ACE. The “sequence” also represents hit priority when ACL bind to an interface. An ACE not specifies |

| | |
|---|---|
| | "sequence" index would assign a sequence index which is the largest existed index plus 20. If packet content can match more than one ACE, the lowest sequence ACE is hit. An ACE cannot be added if has the same conditions as existed ACE. Use "shutdown" to shutdown interface while ACE hit. |
| **Example** | The example shows how to add an ACE that denies packets with destination MAC address aa:bb:cc:xx:xx:xx and VLAN 9. You can verify settings by the following **show acl** command<br><br>Switch(config)# **mac acl test**<br>Switch(mac-al)# **sequence 30 permit any any**<br>Switch(mac-al)# **deny any aa:bb:cc:00:0:00/FF:FF:FF:00:00:00 vlan 9 shutdown**<br>Switch(mac-al)# **show acl**<br>  <br>`Switch(config)# mac acl test`<br>`Switch(config-mac-acl)# sequence 30 permit any any`<br>`ky any aa:bb:cc:00:0:00/FF:FF:FF:00:00:00 vlan 9 shutdown`<br>`Switch(config-mac-acl)# show acl`<br><br>`MAC access list test`<br>`sequence 30 permit any any`<br>`sequence 999 permit 22:33:44:55:66:77/FF:FF:FF:FF:FF:FF any vlan 3 ethtype 0x2800`<br>`sequence 1019 deny any AA:BB:CC:00:00:00/FF:FF:FF:00:00:00 vlan 9 shutdown` |

### 2.2.4 ip acl

| | |
|---|---|
| **Syntax** | **ip acl NAME no ip acl NAME** |
| **Parameter** | NAME Specify the name of IPv4 ACL |
| **Default** | No default value for this command |
| **Mode** | Global Configuration |
| **Usage** | Use the **ip acl** command to create an IPv4 access list and to enter ip-acl configuration mode. The name of ACL must be unique that can not have same name with other ACL or QoS policy. Once an ACL is created, an implicit "deny any" ACE created at the end of the ACL. That is, if there are no matches, the packets are denied. Use the no form of this command to delete. |
| **Example** | The example shows how to create an IP ACL. You can verify settings by the following show acl command<br><br>Switch(config)#**ip acl iptest**<br>Switch(ip-al)# **show acl**<br>  <br>`Switch(config)# ip acl iptest`<br>`Switch(config-ip-acl)# show acl`<br><br>`IP access list iptest` |

### 2.2.5 permit(IP)

**Syntax**

[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_RANGE|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** | **<1-2147483647>** | (Optional) Specify sequence index of ACE, the sequence index represent the |

priority of an ACE in ACL.

| | |
|---|---|
| **(A.B.C.D/A.B.C.D\|any)** | Specify the source IPv4 address and mask of packet or any IPv4 address. |
| **(A.B.C.D/A.B.C.D\|any)** | Specify the destination IPv4 address and mask of packet or any IPv4 address. |
| **[dscp VALUE]** | (Optional) Specify the DSCP of packet. |
| **[precedence VLAUE]** | (Optional) Specify the IP precedence of packet. |
| **icmp-type** | Specify ICMP message type for filtering ICMP packet. Enter a type name of list or a number of ICMP message type. |
| **icmp-code** | Specify ICMP message code for filtering ICMP packet. |
| **l4-source-port** | Specify TCP/UDP source port of for filtering TCP/UDP packet. Enter a port name of list or a number of TCP/UDP port. |
| **l4-destination-port** | Specify TCP/UDP destination port of for filtering TCP/UDP packet. Enter a port name of list or a number of TCP/UDP port. |
| **match-all** | Specify tcp flag for TCP packet. If a flag should be set it is prefixed by\"+\".If a flag should be unset it is prefixed by \"-\". Available optionsare +urg, +ack, +psh, +rst, +syn, +fin, -urg, -ack, -psh, -rst, -syn and -fin.To define more than 1 flag - enter additional flags one after another without a space (example +syn-ack) |

**Default** No default value for this command

**Mode** IP ACL Configuration

**Usage**

Use the permit command to add permit conditions for an IP ACE that bypasses those packets hit the ACE. The "**sequence**" also represents hit priority when ACL bind to an interface. An ACE not specifies "**sequence**" index would assign a sequence index which is the largest existed index plus 20. If packet content can match more than one ACE, the lowest sequence ACE is hit. An ACE can not be added if has the same conditions as existed ACE.

**Example**

The example shows how to add a set of ACEs. You can verify settings by the following **show acl** command.

This command shows how to permit a source IP address subnet.
Switch(ip-al)# **permit ip 192.168.1.0/255.255.255.0**

This command shows how to permit ICMP echo-request packet with any IP address.
Switch(ip-al)# **permit icmp any any echo-request any**

This command shows how to permit any IP address HTTP packets with DSCP 5.
Switch (ip-al)# **permit tcp any any any www dscp 5**

This command shows how to permit any source IP address SNMP packet connect to 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

### 2.2.6 deny(IP)

**Syntax**

[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]] [shutdown]

[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] [shutdown]

[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_RANGE|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|drip|PORT_RANGE|any) [match-all TCP_FLAG] [(dscp|precedence) VALUE] [shutdown]

[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] [shutdown]

no sequence <1-2147483647>

| | | |
|---|---|---|
| **Parameter** | **<1-2147483647>** | (Optional) Specify sequence index of ACE, the sequence index represent the priority of an ACE in ACL**.** |

| | |
|---|---|
| **(A.B.C.D/A.B.C.D\|any)** | Specify the source IPv4 address and mask of packet or any IPv4 address. |
| **(A.B.C.D/A.B.C.D\|any)** | Specify the destination IPv4 address |
| **[dscp VALUE]** | (Optional) Specify the DSCP of packet. |
| **[precedence VLAUE]** | (Optional) Specify the IP precedence of packet. |
| **icmp-type** | Specify ICMP message type for filtering ICMP packet. Enter a type name of list or a number of ICMP message type. |
| **icmp-code** | Specify ICMP message code for filtering ICMP packet. |
| **l4-source-port** | Specify TCP/UDP source port of for filtering TCP/UDP packet. Enter a port name of list or a number of TCP/UDP port. |
| **l4-destination-port** | Specify TCP/UDP destination port of for filtering TCP/UDP packet. Enter a port name of list or a number of TCP/UDP port. |
| **match-all** | Specify tcp flag for TCP packet. If a flag should be set it is prefixed by \"+\".If a flag should be unset it is prefixed by \"-\". Available options are +urg, +ack, +psh, +rst, +syn, +fin,-urg, -ack, -psh, -rst, -syn and -fin.To define more than 1 flag - enter additional flags one after another without a space (example +syn-ack). |
| **[shutdown]** | (Optional) Shutdown interface while ACE hit |

**Default** No default value for this command

**Mode** IP ACL Configuration

**Usage** Use the deny command to add deny conditions foran IP ACE that drop those packets hit the ACE. The “sequence” also represents hit priority when ACL bind to an interface. An ACE not specifies “sequence” index would assign a sequence index which is the largest existed index plus 20. If packet content can match more than one ACE, the lowest sequence ACE is hit. An ACE can not be added if has the same conditions as existed ACE. Use “shutdown” to shutdown interface while ACE hit.

**Example** The example shows how to add an ACE that denies packets with source IP address 192.168.1.80. You can verify settings by the following show acl command

Switch(config)# ip acl iptest
Switch(ip-al)# deny ip 192.168.1.80/255.255.255.255 any

Switch(ip-al)# show acl

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

IP access list iptest
    sequence 1 deny ip 192.168.1.80/255.255.255.255 any

Switch(config)#
```

### 2.2.7 ipv6 acl

| | |
|---|---|
| **Syntax** | **ipv6 acl NAME**<br>**no ipv6 acl NAME** |
| **Parameter** | NAME Specify the name of IPv6 ACL |
| **Default** | No default value for this command |
| **Mode** | Global Configuration |
| **Usage** | Use the **ipv6 acl** command to create an IPv6 access list and to enter ipv6-acl configuration mode. The name of ACL must be unique that can not have same name with other ACL or QoS policy. Once an ACL is created, an implicit “deny any” ACE created at the end of the ACL. That is, if there are no matches, the packets are denied. Use the no form of this command to delete. |

**Example** The example shows how to create an IPv6 ACL. You can verify settings by the following show acl command

Switch(config)#ipv6 acl ipv6test
Switch(ipv6-al)# show acl

```
Switch# config
Switch(config)# ipv6 acl ipv6test
Switch(config-ipv6-acl)# show acl

IPv6 access list ipv6test
```

### 2.2.8 permit(IPv6)

**Syntax**

[sequence <1-2147483647>] permit (<0-255>|ipv6) (X:X::X:X/<0-128>|any) (X:X::X:X/<0-128>|any) [(dscp|precedence) VALUE]

[sequence <1-2147483647>] permit 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>] permit 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_RANGE|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|an
y) [match-all TCP_FLAG] [(dscp|precedence) VALUE]

[sequence <1-2147483647>] permit 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]

no sequence <1-2147483647>

**Parameter**

| | |
|---|---|
| **<1-2147483647>** | (Optional) Specify sequence index of ACE, the sequence index represent the priority of an ACE in ACL. |
| **(X:X::X:X/<0-128>|any)** | Specify the source IPv6 address and prefix of packet or any IPv6 address. |
| **(X:X::X:X/<0-128>|any)** | Specify the destination IPv6 address and prefix of packet or any IPv6 address. |

| | | |
|---|---|---|
| | **[dscp VALUE]** | (Optional) Specify the DSCP of packet. |
| | **[precedence VLAUE]** | (Optional) Specify the IP precedence of packet. |
| | **icmp-type** | Specify ICMP message type for filtering ICMP packet. Enter a type name of list or a number of ICMP message type. |
| | **icmp-code** | Specify ICMP message code for filtering ICMP packet. |
| | **l4-source-port** | Specify TCP/UDP source port of for filtering TCP/UDP packet. Enter a port name of list or a number of TCP/UDP port. |
| | **l4-destination-port** | Specify TCP/UDP destination port of for filtering TCP/UDP packet. Enter a port name of list or a number of TCP/UDP port. |
| | **Match-all** | Specify tcp flag for TCP packet. If a flag should be set it is prefixed by \"+\".If a flag should be unset it is prefixed by \"-\". Available options are +urg, +ack, +psh, +rst, +syn, +fin, -urg, -ack, -psh, -rst, -syn and -fin.To define more than 1 flag - enter additional flags one after another without a space (example +syn-ack). |

| | |
|---|---|
| **Default** | No default value for this command |
| **Mode** | IPv6 ACL Configuration |
| **Usage** | Use the permit command to add permit conditions for an IPv6 ACE that bypasses those packets hit the ACE. The “sequence” also represents hit priority when ACL bind to an interface. An ACE not specifies “**sequence**” index would assign a sequence index which is the largest existed index plus 20. If packet content can match more than one ACE, the lowest sequence ACE is hit. An ACE can not be added if has the same conditions as existed ACE. |
| **Example** | The example shows how to add a set of ACEs. You can verify settings by the following **show acl** command.<br><br>This command shows how to permit a source IP address 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

### 2.2.9 deny(IPv6)

**Syntax**

[sequence <1-2147483647>] deny (<0-255>|ipv6) (X:X::X:X/<0-128>|any) (X:X::X:X/<0-128>|any) [(dscp|precedence) VALUE] [shutdown]

[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] [shutdown]

[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_RANGE|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] [shutdown]

[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** | **<1-2147483647>** | (Optional) Specify sequence index of ACE, the sequence index represent the priority of an ACE in ACL. |
| | **(A.B.C.D/A.B.C.D\| any)** | Specify the source IPv4 address and mask of packet or any IPv4 address. |
| | **(A.B.C.D/A.B.C.D\| any)** | Specify the destination IPv4 address and mask of packet or any IPv4 |
| | **[dscp VALUE]** | (Optional) Specify the DSCP of packet. |
| | **[precedenc VLAUE]** | (Optional) Specify the IP precedence of packet. |
| | **icmp-type** | Specify ICMP message type for filtering ICMP packet. Enter a type name of list or a number of ICMP message type. |
| | **icmp-code** | Specify ICMP message code for filtering ICMP packet. |
| | **l4-source-port** | Specify TCP/UDP source port of for filtering TCP/UDP packet. Enter a port name of list or a number of TCP/UDP port. |
| | **l4-destination-port** | Specify TCP/UDP destination port of for filtering TCP/UDP packet. Enter a port name of list or a number of TCP/UDP port. |
| | **match-all** | Specify tcp flag for TCP packet. If a flag should be set it is prefixed by \"+\".If a flag should be unset it is prefixed by \"-\". Available options are +urg, +ack, +psh, +rst, +syn, +fin, -urg, -ack, -psh, -rst, -syn and -fin.To define more than 1 flag - enter additional flags one after another without a space (example +syn-ack). |
| | **[shutdown]** | (Optional) Shutdown interface while ACE hit |
| **Default** | No default value for this command | |
| **Mode** | IP ACL Configuration | |
| **Usage** | Use the deny command to add deny conditions for an IPv6 ACE that drop those packets hit the ACE. The “sequence” also represents hit priority when ACL bind to an interface. An ACE not specifies “sequence” index would assign a sequence index which is the largest | |

existed index plus 20. If packet content can match more than one ACE, the lowest sequence ACE is hit. An ACE can not be added if has the same conditions as existed ACE. Use “shutdown” to shutdown interface while ACE hit.

**Example**

The example shows how to add an ACE that denies packets with destination IP address fe80::abcd. You can verify settings by the following show acl command

Switch(config)# **ipv6 acl ipv6test**
Switch3(ip-al)# **deny**
**ipv6 any fe80::abcd/128 Switch334455(ip-al)**
Switch3(ip-al)# **show acl**

IPv6 access list ipv6test
sequence 1 deny ipv6 any fe80::abcd/128

### 2.2.10 bind acl

**Syntax**

**(mac|ip|ipv6) acl NAME [no] (mac|ip|ipv6) acl NAME**

**Parameter**

(mac|ip|ipv6)Specify a type of ACL to binding to interface
NAME Specify the name of ACL

**Default**

No default value for this command

**Mode**

Interface Configuration

**Usage**

Use the **(mac|ip|ipv6) acl NAME** command to bind an ACL to interfaces. An interface can bind only one ACL or QoS policy. Use the no form of this command to return to unbind an ACL from interface.

**Example**

The example shows how to bind an existed ACL to interface.

switch(config)# **interface fa1**
switch(config-if)# **mac acl test**
switch(config-if)# **do show running-config interfaces fa1**

```
Switch(config)# interface GigabitEthernet 1
Switch(config-if-GigabitEthernet1)# mac acl test
K# do show running-config interfaces GigabitEthernet 1
interface gi1
 mac acl "test"
```

### 2.2.11 show acl

| | |
|---|---|
| **Syntax** | **show acl**<br>**show (mac\|ip\|ipv6) acl**<br>**show (mac\|ip\|ipv6) acl NAME** |
| **Parameter** | (mac\|ip\|ipv6)Specify a type of ACL to show<br>NAME Specify the name of ACL |
| **Default** | No default value for this command |
| **Mode** | Global<br>Configuration<br>Context<br>Configuration |
| **Usage** | Use the show acl command to show created ACLs. You can specify mac、ip or ipv6 to show specific type ACL or specify unique name string to show ACL with the name |
| **Example** | The example shows how to show all IP ACL.<br>`Switch(config)# show ip acl`<br><br>IP access list iptest<br>sequence 1 deny ip 192.168.1.80/255.255.255.255 any |

### 2.2.12 show acl utilization

| | |
|---|---|
| **Syntax** | **show acl utilization** |
| **Parameter** | None |
| **Default** | No default value for this command |
| **Mode** | Global Configuration |
| **Usage** | Use the **show acl utilization** command to show the usage of PIE of ASIC. When an ACL bind to interface, it needs ASIC resource to help to filter packet. An ASIC has limited resource. This command help user to know the PIE usage of AISC. |
| **Example** | The example shows how to show utilization<br><br>`Switch(config-if)# do show acl utilization` |

| | |
|---|---|
| | Type: sys usage: 128<br>Type: mac ACL usage: 128<br>Type: IPv4 ACL usage: 128<br>Type: IPv6 ACL usage: 128 |

## 2.3 Administration

### 2.3.1 Configure

| | |
|---|---|
| **Syntax** | **configure** |
| **Parameter** | None |
| **Default** | No default value for this command |
| **Mode** | Privileged EXEC |
| **Usage** | Use "**configure**" command to enter global configuration mode. In global configuration mode, the prompt will show as "**Switch(config)#**". |
| **Example** | This example shows how to enter global configuration mode.<br>Switch# **configure**<br>Switch(config)# |

### 2.3.2 clear arp

| | |
|---|---|
| **Syntax** | **clear arp [A.B.C.D]** |
| **Parameter** | A.B.C.D Specify specific arp entry to clear. |
| **Default** | No default value for this command |
| **Mode** | User EXEC<br>Privileged EXEC |
| **Usage** | Use "clear arp" command to clear all or specific one arp entry. |
| **Example** | This example shows how to clear all arp entries.<br>Switch(config)# clear arp |

### 2.3.3 clear service

| | |
|---|---|
| **Syntax** | **clear (telnet \| ssh)** |
| **Parameter** | **telnet** Clear all telnet sessions.<br>**ssh** Clear all ssh sessions. |
| **Default** | No default value for this command |
| **Mode** | Privileged EXEC |
| **Usage** | Use "**clear service**" command to kill all existing sessions for the select service. |
| **Example** | This example shows how to enable telnet service and show current telnet service status.<br>Switch# clear telnet |

### 2.3.4 enable

| | |
|---|---|
| **Syntax** | **enable [<1-15>]**<br>**disable [<1-14>]** |
| **Parameter** | <1-15> Specify privileged level to enable<br><1-14>Specify privileged level to disable |
| **Default** | Default privilege level is 15 if no privilege level is specified on enable command.<br>Default privilege level is 1 if no privilege level is specified on disable command. |
| **Mode** | User EXEC |
| **Usage** | In User EXEC mode, user only allows to do a few actions. Most of commands are only available in privileged EXEC mode. Use "**enable**" command to enter the privileged mode to do more actions on switch.<br><br>In privileged EXEC mode, use "exit" command is able to go back to user EXEC mode with original user privilege level. If you need to go back to user EXEC mode with different privilege level, use "**disable**" command to specify the privilege level you need. |

| | |
|---|---|
| | In privileged EXEC mode, the prompt will show "**Switch**#" |
| **Example** | This example shows how to enter privileged EXEC mode and show current privilege level.<br>Switch> enable<br>Switch# show privilege<br>  <br>This example show how to enter user EXEC mode with privilege 3.<br>Switch# disable 3<br>Switch> show privilege Current CLI Username:<br>Current CLI Privilege: 3 |



### 2.3.5 end

| | |
|---|---|
| **Syntax** | **end** |
| **Parameter** | None |
| **Default** | No default value for this command. |
| **Mode** | Privileged EXEC<br>Global<br>Configuration<br>Interface<br>Configuration Line<br>Configuration<br>..... |
| **Usage** | Use "end" command to return to privileged EXEC mode directly. Every mode except User EXEC mode has the "end" command. |
| **Example** | This example shows how to enter Interface Configuration mode and use end command to go back to privileged EXEC mode<br>Switch# configure<br>Switch(config)# interface fa1<br>Switch(config-if)# end<br>Switch# |

### 2.3.6 exit

| | |
|---|---|
| **Syntax** | **exit** |
| **Parameter** | None |
| **Default** | No default value for this command. |
| **Mode** | User EXEC<br>Privileged EXEC<br>Global Configuration<br>Interface<br>Configuration Line<br>Configuration<br>……. |
| **Usage** | In User EXEC mode, "**exit**" command will close current CLI session. In other modes, "**exit"** command will go to the parent mode. And every mode has the "exit" command. |
| **Example** | This example shows how to enter privileged EXEC mode and use exit command to go back to user EXEC mode.<br>Switch> **enable**<br>Switch# **exit**<br>Switch> |

### 2.3.7 history

| | |
|---|---|
| **Syntax** | **history** <1-256><br>**no history** |
| **Parameter** | <1-256> Specify maximum CLI history entry number. |
| **Default** | Default maximum history entry number is 128. |
| **Mode** | Line Configuration |
| **Usage** | Use "**history"** command to specify the maximum commands history number for CLI running on console, telnet or ssh service. Every command input by user will record in history buffer. If all history commands exceed configured history number, older ones will be deleted from buffer. |

Use "**no history**" to disable the history feature. And use "**show history**" to show all history commands.

**Example**

This example shows how to change console history number to 100, telnet history number to 150 and ssh history number 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**

This example shows how show line information.

**Switch# show line**

```
Switch(config)# line ssh
Switch(config-line)# history 200
Switch(config-line)# exit
Switch(config)#
Switch(config)# do show line
Console ============================
    Session Timeout : 10 (minutes)
    History Count   : 100
    Password Retry  : 3
    Silent Time     : 0 (seconds)
Telnet =============================
    Telnet Server   : enabled
    Session Timeout : 10 (minutes)
    History Count   : 150
    Password Retry  : 3
    Silent Time     : 0 (seconds)
SSH ================================
    SSH Server      : enabled
    Session Timeout : 10 (minutes)
    History Count   : 200
    Password Retry  : 3
    Silent Time     : 0 (seconds)
```

This example shows how show history commands.

Switch# **show history**

```
Switch(config)# do show history
Maximun History Count: 100
-----------------------------------------------------
1. show line
2. show history
3. 2
4. config
5. line console
6. history 100
7. exit
8. line telnet
9. history 150
10. exit
11. line ssh
12. history 200
13. exit
14. do show line
15. do show history
```

### 2.3.8 hostname

| | |
|---|---|
| **Syntax** | **hostname** WORD |
| **Parameter** | WORD Specify the hostname of the switch. |
| **Default** | Default name string is “Switch”. |
| **Mode** | Global Configuration |
| **Usage** | Use “hostname” command to modify hostname of the switch. The system name is also used to be CLI prompt. |
| **Example** | This example shows how to modify contact information<br>Switch(config)# hostname fiberroad<br>fiberroad(config)#<br>  |



### 2.3.9 interface

| | |
|---|---|
| **Syntax** | **interface** IF_PORTS<br>**interface range** IF_PORTS |
| **Parameter** | **IF_PORTS** Specify the port to select. This parameter allows partial port name and ignore case. For Example:<br>fa1 FastEthernet3 Gigabit4<br>……<br><br>If port range is specified, the list format is also available. For Example:<br>fa1,3,5<br>fa2,gi1-3<br>…… |
| **Default** | No default value for this command. |
| **Mode** | Global Configuration |
| **Usage** | Some configurations are port based. In order to configure these configurations, we need to enter Interface Configuration mode to configure them. Use “interface” command to enter the Interface Configuration mode and select the port to be configured. |

In Interface Configuration mode, the prompt will show as "**Switch(config- if**)#"

**Example** This example shows how to enter Interface Configuration mode

Switch# configure

Switch(config)# interface ?

```
fiberroad(config)# interface
  GigabitEthernet     Gigabit ethernet interface to configure
  LAG                 IEEE 802.3 Link Aggregateion interface
  Loopback            Loopback interface
  TenGigabitEthernet  10 Gigabit ethernet interface to configure
  vlan                Vlan interface
  range               interface range command
fiberroad(config)# interface
```

### 2.3.10 ip address

| | |
|---|---|
| **Syntax** | **ip address** A.B.C.D **[mask** A.B.C.D**]** |
| **Parameter** | **address** A.B.C.D Specify IPv4 address for switch<br>**mask** A.B.C.D Specify net mask address for switch |
| **Default** | Default IP address is 192.168.1.6 and default net mask is 255.255.255.0 |
| **Mode** | Global Configuration |
| **Usage** | Use "**ip address**" command to modify administration ipv4 address. 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. |
| **Example** | This example shows how to modify the ipv4 address of the switch.<br><br>Switch(config)# **ip address 192.168.1.200 mask 255.255.255.0**<br><br>This example shows how to show current ipv4 address of the switch.<br>Switch# **show ip**<br>IP Address: 192.168.1.200<br>Subnet Netmask: 255.255.255.0<br>Default Gateway: 192.168.1.254 |

### 2.3.11 ip default-gateway

| | |
|---|---|
| **Syntax** | **ip default-gateway** A.B.C.D<br>**no ip default-gateway** |
| **Parameter** | A.B.C.D Specify default gateway IPv4 address for switch |
| **Default** | Default IP address of default gateway is 192.168.1.254. |
| **Mode** | Global Configuration |
| **Usage** | Use "**ip default-gateway**" command to modify default gateway address. And use "**no ip default-gateway**" to restore default gateway address to factory default. |
| **Example** | This example shows how to modify the ipv4 address of the switch.<br><br>Switch(config)# ip default-gateway 192.168.1.100<br><br>This example shows how to show current ipv4 default gateway of the switch.<br>Switch# **show ip**<br>IP Address: 192.168.1.1<br>Subnet Netmask: 255.255.255.0<br>Default Gateway: 192.168.1.100 |

### 2.3.12 ip dhcp

| | |
|---|---|
| **Syntax** | **ip dhcp**<br>**no ip dhcp** |
| **Parameter** | None |
| **Default** | Default DHCP client is disabled. |
| **Mode** | Global Configuration |
| **Usage** | Use "**ip dhcp**" command to enabled dhcp client to get IP address from remote DHCP server.<br>Use "**no ip dhcp**" command to disabled dhcp client and use static ip address. |
| **Example** | This example shows how to enable dhcp client. |

| | |
|---|---|
| | Switch(config)# **ip dhcp**<br><br>This example shows how to show current dhcp client state of the switch.<br>Switch# **show ip dhcp**<br>DHCP Status : enabled |

### 2.3.13 ip dns

| | |
|---|---|
| **Syntax** | **ip dns** A.B.C.D [A.B.C.D]<br>**no ip dns** [A.B.C.D] |
| **Parameter** | A.B.C.D Specify the DNS server ip address. |
| **Default** | Default IP address of DNS server is 168.95.1.1 and 168.95.192.1. |
| **Mode** | Global Configuration |
| **Usage** | Use “ip dns” command to modify DNS server address. And use “no ip dns”to delete existing DNS server. |
| **Example** | This example shows how to modify the DNS server of the switch.<br>Switch(config)# **ip dns 111.111.111.111 222.222.222.222**<br><br>This example shows current DNS server of the switch.<br>Switch# **show ip dns**<br>DNS lookup is enabled<br>DNS Server 1 : 111.111.111.111<br>DNS Server 2 : 222.222.222.222 |

### 2.3.13 ip dns lookup

| | |
|---|---|
| **Syntax** | **ip dns lookup**<br>**no ip dns lookup** |
| **Parameter** | None |
| **Default** | Default DNS lookup is enabled |
| **Mode** | Global Configuration |

| | |
|---|---|
| **Usage** | Use “ip dns lookup” command to enable the Domain Name to IP address service. And use “no ip dns” to disable the DNS service. |
| **Example** | This example enables the DNS service on the system.<br>Switch(config)# **ip dns lookup**<br><br>This example shows the DNS service status.<br>Switch# **show ip dns**<br>DNS Server 1 : 111.111.111.111<br>DNS Server 2 : 222.222.222.222 |

### 2.3.14 ipv6 autoconfig

| | |
|---|---|
| **Syntax** | **ipv6 autoconfig**<br>**no ipv6 autoconfig** |
| **Parameter** | None |
| **Default** | Default IPv6 auto config is enabled. |
| **Mode** | Global Configuration |
| **Usage** | Use “ipv6 autoconfig” command to enabled IPv6 auto configuration feature. Use “no ipv6 autoconfig” command to disabled IPv6 auto configuration feature. |
| **Example** | This example shows how to disable IPv6 auto config.<br>Switch(config)# **no ipv6 autoconfig**<br><br>This example shows how to show current IPv6 auto config state.<br>Switch# show ipv6<br>IPv6 DHCP Configuration : Disabled<br>IPv6 DHCP DUID :<br>IPv6 Auto Configuration : Disabled<br>IPv6 Link Local Address : fe80::dcad:beff:feef:102/64<br>IPv6 static Address : fe80::20e:2eff:fef1:4b3c/128<br>IPv6 static Gateway Address : ::<br>IPv6 in use Address : fe80::dcad:beff:feef:102/64<br>IPv6 in use Gateway Address : :: |

### 2.3.15 ipv6 address

| | |
|---|---|
| **Syntax** | **ipv6 address** X:X::X:X **prefix** <0-128> |
| **Parameter** | **address** X:X::X:X Specify IPv6 address for switch<br>**prefix** <0-128> Specify IPv6 prefix length for switch |
| **Default** | No default ipv6 address on the switch. |
| **Mode** | Global Configuration |
| **Usage** | Use "**ipv6 address**" command to specify static IPv6 address. |
| **Example** | This example shows how to add static ipv6 address of the switch.<br>Switch(config)# **ipv6 address fe80::20e:2eff:fef1:4b3c prefix 128**<br><br>This example shows how to show current ipv6 address of the switch.<br>Switch# show ipv6<br>IPv6 DHCP Configuration : Disabled IPv6 DHCP DUID :<br>IPv6 Auto Configuration : Enabled<br>IPv6 Link Local Address : fe80::dcad:beff:feef:102/64<br>IPv6 static Address : fe80::20e:2eff:fef1:4b3c/128<br>IPv6 static Gateway Address : ::<br>IPv6 in use Address : fe80::dcad:beff:feef:102/64<br>IPv6 in use Gateway Address : :: |

### 2.3.16 ipv6 default-gateway

| | |
|---|---|
| **Syntax** | **ipv6 default-gateway** X:X::X:X |
| **Parameter** | X:X::X:X Specify default gateway IPv6 address for switch |
| **Default** | No default ipv6 default gateway address on the switch. |
| **Mode** | Global Configuration |
| **Usage** | Use "ipv6 default-gateway" command to modify default gateway IPv6 address. |
| **Example** | This example shows how to modify the ipv6 default gateway address of the switch.<br>Switch(config)# **ipv6 default-gateway fe80::dcad:beff:feef:103** |

Switch# show ipv6
IPv6 DHCP Configuration : Disabled IPv6 DHCP DUID :
IPv6 Auto Configuration : Enabled
IPv6 Link Local Address : fe80::dcad:beff:feef:102/64
IPv6 static Address : fe80::20e:2eff:fef1:4b3c/128
IPv6 static Gateway Address : ::
IPv6 in use Address : fe80::dcad:beff:feef:102/64
IPv6 in use Gateway Address : ::

### 2.3.17 ipv6 dhcp

| | |
|---|---|
| **Syntax** | **ipv6 dhcp**<br>**no ipv6 dhcp** |
| **Parameter** | |
| **Default** | Default DHCPv6 client is disabled. |
| **Mode** | Global Configuration |
| **Usage** | Use “ipv6 dhcp” command to enabled dhcpv6 client to get IP address from remote DHCPv6 server.<br>Use “no ipv6 dhcp” command to disabled dhcpv6 client and use static ipv6 |
| **Example** | This example shows how to enable dhcp client.<br>Switch(config)# **ipv6 dhcp**<br><br>This example shows how to show current dhcpv6 client state of the switch.<br>Switch# **show ipv6 dhcp**<br>DHCPv6 Status : enabled |

### 2.3.18 ip service

| | |
|---|---|
| **Syntax** | **ip (telnet \| ssh \| http \| https)**<br>**no ip (telnet \| ssh \| http \| https)** |
| **Parameter** | telnet Enable/Disable telnet service<br>ssh Enable/Disable ssh service<br>http Enable/Disable http service<br>https Enable/Disable https service |
| **Default** | Default telnet service is disabled.<br>Default ssh service is disabled.<br>Default http service is enabled.<br>Default https service is disabled. |
| **Mode** | Global Configuration |
| **Usage** | Use “ip service” command to enable all kinds of ip services. Such as telnet, ssh, http and https.<br>Use no form to disable service. |
| **Example** | This example shows how to enable telnet service and show current telnet service status.<br>Switch(config)# **ip telnet**<br>Telnetd daemon enabled.<br>Switch(config)# **exit**<br>Switch# **show line telnet**<br>Telnet ==========<br>Telnet Server : enabled Session Timeout : 10 (minutes) History Count : 128<br>Password Retry : 3<br>Silent Time : 0 (seconds)<br><br>This example shows how to enable https service and show current https service status.<br>Switch(config)# **ip https**<br><br>Switch(config)# **exit**<br>Switch# **show ip https**<br>HTTPS daemon : **enabled**<br>Session Timeout : **10 (minutes)** |

### 2.3.19 ip session-timeout

| | | |
|---|---|---|
| **Syntax** | **ip (http \| https) session-timeout** <0-86400> | |
| **Parameter** | http | Specify session timeout for http service. |
| | https | Specify session timeout for https service. |
| | <0-86400> | Specify session timeout minutes. 0 means never timeout. |
| **Default** | Default session timeout for http and https is 10 minutes. | |
| **Mode** | Global Configuration | |
| **Usage** | Use "**ip session-timeout**" command to specify the session timeout value for http or https service. When user login into WEBUI and do not do any action after session timeout will be logged out. | |
| **Example** | This example shows how to change http session timeout to 15min and https session timeout to 20min<br>Switch(config)# **ip http session-timeout 15**<br>Switch(config)# **ip https session-timeout 20**<br><br>This example shows how to enable https service and show current https service status.<br>Switch# **show ip http**<br>HTTPS daemon : enabled<br>Session Timeout : 15 (minutes)<br>Switch# **show ip https**<br>HTTPS daemon : disabled<br>Session Timeout : 20 (minutes) | |

## 2.3.20 ip ssh

| | |
|---|---|
| **Syntax** | **ip ssh (v1\|v2\|all)**<br>**no ip ssh (v1\|v2\|all)** |
| **Parameter** | v1 Generate/Delete version 1 key files<br>v2 Generate/Delete version 2 key files<br>all Generate/Delete version 1 and 2 key files |
| **Default** | Version 2 key files will be generated by default |
| **Mode** | Global Configuration |
| **Usage** | Use “ip ssh” command to generate the key files for ssh connection.<br><br>Use no form to delete key files. SSH connection may not connect if no any v1 or v2 ssh key files exist. |
| **Example** | This example shows how to delete and re-generate ssh version 2 key files.<br>Switch(config)# no ip ssh v2<br>Switch(config)# do show flash |

```
Switch(config)# no ip ssh v2
Switch(config)# do show flash
       File Name           File Size       Modified
----------------------- --------------- ----------------------
startup-config          1246            2022-01-01 00:02:02
ssl_cert                1245            2022-01-01 00:00:29
image                   8557717         2022-11-01 13:37:51
```

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.

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

```
Switch(config)# do show flash
       File Name           File Size       Modified
----------------------- --------------- ----------------------
startup-config          1246            2022-01-01 00:02:02
rsa2                    1679            2022-01-01 00:20:28
dsa2                    672             2022-01-01 00:20:36
ssl_cert                1245            2022-01-01 00:00:29
image                   8557717         2022-11-01 13:37:51
```

### 2.3.21 line

| | |
|---|---|
| **Syntax** | **line ( console \| telnet \| ssh )** |
| **Parameter** | console Select console line to configure.<br>telnet Select telnet line to configure.<br>ssh Select ssh line to configure. |
| **Default** | No default value for this command. |
| **Mode** | Global Configuration |
| **Usage** | Some configurations are line based. In order to configure these configurations, we need to enter Line Configuration mode to configure them. Use "line" command to enter the Line Configuration mode and select the line to be configured.<br><br>In Line Configuration mode, the prompt will show as "**Switch(config-line)**#" |
| **Example** | This example shows how to enter Interface Configuration mode<br>Switch# **configure**<br>Switch(config)# **line console**<br>Switch(config-line)# |

### 2.3.22 reboot

| | |
|---|---|
| **Syntax** | **reboot** |
| **Parameter** | |
| **Default** | No default value for this command. |
| **Mode** | Privileged EXEC |
| **Usage** | Use "**reboot**" command to make system hot restart. |
| **Example** | This example shows how to restart the system<br>Switch# **reboot** |

### 2.3.23 enable password

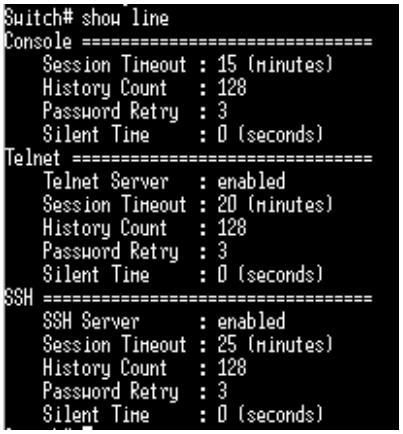
| | |
|---|---|
| **Syntax** | **enable [privilege <1-15>]** (**password** UNENCRYPY PASSWOR\|secrect UNENCRYPY-PASSWORD \| secret encrypted ENCRYPT-PASSWORD) no enable [privilege <0-15>] |

**Parameter**

| | |
|---|---|
| **privilege** *<0-15>* | Specify the privilege level to configure. If no privilege level is specified, default is 15. |
| **password** UNENCRYPY-PASSWORD | Specify password string and make it not encrypted. |
| **secret** UNENCRYPY-PASSWORD | Specify password string and make it encrypted. |
| **secret encrypted** ENCRYPT-PASSWORD | Enter an encrypted password. Use this keyword to enter a password that is already encrypted (for instance, a password that you copied from another the configuration file of another device). |

| | |
|---|---|
| **Default** | Default enable password for all privilege levels are “”. |
| **Mode** | Global Configuration |
| **Usage** | Use “enable password” command to edit password for each privilege level for enable authentication. And use “no enable” command to restore enable password to default empty value.<br>The only way to show this configuration is using “show running-config” command. |
| **Example** | This example shows how to edit enable password for privilege level 15<br><br>Switch(config)# **enable secret enblpasswd** |

### 2.3.24 exec-timeout

| | |
|---|---|
| **Syntax** | **exec-timeout** <0-65535> |
| **Parameter** | <0-65535> Specify session timeout minutes. 0 means never timeout |
| **Default** | Default session timeout for all lines are 10 minutes. |
| **Mode** | Line Configuration |
| **Usage** | Use “exec-timeout” command to specify the session timeout value for CLI running on console, telnet or ssh service. When user login into CLI and do not do any action after session timeout will be logged out from the CLI session. |
| **Example** | This example shows how to change console session timeout to 15min ,telnet session timeout to 20min and ssh session timeout to 25min.<br>Switch(config)# **line console**<br>Switch(config-line)# **exec-timeout 15**<br>Switch(config-line)# **exit**<br>Switch(config)# **line telnet**<br>Switch(config-line)# **exec-timeout 20**<br>Switch(config-line)# **exit**<br>Switch(config)# **line ssh**<br>Switch(config-line)# **exec-timeout 25**<br>Switch(config-line)# **exit**<br><br>This example shows how show line information.<br>Switch# **show line**<br>  |

```
Switch# show line
Console ==============================
    Session Timeout : 15 (minutes)
    History Count   : 128
    Password Retry  : 3
    Silent Time     : 0 (seconds)
Telnet ===============================
    Telnet Server   : enabled
    Session Timeout : 20 (minutes)
    History Count   : 128
    Password Retry  : 3
    Silent Time     : 0 (seconds)
SSH ==================================
    SSH Server      : enabled
    Session Timeout : 25 (minutes)
    History Count   : 128
    Password Retry  : 3
    Silent Time     : 0 (seconds)
```

### 2.3.25 password-thresh

| | |
|---|---|
| **Syntax** | **password-thresh** <0-120> |
| **Parameter** | <0-120> Specify password fail retry number. 0 means no limit. |
| **Default** | Default password fail retry number is 3. |
| **Mode** | Line Configuration |
| **Usage** | Use "**password-thresh**" command to specify the password fail retry number for CLI running on console, telnet or ssh service. When user input password to login and authenticate failed, the fail retry number will increase one. After fail retry number exceed configured one, the CLI will block login for the period of silent time which configured by the command "**silent-time**". |
| **Example** | This example shows how to change console fail retry number to 4, telnet fail retry number to 5 and ssh fail retry number to 6.<br>Switch(config)# **line console**<br>Switch(config-line)# **password-thresh 4**<br>Switch(config-line)# **exit**<br>Switch(config)# **line telnet**<br><br>Switch(config-line)# password-thresh 5<br>Switch(config-line)# exit<br>Switch(config)# line ssh<br>Switch(config-line)# password-thresh 6<br>Switch(config-line)# exit<br><br>This example shows how show line information.<br>Switch# **show line**<br>Console ==========<br>Session Timeout : 10 (minutes)<br>History Count : 128<br>Password Retry : 4<br>Silent Time : 0 (seconds)<br>Telnet ==========<br>Telnet Server : disabled<br>Session Timeout : 10 (minutes)<br>History Count : 128<br>Password Retry : 5<br>Silent Time : 0 (seconds) |

SSH ==========
SSH Server : disabled
Session Timeout : 10 (minutes)
History Count : 128
Password Retry : 6
Silent Time : 0 (seconds)

### 2.3.26 ping

| | |
|---|---|
| **Syntax** | **ping** HOSTNAME **[count** <1-999999999>**]** |
| **Parameter** | HOSTNAME Specify IPv4/IPv6 address or domain name to ping.<br>**count** <1-999999999> Specify how many times to ping. |
| **Default** | No default value for this command. |
| **Mode** | User EXEC<br>Privileged EXEC |
| **Usage** | **Use "**ping**" command to do network ping diagnostic.** |
| **Example** | **This example shows how to ping remote host 192.168.1.111.**<br>**Switch# ping 192.168.1.111**<br>PING 192.168.1.111 (192.168.1.111): 56 data bytes<br>64 bytes from 192.168.1.111: icmp_seq=0 ttl=128 time=10.0 ms<br>64 bytes from 192.168.1.111: icmp_seq=1 ttl=128 time=0.0 ms<br>64 bytes from 192.168.1.111: icmp_seq=2 ttl=128 time=0.0 ms<br>64 bytes from 192.168.1.111: icmp_seq=3 ttl=128 time=0.0 ms<br><br>--- 192.168.1.111 ping statistics ---<br>4 packets transmitted, 4 packets received, 0% packet loss<br>round-trip min/avg/max = 0.0/2.5/10.0 ms |

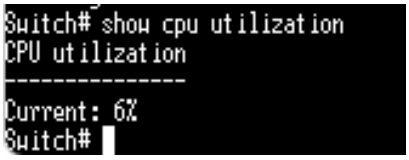
### 2.3.27 traceroute

| | |
|---|---|
| **Syntax** | **traceroute** A.B.C.D **[max_hop** <2-255>**]** |
| **Parameter** | A.B.C.D Specify IPv4 to trace.<br>**max_hop** <2-255> Specify maximum hop to trace. |
| **Default** | No default value for this command. |
| **Mode** | User EXEC<br>Privileged EXEC |
| **Usage** | Use "**traceroute**" command to do network trace route diagnostic. |
| **Example** | This example shows how to trace route host 192.168.1.111.<br>Switch# **traceroute 192.168.1.111**<br>`traceroute to 192.168.1.111 (192.168.1.111), 30 hops max, 40 byte packets`<br>`1 192.168.1.111 (192.168.1.111)  0 ms  10 ms  0 ms` |

### 2.3.28 show arp

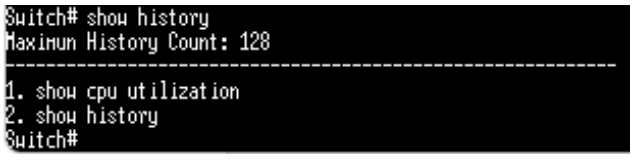
| | |
|---|---|
| **Syntax** | **show arp** |
| **Parameter** | |
| **Default** | No default value for this command. |
| **Mode** | User EXEC<br>Privileged EXEC |
| **Usage** | Use "**show arp**" command to show all arp entries. |
| **Example** | This example shows how to show arp entries.<br>Switch# **show arp**<br>`Address  HWtype  HWaddress  Flags Mask  Iface`<br>`192.168.1.111  ether 00:0E:2E:F1:4B:3C  C  eth0` |

### 2.3.29 show cpu utilization

| | |
|---|---|
| **Syntax** | **show cpu utilization** |
| **Parameter** | |
| **Default** | No default value for this command. |
| **Mode** | Privileged EXEC |
| **Usage** | Use "**show cpu utilization**" command to show current CPU utilization. |
| **Example** | This example shows how to show current CPU utilization.<br>**Switch# show cpu utilization**<br>  |

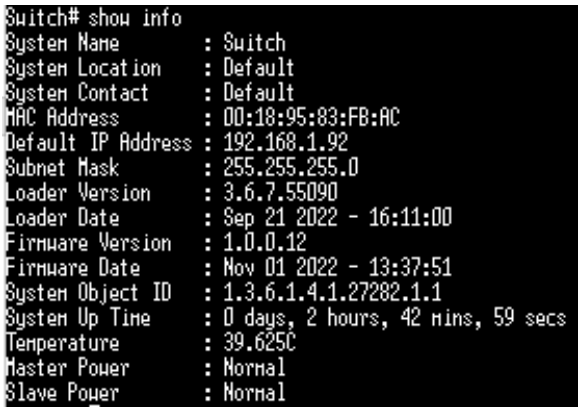
```
Switch# show cpu utilization
CPU utilization
---------------

Current: 6%
Switch#
```

### 2.3.30 show history

| | |
|---|---|
| **Syntax** | **show history** |
| **Parameter** | |
| **Default** | No default value for this command |
| **Mode** | User EXEC /Privileged EXEC /Global Configuration |
| **Usage** | Use "**show history**" to show commands we input before. |
| **Example** | The example shows how show history commands<br>Switch# **show history**<br>  |

```
Switch# show history
Maximun History Count: 128
------------------------------------------------------------

1. show cpu utilization
2. show history
Switch#
```

### 2.3.31 show info

| | |
|---|---|
| **Syntax** | **show info** |
| **Parameter** | |
| **Default** | No default value for this command |
| **Mode** | User EXEC /Privileged EXEC |
| **Usage** | Use "**show info**" command to show system summary information. |
| **Example** | The example shows how show system version<br>Switch# **show info**<br>  |

```
Switch# show info
System Name        : Switch
System Location    : Default
System Contact     : Default
MAC Address        : 00:18:95:83:FB:AC
Default IP Address : 192.168.1.92
Subnet Mask        : 255.255.255.0
Loader Version     : 3.6.7.55090
Loader Date        : Sep 21 2022 - 16:11:00
Firmware Version   : 1.0.0.12
Firmware Date      : Nov 01 2022 - 13:37:51
System Object ID   : 1.3.6.1.4.1.27282.1.1
System Up Time     : 0 days, 2 hours, 42 mins, 59 secs
Temperature        : 39.625C
Master Power       : Normal
Slave Power        : Normal
```

### 2.3.32 show ip

| | |
|---|---|
| **Syntax** | **show ip** |
| **Parameter** | |
| **Default** | No default value for this command |
| **Mode** | User EXEC /Privileged EXEC |
| **Usage** | Use "**show ip**" command to show system IPv4 address, net mask and default gateway. |
| **Example** | The example shows how to show current ipv4 address of the switch.<br>Switch# **show info**<br>`IP Address: 192.168.1.200`<br>`Subnet Netmask: 255.255.255.0`<br>`Default Gateway: 192.168.1.254` |

### 2.3.33 show ip dhcp

| | |
|---|---|
| **Syntax** | **show ip dhcp** |
| **Parameter** | |
| **Default** | No default value for this command |
| **Mode** | User EXEC /Privileged EXEC |
| **Usage** | Use "**show ip dhcp**" command to show IPv4 dhcp client enable state. |
| **Example** | This example shows how to show current dhcp client state of the switch.<br>Switch# **show ip dhcp**<br>`DHCP Status : enabled` |

### 2.3.34 show ip dns

| | |
|---|---|
| **Syntax** | **show ip dns** |
| **Parameter** | |
| **Default** | No default value for this command |
| **Mode** | User EXEC /Privileged EXEC |
| **Usage** | Use "**show ip dns**" command to show system IPv4 DNS addresses. |
| **Example** | This example shows how to show current ipv4 address of the switch.<br>Switch# **show ip dns**<br>`DNS lookup is enabled`<br>`DNS Server 1 : 168.95.1.1`<br>`DNS Server 2 : 168.95.192.1` |

### 2.3.35 show ip http

| | |
|---|---|
| **Syntax** | **show ip（http\|https）** |
| **Parameter** | |
| **Default** | No default value for this command |
| **Mode** | Privileged EXEC |
| **Usage** | Use "**show ip http**" command to show HTTP/HTTPS information. |
| **Example** | This example shows how to show current ipv4 address of the switch.<br>Switch# **show ip http**<br>`HTTP daemon : enabled`<br>`Session Timeout : 10 (minutes)`<br><br>`Switch# show ip https`<br>`HTTPS daemon : enabled`<br>`Session Timeout : 10 (minutes)` |

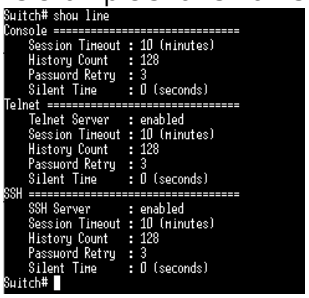
### 2.3.36 show ipv6

| | |
|---|---|
| **Syntax** | **show ipv6** |
| **Parameter** | |
| **Default** | No default value for this command |
| **Mode** | User EXEC /Privileged EXEC |
| **Usage** | Use "**show ipv6**" command to show system IPv6 address, net mask, default gateway and auto config state. |
| **Example** | This example shows how to show current ipv6 address of the switch.<br>`Switch# show ipv6`<br>`IPv6 DHCP Configuration : Disabled`<br>`IPv6 DHCP DUID :`<br>`IPv6 Auto Configuration : Enabled`<br>`IPv6 Link Local Address :fe80::dcad:beff:feef:102/64`<br>`IPv6 static Address :fe80::20e:2eff:fef1:4b3c/128`<br>`IPv6 static Gateway Address : ::`<br>`IPv6 in use Address :fe80::dcad:beff:feef:102/64`<br>`IPv6 in use Gateway Address : ::` |

### 2.3.37 show ipv6 dhcp

| | |
|---|---|
| **Syntax** | **show ipv6** |
| **Parameter** | |
| **Default** | No default value for this command |
| **Mode** | User EXEC /Privileged EXEC |
| **Usage** | Use “show ipv6 dhcp” command to show system IPv6 dhcp client enable state. |
| **Example** | This example shows how to show current dhcpv6 client state of the switch.<br>`Switch# show ipv6 dhcp`<br>`DHCPv6 Status : enabled` |

### 2.3.38 show line

| | |
|---|---|
| **Syntax** | **show line [(console \| telnet \| ssh)]** |
| **Parameter** | **console** Select console line to show.<br>**telnet** Select telnet line to show.<br>**ssh** Select ssh line to show. |
| **Default** | No default value for this command |
| **Mode** | Privileged EXEC |
| **Usage** | Use “**show line**” command to show all line configurations including session timeout, history count, password retry number and silent time. For telnet and ssh, it also shows the service enable/disable state. |
| **Example** | This example shows how show all lines’ information.<br>  |

```
Switch# show line
Console ==============================
    Session Timeout : 10 (minutes)
    History Count   : 128
    Password Retry  : 3
    Silent Time     : 0 (seconds)
Telnet ===============================
    Telnet Server   : enabled
    Session Timeout : 10 (minutes)
    History Count   : 128
    Password Retry  : 3
    Silent Time     : 0 (seconds)
SSH ==================================
    SSH Server      : enabled
    Session Timeout : 10 (minutes)
    History Count   : 128
    Password Retry  : 3
    Silent Time     : 0 (seconds)
Switch#
```

### 2.3.39 show memory statistics

| | |
|---|---|
| **Syntax** | **show memory statistics** |
| **Parameter** | |
| **Default** | No default value for this command |
| **Mode** | Privileged EXEC |
| **Usage** | Use “show memory statistics” command to show current memory utilization. |
| **Example** | This example show how to show current system memory statistics.<br>Switch# show memory statistics<br>total(KB) used(KB) free(KB) shared(KB) buffer(KB) cache(KB)<br>Mem: 255176 83076 172100 0 0 0<br>-/+ buffers/cache: 83076 172100<br>Swap: 0 0 0<br>Switch# |

### 2.3.40 show privilege

| | |
|---|---|
| **Syntax** | **show privilege** |
| **Parameter** | |
| **Default** | No default value for this command |
| **Mode** | User EXEC/Privileged EXEC |
| **Usage** | Use “show privilege” command to show the privilege level of the current user. |
| **Example** | This example shows how to show privilege.<br>Switch# show privilege<br>Current CLI Username: admin<br>Current CLI Privilege: 15<br>Switch# |

### 2.3.41 show username

| | |
|---|---|
| **Syntax** | **show username** |
| **Parameter** | |
| **Default** | No default value for this command |
| **Mode** | Privileged EXEC |
| **Usage** | Use "**show username**" command show all user accounts in local database. |
| **Example** | This example shows how to show privilege. |

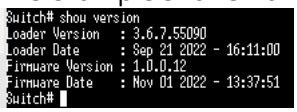
```
Switch# show username
 Priv  |  Type  |          User Name          |          Password
-------+--------+-----------------------------+-----------------------------
  15   | secret |                       admin | MjEyMzJmMjk3YTU3YTVhNzQzODk0YTB1NGE4MDFmYzM=
Switch#
```

### 2.3.42 show users

| | |
|---|---|
| **Syntax** | **show users** |
| **Parameter** | |
| **Default** | No default value for this command |
| **Mode** | Privileged EXEC |
| **Usage** | Use "**show users**" command show information of all active users. |
| **Example** | This example shows how to show existing user accounts. |

```
Switch# show users
  Username       Protocol        Location
-------------- ---------- --------------------
       admin      console     0.0.0.0
Switch#
```

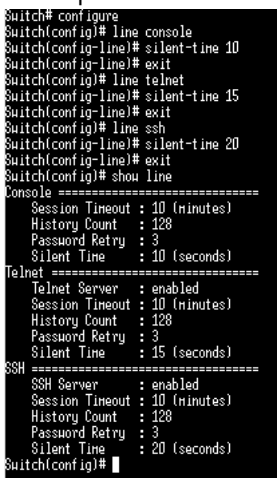
### 2.3.43 show version

| | |
|---|---|
| **Syntax** | **show versions** |
| **Parameter** | |
| **Default** | No default value for this command |
| **Mode** | User EXEC/Privileged EXEC |
| **Usage** | Use "**show version**" command to show loader and firmware version and build date. |
| **Example** | This example shows how to show system version.<br>  |

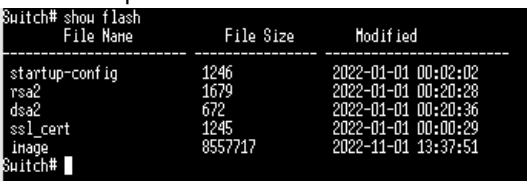
### 2.3.44 silent-time

| | |
|---|---|
| **Syntax** | **silent-time** <0-65535> |
| **Parameter** | <0-65535> Specify silent time with unit seconds. 0 means do not silent. |
| **Default** | Default silent time is 0. |
| **Mode** | Line Configuration |
| **Usage** | Use "**silent time**" command to specify the silent time for CLI running on console, telnet or ssh service. When user input password to login and authenticate failed, the fail retry number will increase one. After fail retry number exceed configured one, the CLI will block login for the period of silent time which configured by the command "**silent-time**". |
| **Example** | This example shows how to change console silent time to 10, telnet silent time to 15 and ssh silent time to 20. |

This example shows how show line information.




### 2.3.44 ssl

| | |
|---|---|
| **Syntax** | **ssl** |
| **Parameter** | |
| **Default** | No default value for this command |
| **Mode** | Global Configuration |
| **Usage** | Use "**ssl**" command to generate security certificate files such as RSA, DSA. |
| **Example** | This example shows how to generate certificate files.<br>`Switch(config)# ssl`<br><br>This example shows how to show the certificate file lists.<br>  |

### 2.3.45 system name

| | |
|---|---|
| **Syntax** | **system name** NAME |
| **Parameter** | NAME Specify system name string. |
| **Default** | Default name string is “Switch”. |
| **Mode** | Global Configuration |
| **Usage** | Use “**system name**” command to modify system name information of the switch. The system name is also used to be CLI prompt. |
| **Example** | This example shows how to modify contact information |

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

This example shows how to show system name information

```
Switch# configure
Switch(config)# system name fiberroad
fiberroad(config)# exit
fiberroad# show info
System Name        : fiberroad
System Location    : Default
System Contact     : Default
MAC Address        : 00:18:95:83:FB:AC
Default IP Address : 192.168.1.92
Subnet Mask        : 255.255.255.0
Loader Version     : 3.6.7.55090
Loader Date        : Sep 21 2022 - 16:11:00
Firmware Version   : 1.0.0.12
Firmware Date      : Nov 01 2022 - 13:37:51
System Object ID   : 1.3.6.1.4.1.27282.1.1
System Up Time     : 0 days, 0 hours, 55 mins, 55 secs
Temperature        : 37.625C
Master Power       : Normal
Slave Power        : Normal
fiberroad#
```

### 2.3.46 system contact

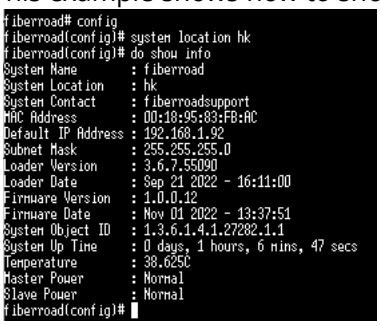
| | |
|---|---|
| **Syntax** | **system contact** CONTACT |
| **Parameter** | CONTACT Specify contact string. |
| **Default** | Default contact string is “Default Contact”. |
| **Mode** | Global Configuration |
| **Usage** | Use “**system contact**” command to modify contact information of the switch. |
| **Example** | This example shows how to modify contact information<br>`Switch(config)# system contact Fiberroadsupport`<br><br>This example shows how to show system contact information<br>  |

```
fiberroad(config)# system contact fiberroadsupport
fiberroad(config)# exit
fiberroad# show info
System Name        : fiberroad
System Location    : Default
System Contact     : fiberroadsupport
MAC Address        : 00:18:95:83:FB:AC
Default IP Address : 192.168.1.92
Subnet Mask        : 255.255.255.0
Loader Version     : 3.6.7.55D90
Loader Date        : Sep 21 2022 - 16:11:00
Firmware Version   : 1.0.0.12
Firmware Date      : Nov 01 2022 - 13:37:51
System Object ID   : 1.3.6.1.4.1.27282.1.1
System Up Time     : 0 days, 0 hours, 59 mins, 16 secs
Temperature        : 38.0C
Master Power       : Normal
Slave Power        : Normal
```

### 2.3.47 system location

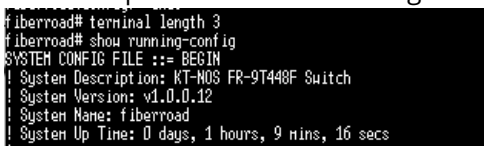
| | |
|---|---|
| **Syntax** | **system location** LOCATION |
| **Parameter** | CONTACT Specify location string. |
| **Default** | Default location string is “Default Location”. |
| **Mode** | Global Configuration |
| **Usage** | Use “**system location**” command to modify location information of the switch. |
| **Example** | This example shows how to modify contact information<br>`Switch(config)# system location home` |

This example shows how to show system location information




### 2.3.48 terminal length

| | |
|---|---|
| **Syntax** | **terminal length** <0-24> |
| **Parameter** | <0-24> Specify terminal length value. 0 means no limit. |
| **Default** | Default terminal length is 24. |
| **Mode** | User EXEC<br>Privileged EXEC |
| **Usage** | Use "**terminal length**" command to specify the maximum line number the terminal is able to print. |
| **Example** | This example shows how to change terminal length. |



### 2.3.49 username

**Syntax**

**username** WORD<0-32> **[privilege (admin|user|**<0-15>**)]** **(nopassword | password** UNENCRYPY-PASSWORD **| secrect** UNENCRYPY-PASSWORD **| secret encrypted** ENCRYPT-PASSWORD)

**no username** WORD<0-32>

**Parameter**

| | |
|---|---|
| **username** *WORD<0-32>* | Specify user name to add/delete/edit. |
| **privilege admin** | Specify privilege level to be admin (privilege 15) |
| **privilege user** | Specify privilege level to be user (privilege 1) |
| **privilege** *<0-15>* | Specify custom privilege level |
| **password** *UNENCRYPY-PASSWORD* | Specify password string and make it not encrypted. |
| **secret** *UNENCRYPY-PASSWORD* | Specify password string and make it encrypted. |
| **secret encrypted** *ENCRYPT-PASSWORD* | Enter an encrypted password. Use this keyword to enter a password that is already encrypted (for instance, a password that you copied from another the configuration file of another device). |

**Default**

Default username “admin” has password “admin” with privilege 15.

**Mode**

Global Configuration

**Usage**

Use “**username**” command to add a new user account or edit an existing user account. And use “**no username**” to delete an existing user account. The user account is a local database for login authentication.

**Example**

This example shows how to add a new user account.

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

This example shows how to show existing user accounts.

```
fiberroad# config
fiberroad(config)# username test secret passwd
fiberroad(config)# exit
fiberroad# show username
 Priv  |  Type  |          User Name          |          Password
-------+--------+-----------------------------+-----------------------------------
  15   | secret |                       admin | MjEyMzJmMjk3YTU3YTVhNzQzODk0YTB1NGE4MDFmYzM=
  15   | secret |                        test | NzZhMjE3M2J1NjM5MzI1NGU3MmZmYTRkNmRmMTHzMGE=
```

## 2.4 Authentication Manager

### 2.4.1 authentication

| | |
|---|---|
| **Syntax** | **authentication (dot1x\|mac\|web)**<br>**no authentication (dot1x\|mac\|web)** |
| **Parameter** | |
| **Default** | Default is disabled for all type |
| **Mode** | Global Configuration |
| **Usage** | Use "**authentication**" command to enable the global setting of 802.1x/MAC/WEB authentication network access control.<br>Use the **no** form of this command to disable 802.1x/MAC/WEB authentication. |
| **Example** | The following example shows how to enable 802.1x/MAC/WEB authentication. |

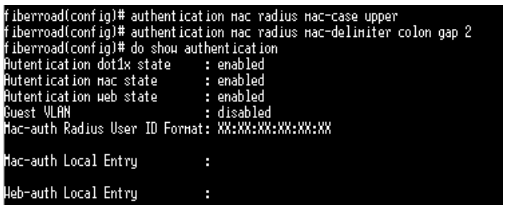
```
fiberroad(config)# authentication dot1x
fiberroad(config)# authentication mac
fiberroad(config)# authentication web
fiberroad(config)# exit
fiberroad# show authentication
Autentication dot1x state     : enabled
Autentication mac state       : enabled
Autentication web state       : enabled
Guest VLAN                    : disabled
Mac-auth Radius User ID Format: XXXXXXXXXXXX

Mac-auth Local Entry          :

Web-auth Local Entry          :

Interface Configurations

Interface GigabitEthernet1
  Admin Control          : disable
  Host Mode              : multi-auth
  Type dot1x State       : disabled
--More--
```

### 2.4.2 authentication (Interface)

| | |
|---|---|
| **Syntax** | **authentication (dot1x\|mac\|web)**<br>**no authentication (dot1x\|mac\|web)** |
| **Parameter** | |
| **Default** | Default is disabled for all type |
| **Mode** | Interface Configuration |
| **Usage** | Use "**authentication**" command to enable the global setting of 802.1x/MAC/WEB authentication network access control.<br>Use the **no** form of this command to disable 802.1x/MAC/WEB authentication. |
| **Example** | The following example shows how to enable 802.1x/MAC/WEB authentication.<br>`Switch(config)# interface GigabitEthernet 1`<br>`Switch(config-if)# authentication dot1x`<br>`Switch(config-if)# authentication mac`<br>`Switch(config-if)# authentication web`<br>`Switch# show authentication interface GigabitEthernet 1` |

```
fiberroad# configure
fiberroad(config)# interface
  GigabitEthernet     Gigabit ethernet interface to configure
  LAG                 IEEE 802.3 Link Aggregateion interface
  Loopback            Loopback interface
  TenGigabitEthernet  10 Gigabit ethernet interface to configure
  vlan                Vlan interface
  range               interface range command
fiberroad(config)# interface  GigabitEthernet
  <1-24>  GigabitEthernet
fiberroad(config)# interface  GigabitEthernet 1
fiberroad(config-if-GigabitEthernet1)# authentication dot1x
fiberroad(config-if-GigabitEthernet1)# authentication  mac
fiberroad(config-if-GigabitEthernet1)# authentication web
fiberroad(config-if-GigabitEthernet1)# exit
fiberroad(config)# shou authentication interfaces GigabitEthernet
Interface Configurations

Interface GigabitEthernet1
  Admin Control          : disable
  Host Mode              : multi-auth
  Type dot1x State       : enabled
  Type mac State         : enabled
  Type web State         : enabled
  Type Order             : dot1x
  MAC/WEB Method Order   : radius
  Guest VLAN             : disabled
  Reauthentication       : disabled
  Max Hosts              : 256
  VLAN Assign Mode       : static
  Common Timers
    Reauthenticate Period: 3600
--More--
```

### 2.4.3 authentication mac radius

| | | |
|---|---|---|
| **Syntax** | **authentication mac radius [mac-case (lower\|upper)] [mac-delimiter(colon\|dot\|hyphen\|none) [gap (2\|4\|6)]]** | |
| **Parameter** | **mac-case** (**lower**\|**upper**) | Select radius user id to be upper case or lower case. |
| | **mac-delimiter** (**colon**\|**dot**\|**hyphen**\|**none**) | Select radius user id delimiter colon: XX:XX:XX:XX:XX:XX dot: XX.XX.XX.XX.XX.XX hyphen: XX-XX-XX-XX-XX-XX none: XXXXXXXXXXXX |
| | **gap** (2\|4\|6) | Select delimiter gap 2: XX-XX-XX-XX-XX-XX 4: XXXX-XXXX-XXXX 6: XXXXXX-XXXXXX |
| **Default** | Default radius id format is upper case with none delimiter. | |
| **Mode** | Global Configuration | |
| **Usage** | Use “authentication mac radius” command to configure the radius user id format used by MAC authentication Radius method. | |
| **Example** | The following example shows how to configure MAC authentication radius id format to be upper case with colon delimiter every 2 chars<br>`Switch(config)# authentication mac radius mac- case upper`<br>`Switch(config)# authentication mac radius mac-delimiter colon gap 2`<br>`Switch# show authentication`<br>  | |

```
fiberroad(config)# authentication mac radius mac-case upper
fiberroad(config)# authentication mac radius mac-delimiter colon gap 2
fiberroad(config)# do show authentication
Autentication dot1x state     : enabled
Autentication mac state       : enabled
Autentication web state       : enabled
Guest VLAN                    : disabled
Mac-auth Radius User ID Format: XX:XX:XX:XX:XX:XX

Mac-auth Local Entry          :

Web-auth Local Entry          :
```

### 2.4.4 authentication mac local

| | |
|---|---|
| **Syntax** | **authentication mac local** mac-addr **control auth [vlan** <1-4094>**]** **[reauth-period** <300-4294967294>**] [inactive-timeout** <60-65535>**]**<br>**authentication mac local** mac-addr **control unauth no authentication mac local** mac-addr |

**Parameter**

| | |
|---|---|
| *mac-addr* | MAC Authentication local MAC address |
| **control auth** | Host with this MAC address will be authorized |
| **control unauth** | Host with this MAC address will be force unauthorized |
| **vlan <1-4094>** | MAC Authentication host assigned VLAN |
| **reauth-period <300-4294967294>** | MAC Authentication host reauthentication period |
| **inactive-timeout <60-65535>** | MAC authentication host inactive timeout |

| | |
|---|---|
| **Default** | Default is no local MAC Authentication entry. |
| **Mode** | Global Configuration |
| **Usage** | Use "**authentication mac local**" command to add local MAC authentication hosts in database. This local host database is used when MAC authentication method is configured as "local". The MAC authentication module will find host in this local database and authenticated it.<br>Use the **no** form of this command to delete local host from database. |
| **Example** | The following example shows how to add a new local mac authentication host.<br>`Switch(config)# authentication mac local 00:11:22:33:00:01 control auth vlan 3 reauth-period 500 inactive-timeout 300`<br>`Switch# show authentication` |


### 2.4.5 authentication guest-vlan

| | |
|---|---|
| **Syntax** | **authentication guest-vlan** <1-4094><br>**no authentication guest-vlan** |
| **Parameter** | <1-4094> Guest VLAN ID |
| **Default** | Default guest VLAN is disabled |
| **Mode** | Global Configuration |
| **Usage** | Use "**authentication guest-vlan**" command to enable the global setting of guest VLAN and specify guest VLAN ID.<br>Use the **no** form of this command to disable guest VLAN. |
| **Example** | The following example shows how to create guest VLAN.<br>`Switch(config)# vlan 3`<br>`Switch(config-vlan)# exit`<br>`Switch(config)# authentication guest-vlan 3`<br>`Switch# show authentication` |

### 2.4.6 authentication guest-vlan(Interface)

| | |
|---|---|
| **Syntax** | **authentication guest-vlan**<br>**no authentication guest-vlan** |
| **Parameter** | |
| **Default** | Default guest VLAN is disabled |
| **Mode** | Interface Configuration |
| **Usage** | Use "**authentication guest-vlan**" command to enable the port setting of guest VLAN.<br>Use the **no** form of this command to disable guest VLAN. |
| **Example** | The following example shows how to enable guest VLAN.<br>`Switch(config)# interface GigabitEthernet 2`<br>`Switch(config-if)# authentication guest-vlan`<br>`fiberroad(config)# interface GigabitEthernet 2`<br>`fiberroad(config-if-GigabitEthernet2)# authentication guest-vlan` |

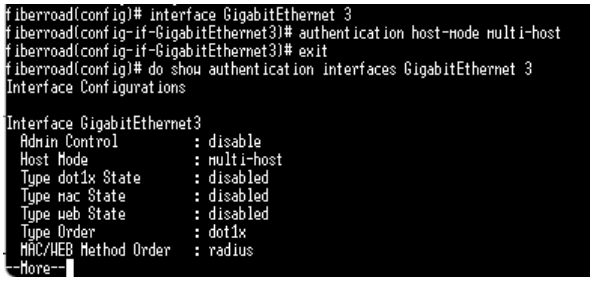
### 2.4.7 authentication host-mode

| | | |
|---|---|---|
| **Syntax** | **authentication host-mode (multi-auth\|multi-host\|single-host)**<br>**no authentication host-mode** | |
| **Parameter** | | |
| | **Multi-auth** | Multiple Authentication Mode. In this mode, every client need to pass authenticate procedure individually. |
| | **multi-host** | Multiple Host Mode. In this mode, only one client need to be authenticated and other clients will get the same access accessibility. |
| | **single-host** | Single Host Mode. In this mode, only one host is allowed to be authenticated. It is the same as multi-auth mode with max hosts number configure to be 1. |
| **Default** | Default is multi-auth mode. | |
| **Mode** | Interface Configuration | |

| | |
|---|---|
| **Usage** | Use "**authentication host-mode**" command to configure the port authentication host mode.<br>Use the **no** form of this command to restore default value. |

**Example** The following example shows how to modify port host mode to multi-host.

```
Switch(config)# interface GigabitEthernet 3
Switch(config-if)# authentication host-mode multi-host
Switch# show authentication interface GigabitEthernet3
```




### 2.4.8 authentication max-hosts

| | |
|---|---|
| **Syntax** | **authentication max-hosts** <1-256><br>**no authentication max-hosts** |
| **Parameter** | <1-256> Available max host number in multi-auth mode. |
| **Default** | Default max host number is 256 |
| **Mode** | Interface Configuration |
| **Usage** | Use "**authentication max-hosts**" command to configure the port max hosts number for multi-auth mode. The host exceed the max host number is not allowed to create authentication session and do authenticating.<br>Use **no** form of this command to restore default value. |

**Example** The following example shows how to change port max hosts number.

```
Switch(config)# interface gigabitethernet 1
Switch(config-if)# authentication max-hosts 100
Switch# show mac-auth interface gigabitethernet 1
Interface GigabitEthernet1
Admin Control  : disable
Host Mode  : multi-auth
Type dot1x State  : disabled
Type mac State : disabled
Type web State : disabled
Type Order : dot1x MAC/WEB Method Order  : radius
Guest VLAN : disabled
Reauthentication  : disabled
Max Hosts  : 100
```

### 2.4.9 authentication method

| | |
|---|---|
| **Syntax** | **authentication method (local [radius] \| radius [local])**<br>**no authentication order** |
| **Parameter** | **local** Use local account to authenticate<br>**radius** Use remote RADIUS server to authenticate |
| **Default** | Default is RADIUS method in first place and no other method. |
| **Mode** | Interface Configuration |
| **Usage** | Use "**authentication method**" command to configure the port authentication method order.<br>Use the **no** form of this command to restore default value. |
| **Example** | The following example shows how to modify port authentication order to local and then RADIUS.<br>`Switch(config)# interface GigabitEthernet 1`<br>`Switch(config-if)# authentication method local radius`<br>`Switch#show authentication interface GigabitEthernet 1` |

```
fiberroad(config)# interface GigabitEthernet 1
fiberroad(config-if-GigabitEthernet1)# authentication method local radius
fiberroad(config-if-GigabitEthernet1)# exit
fiberroad(config)# do show authentication interfaces GigabitEthernet 1
Interface Configurations

Interface GigabitEthernet1
  Admin Control         : disable
  Host Mode             : multi-auth
  Type dot1x State      : enabled
  Type mac State        : enabled
  Type web State        : enabled
  Type Order            : dot1x
  MAC/WEB Method Order  : local radius
  Guest VLAN            : disabled
  Reauthentication      : disabled
  Max Hosts             : 100
  VLAN Assign Mode      : static
  Common Timers
    Reauthenticate Period: 3600
    Inactive Timeout    : 60
```

### 2.4.10 authentication order

| | |
|---|---|
| **Syntax** | **authentication order (dot1x [mac] [web] \| mac [dot1x] [web] \|web)**<br>**no authentication order** |
| **Parameter** | **dot1x** Authenticating user by IEEE 802.1X<br>**mac** Authenticating user by mac based authentication<br>**web** Authenticating user by web based authentication |
| **Default** | Default is dot1x type in first place and no other types. |
| **Mode** | Interface Configuration |
| **Usage** | Use "**authentication order**" command to configure the port authentication type order.<br>Use the **no** form of this command to restore default value. |
| **Example** | The following example shows how to modify port authentication order to dot1x, mac and web.<br>`Switch(config)# interface fa1`<br>`Switch(config-if)# authentication order dot1x mac web`<br>`Switch# show authentication interface fa1` |

```
fiberroad(config)# interface GigabitEthernet 1
fiberroad(config-if-GigabitEthernet1)# authentication order dot1x mac web
fiberroad(config-if-GigabitEthernet1)# exit
fiberroad(config)# do show authentication interfaces GigabitEthernet 1
Interface Configurations

Interface GigabitEthernet1
  Admin Control          : disable
  Host Mode              : multi-auth
  Type dot1x State       : enabled
  Type mac State         : enabled
  Type web State         : enabled
  Type Order             : dot1x mac web
  MAC/WEB Method Order   : local radius
  Guest VLAN             : disabled
  Reauthentication       : disabled
  Max Hosts              : 100
  VLAN Assign Mode       : static
  Common Timers
    Reauthenticate Period: 3600
```

### 2.4.11 authentication port-control

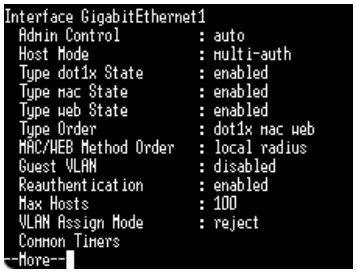
| | | |
|---|---|---|
| **Syntax** | **authentication port-control (auto\|force-auth\|force-unauth)**<br>**no authentication port-control** | |
| **Parameter** | **auto** | Need passing authentication procedure to get network accessibility |
| | **force-auth** | Port is force authorized and all clients have network accessibility |
| | **force-unauth** | Port is force unauthorized and all clients have no network accessibility |
| **Default** | Default is disabled. | |
| **Mode** | Interface Configuration | |
| **Usage** | Use "**authentication port-control**" command to enable the port authentication control mode.<br>Use the **no** form of this command to disable authentication port control. | |
| **Example** | The following example shows how to configure port control to auto mode.<br>`Switch(config)# interface GigabitEthernet 1`<br>`Switch(config-if)# authentication port-control auto`<br>`Switch#show authentication interface GigabitEthernet1` | |

### 2.4.12 authentication radius-attribution vlan

| | | |
|---|---|---|
| **Syntax** | **authentication radius-attributes vlan (reject \| static)**<br>**no authentication radius-attributes vlan** | |
| **Parameter** | **reject** | If get VLAN authorized information, just use it. However, if there is no VLAN authorized information, reject the host and make it unauthorized. |
| | **static** | If get VLAN authorized information, just use it. If there is no VLAN authorized information, keep original VLAN of host. |
| **Default** | Default radius attributes VLAN assign mode is static. | |
| **Mode** | Interface Configuration | |
| **Usage** | Use "**authentication radius-attributes vlan**" command to configure the port RADIUS VLAN assign mode.<br>Use the **no** form of this command to disable the port RADIUS VLAN assign. | |
| **Example** | The following example shows how to configure port VLAN assign to reject mode.<br>`Switch(config)# interface GigabitEthernet 1`<br>`Switch(config-if)# authentication radius-attributes vlan reject`<br>`Switch# show authentication interface GigabitEthernet 1`<br>  | |

```
fiberroad(config)# interface GigabitEthernet 1
(Ethernet1)# authentication radius-attributes vlan reject
fiberroad(config-if-GigabitEthernet1)# exit
fiberroad(config)# do show authentication interfaces GigabitEthernet 1
Interface Configurations

Interface GigabitEthernet1
  Admin Control         : auto
  Host Mode             : multi-auth
  Type dot1x State      : enabled
  Type mac State        : enabled
  Type web State        : enabled
  Type Order            : dot1x mac web
  MAC/WEB Method Order  : local radius
  Guest VLAN            : disabled
  Reauthentication      : disabled
  Max Hosts             : 100
  VLAN Assign Mode      : reject
  Common Timers
    Reauthenticate Period: 3600
    Inactive Timeout    : 60
    Quiet Period        : 60
  802.1x Parameters
--More--
```

### 2.4.13 authentication reauth

| | |
|---|---|
| **Syntax** | **authentication reauth**<br>**no authentication reauth** |
| **Parameter** | |
| **Default** | Default is disabled. |
| **Mode** | Interface Configuration |
| **Usage** | Use "**authentication reauth**" command to enable the port reauthentication.<br>Use the no form of this command to disable reauthentication. |
| **Example** | The following example shows how to enable port reauthentication.<br>`Switch(config)# interface GigabitEthernet 1`<br>`Switch(config-if)# authentication reauth`<br>`Switch# show authentication interface GigabitEthernet 1`<br>  |

### 2.4.14 authentication timer inactive

| | |
|---|---|
| **Syntax** | **authentication timer inactive** <60-65535><br>**no authentication timer inactive** |
| **Parameter** | <60-65535> **Interval in seconds after which if there is no activity from the client then it will be unauthorized** |
| **Default** | Default inactive timeout is 60 seconds. |
| **Mode** | Interface Configuration |
| **Usage** | Use "**authentication timer inactive**" command to configure the port inactive timeout value.<br>Sometimes, we may assign a long aging time for a host, but in fact, it is not active. This inactive timeout will detect the host is active or not. If the host is inactive exceed this timeout, it should be removed.<br>Use **no** form of this command to restore default value. |
| **Example** | The following example shows how to configure port inactive period.<br>`Switch(config)# interface GigabitEthernet 1`<br>`Switch(config-if)# authentication timer inactive 300`<br>`Switch#show authentication interface GigabitEthernet 1` |

```
fiberroad(config)# interface GigabitEthernet 1
fiberroad(config-if-GigabitEthernet1)# authentication timer inactive 300
fiberroad(config-if-GigabitEthernet1)# exit
fiberroad(config)# do show authentication interfaces GigabitEthernet 1
Interface Configurations

Interface GigabitEthernet1
  Admin Control          : auto
  Host Mode              : multi-auth
  Type dot1x State       : enabled
  Type mac State         : enabled
  Type web State         : enabled
  Type Order             : dot1x mac web
  MAC/WEB Method Order   : local radius
  Guest VLAN             : disabled
  Reauthentication       : enabled
  Max Hosts              : 100
  VLAN Assign Mode       : reject
  Common Timers
    Reauthenticate Period: 3600
    Inactive Timeout     : 300
    Quiet Period         : 60
  802.1x Parameters
--More--
```

### 2.4.15 authentication timer quiet

| | |
|---|---|
| **Syntax** | **authentication timer quiet** <0-65535><br>**no authentication timer quiet** |
| **Parameter** | <0-65535> **Interval in seconds to wait following a failed authentication exchange** |
| **Default** | Default quiet period is 60 seconds. |
| **Mode** | Interface Configuration |
| **Usage** | Use "**authentication timer quiet**" command to configure the port quiet period value.<br>After authenticating fail many times and the port is guest VLAN disabled, the port/host will enter lock state until quiet period expired. In lock state, the port/host is not allowed to do authenticating.<br>Use **no** form of this command to restore default value. |
| **Example** | The following example shows how to configure port quiet period.<br>`Switch(config)# interface GigabitEthernet 1`<br>`Switch(config-if)# authentication timer quiet 300`<br>`Switch#show authentication interface GigabitEthernet 1` |

```
fiberroad(config)# interface GigabitEthernet 1
fiberroad(config-if-GigabitEthernet1)# authentication timer quiet 300
fiberroad(config-if-GigabitEthernet1)# exit
fiberroad(config)# do show authentication interfaces GigabitEthernet 1
Interface Configurations

Interface GigabitEthernet1
  Admin Control          : auto
  Host Mode              : multi-auth
  Type dot1x State       : enabled
  Type mac State         : enabled
  Type web State         : enabled
  Type Order             : dot1x mac web
  MAC/WEB Method Order   : local radius
  Guest VLAN             : disabled
  Reauthentication       : enabled
  Max Hosts              : 100
  VLAN Assign Mode       : reject
  Common Timers
    Reauthenticate Period: 3600
    Inactive Timeout     : 300
    Quiet Period         : 300
  802.1x Parameters
    EAP Max Request      : 2
    EAP TX Period        : 30
--More--
```

### 2.4.16 authentication timer reauth

| | | |
|---|---|---|
| **Syntax** | **authentication timer reauth** <300-4294967294><br>**no authentication timer reauth** | |
| **Parameter** | <300-4294967294> | Time in seconds after which an automatic re-authentication should be initiated |
| **Default** | Default reauthentication period is 3600 seconds. | |
| **Mode** | Interface Configuration | |
| **Usage** | Use "**authentication timer reauth**" command to configure the port reauthentication period value with unit second if the reauthentication time is not assigned by local database or remote authentication server. On the other hand, if the reauthentication time is assigned by local database or remote server, this configured reauthentication time will be ignored.<br>Use **no** form of this command to restore default value. | |
| **Example** | The following example shows how to configure port reauthentication period.<br>`Switch(config)# interface GigabitEthernet 1`<br>`Switch(config-if)# authentication timer reauth 300`<br>`Switch# show authentication interface GigabitEthernet1` | |

```
fiberroad(config-if-GigabitEthernet1)# authentication timer reauth 300
fiberroad(config-if-GigabitEthernet1)# exit
fiberroad(config)# do show authentication interfaces GigabitEthernet 1
Interface Configurations

Interface GigabitEthernet1
  Admin Control          : auto
  Host Mode              : multi-auth
  Type dot1x State       : enabled
  Type mac State         : enabled
  Type web State         : enabled
  Type Order             : dot1x mac web
  MAC/WEB Method Order   : local radius
  Guest VLAN             : disabled
  Reauthentication       : enabled
  Max Hosts              : 100
  VLAN Assign Mode       : reject
  Common Timers
    Reauthenticate Period: 300
    Inactive Timeout     : 300
    Quiet Period         : 300
  802.1x Parameters
    EAP Max Request      : 2
    EAP TX Period        : 30
    Supplicant Timeout   : 30
    Server Timeout       : 30
  Web-auth Parameters
    Login Attempt        : 3
```

### 2.4.17 authentication web local

**Syntax**

**authentication web local username USERNAME password (encrypted CRYPT-PASSWORD | PASSWORD) [vlan <1-4094>] [reauth-period <300-4294967294>] [inactive-timeout <60-65535>]**
**no authentication web local username USERNAME**

**Parameter**

| | |
|---|---|
| **USERNAME** | Local account user name |
| **encrypted** CRYPT-PASSWORD | Encrypted password. |
| PASSWORD | Un-encrypted password. |
| **vlan** <1-4094> | Assigned VLAN of this local account |
| **reauth-period** <300-4294967294> | Reauthentication period of this local account |
| **inactive-timeout** <60-65535> | Inactive timeout of this local account |

**Default**

Default is no local authentication entry.

**Mode**

Global Configuration

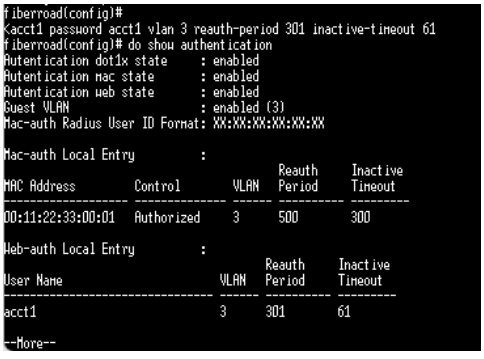
**Usage**

Use "**authentication web local**" command to add local account in database. This local account database is used when web authentication method is configured as "local". The web authentication module will find account in this local database and authenticated it.
Use the **no** form of this command to delete local account from database.

**Example**

The following example shows how to add/delete a new local account.

```
Switch(config)# authentication web local username
acct1 password acct1 vlan 3 reauth-period 301
inactive-timeout 61
Switch# show authentication
```



### 2.4.18 authentication web max-login-attempts

| | |
|---|---|
| **Syntax** | **authentication web max-login-attempts (infinite\|<3-10>)**<br>**no authentication web max-login-attempts** |
| **Parameter** | **infinite** Do not care user login fail number<br>**<3-10>** Allow user login fail number |
| **Default** | Default max login attempt number is 3. |
| **Mode** | Interface Configuration |
| **Usage** | Use "**authentication web max-login-attempts**" command to configure the port WEB authentication max login attempt number. After login fail number exceed, the host will enter Lock state and is not able to authenticate until quiet period exceed.<br>Use **no** form of this command to restore default value. |
| **Example** | The following example shows how to configure port max login attempt number.<br>`Switch(config)# interface GigabitEthernet 1`<br>`Switch(config-if)# authentication web max-login-attempts 5`<br>`Switch# show authentication interface GigabitEthernet 1` |

```
fiberroad(config)# interface GigabitEthernet 1
(Ethernet1)# authentication web max-login-attempts 5
fiberroad(config-if-GigabitEthernet1)# exit
fiberroad(config)# do show authentication interfaces GigabitEthernet 1
Interface Configurations

Interface GigabitEthernet1
  Admin Control          : auto
  Host Mode              : multi-auth
  Type dot1x State       : enabled
  Type mac State         : enabled
  Type web State         : enabled
  Type Order             : dot1x mac web
  MAC/WEB Method Order   : local radius
  Guest VLAN             : disabled
  Reauthentication       : enabled
  Max Hosts              : 100
  VLAN Assign Mode       : reject
  Common Timers
    Reauthenticate Period: 300
    Inactive Timeout     : 300
    Quiet Period         : 300
  802.1x Parameters
    EAP Max Request      : 2
    EAP TX Period        : 30
    Supplicant Timeout   : 30
    Server Timeout       : 30
  Web-auth Parameters
    Login Attempt        : 5
fiberroad(config)#
```

### 2.4.19 clear authentication sessions

| | |
|---|---|
| **Syntax** | **clear authentication sessions**<br>**clear authentication sessions interfaces IF_PORTS**<br>**clear authentication sessions mac mac-addr**<br>**clear authentication sessions session-id WORD**<br>**clear authentication sessions type (dot1x\|mac\|web)** |

**Parameter**

| | |
|---|---|
| **interfaces** IF_PORTS | Clear sessions on specific interface |
| **mac** mac-addr | Clear session with specific MAC address |
| **session-id** WORD | Clear session with specific session ID |
| **type (dot1x\|mac\|web)** | Clear session with specific authentication type |

| | |
|---|---|
| **Default** | Default is no local authentication entry. |
| **Mode** | Privileged EXEC |
| **Usage** | Use "**clear authentication sessions**" command to delete existing authentication sessions. If no parameter is specified, all sessions will be deleted.<br>After authentication session is deleted, host need to do authentication procedure again. |
| **Example** | The following example shows how to clear all authentication sessions.<br>`Switch# clear authentication sessions`<br>`Switch# show authentication sessions`<br>  |

### 2.4.20 dot1x

| | |
|---|---|
| **Syntax** | **dot1x / no dot1x** |
| **Parameter** | |
| **Default** | Default 802.1x is disabled |
| **Mode** | Global Configuration |
| **Usage** | Use "**dot1x**" command to enable the global setting of 802.1x. The "**authentication dot1x**" command has the same effect as this one. This command is a backward compatible command. Use the **no** form of this command to disable 802.1x authentication. |
| **Example** | The following example shows how to enable 802.1x authentication.<br>`Switch(config)# dot1x`<br>`Switch# show authentication`<br>  |

```
fiberroad(config)# dot1x
fiberroad(config)# do show authentication
Autentication dot1x state     : enabled
Autentication mac state       : enabled
Autentication web state       : enabled
Guest VLAN                    : enabled (3)
Mac-auth Radius User ID Format: XX:XX:XX:XX:XX:XX

--More--
```

### 2.4.21 dot1x guest-vlan

| | |
|---|---|
| **Syntax** | **dot1x guest-vlan <1-4094>**<br>**no dot1x guest-vlan** |
| **Parameter** | <1-4094> Guest VLAN ID |
| **Default** | Default guest VLAN is disabled |
| **Mode** | Global Configuration |
| **Usage** | Use "**dot1x guest-vlan**" command to enable the global setting of guest VLAN and specify guest VLAN ID.<br>Use the **no** form of this command to disable guest VLAN. |
| **Example** | The following example shows how to enable 802.1x authentication.<br>The following example shows how to create guest VLAN.<br>  |

```
fiberroad(config)# vlan 3
fiberroad(config-vlan)# exit
fiberroad(config)# dot1x guest-vlan 3
fiberroad(config)# exit
fiberroad# show authentication
Autentication dot1x state     : enabled
Autentication mac state       : enabled
Autentication web state       : enabled
Guest VLAN                    : enabled (3)
Mac-auth Radius User ID Format: XX:XX:XX:XX:XX:XX
```

### 2.4.22 dot1x max-req

| | | |
|---|---|---|
| **Syntax** | **dot1x max-req <1-10>**<br>**no dot1x max-req** | |
| **Parameter** | <1-10> | The maximum number of EAP requests that can be sent. If a response is not received after the defined period (supplicant timeout),the authentication process is restarted. |
| **Default** | Default EAP max request number is 2. | |
| **Mode** | Interface Configuration | |
| **Usage** | Use "**dot1x max-req**" command to configure the port 802.1x max EAP request value. The max request is the maximum number of EAP requests that can be sent. If a response is not received after the defined period (supplicant timeout), the authentication process is restarted.<br>Use **no** form of this command to restore default value. | |
| **Example** | The following example shows how to configure port 802.1x EAP TX period.<br>`Switch(config)# interface GigabitEthernet 1`<br>`Switch(config-if)# dot1x max-req 1`<br>`Switch# show authentication interface GigabitEthernet 1` | |

```
fiberroad(config)# interface GigabitEthernet 1
fiberroad(config-if-GigabitEthernet1)# dot1x max-req 1
fiberroad(config-if-GigabitEthernet1)# exit
fiberroad(config)# do shou authentication interfaces GigabitEthernet 1
Interface Configurations

Interface GigabitEthernet1
  Admin Control          : auto
  Host Mode              : multi-auth
  Type dot1x State       : enabled
  Type mac State         : enabled
  Type web State         : enabled
  Type Order             : dot1x mac web
  MAC/WEB Method Order   : local radius
  Guest VLAN             : disabled
  Reauthentication       : enabled
  Max Hosts              : 100
  VLAN Assign Mode       : reject
  Common Timers
    Reauthenticate Period: 300
    Inactive Timeout     : 300
    Quiet Period         : 300
  802.1x Parameters
    EAP Max Request      : 1
    EAP TX Period        : 30
    Supplicant Timeout   : 30
    Server Timeout       : 30
  Web-auth Parameters
    Login Attempt        : 5
```

### 2.4.23 dot1x port-control

| | |
|---|---|
| **Syntax** | **dot1x port-control (auto\|force-auth\|force-unauth)**<br>**no dot1x port-control** |
| **Parameter** | **auto** — Need passing authentication procedure to get network accessibility<br>**force-auth** — Port is force authorized and all clients have network accessibility.<br>**Force-unauth** — Port is force unauthorized and all clients have no network accessibility. |
| **Default** | Default is disabled. |
| **Mode** | Interface Configuration |
| **Usage** | Use "**dot1x port-control**" command to enable the port authentication control mode. The "**authentication port-control**" command has the same effect. Use the **no** form of this command to disable authentication port control. |
| **Example** | The following example shows how to configure port control to auto mode.<br>`Switch(config)# interface fa1`<br>`Switch(config-if)# dot1x port-control auto`<br>`Switch# show authentication interface fa1` |

```
fiberroad(config)# interface GigabitEthernet 1
fiberroad(config-if-GigabitEthernet1)# dot1x port-control auto
fiberroad(config-if-GigabitEthernet1)# exit
fiberroad(config)# do show authentication interfaces GigabitEthernet 1
Interface Configurations

Interface GigabitEthernet1
  Admin Control          : auto
  Host Mode              : multi-auth
  Type dot1x State       : enabled
  Type mac State         : enabled
  Type web State         : enabled
  Type Order             : dot1x mac web
```

### 2.4.24 dot1x reauth

| | |
|---|---|
| **Syntax** | **dot1x reauth / no dot1x reauth** |
| **Parameter** | |
| **Default** | Default is disabled. |
| **Mode** | Interface Configuration |
| **Usage** | Use "**dot1x reauth**" command to enable the port reauthentication. The "**authentication reauth**" command has the same effect, it is a backward compatible command<br>Use the **no** form of this command to disable reauthentication. |
| **Example** | The following example shows how to enable port reauthentication.<br>`Switch(config)# interface GigabitEthernet 1`<br>`Switch(config-if)# dot1x reauth`<br>`Switch# show authentication interface GigabitEthernet 1` |

```
fiberroad(config)# interface GigabitEthernet 1
fiberroad(config-if-GigabitEthernet1)# dot1x reauth
fiberroad(config-if-GigabitEthernet1)# exit
fiberroad(config)# do show authentication interfaces GigabitEthernet 1
Interface Configurations

Interface GigabitEthernet1
  Admin Control          : auto
  Host Mode              : multi-auth
  Type dot1x State       : enabled
  Type mac State         : enabled
  Type web State         : enabled
  Type Order             : dot1x mac web
  MAC/WEB Method Order   : local radius
  Guest VLAN             : disabled
  Reauthentication       : enabled
  Max Hosts              : 100
  VLAN Assign Mode       : reject
  Common Timers
    Reauthenticate Period: 300
    Inactive Timeout     : 300
    Quiet Period         : 300
  802.1x Parameters
    EAP Max Request      : 1
--More--
```

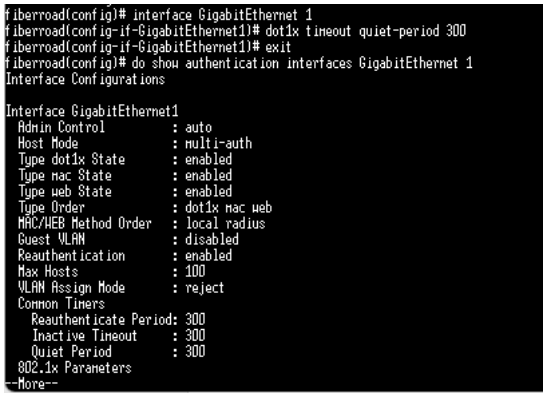
### 2.4.25 dot1x timeout reauth-period

| | |
|---|---|
| **Syntax** | **dot1x timeout reauth-period** <300-4294967294><br>**no dot1x timeout reauth-period** |
| **Parameter** | <300-4294967294> Time in seconds after which an automatic re-authentication should be initiated |
| **Default** | Default reauthentication period is 3600 seconds. |
| **Mode** | Interface Configuration |
| **Usage** | Use "**dot1x timout reauth**" command to configure the port reauthentication period value with unit second if the reauthentication time is not assigned by local database or remote authentication server. On the other hand, if the reauthentication time is assigned by local database or remote server, this configured reauthentication time will be ignored.<br>The "**authentication timer reauth**" command has the same effect and it is a backward compatible command.<br><br>Use no form of this command to restore default value. |
| **Example** | The following example shows how to configure port 802.1x reauthentication period.<br>`Switch(config)#interface GigabitEthernet 1`<br>`Switch(config-if)#dot1x timeout reauth-period 300`<br>`Switch#show authentication interface GigabitEthernet 1` |

```
fiberroad(config)# interface GigabitEthernet 1
fiberroad(config-if-GigabitEthernet1)# dot1x timeout reauth-period 300
fiberroad(config-if-GigabitEthernet1)# exit
fiberroad(config)# do show authentication interfaces GigabitEthernet 1
Interface Configurations

Interface GigabitEthernet1
  Admin Control          : auto
  Host Mode              : multi-auth
  Type dot1x State       : enabled
  Type mac State         : enabled
  Type web State         : enabled
  Type Order             : dot1x mac web
  MAC/WEB Method Order   : local radius
  Guest VLAN             : disabled
  Reauthentication       : enabled
  Max Hosts              : 100
  VLAN Assign Mode       : reject
  Common Timers
    Reauthenticate Period: 300
    Inactive Timeout     : 300
    Quiet Period         : 300
  802.1x Parameters
    EAP Max Request      : 1
    EAP TX Period        : 30
    Supplicant Timeout   : 30
    Server Timeout       : 30
--More--
```

### 2.4.26 dot1x timeout quiet-period

| | |
|---|---|
| **Syntax** | **dot1x timeout quiet-period** <0-65535><br>**no dot1x timeout quiet-period** |
| **Parameter** | <0-65535> Interval in seconds to wait following a failed authentication exchange |
| **Default** | Default quiet period is 60 seconds. |
| **Mode** | Interface Configuration |
| **Usage** | Use "**dot1x timeout quiet-period**" command to configure the port quiet period value. The "**authentication timer quiet**" command has the same effect and it is backward compatible command.<br>After authenticating fail many times and the port is guest VLAN disabled, the port/host will enter lock state until quiet period expired. In lock state, the port/host is not allowed to do authenticating.<br>Use **no** form of this command to restore default value. |
| **Example** | The following example shows how to configure port 802.1x quiet period.<br>`Switch(config)# interface GigabitEthernet 1`<br>`Switch(config-if)# dot1x timeout quiet-period 300`<br>`Switch# show authentication GigabitEthernet 1` |



### 2.4.27 dot1x timeout server-timeout

| | |
|---|---|
| **Syntax** | **dot1x timeout server-timeout** <1-65535><br>**no dot1x timeout server-timeout** |
| **Parameter** | <1-65535> Number of seconds that lapses before the device resends a request to the authentication server. |
| **Default** | Default server timeout is 30 seconds. |
| **Mode** | Interface Configuration |
| **Usage** | Use "**dot1x timeout server-timeout**" command to configure the port 802.1x server timeout value. The server timeout is the number of seconds that lapses before the device resends a request to the authentication server.<br>Use **no** form of this command to restore default value. |
| **Example** | The following example shows how to configure port 802.1x server timeout.<br>`Switch(config)# interface GigabitEthernet 1`<br>`Switch(config-if)# dot1x timeout supp-timeout 150`<br>`Switch# show authentication interface GigabitEthernet 1` |

```
fiberroad(config)# interface GigabitEthernet 1
fiberroad(config-if-GigabitEthernet1)# dot1x timeout supp-timeout 150
fiberroad(config-if-GigabitEthernet1)# exit
fiberroad(config)# do show authentication interfaces GigabitEthernet 1
Interface Configurations

Interface GigabitEthernet1
  Admin Control          : auto
  Host Mode              : multi-auth
  Type dot1x State       : enabled
  Type mac State         : enabled
  Type web State         : enabled
  Type Order             : dot1x mac web
  MAC/WEB Method Order   : local radius
  Guest VLAN             : disabled
  Reauthentication       : enabled
  Max Hosts              : 100
  VLAN Assign Mode       : reject
  Common Timers
    Reauthenticate Period: 300
    Inactive Timeout     : 300
    Quiet Period         : 300
  802.1x Parameters
    EAP Max Request      : 1
    EAP TX Period        : 30
    Supplicant Timeout   : 150
    Server Timeout       : 30
  Web-auth Parameters
```

### 2.4.28 dot1x timeout supp-timeout

| | |
|---|---|
| **Syntax** | **dot1x timeout supp-timeout** <1-65535><br>**no dot1x timeout supp-timeout** |
| **Parameter** | <1-65535> Number of seconds that lapses before EAP requests are resent to the supplicant |
| **Default** | Default supplicant timeout is 30 seconds. |
| **Mode** | Interface Configuration |
| **Usage** | Use "**dot1x timeout supp-timeout**" command to configure the port supplicant timeout value. The supplicant timeout is the number of seconds that lapses before EAP requests are resent to the supplicant. Use **no** form of this command to restore default value. |
| **Example** | The following example shows how to configure port 802.1x supplicant timeout.<br>`Switch(config)# interface GigabitEtheret`<br>`Switch(config-if)# dot1x timeout supp-timeout 120`<br>`Switch# show authentication interface GigabitEthernet 1` |

```
Interface GigabitEthernet1
  Admin Control          : auto
  Host Mode              : multi-auth
  Type dot1x State       : enabled
  Type mac State         : enabled
  Type web State         : enabled
  Type Order             : dot1x mac web
  MAC/WEB Method Order   : local radius
  Guest VLAN             : disabled
  Reauthentication       : enabled
  Max Hosts              : 100
  VLAN Assign Mode       : reject
  Common Timers
    Reauthenticate Period: 300
    Inactive Timeout     : 300
    Quiet Period         : 300
  802.1x Parameters
    EAP Max Request      : 1
    EAP TX Period        : 30
    Supplicant Timeout   : 120
    Server Timeout       : 30
  Web-auth Parameters
    Login Attempt        : 5
```

### 2.4.29 dot1x timeout tx-period

| | |
|---|---|
| **Syntax** | **dot1x timeout tx-period** <1-65535><br>**no dot1x timeout tx-period** |
| **Parameter** | <1-65535> Number of seconds that the device waits for a r esponse to an Extensible Authentication Protocol (EAP) request/identity frame from the supplicant (client) before resending the request. |
| **Default** | Default EAP TX period is 30 seconds. |
| **Mode** | Interface Configuration |
| **Usage** | Use "**dot1x timeout tx-period**" command to configure the port 802.1x EAP TX period value. The TX period is the number of seconds that the device waits for a response to an Extensible Authentication Protocol (EAP) request/identity frame from the supplicant (client) before resending the request.<br>Use **no** form of this command to restore default value. |
| **Example** | The following example shows how to configure port 802.1x EAP TX period.<br>`Switch(config)# interface GigabitEthernet 1`<br>`Switch(config-if)# dot1x timeout tx-period 10`<br>`Switch# show authentication interface GigabitEthernet 1` |

```
fiberroad# configure
fiberroad(config)# interface GigabitEthernet 1
fiberroad(config-if-GigabitEthernet1)# dot1x timeout tx-period 10
fiberroad(config-if-GigabitEthernet1)# end
fiberroad# show authentication interfaces GigabitEthernet 1
Interface Configurations

Interface GigabitEthernet1
  Admin Control         : auto
  Host Mode             : multi-auth
  Type dot1x State      : enabled
  Type mac State        : enabled
  Type web State        : enabled
  Type Order            : dot1x mac web
  MAC/WEB Method Order  : local radius
  Guest VLAN            : disabled
  Reauthentication      : enabled
  Max Hosts             : 100
  VLAN Assign Mode      : reject
  Common Timers
    Reauthenticate Period: 300
    Inactive Timeout    : 300
    Quiet Period        : 300
  802.1x Parameters
    EAP Max Request     : 1
    EAP TX Period       : 10
    Supplicant Timeout  : 120
    Server Timeout      : 30
  Web-auth Parameters
    Login Attempt       : 5
```

## 2.4.30 show authentication

| | |
|---|---|
| **Syntax** | **show authentication**<br>**show authentication interfaces** IF_PORTS |
| **Parameter** | **interfaces** Specify port list to show port configurations.<br>IF_PORTS |
| **Default** | No default value for this command. |
| **Mode** | Privileged EXEC |
| **Usage** | Use "**show authentication**" command to show all authentication manager configurations.<br>Use "**show authentication interface**" command to show authentication manager configuration of specific port. |
| **Example** | This example shows how to show the mac authentication configurations of port GigabitEthernet 1. |

```
fiberroad# show authentication
Autentication dot1x state     : enabled
Autentication mac state       : enabled
Autentication web state       : enabled
Guest VLAN                    : enabled (3)
Mac-auth Radius User ID Format: XX:XX:XX:XX:XX:XX

Mac-auth Local Entry          :
                                          Reauth     Inactive
MAC Address        Control       VLAN     Period     Timeout
------------------ ------------- ------ ---------- ----------
00:11:22:33:00:01  Authorized    3      500        300

Web-auth Local Entry          :
                                          Reauth     Inactive
User Name                         VLAN    Period     Timeout
-------------------------------- ------ ---------- ---------
acct1                             3      301        61

Interface Configurations

Interface GigabitEthernet1
  Admin Control          : auto
  Host Mode              : multi-auth
  Type dot1x State       : enabled
  Type mac State         : enabled
  Type web State         : enabled
  Type Order             : dot1x mac web
  MAC/WEB Method Order   : local radius
  Guest VLAN             : disabled
  Reauthentication       : enabled
  Max Hosts              : 100
  VLAN Assign Mode       : reject
  Common Timers
    Reauthenticate Period: 300
    Inactive Timeout     : 300
    Quiet Period         : 300
  802.1x Parameters
    EAP Max Request      : 1
    EAP TX Period        : 10
    Supplicant Timeout   : 120
    Server Timeout       : 30
  Web-auth Parameters
    Login Attempt        : 5
```

## 2.4.31 show authentication sessions

**Syntax**

**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** | Show session detail information. |
| **interface** | Show session detail information of specific |
| **IF_PORTS** | port |
| **session-id** WORD | Show session detail information of specific session id |
| **type (dot1x\|mac\|web)** | Show session detail information of specific authentication type |

**Default**

No default value for this command.

**Mode**

Privileged EXEC

**Usage**

Use "**show authentication sessions**" command to show authentication detail session information.

**Example**

This example shows how to show current authentication session brief and detail information.

```
Switch# show authentication sessions
Interface  MAC Address       Type    Status       Session ID
---------- ----------------- ------- ------------ ----------------
fa7        00:01:6C:CB:29:4A dot1x   Authorized   000000010000A028

Switch# show authentication sessions detail
Interface               : FastEthernet7
MAC Address             : 00:01:6C:CB:29:4A
Session ID              : 000000010000A028
Current Type            : dot1x
Status                  : Authorized
Authorized Information
  VLAN                  : 5 (from RADIUS)
  Reauthenticate Period: 301 (from RADIUS)
  Inactive Timeout      : 600 (from RADIUS)
Operational Information
  VLAN                  : 5
  Session Time          : 1143
  Inactive Time         : 168
  Quiet Time            : N/A
```

## 2.5 Diagnostic

### 2.5.1 show cable-diag

| | | |
|---|---|---|
| **Syntax** | **show cable-diag interfaces** IF_NMLPORTS | |
| **Parameter** | **interfaces** IF_NMLPORTS | Display the cable diagnostic information of the copper media for an interface ID or a list of interfaces IDs. |
| **Default** | N/A | |
| **Mode** | Privileged EXEC | |
| **Usage** | To show the estimated copper cable length attached to a specific interface, use the command **show cable-diag** in the Privilegeg EXEC mode. For the proper information of the cable length, the interface must be active and linked up. | |
| **Example** | The following example shows the result of cable diagnostic for the interface GigabitEthernet 24 | |

```
fiberroad# shou cable-diag interfaces GigabitEthernet 24
 Port    | Speed | Local pair | Pair length | Pair status
---------+-------+------------+-------------+--------------
 gi24    | auto  |   Pair A   |     9.00    | Normal
                   |   Pair B   |     9.00    | Normal
                   |   Pair C   |     9.00    | Normal
                   |   Pair D   |     9.00    | Normal
```

### 2.5.2 show fiber-transceiver

| | |
|---|---|
| **Syntax** | **show fiber-transceiver interfaces** IF_NMLPORTS |
| **Parameter** | **interfaces** IF_NMLPORTS Display the o diagnostic information of the fiber transceiver for an interface ID or a list of interface IDs. |
| **Default** | N/A |
| **Mode** | Privileged EXEC |
| **Usage** | To show the diagnostic information of the fiber transceiver use the command **show fiber-transceiver** in the Privilegeg EXEC mode. |
| **Example** | The following example shows the diagnostic information for the interface gi1 and gi2, where the interface fiber media ports with the transceiver inserted. |

## 2.6 DHCP Snooping

### 2.6.1 ip dhcp snooping

| | |
|---|---|
| **Syntax** | **ip dhcp snooping**<br>**no ip dhcp snooping** |
| **Parameter** | N/A |
| **Default** | DHCP snooping is disabled |
| **Mode** | Global Configuration |
| **Usage** | Use the ip dhcp snooping command to enable DHCP Snooping function. Use the no form of this command to disable. |
| **Example** | The example shows how to enable DHCP Snooping on VLAN 1. You can verify settings by the following show ip dhcp snooping command. |

```
fiberroad# configure
fiberroad(config)# ip dhcp snooping
fiberroad(config)# ip dhcp snooping vlan 1
fiberroad(config)# do show ip dhcp snooping

DHCP Snooping            : enabled
Enable on following Vlans : 1
    circuit-id default format: vlan-port
    remote-id:              : 00:18:95:83:fb:ac (Switch Mac in Byte Order)
```

### 2.6.2 ip dhcp snooping vlan

| | |
|---|---|
| **Syntax** | **ip dhcp snooping vlan VLAN-LIST** |
| **Parameter** | **VLAN-LIST** Specify VLAN ID or a range of VLANs to enable or disable dynamic Arp inspection |
| **Default** | Default is disabled on all VLANs |
| **Mode** | Global Configuration |
| **Usage** | Use the **ip dhcp snooping vlan** command to enable VLANs on DHCP Snooping function. Use the **no** form of this command to disable VLANs on DHCP Snooping function. |
| **Example** | The example shows how to enable VLAN 1-100 on DHCP Snooping, and then disable VLAN 30-40 on DHCP Snooping. You can verify settings by the following **show ip dhcp snooping** command. |

```
fiberroad(config)# vlan 1-100
fiberroad(config-vlan)# exit
fiberroad(config)# ip dhcp snooping
fiberroad(config)# ip dhcp snooping vlan 1-100
fiberroad(config)# do show ip dhcp snooping

DHCP Snooping            : enabled
Enable on following Vlans : 1-100
    circuit-id default format: vlan-port
    remote-id:               : 00:18:95:83:fb:ac (Switch Mac in Byte Order)

fiberroad(config)#
fiberroad(config)# no ip dhcp snooping vlan 30-40
fiberroad(config)# do show ip dhcp snooping

DHCP Snooping            : enabled
Enable on following Vlans : 1-29,41-100
    circuit-id default format: vlan-port
    remote-id:               : 00:18:95:83:fb:ac (Switch Mac in Byte Order)

fiberroad(config)#
fiberroad(config)#
```

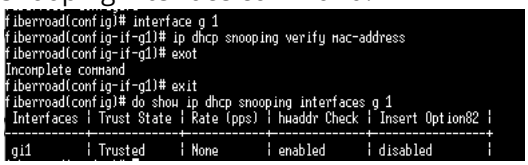
### 2.6.3 ip dhcp snooping trust

| | |
|---|---|
| **Syntax** | **ip dhcp snooping /trust no ip dhcp / snooping trust** |
| **Parameter** | |
| **Default** | DHCP snooping trust is disabled |
| **Mode** | Interface Configuration |
| **Usage** | Use the **ip dhcp snooping trust** command to set trusted interface. The switch does not check DHCP packets that are received on the trusted interface; it simply forwards it. Use the no form of this command to set untrusted interface. |
| **Example** | The example shows how to set interface gi1 to trust. You can verify |

settings by the following show ip dhcp snooping interface command.


### 2.6.4 ip dhcp snooping verify

| | |
|---|---|
| **Syntax** | **ip dhcp snooping verify mac-address**<br>**[no] ip dhcp snooping verify mac-address** |
| **Parameter** | N/A |
| **Default** | DHCP snooping verify mac-address is disabled |
| **Mode** | Interface Configuration |
| **Usage** | Use the **ip dhcp snooping verify** command to verify MAC address function on interface.<br>The “mac-address” drop DHCP packets that chaddr and ethernetsource-mac is not match. |
| **Example** | The example shows how to set interface gi1 to validate “mac-address”. You can verify settings by the following show ip dhcp snooping interface command. |



### 2.6.5 ip dhcp snooping rate-limit

| | |
|---|---|
| **Syntax** | **ip dhcp snooping rate-limit <1-300>**<br>**[no] ip dhcp snooping rate-limit** |
| **Parameter** | <1-300> Set 1 to 300 PPS of DHCP packet rate limitation |
| **Default** | Default is un-limited of DHCP packet |
| **Mode** | Interface Configuration |
| **Usage** | Use the ip dhcp snooping rate-limit command to set rate limitation on interface. The switch drop DHCP packets after receives more than configured rate of packets per second. Use the no form of this command to return to default settings. |
| **Example** | The example shows how to set rate limit to 30 pps on interface gi1.You can verify settings by the following **show ip dhcp snooping interface** command. |

```
fiberroad(config-if-g1)# ip dhcp snooping rate-limit 30
fiberroad(config-if-g1)# exit
fiberroad(config)# do show ip dhcp snooping interfaces g 1
 Interfaces | Trust State | Rate (pps) | hwaddr Check | Insert Option82 |
------------+------------+------------+--------------+-----------------+
 gi1        | Trusted    | 30         | enabled      | disabled        |
```

### 2.6.6 clear ip dhcp snooping statistics

| | |
|---|---|
| **Syntax** | **clear ip dhcp snooping interfaces IF_PORTS statistics** |
| **Parameter** | IF_PORTS specifies ports to clear statistics |
| **Default** | No default is defined |
| **Mode** | Privileged EXEC |
| **Usage** | Use the clear ip dhcp snooping interfaces statistics command to clear statistics that are recorded on interface. |
| **Example** | The example shows how to clear statistics on interface gi1. You can verify settings by the following s**how ip dhcp snooping interface statistics** command. |

```
fiberroad# clear ip dhcp snooping interfaces g 1 statistics
fiberroad# show ip dhcp snooping interfaces g 1 statistics
 Interfaces | Forwarded | Chaddr Check Dropped | Untrust Port Dropped | Untrust Port With Option82 Dropped | Invalid Drop
------------+-----------+----------------------+----------------------+------------------------------------+-------------
 gi1        | 0         | 0                    | 0                    | 0                                  | 0
```

### 2.6.7 show ip dhcp snooping

| | |
|---|---|
| **Syntax** | **show ip dhcp snooping** |
| **Parameter** | N/A |
| **Default** | No default is defined |
| **Mode** | Privileged EXEC |
| **Usage** | Use the show **ip dhcp snooping** command to show settings of DHCP Snooping. |
| **Example** | The example shows how to show settings of DHCP Snooping. |

```
DHCP Snooping            : enabled
Enable on following Vlans : 1-29,41-100
   circuit-id default format: vlan-port
   remote-id:              : 00:18:95:83:fb:ac (Switch Mac in Byte Order)
```

### 2.6.8 show ip dhcp snooping interface

| | |
|---|---|
| **Syntax** | **show ip dhcp snooping interfaces IF_PORTS**<br>**show ip dhcp snooping interfaces IF_PORTS statistics** |
| **Parameter** | **IF_PORTS** specifies ports to show statistics |
| **Default** | No default is defined |
| **Mode** | Privileged EXEC |
| **Usage** | Use the show ip dhcp snooping interfaces command to show settings or statistics of interface. |
| **Example** | The example shows how to show settings of interface g 1. |

```
switch# show ip dhcp snooping interface g 1
switch# show ip dhcp snooping interfaces gi1
        statistics
```

```
Interfaces | Trust State | Rate (pps) | hwaddr Check | Insert Option82 |
-----------+-------------+------------+--------------+-----------------+
gi1        | Untrusted   | None       | disabled     | disabled        |
Switch# show ip dhcp snooping interfaces g 1 statistics
 Interfaces | Forwarded | Chaddr Check Dropped | Untrust Port Dropped | Untrust Port With Option82 Dropped | Invalid Drop
------------+-----------+----------------------+----------------------+------------------------------------+-------------
 gi1        | 0         | 0                    | 0                    | 0                                  | 0

Switch#
```

### 2.6.9 show ip dhcp snooping binding

| | |
|---|---|
| **Syntax** | **show ip dhcp snooping binding** |
| **Parameter** | **None** |
| **Default** | No default is defined |
| **Mode** | Privileged EXEC |
| **Usage** | Use the show **ip dhcp snooping binding** command to show binding entries that learned by DHCP Snooping. |
| **Example** | The example shows how to show binding entries that learned by DHCP Snooping. |

```
switch# show ip dhcp snooping binding
Bind Table: Maximun Binding Entry Number 192
 Port | VID | MAC Address   |        IP        |   Type    | Lease Time
--------+------+--------------------+----------------------------------+---------------------+-----------
 fa1 | 1 | 48:5B:39:C7:12:62 | 192.168.1.100(255.255.255.255)|DHCP Snooping | 86400
```

### 2.6.10 ip dhcp snooping option

| | |
|---|---|
| **Syntax** | **ip dhcp snooping option**<br>**no ip dhcp snooping option** |
| **Parameter** | **None** |
| **Default** | DHCP snooping option82 is disabled |
| **Mode** | Interface Configuration |
| **Usage** | Use the ip dhcp snooping option command to enable that insert option82 content into packet. Use the no form of this command to disable. |
| **Example** | The example shows how to enable option82 insertion. You can verify settings by the following **show ip dhcp snooping interface** command. |

```
Switch(config)# interface g 1
Switch(config-if-g1)# ip dhcp snooping option
Switch(config-if-g1)# exit
Switch(config)# do show ip dhcp s*Jan 01 2022 08:13:55: %LLDP-5-NEIGHBOR_LIMIT: Maximun co
et24


DHCP Snooping            : disabled
Enable on following Vlans : None
    circuit-id default format: vlan-port
    remote-id:                : 00:18:95:83:fb:ac (Switch Mac in Byte Order)

Switch(config)# do show ip dhcp snooping interfaces g 1
 Interfaces | Trust State | Rate (pps) | hwaddr Check | Insert Option82 |
------------+-------------+-------------+--------------+-----------------+
 gi1        | Untrusted   | None        | disabled     | enabled         |
```

### 2.6.11 ip dhcp snooping option action

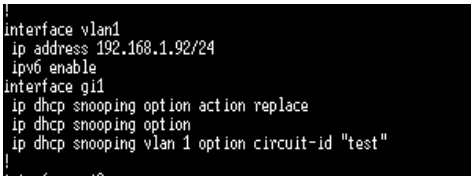
| | |
|---|---|
| **Syntax** | **ip dhcp snooping option action (drop\|keep\|replace)**<br>**no ip dhcp snooping option action** |
| **Parameter** | **Drop** — Drop packets with option82 that are received from un trusted port<br>**Keep** — Keep original option82 content in packet<br>**Replace** — Replace option82 content by switch setting |
| **Default** | DHCP snooping option82 is drop |
| **Mode** | Interface Configuration |
| **Usage** | Use the **ip dhcp snooping option action** command to set the action when receive packets that with option82 content. Use the no form of this command to default setting. |
| **Example** | The example shows how to set action to replace option82 content. You can verify settings by the following **show running-config** command.<br>`switch(config)# interface gi1`<br>`switch(config-if)# ip dhcp snooping option action replace` |

```
!
interface vlan1
 ip address 192.168.1.92/24
 ipv6 enable
interface gi1
 ip dhcp snooping option action replace
 ip dhcp snooping option
!
```

### 2.6.12 ip dhcp snooping option circuit-id

| | |
|---|---|
| **Syntax** | **ip dhcp snooping [vlan <1-4094>] option circuit-id STRING**<br>**no ip dhcp snooping [vlan <1-4094>] option circuit-id** |
| **Parameter** | **Vlan <1-4094>** — VLAN ID to set user defined circuit-id string<br>**STRING** — Circuit-id string, 1 to 63 ASCII characters, no spaces. |
| **Default** | Default circuit-id is port id + vlan id in byte format. |
| **Mode** | Interface Configuration |
| **Usage** | Use the **ip dhcp snooping option circuit-id** command to set user-defined circuit-id string. Circuit-id is per port per VLAN setting. If a VLAN is not found user-defined circuit-id then use per port circuit-id string. Use the **no** form of this command to default setting. |
| **Example** | The example shows how to set a user-defined circuit-id string on interface gi1 and VLAN 1. You can verify settings by the following **show running-config** command |

```
switch(config)# interface gi1
switch(config-if)# ip dhcp snooping vlan 1 option
                   circuit-id test
```



### 2.6.13 ip dhcp snooping option remote-id

| | |
|---|---|
| **Syntax** | **ip dhcp snooping option remote-id STRING**<br>**no ip dhcp snooping option remote-id** |
| **Parameter** | STRING Remote-id string, 1 to 63 ASCII characters, no spaces. |
| **Default** | Default remote-id is the switch MAC address in byte order |
| **Mode** | Global Configuration |
| **Usage** | Use the **ip dhcp snooping option remote-id** command to set user-defined remote-id string.<br>Remote-id is a global and unique string. Use the no form of this command to default setting. |
| **Example** | The example shows how to set a user-defined remote-id string on switch. You can verify settings by the following **show ip dhcp snooping option remote- id**<br><br>`switch(config)# ip dhcp snooping option remote-id test_remote switch(config)# do show ip dhcp snooping option remote-id`<br>  <br> |

### 2.6.14 show ip dhcp snooping option

| | |
|---|---|
| **Syntax** | **show ip dhcp snooping option remote-id** |
| **Parameter** | None |
| **Default** | No default is defined |
| **Mode** | Privileged EXEC |
| **Usage** | Use the show **ip dhcp snooping option remote-id** command to show remote-id string. |
| **Example** | The example shows how to show remote-id string<br><br>`switch(config)# do show ip dhcp snooping option remote-id` |

### 2.6.13 ip dhcp snooping database

| | |
|---|---|
| **Syntax** | **ip dhcp snooping database flash**<br>**ip dhcp snooping database tftp (A.B.C.D\|HOSTNAME) NAME**<br>**no ip dhcp snooping database** |
| **Parameter** | **(A.B.C.D\|HOSTNAME)** Specify the IP address or hostname of remote TFTP server<br>**NAME** Input name of backup file |
| **Default** | DHCP snooping database is disabled |
| **Mode** | Global Configuration |
| **Usage** | Use the **ip dhcp snooping database** command to enable DHCP Snooping database agent. The "**flash**" means that write backup file to switch local drive. The "**tftp**" means that write backup file to remote TFTP server. Use the **no** form of this command to disable. |
| **Example** | The example shows how to enable DHCP Snooping database agent and write backup file to remote TFTP server with file name "backup_file". You can verify settings by the following s**how ip dhcp snooping database** command. |

```
switch(config)# ip dhcp snooping database tftp
                192.168.1.50 backup_file
switch(config)# do show ip dhcp snooping database
```

```
Switch(config)# ip dhcp snooping database tftp 192.168.1.50 backup_file
Switch(config)# do show ip dhcp snooping database

Type : tftp: 192.168.1.50
FileName : backup_file
Write delay Timer : 300 seconds
Abort Timer : 300 seconds

Agent Running : Running
Delay Timer Expiry : 300 seconds
Abort Timer Expiry : 289

Last Succeded Time : None
Last Failed Time : None
Last Failed Reason : No failure recorded.

Total Attempts      :    1
Successful Transfers :    0   Failed Transfers :    0
Successful Reads    :    0   Failed Reads     :    0
Successful Writes   :    0   Failed Writes    :    0
```

### 2.6.14 ip dhcp snooping database write-delay

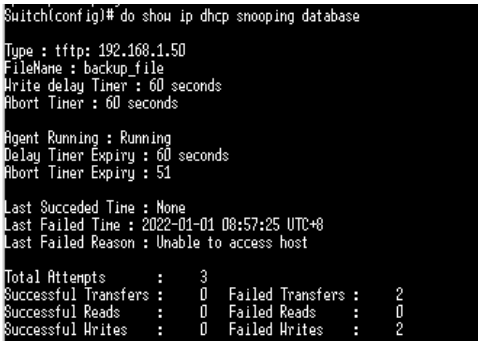
| | |
|---|---|
| **Syntax** | **ip dhcp snooping database write-delay <15-86400> no ip dhcp snooping database write-delay** |
| **Parameter** | **<15-86400>** Specifies the seconds of timeout. Specify the duration for which the transfer should be delayed after the binding database changes |
| **Default** | DHCP snooping database write-delay is 300 seconds |
| **Mode** | Global Configuration |
| **Usage** | Use the **ip dhcp snooping database write-delay** command to modify the write-delay timer. Use the **no** form of this command to default setting. |
| **Example** | The example shows how to set write-delay timer to 60 seconds. You can verify settings by the following **show ip dhcp snooping database** command. |

```
switch(config)# ip dhcp snooping database write-delay 60
switch(config)# do show ip dhcp snooping database
```

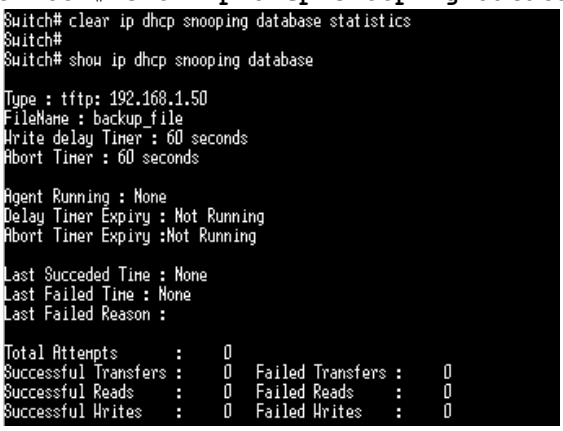
### 2.6.15 ip dhcp snooping database timeout

| | |
|---|---|
| **Syntax** | **ip dhcp snooping database timeout <0-86400>**<br>**no ip dhcp snooping database timeout** |
| **Parameter** | **<15-86400>** Specifies the seconds of timeout。Specify (in seconds) how long to wait for the database transfer process to finish before stopping the process. Use 0 to define an infinite duration, which means to continue trying the transfer indefinitely |
| **Default** | DHCP snooping database timeout is 300 seconds |
| **Mode** | Global Configuration |
| **Usage** | Use the ip dhcp snooping database timeout command to modify the timeout timer. Use the no form of this command to default setting. |
| **Example** | The example shows how to set timeout timer to 60 seconds. You can verify settings by the following show ip dhcp snooping database command. |

```
switch(config)# ip dhcp snooping database timeout 60
switch(config)# do show ip dhcp snooping database
```



### 2.6.16 clear ip dhcp snooping database statistics

| | |
|---|---|
| **Syntax** | **clear ip dhcp snooping database statistics** |
| **Parameter** | None |
| **Default** | No default is defined |
| **Mode** | Privileged EXEC |
| **Usage** | Use the **clear ip dhcp snooping database statistics** command to clear statistics of DHCP Snooping databae. |
| **Example** | The example shows how to clear statistics of DHCP Snooping agent. You can verify settings by the following **show ip dhcp snooping database** command.<br><br>`switch# clear ip dhcp snooping database statistics`<br>`switch# show ip dhcp snooping database`<br>  |

```
Switch# clear ip dhcp snooping database statistics
Switch#
Switch# show ip dhcp snooping database

Type : tftp: 192.168.1.50
FileName : backup_file
Write delay Timer : 60 seconds
Abort Timer : 60 seconds

Agent Running : None
Delay Timer Expiry : Not Running
Abort Timer Expiry :Not Running

Last Succeded Time : None
Last Failed Time : None
Last Failed Reason :

Total Attempts       :    0
Successful Transfers :    0   Failed Transfers :    0
Successful Reads     :    0   Failed Reads     :    0
Successful Writes    :    0   Failed Writes    :    0
```

## 2.6.17 renew ip dhcp snooping database

| | |
|---|---|
| **Syntax** | **renew ip dhcp snooping database** |
| **Parameter** | None |
| **Default** | No default is defined |
| **Mode** | Privileged EXEC |
| **Usage** | Use the **renew ip dhcp snooping database** command to renew DHCP<br>Snooping database from backup file. |
| **Example** | The example shows how to renew DHCP Snooping database. You can verify settings by the following **show ip dhcp snooping database** and s**how ip dhcp snooping binding** command. |

switch# **show ip dhcp snooping database**

```
Switch# show ip dhcp snooping database

Type : tftp: 192.168.1.50
FileName : backup_file
Write delay Timer : 60 seconds
Abort Timer : 60 seconds

Agent Running : Running
Delay Timer Expiry : 60 seconds
Abort Timer Expiry : 57

Last Succeded Time : None
Last Failed Time : 2022-01-01 09:06:54 UTC+8
Last Failed Reason : Unable to access host

Total Attempts       :    2
Successful Transfers :    0   Failed Transfers :    1
Successful Reads     :    0   Failed Reads     :    0
Successful Writes    :    0   Failed Writes    :    1
```

switch# **show ip dhcp snooping binding**

```
Switch# show ip dhcp snooping binding

Bind Table: Maximun Binding Entry Number 256
  Port  | VID  |    MAC Address    |            IP              |   Type
  | Lease Time
--------+------+-------------------+----------------------------+----------
--+----------
```

### 2.6.18 show ip dhcp snooping database

| | |
|---|---|
| **Syntax** | **show ip dhcp snooping database** |
| **Parameter** | None |
| **Default** | No default is defined |
| **Mode** | Privileged EXEC |
| **Usage** | Use the show ip dhcp snooping database command to show settings of DHCP Snooping agent. |
| **Example** | The example shows how to show settings of DHCP Snooping agent. |

```
switch(config)# show ip dhcp snooping database
```

```
Switch(config)# show ip dhcp snooping database

Type : tftp: 192.168.1.50
FileName : backup_file
Write delay Timer : 60 seconds
Abort Timer : 60 seconds

Agent Running : None
Delay Timer Expiry : Not Running
Abort Timer Expiry :Not Running

Last Succeded Time : None
Last Failed Time : 2022-01-01 09:11:04 UTC+8
Last Failed Reason : Unable to access host

Total Attempts       :    3
Successful Transfers :    0   Failed Transfers :    3
Successful Reads     :    0   Failed Reads     :    0
Successful Writes    :    0   Failed Writes    :    3
```

# 2.7 DoS

## 2.7.1 dos

**Syntax**

**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-sportl1024-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-sportl1024-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** | Drops the packets if the destination MAC address is equal to the source MAC address. |
| **icmp-frag-pkts-deny** | Drops the fragmented ICMP packets. |
| **icmpv4-ping-max-check** | Checks the maximum size of ICMP ping packets, and drops the packets larger than the maximum packet size defined by the command **dos icmp-ping-max-length** MAX_LEN. |
| **icmpv6-ping-max-check** | Checks the maximum size of ICMPv6 ping packets, and drops the packets larger than the maximum packet size defined by the command **dos icmp-ping-max- length** MAX_LEN. |
| **ipv6-min-frag- size-check** | Checks the minimum size of IPv6 fragments, and drops the packets smaller than the minimum size defined by the command dos **ipv6-min-frag-size-length** MIN_LEN. |
| **land-deny** | Drops the packets if the source IP address is equal to the destination IP address. |
| **nullscan-deny** | Drops the packets with NULL scan. |
| **pod-deny** | Avoids ping of death attack. |
| **smurf-deny** | Avoids smurf attack. |
| **syn-sportl1024-deny** | Drops SYN packets with sport less than 1024. |
| **synfin-deny** | Drops the packets with SYN and FIN bits set. |
| **synrst-deny** | Drops the packets with SYN and RST bits set. |
| **tcp-frag-off-min-check** | Drops the TCP fragment packets with offset equals to one. |
| **tcpblat-deny** | Drops the packages if the TCP source port is equal to the TCP destination port. |
| **tcphdr-min-check** | Checks the minimum TCP header and drops the TCP packets with the header smaller than the minimum size defined by the command **dos tcphdr-min-length** HDR_MIN_LEN. |
| **udpblat-deny** | Drops the packets if the UDP source port equals to the UDP destination port. |

| | |
|---|---|
| **xmas-deny** | Drops the packets if the sequence number is zero, and the FIN, URG and PSH bits are set. |
| **icmp-ping-max-length** MAX_LEN | Specify the maximum size of the ICMPv4/ICMPv6 ping packets. The valid range is from 0 to 65535 bytes, and the default value is 512 bytes. |
| **ipv6-min-frag- size-length** MIN_LEN | Specify the minimum size of IPv6 fragments. The valid range is from 0 to 65535 bytes, and default value is 1240 bytes. |
| **smurf-netmask** MASK | Specify the netmask of smurf attack. The length range is from 0 to 323 bytes, and default length is 0 bytes. |
| **tcphdr-min-length** HDR_MIN_LEN | Specify the minimum TCP header length. The length range is from 0 to 31 bytes, and default length is 20 bytes. |

**Default** All of DoS protections are enabled by default. The default parameter are:

- The maximum size of ICMP ping packages is 512 bytes
- The minimum size of IPv6 fragments is 1240 bytes.
- The Smurf netmask length is 0 bytes.
- The minimum TCP header length is 20 bytes.

**Mode** Global Configuration

**Usage** To enable the specific Deniel of Service (DoS) protection, use the command **dos** in the Global Configuration mode. Otherwise, use the **no** form of the command to disable the specific DoS protection.

**Example** The following example sets the minimum fragment size to 1024 bytes, and enables the minimum size of IPv6 fragments validation.

```
Switch(config)# dos ipv6-min-frag-size-length 1024
Switch(config)# dos ipv6-min-frag-size-check
```

### 2.7.2 dos(interface)

| | |
|---|---|
| **Syntax** | **dos / no dos** |
| **Parameter** | N/A |
| **Default** | DoS protection is disabled on each interface. |
| **Mode** | Interface Configuration |
| **Usage** | To enable the DoS on the specific interface, use the command **dos** in the Interface Configuration mode. Otherwise, use the **no** form of the command to disable the DoS on the interface. |
| **Example** | The following example enables the DoS on the interface fa1.<br>`Switch(config)# interface g 1`<br>`Switch(config-if)# dos` |

### 2.7.3 show dos

| | |
|---|---|
| **Syntax** | **show dos**<br>**show dos interface** IF_PORTS |
| **Parameter** | **interface** IF_PORTS An interface ID or the list of interface IDs. |
| **Default** | N/A |
| **Mode** | Privileged EXEC |
| **Usage** | To show the DoS protection configuration, use the command show dos in the Privileged EXEC mode. For the status of DoS protection on each interface, use the command show dos interface in the Priveleged EXEC mode. |
| **Example** | The following example shows the global DoS protection configuration. |

```
Switch(config)# do show dos interfaces g 1
  Port    | DoS Protection
----------+---------------
    gi1   |    enabled
```

```
Switch(config)# do show dos
  Type                      | State (Length)
----------------------------+--------------------------------
  DMAC equal to SMAC        | enabled
  Land (DIP = SIP)          | enabled
  UDP Blat (DPORT = SPORT)  | enabled
  TCP Blat (DPORT = SPORT)  | enabled
  POD (Ping of Death)       | enabled
  IPv6 Min Fragment Size    | enabled  (1024 Bytes)
  ICMP Fragment Packets     | enabled
  IPv4 Ping Max Packet Size | enabled  (512 Bytes)
  IPv6 Ping Max Packet Size | enabled  (512 Bytes)
  Smurf Attack              | enabled  (Netmask Length: 0)
  TCP Min Header Length     | enabled  (20 Bytes)
  TCP Syn (SPORT < 1024)    | enabled
  Null Scan Attack          | enabled
  X-Mas Scan Attack         | enabled
  TCP SYN-FIN Attack        | enabled
  TCP SYN-RST Attack        | enabled
  TCP Fragment (Offset = 1) | enabled
```

## 2.8 Dynamic ARP Inspection

### 2.8.1 ip arp inspection

| | |
|---|---|
| **Syntax** | **ip arp / inspection no ip / arp inspection** |
| **Parameter** | None |
| **Default** | Dynamic Arp inspection is disabled |
| **Mode** | Global Configuration |
| **Usage** | Use the **ip arp inspection** command to enable Dynamic Arp Inspection function. Use the **no** form of this command to disable. |
| **Example** | The example shows how to enable Dynamic Arp Inspection on VLAN 1. You can verify settings by the following **show ip arp inspection** command.<br><br>`switch(config)# ip arp inspection`<br>`switch(config)# ip arp inspection vlan 1`<br>`switch(config)# show ip arp inspection` |

### 2.8.2 ip arp inspection vlan

| | |
|---|---|
| **Syntax** | **ip arp inspection vlan VLAN-LIST**<br>**no ip arp inspection vlan VLAN-LIST** |
| **Parameter** | VLAN-LIST Specify VLAN ID or a range of VLANs to enable or disable dynamic Arp inspection |
| **Default** | Default is disabled on all VLANs |
| **Mode** | Global Configuration |
| **Usage** | Use the **ip arp inspection vlan** command to enable VLANs on Dynamic Arp Inspection function. Use the **no** form of this command to disable VLANs on Dynamic Arp Inspection function. |
| **Example** | The example shows how to enable VLAN 1-100 on Dynamic Arp Inspection, and then disable VLAN 30-40 on Dynamic Arp Inspection. You can verify settings by the following **show ip arp inspection** command. |

```
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

switch(config)# no ip arp inspection vlan 30-40
switch(config)# show ip arp inspection
```

### 2.8.3 ip arp inspection trust

| | |
|---|---|
| **Syntax** | **ip arp inspection trust**<br>**no ip arp inspection trust** |
| **Parameter** | None |
| **Default** | Dynamic Arp inspection is disabled |
| **Mode** | Interface Configuration |
| **Usage** | Use the **ip arp inspection** trust command to set trusted interface. The switch does not check ARP packets that are received on the trusted interface; it simply forwards it. Use the **no** form of this command to set untrusted interface. |
| **Example** | The example shows how to set interface gi1 to trust. You can verify settings by the following show ip arp inspection interface command. |

```
switch(config)# interface g 1
switch(config)# ip arp inspection trust
switch(config)# do show ip arp inspection interface g 1
```

### 2.8.4 ip arp inspection validate

| | |
|---|---|
| **Syntax** | **ip arp inspection validate src-mac ip arp inspection validate dst-mac**<br>**ip arp inspection validate ip [allow-zeros] no ip arp inspection validate src-mac**<br>**no ip arp inspection validate dst-mac**<br>**no ip arp inspection validate ip [allow-zeros]** |
| **Parameter** | None |
| **Default** | Default is disabled of all validation |
| **Mode** | Interface Configuration |
| **Usage** | Use the **ip arp inspection validate** command to enable validate function on interface. The "**src-mac**" drop ARP requests and reply packets that arp-sender-mac and ethernet- source-mac is not match. The "**dst-mac**" drops ARP reply packets that arp-target-mac and ethernet-dst-mac is not match. The "**ip**" drop ARP request and reply packets that sender-ip is invalid such as broadcast 、 multicast 、 all zero IP address and drop ARP reply packets that target-ip is invalid. The "**allow-zeros**" means won't drop all zero IP address. Use the no form of this command to disable validation. |
| **Example** | The example shows how to set interface gi1 to validate "src-mac" 、 "dst-mac" and "ip allow zeros". You can verify settings by the following show ip arp inspection interface command.<br><br>`switch(config)# interface g 1`<br>`switch(config-if)# ip arp inspection validate src-mac`<br>`switch(config-if)# ip arp inspection validate dst-ma`<br>`switch(config-if)# ip arp inspection validate ip`<br>`allow-zeros switch(config)# do show ip arp inspection interface g 1` |

### 2.8.4 ip arp inspection rate-limit

| | | |
|---|---|---|
| **Syntax** | **ip arp inspection rate-limit <1-50> [no] ip arp inspection rate-limit** | |
| **Parameter** | <1-50> | Set 1 to 50 PPS of DHCP packet rate limitation |
| **Default** | Default is un-limited of ARP packet | |
| **Mode** | Interface Configuration | |
| **Usage** | Use the ip arp inspection rate-limit command to set rate limitation on interface. The switch drop ARP packets after receives more than configured rate of packets per second. Use the no form of this command to return to default settings. | |
| **Example** | The example shows how to set rate limit to 30 pps on interface gi1. You can verify settings by the following show ip arp inspection interface command. | |

```
switch(config)# interface g 1
switch(config)# ip arp inspection rate-limit 30
switch(config)# do show ip arp inspection interface g 1
```

### 2.8.5 clear ip arp inspection statistics

| | | |
|---|---|---|
| **Syntax** | **clear ip arp inspection interfaces IF_PORTS statistics** | |
| **Parameter** | IF_PORTS | specifies ports to clear statistics |
| **Default** | No default is defined | |
| **Mode** | Privileged EXEC | |
| **Usage** | Use the clear ip arp inspection interfaces statistics command to clear statistics that are recorded on interface. | |
| **Example** | The example shows how to set rate limit to 30 pps on interface gi1. You can verify settings by the following show ip arp inspection interface command. | |

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

### 2.8.6 show ip arp inspection

| | |
|---|---|
| **Syntax** | **show ip dhcp snooping** |
| **Parameter** | None |
| **Default** | No default is defined |
| **Mode** | Privileged EXEC |
| **Usage** | Use the show ip arp inspection command to show settings of Dynamic Arp Inspection |
| **Example** | The example shows how to show settings of Dynamic Arp Inspection<br><br>`switch(config)# show ip arp inspection` |

### 2.8.7 show ip arp inspection interface

| | |
|---|---|
| **Syntax** | **show ip arp inspection interfaces IF_PORTS**<br>**show ip arp inspection interfaces IF_PORTS statistics** |
| **Parameter** | IF_PORTS specifies ports to show statistics |
| **Default** | No default is defined |
| **Mode** | Privileged EXEC |
| **Usage** | Use the show ip arp inspection interfaces command to show settings or statistics of interface. |
| **Example** | `switch# show ip arp inspection interface g 1`<br><br>`switch# show ip arp inspection interfaces g 1 statistics` |

## 2.9 GVRP

### 2.9.1 gvrp(Global)

| | |
|---|---|
| **Syntax** | **gvrp / no gvrp** |
| **Parameter** | None |
| **Default** | GVRP is disabled |
| **Mode** | Global Configuration |
| **Usage** | Disable gvrp will clear all learned dynamic vlan entry and do not learn dynamic vlan anymore.<br>Use '**show gvrp**' to show configuration. |
| **Example** | The following example specifies that set global gvrp test**.**<br>`Switch(config)# gvrp`<br>`Switch# show gvrp`<br>  |



### 2.9.2 gvrp(Interface)

| | |
|---|---|
| **Syntax** | **gvrp / no gvrp** |
| **Parameter** | None |
| **Default** | GVRP is disabled on interface |
| **Mode** | Interface mode |
| **Usage** | 'no gvrp' will remove dynamic port from vlan.<br>'gvrp' must work at port mode is trunk. |
| **Example** | The following example specifies that set port gvrp test. The port gvrp enable must set port mode is trunk firstly.<br><br>`Switch(config)#interface g 1`<br>`Switch(config-if)# switchport mode trunk`<br>`Switch(config-if)# gvrp`<br>`Switch# show gvrp configuration interfaces gi1` |

```
Switch(config)# do show gvrp configuration int g 1
  Port   |  GVRP-Status   | Registration   | Dynamic VLAN Creation
---------+--------------+--------------+---------------------
gi1             Enabled          Normal             Enabled
```

### 2.9.3 gvrp registration-mode

| | | |
|---|---|---|
| **Syntax** | **gvrp registration-mode (normal \| fixed \| forbidden)** | |
| **Parameter** | **(normal \| fixed \| forbidden)** | **normal:** register dynamic vlan, and transmit all vlan attribute.<br>**fixed:** do not register dynamic vlan, and only transmit static vlan attribute.<br>**forbidden:** do not register dynamic vlan, and only transmit default vlan attribute. |
| **Default** | Default is Normal | |
| **Mode** | Interface mode | |
| **Usage** | When set registration-mode is fixed or forbidden, will remove the port from vlan witch is dynamic port. And do not learning vlan. | |
| **Example** | The following example specifies that set gvrp registration mode test.<br>`Switch(config)# interface g 1`<br>`Switch(config-if)# gvrp registration-mode fixed`<br>`Switch# show gvrp configuration interfaces g 1` | |

```
Switch(config)# int g 1
Switch(config-if-g1)# gvrp registration-mode fixed
Switch(config-if-g1)# exit
Switch(config)# do show gvrp configuration int g 1
  Port   |  GVRP-Status   | Registration   | Dynamic VLAN Creation
---------+--------------+--------------+---------------------
gi1             Enabled          Fixed              Enabled
```

### 2.9.4 gvrp vlan-creat-forbid

| | |
|---|---|
| **Syntax** | **gvrp vlan-creation-forbid**<br>**no gvrp vlan-creation-forbid** |
| **Parameter** | None |
| **Default** | Default is disable |
| **Mode** | Interface mode |
| **Usage** | 'gvrp vlan-creation-forbid' will not remove dynamic port from vlan immediate. |
| **Example** | The following example specifies that set port gvrp vlan-creation-forbid test. Switch(config)#interface g 1<br>`Switch(config-if)# gvrp vlan-creation-forbid`<br>`Switch(config-if)# exit`<br>`Switch# show gvrp configuration interfaces g 1` |

### 2.9.5 clear gvrp statistics

| | | |
|---|---|---|
| **Syntax** | **clear gvrp (error-statistics \| statistics) [interfaces IF_PORTS]** | |
| **Parameter** | **(error-statistics \| statistics)** | Error-statistics: error gvrp packet statistics<br>Statistics: gvrp event message |
| | **[interfaces** IF_PORTS**]** | statistics Specifies posts to clear statistics |
| **Default** | none | |
| **Mode** | Privileged EXEC | |
| **Usage** | This command will clear the ports error statistics or statistics info. | |
| **Example** | The following example specifies that clear gvrp error statistics and statistics test.<br>`Switch# clear gvrp statistics`<br>`Switch# clear gvrp error-statistics` | |

### 2.9.6 show gvrp statistics

| | |
|---|---|
| **Syntax** | **show gvrp (statistics \| error-statistics) [interfaces IF_PORTS]** |
| **Parameter** | **none** Display all ports<br>**(statistics\| error-statistics)** statistics – GVRP statistics<br>error-statistics GVRP error<br>**[interfaces** IF_PORTS**]** statistics Specifies posts |
| **Default** | Display all ports statistics info |
| **Mode** | Privileged EXEC |
| **Usage** | This command will display the ports error statistics or statistics info. |
| **Example** | The following example specifies that display gvrp error statistics and statistics test. |

Switch# **show gvrp statistics**

```
Switch(config)# do show gvrp statistics
Port id         : gi1
Total RX        :   0
JoinEmpty RX    :   0
JoinIn RX       :   0
Empty RX        :   0
LeaveIn RX      :   0
LeaveEmpty RX   :   0
LeaveAll RX     :   0
Total TX        :   0
JoinEmpty TX    :   0
JoinIn TX       :   0
Empty TX        :   0
LeaveIn TX      :   0
LeaveEmpty TX   :   0
LeaveAll TX     :   0

Port id         : gi2
Total RX        :   0
JoinEmpty RX    :   0
JoinIn RX       :   0
Empty RX        :   0
LeaveIn RX      :   0
LeaveEmpty RX   :   0
LeaveAll RX     :   0
Total TX        :   0
--More--
```

**Switch# show gvrp error-statistics**

```
Switch(config)# show gvrp error-statistics
Legend:
INVPROT : Invalid protocoal Id
INVATYP : Invalid Attribute Type   INVALEN : Invalid Attribute Length
INVAVAL : Invalid Attribute Value  INVEVENT: Invalid Event
  Port   | INVPROT | INVATYP | INVALEN | INVAVAL | INVEVENT
   gi1          0         0         0         0         0
   gi2          0         0         0         0         0
   gi3          0         0         0         0         0
   gi4          0         0         0         0         0
   gi5          0         0         0         0         0
   gi6          0         0         0         0         0
   gi7          0         0         0         0         0
   gi8          0         0         0         0         0
   gi9          0         0         0         0         0
  gi10          0         0         0         0         0
  gi11          0         0         0         0         0
  gi12          0         0         0         0         0
  gi13          0         0         0         0         0
  gi14          0         0         0         0         0
  gi15          0         0         0         0         0
  gi16          0         0         0         0         0
  gi17          0         0         0         0         0
  gi18          0         0         0         0         0
  gi19          0         0         0         0         0
--More--
```

### 2.9.7 show gvrp

| | |
|---|---|
| **Syntax** | **show gvrp** |
| **Parameter** | none |
| **Default** | none |
| **Mode** | Privileged EXEC |
| **Usage** | This command will display the gvrp global info. |
| **Example** | The following example specifies that display gvrp test. |

```
Switch# show gvrp
```

```
Switch(config)# do show gvrp

              GVRP    Status
              --------------------

   GVRP                          : Enabled
   Join time                     : 200 ms
   Leave time                    : 600 ms
   LeaveAll time                 : 10000 ms
```

### 2.9.8 show gvrp configuration

| | |
|---|---|
| **Syntax** | **show gvrp configuration [interface IF_PORTS]** |
| **Parameter** | **none** — Display all ports configuration<br>**(statistics\| error-statistics)** — Display Specifies posts configuration |
| **Default** | Display all ports configuration info |
| **Mode** | Privileged EXEC |
| **Usage** | This command will display the ports configuration info. |
| **Example** | The following example specifies that display gvrp port configuration test. |

```
Switch# show gvrp configuration
```

```
Switch(config)# do show gvrp configuration
  Port  |  GVRP-Status  | Registration  | Dynamic VLAN Creation
--------+---------------+---------------+----------------------
gi1           Enabled         Fixed           Disabled
gi2          Disabled         Normal           Enabled
gi3          Disabled         Normal           Enabled
gi4          Disabled         Normal           Enabled
gi5          Disabled         Normal           Enabled
gi6          Disabled         Normal           Enabled
gi7          Disabled         Normal           Enabled
```

## 2.10 IGMP Snooping

### 2.10.1 ip igmp snooping

| | |
|---|---|
| **Syntax** | **ip igmp**<br>**snooping no ip**<br>**igmp snooping** |
| **Parameter** | None |
| **Default** | Default is enabled |
| **Mode** | Global Configuration |
| **Usage** | Use the **ip igmp snooping** command to enable IGMP snooping function.<br>Use the no form of this command to disable.<br>You can verify settings by the **show ip igmp snooping** command. |
| **Example** | **The following example specifies that set ip igmp snooping test.**<br>`Switch(config)# no ip igmp snooping` |

### 2.10.2 ip igmp snooping report-suppression

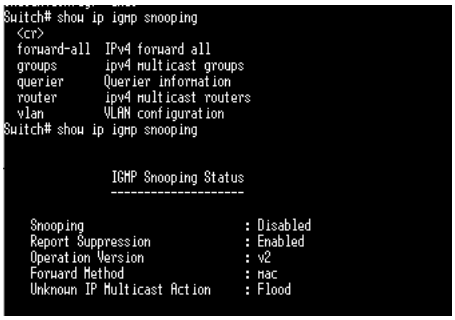
| | |
|---|---|
| **Syntax** | **ip igmp snooping report-suppression**<br>**no ip igmp snooping report-suppression** |
| **Parameter** | None |
| **Default** | Default is enabled |
| **Mode** | Global Configuration |
| **Usage** | Use the **ip igmp snooping report-suppression** command to enable IGMP snooping report-suppression function.<br>Use the no form of this command to disable. Disable report-supression will forward all received reports to the vlan router ports.<br>You can verify settings by the **show ip igmp snooping** command. |
| **Example** | The following example specifies that disable ip igmp snooping report-suppression test. |

```
Switch(config)# ip igmp snooping report-suppression
Switch(config)# do show ip igmp snooping

              IGMP Snooping Status
              --------------------

  Snooping                      : Disabled
  Report Suppression            : Enabled
  Operation Version             : v2
  Forward Method                : mac
  Unknown IP Multicast Action   : Flood

              Packet Statistics
  Total RX                      : 0
  Valid RX                      : 0
  Invalid RX                    : 0
  Other RX                      : 0
  Leave RX                      : 0
  Report RX                     : 0
  General Query RX              : 0
  Specail Group Query RX        : 0
  Specail Group & Source Query RX : 0
```

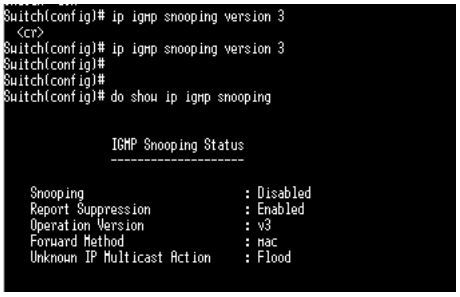
### 2.10.3 ip igmp snooping version

| | |
|---|---|
| **Syntax** | **ip igmp snooping version (2\|3)** |
| **Parameter** | (2\|3) IGMP version 2 or IGMP version 3 basic mode |
| **Default** | Default is version 2 |
| **Mode** | Global Configuration |
| **Usage** | Use the **ip igmp snooping** version command to change IGMP support version. Only basic mode is supported in v3. When change version from v3 to v2, all querier version will update to version 2.<br>You can verify settings by the **show ip igmp snooping** command. |
| **Example** | The following example specifies that set ip igmp snooping version 3. |

```
Switch # ip igmp snooping
```




```
Switch(config)# ip igmp snooping version 3
```



### 2.10.4 ip igmp snooping unknown-multicast action

| | |
|---|---|
| **Syntax** | **ip igmp snooping unknown-multicast action (drop \| flood \|router-port)**<br>**no ip igmp snooping unknown-multicast action** |
| **Parameter** | (drop \| flood \| router- port) — Drop、flood in vlan or forward to router port of unknown multicast packet |
| **Default** | Default is flood. |
| **Mode** | Global Configuration |
| **Usage** | When igmp and mld snooping disabled, it can't set action router-port. When disable igmp snooping & mld snooping, it set unknown multicast action flood. When action is router-port to flood or drop, it will delete the unknown multicast group entry.<br><br>Use the **ip igmp snooping unknown-multicast action** command to change action.<br>Use the **no** form of this command to restore to default.<br>You can verify settings by the **show ip igmp snooping** command. |
| **Example** | The following example specifies that set ip igmp unknown multicast action router-port test.<br>`Switch(config)# ip igmp snooping`<br>`Switch(config)# ip igmp snooping unknown-multicast action router-port` |

### 2.10.5 ip igmp snooping querier

| | |
|---|---|
| **Syntax** | **ip igmp snooping vlan <VLAN-LIST> querier [version (2\|3)]**<br>**no ip igmp snooping [vlan <VLAN-LIST>] querier** |
| **Parameter** | VLAN-LIST — specifies VLAN ID list to set<br>(2\|3) — Query version 2 or 3 |
| **Default** | No ip igmp snooping querier by default |
| **Mode** | Global Configuration |
| **Usage** | When enable ip igmp vlan querier, there will process router select, the select successful will send general and specific query.<br>Use the **ip igmp snooping querier** command to add querier. Use the |

**no** form of this command to delete querier.
You can verify settings by the show ip igmp snooping querier command.

**Example** **The following example specifies that set ip igmp snooping querier test.**

```
Switch(config)# ip igmp snooping vlan 2 querier version 3
```

### 2.10.6 ip igmp snooping vlan

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

**Parameter** VLAN-LIST specifies VLAN ID list to set

**Default** Default is disabled for all VLANs

**Mode** Global Configuration

**Usage** Disable will clear all ip igmp snooping dynamic group and dynamic router port and make all static ip igmp group invalid of this vlan. Will not learn dynamic group and router port by igmp message any more.
Use the **ip igmp snooping vlan** command to enable IGMP on VLAN.
Use the **no** form of this command to disable
You can verify settings by the **show ip igmp snooping vlan** command.

**Example** The following example specifies that set ip igmp snooping vlan test.

```
Switch(config)# ip igmp snooping
Switch(config)# ip igmp snooping vlan 2
```

### 2.10.7 ip igmp snooping vlan fastleave

| | |
|---|---|
| **Syntax** | **ip igmp snooping vlan <VLAN-LIST> fastleave**<br>**no ip igmp snooping vlan <VLAN-LIST> fastleave** |
| **Parameter** | VLAN-LIST specifies VLAN ID list to set |
| **Default** | Default is disabled |
| **Mode** | Global Configuration |
| **Usage** | Use the **ip igmp snooping vlan fastleave** command to enable fastleave function. Group will remove port immediately when receive leave packet. Use the **no** form of this command to disable.<br>You can verify settings by the show **ip igmp snooping vlan** command |
| **Example** | The following example specifies that set ip igmp snooping vlan fastleave test.<br>`Switch(config)# ip igmp snooping vlan 1 fastleave` |

### 2.10.8 ip igmp snooping vlan last-member-query-count

| | |
|---|---|
| **Syntax** | **ip igmp snooping vlan <VLAN-LIST> last-member-query-count <1-7>**<br>**no ip igmp snooping vlan <VLAN-LIST> last-member-query-count** |

**Parameter**

| | |
|---|---|
| VLAN-LIST | specifies VLAN ID list to set |
| last-member-query-count <1-7> | specifies last member query count to set. |

| | |
|---|---|
| **Default** | Default is 2 |
| **Mode** | Global Configuration |
| **Usage** | Use the **ip igmp snooping vlan last-member-query-count** command to change how many query packets will send.<br>Use the no form of this command to restore to default.<br>You can verify settings by the **show ip igmp snooping vlan** command |
| **Example** | The following example specifies that set ip igmp snooping vlan last-member-query-count test.<br>`Switch(config)# ip igmp snooping vlan 1 last-member-query-count 5` |

### 2.10.9 ip igmp snooping vlan last-member-query-interval

**Syntax** **ip igmp snooping vlan <VLAN-LIST> last-member-query-interval <1- 60>**
**no ip igmp snooping vlan <VLAN-LIST> last-member-query-interval**

**Parameter**

| | |
|---|---|
| VLAN-LIST | specifies VLAN ID list to set |
| last-member-query-interval <1-60> | specifies last member query interval to set |

**Default** Default is 1

**Mode** Global Configuration

**Usage** Use the ip igmp snooping vlan last-member-query-interval command to set interval between each query packet.
Use the no form of this command to restore to default.
You can verify settings by the show **ip igmp snooping vlan** command

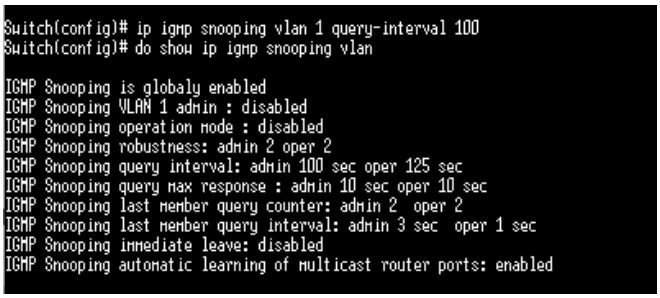
**Example** The following example specifies that set ip igmp snooping vlan last-member-query-interval test.

```
Switch(config)# ip igmp snooping vlan 1 last-member-query-interval 3
```

```
Switch(config)# do show ip igmp snooping vlan

IGMP Snooping is globaly 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 3 sec  oper 1 sec
IGMP Snooping immediate leave: disabled
IGMP Snooping automatic learning of multicast router ports: enabled
```

### 2.10.10 ip igmp snooping vlan query-interval

| | |
|---|---|
| **Syntax** | **ip igmp snooping vlan <VLAN-LIST> query-interval <30-18000>**<br>**no ip igmp snooping vlan <VLAN-LIST> query-interval** |
| **Parameter** | VLAN-LIST — specifies VLAN ID list to set<br>query-interval <1-18000> — specifies query interval to set |
| **Default** | Default is 125 |
| **Mode** | Global Configuration |
| **Usage** | Use the **ip igmp snooping vlan query-interval** command to set interval between each query.<br>Use the no form of this command to restore to default<br>You can verify settings by the show **ip igmp snooping vlan** command |
| **Example** | The following example specifies that set **ip igmp snooping vlan query-interval** test. |



### 2.10.11 ip igmp snooping vlan response-time

| | |
|---|---|
| **Syntax** | **ip igmp snooping vlan <VLAN-LIST> response-time <5-20>**<br>**no ip igmp snooping vlan <VLAN-LIST> response-time** |

**Parameter**

| | |
|---|---|
| VLAN-LIST | specifies VLAN ID list to set |
| response-time <5-20> | specifies a response time to set |

| | |
|---|---|
| **Default** | Default is 10 |
| **Mode** | Global Configuration |
| **Usage** | Use the **ip igmp snooping vlan response-time** command to set response time<br>Use the **no** form of this command to restore to default.<br>You can verify settings by the show **ip igmp snooping vlan** command |
| **Example** | The following example specifies that set ip igmp snooping vlan response- time test.<br>`Switch(config)# ip igmp snooping vlan 1 response-time 12` |

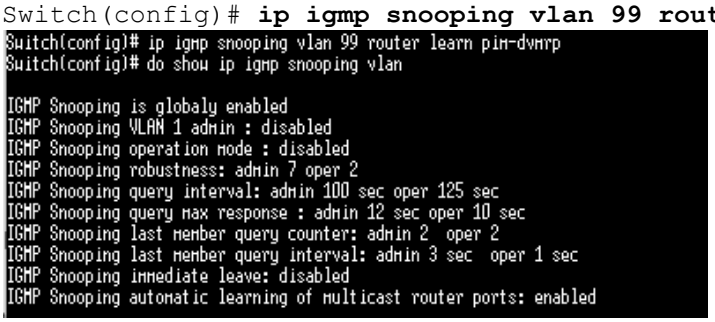
```
Switch(config)# ip igmp snooping vlan 1 response-time 12
Switch(config)# do show ip igmp snooping vlan

IGMP Snooping is globaly enabled
IGMP Snooping VLAN 1 admin : disabled
IGMP Snooping operation mode : disabled
IGMP Snooping robustness: admin 2 oper 2
IGMP Snooping query interval: admin 100 sec oper 125 sec
IGMP Snooping query max response : admin 12 sec oper 10 sec
IGMP Snooping last member query counter: admin 2  oper 2
IGMP Snooping last member query interval: admin 3 sec  oper 1 sec
IGMP Snooping immediate leave: disabled
IGMP Snooping automatic learning of multicast router ports: enabled
```

## 2.10.12 ip igmp snooping vlan robustness-variable

| | |
|---|---|
| **Syntax** | **ip igmp snooping vlan <VLAN-LIST> robustness-variable <1-7>**<br>**no ip igmp snooping vlan <VLAN-LIST> robustness-variable** |
| **Parameter** | VLAN-LIST — specifies VLAN ID list to set<br>Robustness-variable<1-7> — specifies a robustness value to set |
| **Default** | Default is 2 |
| **Mode** | Global Configuration |
| **Usage** | Use the **ip igmp snooping vlan robustness-variable** command to times to retry.<br>Use the no form of this command to restore to default<br>You can verify settings by the **show ip igmp snooping vlan** command |
| **Example** | The following example specifies that set ip igmp snooping vlan parameters test.<br>`Switch(config)# ip igmp snooping vlan 1 robustness-variable` |

```
Switch(config)# ip igmp snooping vlan 1 robustness-variable 7
Switch(config)# do show ip igmp snooping vlan

IGMP Snooping is globaly enabled
IGMP Snooping VLAN 1 admin : disabled
IGMP Snooping operation mode : disabled
IGMP Snooping robustness: admin 7 oper 2
IGMP Snooping query interval: admin 100 sec oper 125 sec
IGMP Snooping query max response : admin 12 sec oper 10 sec
IGMP Snooping last member query counter: admin 2  oper 2
IGMP Snooping last member query interval: admin 3 sec  oper 1 sec
IGMP Snooping immediate leave: disabled
IGMP Snooping automatic learning of multicast router ports: enabled
```

### 2.10.13 ip igmp snooping vlan router

| | |
|---|---|
| **Syntax** | **ip igmp snooping vlan VLAN-LIST router learn pim-dvmrp**<br>**no ip igmp snooping vlan VLAN-LIST router learn pim-dvmrp** |
| **Parameter** | VLAN-LIST specifies VLAN ID list to set |
| **Default** | Default is enabled |
| **Mode** | Global Configuration |
| **Usage** | Use the **ip igmp snooping vlan router** command to enable learning router port by routing protocol packets such as PIM/PIMv2, DVMRP, MOSPF. Use the no form of this command to disable.<br>You can verify settings by the show **ip igmp snooping vlan** command |
| **Example** | The following example specifies that set ip igmp snooping vlan router test.<br>`Switch(config)# ip igmp snooping vlan 99 router`<br>  |

```
Switch(config)# ip igmp snooping vlan 99 router learn pim-dvmrp
Switch(config)# do show ip igmp snooping vlan

IGMP Snooping is globaly enabled
IGMP Snooping VLAN 1 admin : disabled
IGMP Snooping operation mode : disabled
IGMP Snooping robustness: admin 7 oper 2
IGMP Snooping query interval: admin 100 sec oper 125 sec
IGMP Snooping query max response : admin 12 sec oper 10 sec
IGMP Snooping last member query counter: admin 2  oper 2
IGMP Snooping last member query interval: admin 3 sec  oper 1 sec
IGMP Snooping immediate leave: disabled
IGMP Snooping automatic learning of multicast router ports: enabled
```

### 2.10.14 ip igmp snooping vlan forbidden-port

**Syntax**

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

**Parameter**

| | |
|---|---|
| VLAN-LIST | specifies VLAN ID list to set |
| IF_PORTS | specifies a port list to set or remove |

**Default**

No forbidden ports by default

**Mode**

Global Configuration

**Usage**

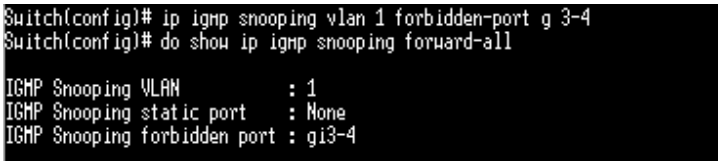
'ip igmp snooping vlan 1 static-port gi1-2' will add static port gi1-2 for vlan 1.the all known vlan 1 ipv4 group will add the static ports.
'ip igmp snooping vlan 1 forbidden-port gi3-4' will add forbidden port gi3-4 for vlan 1.the all known vlan 1 ipv4 group will remove the forbidden ports. The configure can use 'show ip igmp snooping forward-all'.

Use the **ip igmp snooping vlan forbidden-port** command to add static non- forwarding port, all known vlan 1 ipv4 group will remove the forbidden ports. Use the no form of this command to delete forbidden port.
You can verify settings by the **show ip igmp snooping forward-all** command.

**Example**

The following example specifies that set ip igmp snooping static/forbidden port test.

```
Switch(config)# ip igmp snooping vlan 1 forbidden-port
                g 3-4
```



### 2.10.15 ip igmp snooping vlan static-port

| | |
|---|---|
| **Syntax** | **ip igmp snooping vlan <VLAN-LIST> static-port IF_PORTS**<br>**no ip igmp snooping vlan <VLAN-LIST> static-port IF_PORTS** |
| **Parameter** | VLAN-LIST — specifies VLAN ID list to set<br>IF_PORTS — specifies a port list to set or remove |
| **Default** | No static port by default |
| **Mode** | Global Configuration |
| **Usage** | Use the **ip igmp snooping vlan static-port** command to add static forwarding port, all known vlan 1 ipv4 group will add the static ports. Use the no form of this command to delete static port.<br>You can verify settings by the **show ip igmp snooping forward-all** command. |
| **Example** | The following example specifies that set ip igmp snooping static port test.<br>`Switch(config)# ip igmp snooping vlan 1 static-port g 1-2` |

```
Switch(config)# ip igmp snooping vlan 1 static-port g 1-2
Switch(config)# do show ip igmp snooping forward-all

IGMP Snooping VLAN          : 1
IGMP Snooping static port   : gi1-2
IGMP Snooping forbidden port : gi3-4
```

### 2.10.16 ip igmp snooping vlan forbidden-router-port

| | |
|---|---|
| **Syntax** | **ip igmp snooping vlan <VLAN-LIST> forbidden-router-port IF_PORTS**<br>**no ip igmp snooping vlan <VLAN-LIST> forbidden-router-port IF_PORTS** |
| **Parameter** | VLAN-LIST — specifies VLAN ID list to set<br>IF_PORTS — specifies a port list to set or remove |
| **Default** | No forbidden router ports by default |
| **Mode** | Global Configuration |
| **Usage** | Use the **ip igmp snooping vlan forbidden-router-port** command to add static forbidden router port. This will also remove port from static router port. The forbidden router port will not forward received query packet.<br>Use the no form of this command to delete forbidden router port.<br>You can verify settings by the **show ip igmp snooping router** command. |
| **Example** | The following example specifies that set ip igmp snooping forbidden test.<br>`Switch(config)# ip igmp snooping vlan 1 forbidden-router-port g 2` |

```
Switch(config)# ip igmp snooping vlan 1 forbidden-router-port g 2
Switch(config)# do show ip igmp snooping router

Dynamic Router Table
 VID  |  Port   | Expiry Time(Sec)
------+---------+-----------------


Total Entry 0


Static Router Table
 VID  | Port Mask
------+-----------------------


Total Entry 0


Forbidden Router Table
 VID  | Port Mask
------+-----------------------
   1  | gi2


Total Entry 1
```

## 2.10.17 ip igmp snooping vlan static-router-port

| | |
|---|---|
| **Syntax** | **ip igmp snooping vlan <VLAN-LIST> static-router-port IF_PORTS**<br>**no ip igmp snooping vlan <VLAN-LIST> static-router-port IF_PORTS** |
| **Parameter** | VLAN-LIST — specifies VLAN ID list to set<br>IF_PORTS — specifies a port list to set or remove |
| **Default** | No static router ports by default |
| **Mode** | Global Configuration |
| **Usage** | Use the **ip igmp snooping vlan static-router-port** command to add static router port. All query packets will forward to this port.<br>Use the **no** form of this command to delete static router port.<br>You can verify settings by the **show ip igmp snooping router** command. |
| **Example** | The following example specifies that set ip igmp snooping static test.<br>`Switch(config)# ip igmp snooping vlan 1 static-router-port g 2` |

```
Switch(config)# show ip igmp snooping router

Dynamic Router Table
 VID  | Port   | Expiry Time(Sec)
------+--------+-----------------


Total Entry 0


Static Router Table
 VID  | Port Mask
------+-----------------------
   1  | gi1


Total Entry 1


Forbidden Router Table
 VID  | Port Mask
------+-----------------------
   1  | gi2


Total Entry 1
```

## 2.10.18 ip igmp snooping vlan static-group

**Syntax**

**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-LIST | specifies VLAN ID list to set |
| ip-add | specifies multicast group ipv4 address |
| IF_PORTS | specifies a port list to set or remove |

**Default**

No static group by default

**Mode**

Global Configuration

**Usage**

Use the **ip igmp snooping vlan static-group** command to add a static group.
The static group will not learn other dynamic ports. If the dynamic group exists, then the static group will overlap the dynamic group. The static group set to valid unless igmp snooping global and vlan enable.

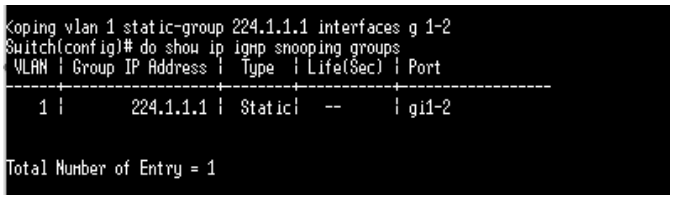
Use the no form of this command to delete a port in static group. If remove the last member of static group, the static group will be delete.

You can verify settings by the **show ip igmp snooping group** command.

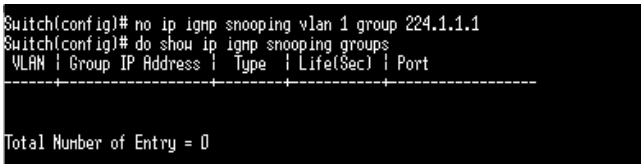
**Example**

The following example specifies that set ip igmp snooping static group test.

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



### 2.10.19 ip igmp snooping vlan group

| | |
|---|---|
| **Syntax** | **no ip igmp snooping vlan <VLAN-LIST> group <ip-addr>** |
| **Parameter** | VLAN-LIST — specifies VLAN ID list to set<br>ip-add — specifies multicast group ipv4 address |
| **Default** | None |
| **Mode** | Global Configuration |
| **Usage** | Use the **no ip igmp snooping vlan group** command to delete a group which could be static or dynamic.<br>You can verify settings by the show ip igmp snooping group command. |
| **Example** | The following example specifies that set ip igmp snooping static group test.<br>`Switch(config)# no ip igmp snooping vlan 1 group 224.1.1.1`<br>  |



### 2.10.20 profile range

| | |
|---|---|
| **Syntax** | **profile range ip <ip-addr> [ip-addr] action (permit \| deny)** |
| **Parameter** | <ip-addr> — Start ipv4 multicast address<br>ip-add — End ipv4 multicast address<br>(permit \| deny) — Permit: allow Multicast address range ip address learning<br>deny: do not allow Multicast address range ip address learning |
| **Default** | None |
| **Mode** | igmp profile configuration mode |
| **Usage** | Use the **profile** command to generate IGMP profile.<br>You can verify settings by the show **ip igmp profile** command |
| **Example** | The following example specifies that set ip igmp profile test.<br>`Switch(config)# ip igmp profile 1`<br>`Switch(config-igmp-profile)# profile range ip 224.1.1.1 224.1.1.8 action permit` |

### 2.10.21 ip igmp profile

| | |
|---|---|
| **Syntax** | **ip igmp profile <1-128>**<br>**no ip igmp profile <1-128>** |
| | <1-128> specifies profile ID |
| **Default** | No profie exist by default |
| **Mode** | Global Configuration |
| **Usage** | Use the **ip igmp profile** command to enter profile configuration<br>Use the **no** form of this command to delete profile<br>You can verify settings by the **show ip igmp profile** command |
| **Example** | The following example specifies that set ip igmp profile test.<br>`Switch(config)# ip igmp profile 1` |

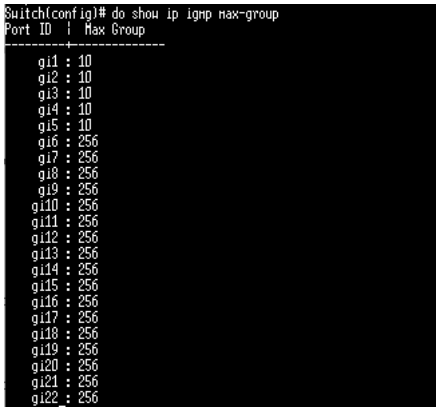
### 2.10.22 ip igmp filter

| | |
|---|---|
| **Syntax** | **ip igmp filter <1-128>**<br>**[no] ip igmp filter** |
| | <1-128> specifies profile ID |
| **Default** | None |
| **Mode** | Port Configuration |
| **Usage** | Use the **ip igmp filter** command to bind a profile for port. When the port bind a profile. Then the port learning group will update, if the group is not match the profile rule it will remove the port from the group. Static group is excluded.<br>Use the **no** form of this command to delete profile<br>You can verify settings by the **show ip igmp filter** command |
| **Example** | The following example specifies that set ip igmp filter test.<br>`Switch(config)# interface gi1`<br>`Switch(config-if)#ip igmp filter 1` |

## 2.10.23 ip igmp max-groups

| | |
|---|---|
| **Syntax** | **ip igmp max-groups <0-1024>**<br>**no ip igmp max-groups** |

| | |
|---|---|
| <0-1024> | The maximum number of IGMP groups that an interface can join |

| | |
|---|---|
| **Default** | Default is 1024 |
| **Mode** | Port Configuration |
| **Usage** | Use the **ip igmp max-groups** command to limit port learning max group number. When the port has reach limitation, new group will not add this port. Static group is excluded.<br><br>Use the no form of this command to restore to default<br>You can verify settings by the **show ip igmp max-groups** command. |
| **Example** | The following example specifies that set ip igmp max-groups test.<br>`Switch(config-if)#ip igmp max-groups 10`<br>  |

### 2.10.24 ip imgp max-groups action

| | |
|---|---|
| **Syntax** | **ip igmp max-groups action (deny \| replace)** |
| | (deny \| replace) — Deny: current port igmp group arrived max-groups, don't add group. Replace: current port igmp group arrived max-groups, remove port for rand group, and add port to new group. |
| **Default** | Default action is deny |
| **Mode** | Port Configuration |
| **Usage** | Use the **ip igmp max-groups action** command to set the action when the numbers of groups reach the limitation.<br>Use the **no** form of this command to restore to default<br>You can verify settings by the **show ip igmp max-groups** command. |
| **Example** | The following example specifies that set action replace test.<br>`Switch(config-if)#ip igmp max-groups action replace` |

### 2.10.25 clear ip igmp snooping groups

| | |
|---|---|
| **Syntax** | **clear ip igmp snooping groups [(dynamic \| static)]** |
| | none — Clear ip igmp groups include dynamic and static<br>(dynamic \| static) — Ip igmp group type is dynamic or static |
| **Default** | None |
| **Mode** | Privileged EXEC |
| **Usage** | This command will clear the ip igmp groups for dynamic or static or all of type.<br>You can verify settings by the **show ip igmp snooping groups** command. |
| **Example** | The following example specifies that clear ip igmp snooping groups test.<br>`Switch# clear ip igmp snooping groups`<br>`Switch# show ip igmp snooping groups` |

### 2.10.26 clear ip igmp snooping statistics

| | |
|---|---|
| **Syntax** | **clear ip igmp snooping statistics** |
| **Parameter** | None |
| **Default** | None |
| **Mode** | Privileged EXEC |
| **Usage** | This command will clear the igmp statistics.<br>You can verify settings by the **show ip igmp snooping** command. |
| **Example** | The following example specifies that clear ip igmp snooping statistics test.<br><br>`Switch# clear ip igmp snooping statistics`<br>`Switch# show ip igmp snooping` |

### 2.10.26 show ip igmp snooping groups counters

| | |
|---|---|
| **Syntax** | **show ip igmp snooping groups** |
| **Parameter** | None |
| **Default** | None |
| **Mode** | Privileged EXEC |
| **Usage** | This command will display the ip igmp group counter include static group. |
| **Example** | The following example specifies that display ip igmp snooping group counter test.<br>`Switch# show ip igmp snooping group counters` |

### 2.10.27 show ip igmp snooping groups

| | |
|---|---|
| **Syntax** | **show ip igmp snooping groups [(dynamic \| static)]** |
| **Parameter** | none — Clear ip igmp groups include dynamic and static<br>(dynamic \| static) — Display Ip igmp group type is dynamic or static |
| **Default** | None |
| **Mode** | Privileged EXEC |
| **Usage** | This command will display the ip igmp groups for dynamic or static or all of type. |
| **Example** | The following example specifies that show ip igmp snooping groups.<br>`Switch# show ip igmp snooping groups` |

### 2.10.28 show ip igmp snooping router

| | |
|---|---|
| **Syntax** | **show ip igmp snooping router [(dynamic \| forbidden \|static )]** |
| **Parameter** | none — Show ip igmp router include dynamic and static and forbidden<br>(dynamic \| forbidden \| static) — Display Ip igmp router info for different type |
| **Default** | None |
| **Mode** | Privileged EXEC |
| **Usage** | This command will display the ip igmp router info. |
| **Example** | The following example specifies that show ip igmp snooping router.<br>`Switch# show ip igmp snooping router` |

```
Switch# show ip igmp snooping router

Dynamic Router Table
 VID  | Port   | Expiry Time(Sec)
------+--------+-----------------


Total Entry 0


Static Router Table
 VID  | Port Mask
------+-----------------------
   1  | gi1

Total Entry 1


Forbidden Router Table
 VID  | Port Mask
------+-----------------------
   1  | gi2

Total Entry 1
```

### 2.10.29 show ip igmp snooping querier

| | |
|---|---|
| **Syntax** | **show ip igmp snooping querier** |
| **Parameter** | none Show all vlan ip igmp querier info. |
| **Default** | None |
| **Mode** | Privileged EXEC |
| **Usage** | This command will display all of the static vlan ip igmp querier info. |
| **Example** | The following example specifies that show ip igmp snooping querier test. |

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

```
Switch# show ip igmp snooping querier

 VID  |   State    |   Status   | Version  | Querier IP
------+------------+------------+----------+-----------------
   1  | Disabled   | Non-Querier |  No      |   ------
Total Entry 1
```

### 2.10.30 show ip igmp snooping

| | |
|---|---|
| **Syntax** | **show ip igmp snooping** |
| **Parameter** | None |
| **Default** | None |
| **Mode** | Privileged EXEC |
| **Usage** | This command will display ip igmp snooping global info. |
| **Example** | The following example specifies that show ip igmp snooping test. |

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

```
show ip igmp snooping

            IGMP Snooping Status
            --------------------

  Snooping                      : Enabled
  Report Suppression            : Enabled
  Operation Version             : v3
  Forward Method                : mac
  Unknown IP Multicast Action   : Router-Port

            Packet Statistics
  Total RX                      :  3932
  Valid RX                      :  1343
  Invalid RX                    :  2589
  Other RX                      :  0
  Leave RX                      :  0
  Report RX                     :  0
  General Query RX              :  0
  Specail Group Query RX        :  0
  Specail Group & Source Query RX  :  0
  Leave TX                      :  0
  Report TX                     :  0
  General Query TX              :  0
  Specail Group Query TX        :  0
  Specail Group & Source Query TX  :  0
```

### 2.10.31 show ip snooping vlan

| | |
|---|---|
| **Syntax** | **show ip igmp snooping vlan [VLAN-LIST]** |
| **Parameter** | none — Show all ip igmp snooping vlan info<br>[VLAN-LIST] — Show specifies vlan ip igmp snooping info |
| **Default** | None |
| **Mode** | Privileged EXEC |
| **Usage** | This command will display ip igmp snooping vlan info. |
| **Example** | The following example specifies that show ip igmp snooping vlan test. |

```
Switch# show ip igmp snooping vlan 1
```

```
Switch# show ip igmp snooping vlan 1

IGMP Snooping is globaly enabled
IGMP Snooping VLAN 1 admin : disabled
IGMP Snooping operation mode : disabled
IGMP Snooping robustness: admin 7 oper 2
IGMP Snooping query interval: admin 100 sec oper 125 sec
IGMP Snooping query max response : admin 12 sec oper 10 sec
IGMP Snooping last member query counter: admin 2  oper 2
IGMP Snooping last member query interval: admin 3 sec  oper 1 sec
IGMP Snooping immediate leave: disabled
IGMP Snooping automatic learning of multicast router ports: enabled
```

### 2.10.32 show ip igmp snooping forward-all

| | |
|---|---|
| **Syntax** | **show ip igmp snooping forward-all [vlan VLAN-LIST]** |
| **Parameter** | none — Show all ip igmp snooping vlan forward-all info<br>[VLAN-LIST] — Show specifies vlan of ip igmp forward info. |
| **Default** | None |
| **Mode** | Privileged EXEC |
| **Usage** | This command will display ip igmp snooping forward all info. |
| **Example** | The following example specifies that show ip igmp snooping forward-all test. |

```
Switch# show ip igmp snooping forward-all 1
```

```
Switch# show ip igmp snooping forward-all

IGMP Snooping VLAN           : 1
IGMP Snooping static port    : gi1-2
IGMP Snooping forbidden port : gi3-4
```

### 2.10.33 show ip igmp profile

| | | |
|---|---|---|
| **Syntax** | **show ip igmp profile [<1-128>]** | |
| **Parameter** | none | Show all ip igmp snooping profile info |
| | [1-128] | Show specifies index profile info |
| **Default** | None | |
| **Mode** | Privileged EXEC | |
| **Usage** | This command will display ip igmp profile info. | |
| **Example** | The following example specifies that show ip igmp profile test.<br>`Switch# show ip igmp profile` | |

### 2.10.34 show ip igmp filter

| | | |
|---|---|---|
| **Syntax** | **show ip igmp filter [interfaces IF_PORTS]** | |
| **Parameter** | none | Show all port filter |
| | [interfaces IF_PORTS] | Show specifies ports filter |
| **Default** | None | |
| **Mode** | Privileged EXEC | |
| **Usage** | This command will display ip igmp port filter info. | |
| **Example** | The following example specifies that show ip igmp filter test.<br>`Switch# show ip igmp filter` | |

### 2.10.35 show ip igmp max-group

| | |
|---|---|
| **Syntax** | **show ip igmp max-group [interfaces IF_PORTS]** |

**Parameter**

| | |
|---|---|
| none | Show all port filter |
| [interfaces IF_PORTS] | Show specifies ports max-group |

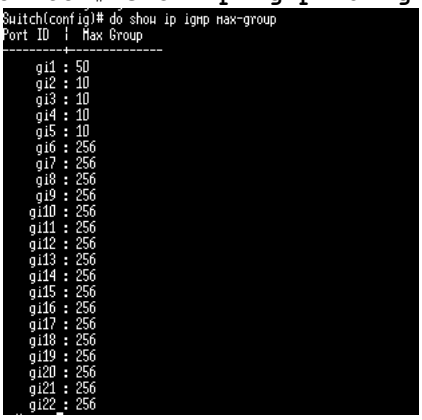
**Default** None

**Mode** Privileged EXEC

**Usage** This command will display ip igmp port max-group.

**Example** The following example specifies that show ip igmp max-group test.

```
Switch(config-if)#ip igmp max-groups 50
Switch# show ip igmp max-group
```



### 2.10.36 show ip igmp max-group action

| | |
|---|---|
| **Syntax** | **show ip igmp max-group action [interfaces IF_PORTS]** |

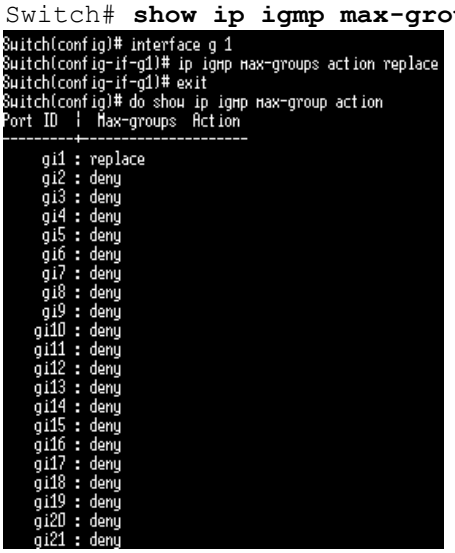
**Parameter**

| | |
|---|---|
| none | Show all port max-group action |
| [interfaces IF_PORTS] | Show specifies ports max-group action |

| | |
|---|---|
| **Default** | None |
| **Mode** | Privileged EXEC |
| **Usage** | This command will display ip igmp port max-group action. |

**Example** The following example specifies that show ip igmp max-group action test.

```
Switch(config)#interface gi1
Switch(config-if)#ip igmp max-groups action replace
Switch# show ip igmp max-group action
```



## 2.11 IP Source Guard

### 2.11.1 ip source verify

| | |
|---|---|
| **Syntax** | **ip source verify [mac-and-ip] / no ip source verify** |
| **Parameter** | mac-and-ip Verify by mac and ip address boundle |
| **Default** | IP Source Guard is disabled on interface. Default is that verifying ip address only |
| **Mode** | Port Configuration |
| **Usage** | Use the **ip source verify** command to enable IP Source Guard function. Default IP Source Guard filter source IP address. The "**mac-and-ip**" filters not only source IP address but also source MAC address.<br>Use the no form of this command to disable.<br>You can verify settings by the **show ip source interfaces** command. |
| **Example** | The example shows how to enable IP Source Guard with source IP address filtering on interface g 1.<br>`Switch(config)# interface g 1`<br>`switch(config-if)# ip source verify`<br><br>The example shows how to enable IP Source Guard with source IP and MAC address filtering on interface g 2.<br><br>`Switch(config)# interface g 2`<br>`switch(config-if)# ip source verify mac-and-ip`<br>`switch(config-if)# do show ip source interfaces g 1-2` |

```
Switch(config)# int g 1
Switch(config-if-g1)# ip source verify
Switch(config-if-g1)# exit
Switch(config)# int g 2
Switch(config-if-g2)# ip source verify mac-and-ip
Switch(config-if-g2)# exit
Switch(config)# do show ip source interfaces GigabitEthernet 1-2
 Port  |     Status     | Max Entry | Current Entry
-------+----------------+-----------+--------------
   gi1 |     Verify IP  | No Limit  |   0
   gi2 |  Verify MAC+IP | No Limit  |   0
```

## 2.11.2 ip source binding

| | |
|---|---|
| **Syntax** | **ip source binding A:B:C:D:E:F vlan <1-4094> A.B.C.D interface IF_PORT**<br>**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 a MAC address of a binding entry |
| VLAN <1-4094> | Specify a VLAN ID of a binding entry |
| A.B.C.D | Specify IP address and MASK of a binding entry. |
| IF_PORT | Specify interface of a binding entry. |

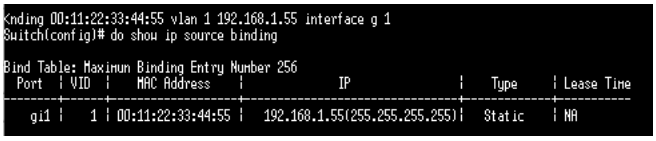
**Default** Default is no binding entry.

**Mode** Global Configuration

**Usage** Use the ip source binding command to create a static IP source binding entry has an IP address, its associated MAC address、VLAN ID、interface.
Use the no form of this command to delete static entry.
You can verify settings by the show ip source binding command.

**Example** The example shows how to add a static IP source binding entry.

```
Switch(config)# ip source binding 00:11:22:33:44:55 vlan 1 192.168.1.55 interface g 1
switch(config)# do show ip source binding
```



### 2.11.3 show ip source interface

| | |
|---|---|
| **Syntax** | **show ip source interfaces IF_PORTS** |
| **Parameter** | IF_PORTS specifies ports to show |
| **Default** | No default is defined |
| **Mode** | Privileged EXEC |
| **Usage** | Use the **show ip source interface** command to show settings of IP Source Guard of interface |
| **Example** | The example shows how to show settings of IP Source Guard of interface g 1 |

```
switch# show ip source interfaces g 1
```

```
Switch(config)# do show ip source interfaces g 1
 Port  |    Status     | Max Entry | Current Entry
-------+---------------+-----------+--------------
  gi1  |    Verify IP  | No Limit  |  1
```

### 2.11.4 show ip source binding

| | | |
|---|---|---|
| **Syntax** | **show ip source binding [(dynamic\|static)]** | |
| **Parameter** | dynamic | Show entries that added by DHCP snooping learn |
| | static | Show entries that added by user |
| **Default** | No default is defined | |
| **Mode** | Privileged EXEC | |
| **Usage** | Use the show ip source binding command to show binding entries of IP Source Guard. | |
| **Example** | The example shows how to show static binding entries of IP Source Guard. | |

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

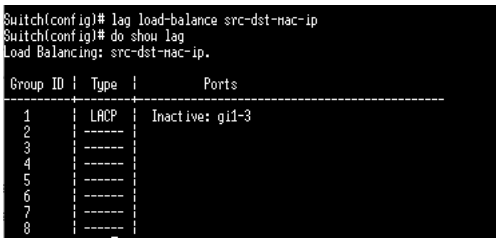
```
Switch(config)# do show ip source binding

Bind Table: Maximun Binding Entry Number 256
 Port  | VID  |   MAC Address    |          IP              |   Type    | Lease Time
-------+------+------------------+--------------------------+-----------+-----------
  gi1  |   1  | 00:11:22:33:44:55 |  192.168.1.55(255.255.255.255)|  Static   | NA
```

## 2.12 Link Aggregation

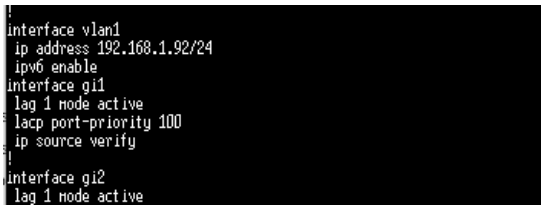
### 2.12.1 lag

| | | |
|---|---|---|
| **Syntax** | **lag <1-8> mode (static \| active \| passive) / no lag** | |
| **Parameter** | <1-8> | Specify the LAG id for the interface |
| | static | Specify the LAG to be static mode and join the interface into this LAG. |
| | active | Specify the LAG to be dynamic mode and join the interface into this LAG with LACP active port. |
| | passive | Specify the LAG to be dynamic mode and join the interface into this LAG with LACP passive port. |
| **Default** | There is no LAG in default. | |
| **Mode** | Interface Configuration | |
| **Usage** | Link aggregation group function allows you to aggregate multiple physical ports into one logic port to increase bandwidth. This command makes normal port join into the specific LAG logic port with static or dynamic mode. And use “no lag” to leave the LAG logic port. | |
| **Example** | This example shows how to create a dynamic LAG and join g1-g3 to this LAG.<br>`Switch(config)# interface range fa1-3`<br>`Switch(config-if)# lag 1 mode active`<br><br>This example shows how to show current LAG status.<br>`Switch# show lag`<br>  | |

### 2.12.2 lag load-balance

| | | |
|---|---|---|
| **Syntax** | **lag load-balance (src-dst-mac \| src-dst-mac-ip)**<br>**no lag load-balance** | |
| **Parameter** | **src-dst-mac** | Specify algorithm to balance traffic by using source and destination MAC address for all packets. |
| | **src-dst-mac-ip** | Specify algorithm to balance traffic by using source and destination IP address for IP packets and using source and destination MAC address for non-IP packet |
| **Default** | Default load balance algorithm is src-dst-mac | |
| **Mode** | Global Configuration | |
| **Usage** | Link aggregation group port should transmit packets spread to all ports to balance traffic loading. There are two algorithm supported and this command allow you to select the algorithm. | |
| **Example** | This example shows how to change load balance algorithm to src-dst-mac-ip.<br>`Switch(config)# lag load-balance src-dst-mac-ip`<br><br>This example shows how to show current load balance algorithm.<br>`Switch# show lag`<br>  | |

### 2.12.3 lacp port-priority

| | |
|---|---|
| **Syntax** | **lacp port-priority <1-65535>**<br>**no lacp port-priority** |
| **Parameter** | **<1-65535>** Specify port priority value |
| **Default** | Default port priority is 1. |
| **Mode** | Interface Configuration |
| **Usage** | LACP port priority is used for two connected DUT to select aggregation ports. Lower port priority value has higher priority. And the port with higher priority will be selected into LAG first.<br><br>The only way to show this configuration is using "**show running-config**" command. |
| **Example** | This example shows how to configure interface fa1 lacp port priority to 100.<br>`Switch(config)# interface g 1`<br>`Switch(config-if)# lacp port-priority 100`<br>  |

### 2.12.4 lacp system-priority

| | |
|---|---|
| **Syntax** | **lacp system-priority** <1-65535><br>**no lacp system-priority** |
| **Parameter** | **<1-65535>** Specify system priority value |
| **Default** | Default system priority is 32768. |
| **Mode** | Global Configuration |
| **Usage** | LACP system priority is used for two connected DUT to select master switch.<br>Lower system priority value has higher priority. And the DUT with higher priority can decide which ports are able to join the LAG.<br><br>Use "**no lacp system-priority**" to restore to the default priority value.<br>The only way to show this configuration is using "**show running-config**" command. |
| **Example** | This example shows how to configure lacp system priority to 1000.<br>`Switch(config)# lacp system-priority 1000` |

```
Switch(config)# lacp system-priority 1000
Switch(config)# do show running-config
SYSTEM CONFIG FILE ::= BEGIN
! System Description: KT-NOS FR-9T448F Switch
! System Version: v1.0.0.12
! System Name: Switch
! System Up Time: 0 days, 0 hours, 36 mins, 46 secs
!
!
!
lag load-balance src-dst-mac-ip
!
lacp system-priority 1000
!
!
!
username "admin" secret encrypted MjEyMzJmMjk3YTU3YTVhNzQzODkOYTB1NGE4MDFmYzM=
!
!
!
voice-vlan oui-table 00:E0:BB "3COM"
voice-vlan oui-table 00:03:6B "Cisco"
voice-vlan oui-table 00:E0:75 "Veritel"
voice-vlan oui-table 00:D0:1E "Pingtel"
voice-vlan oui-table 00:01:E3 "Siemens"
voice-vlan oui-table 00:60:B9 "NEC/Philips"
--More--
```

### 2.12.5 lacp timeout

| | | |
|---|---|---|
| **Syntax** | **lacp timeout (long \| short)**<br>**no lacp timeout** | |
| **Parameter** | **Long** | Send LACP packet every 30 seconds. |
| | **Short** | Send LACP packet every 1 second. |
| **Default** | Default LACP timeout is long. | |
| **Mode** | Interface Configuration | |
| **Usage** | LACP need to send LACP packet to partner switch to check the link status. This command configure the interval of sending LACP packets.<br><br>The only way to show this configuration is using "**show running-config**" command. | |

**Example** This example shows how to configure interface fa1 lacp timeout to short.

```
Switch(config)# interface g 1
Switch(config-if)# lacp timeout short
```

```
!
interface vlan1
 ip address 192.168.1.92/24
 ipv6 enable
interface gi1
 lacp timeout short
!
```

### 2.12.6 show lacp

| | |
|---|---|
| **Syntax** | **show lacp sys-id**<br>**show lacp** [<1-8>] **counters**<br>**show lacp** [<1-8>] **(internal \| neighbor) [detail]** |
| **Parameter** | |
| **Default** | No default values for this command. |
| **Mode** | Privileged EXEC |
| **Usage** | Use "**show lacp sys-id**" command to displays the system identifier that is being used by LACP. The system identifier is made up of the LAPC system priority and the switch MAC address.<br><br>Use "**show lacp counter**" command to display LACP statistic information. Use "**show lacp internal**" command to display local information.<br>Use "**show lacp neighbor**" command to display remote information.<br><br>State of the specific port. These are the allowed values:<br>• -—Port is in an unknown state.<br>• **bndl**—Port is attached to an aggregator and bundled with other ports.<br>• **susp**—Port is in a suspended state; it is not attached to any aggregator.<br>• **hot-sby**—Port is in a hot-standby state.<br>• **1indiv**—Port is incapable of bundling with any other port.<br>• **1indep**—Port is in an independent state (not bundled but able to switch data traffic. In this case, LACP is not running on the partner port).<br>• **down**—Port is down.<br>State variables for the port, encoded as individual bits within a single octet with these meanings:<br>• bit0—LACP_Activity<br>• bit1—LACP_Timeout<br>• bit2—Aggregation<br>• bit3—Synchronization<br>• bit4—Collecting<br>• bit5—Distributing<br>• bit6—Defaulted<br>• bit7—Expired |

| | |
|---|---|
| **Example** | **This example shows how to show LACP statistics.**<br>`Switch# show lacp counters`<br>`Switch# show lacp internal`<br>`Switch# show lacp neighbor` |

### 2.12.7 show lag

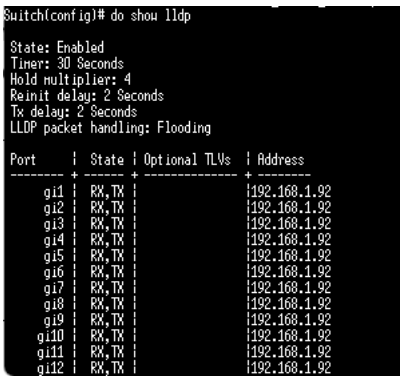
| | |
|---|---|
| **Syntax** | **show lag** |
| **Parameter** | |
| **Default** | No default values for this command. |
| **Mode** | Privileged EXEC |
| **Usage** | Use "**show lag**" command to show current LAG load balance algorithm and members active/inactive status. |
| **Example** | **This example shows how to show current LAG status.**<br>`Switch# show lag` |

## 2.13 LLDP

### 2.13.1 clear lldp statistics

| | |
|---|---|
| **Syntax** | **clear lldp statistics** |
| **Parameter** | N/A |
| **Default** | There is no default configuration for this command |
| **Mode** | Privileged EXEC |
| **Usage** | Use "**clear lldp statistics**" command to clear the LLDP RX/TX statistics. |
| **Example** | This example shows how to clear LLDP statistics.<br>`Switch# clear lldp statistics` |

### 2.13.2 lldp

| | |
|---|---|
| **Syntax** | **lldp**<br>**no lldp** |
| **Parameter** | N/A |
| **Default** | Default is enabled |
| **Mode** | Global Configuration |
| **Usage** | Use "**lldp**" command to enable LLDP RX/TX ability. The LLDP enable status is displayed by "**show lldp**" command.<br><br>Use the no form of this command to disable the LLDP. When LLDP is disabled, the behavior of receiving LLDP PDU would be decided by "**lldp lldpdu**" command. |
| **Example** | The following example sets LLDP enable/disable.<br>`Switch (config)# lldp`<br>`Switch# show lldp`<br>  |

```
Switch(config)# do show lldp

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

Port     | State | Optional TLVs  | Address
-------- + ------ + -------------- + --------
    gi1  | RX,TX |                |192.168.1.92
    gi2  | RX,TX |                |192.168.1.92
    gi3  | RX,TX |                |192.168.1.92
    gi4  | RX,TX |                |192.168.1.92
    gi5  | RX,TX |                |192.168.1.92
    gi6  | RX,TX |                |192.168.1.92
    gi7  | RX,TX |                |192.168.1.92
    gi8  | RX,TX |                |192.168.1.92
    gi9  | RX,TX |                |192.168.1.92
   gi10  | RX,TX |                |192.168.1.92
   gi11  | RX,TX |                |192.168.1.92
   gi12  | RX,TX |                |192.168.1.92
```

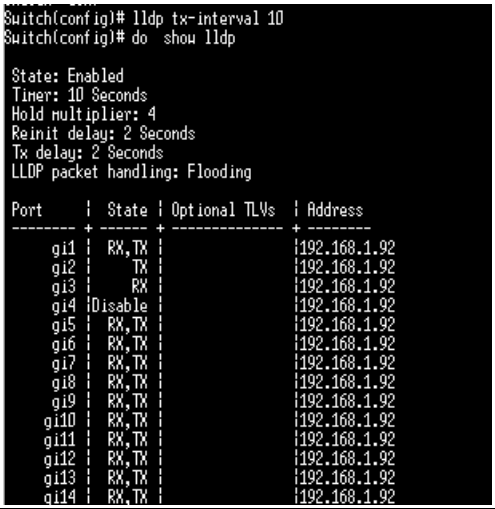
### 2.13.3 lldp rx

| | |
|---|---|
| **Syntax** | **lldp rx**<br>**no lldp rx** |
| **Parameter** | N/A |
| **Default** | Default is enabled |
| **Mode** | Port Configuration |
| **Usage** | Use "**lldp rx**" command to enable the LLDP PDU RX ability. The configuration could be shown by "**show lldp**" command. |

**Example** This example sets port gi1 to enable LLDP TX, port g 2 to disable RX but enable TX, port g 3 to enable RX but disable TX, port g 4 to disable RX and TX.

```
Switch(config)# int g 1
Switch(config-if-g1)# lldp rx
Switch(config-if-g1)# lldp tx
Switch(config-if-g1)# exit
Switch(config)# int g 2
Switch(config-if-g2)# np lldp rx
Incomplete command
Switch(config-if-g2)# no lldp rx
Switch(config-if-g2)# lldp tx
Switch(config-if-g2)# exit
Switch(config)# int g 3
Switch(config-if-g3)# lldp rx
Switch(config-if-g3)# no lldp tx
Switch(config-if-g3)# exit
Switch(config)# int g 4
Switch(config-if-g4)# no lldp rx
Switch(config-if-g4)# no lldp tx
Switch(config-if-g4)# end
Switch# show lldp int g 1-4

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

Port     |  State | Optional TLVs  | Address
-------- + ------ + -------------- + --------
     gi1 |  RX,TX |                |192.168.1.92
     gi2 |     TX |                |192.168.1.92
     gi3 |     RX |                |192.168.1.92
     gi4 |Disable |                |192.168.1.92

Port ID: gi1
802.3 optional TLVs:
802.1 optional TLVs
PVID: Enabled
```

### 2.13.4 lldp tx-interval

| | |
|---|---|
| **Syntax** | **lldp tx-interval** <5-32768><br>**no lldp tx-interval** |
| **Parameter** | <5-32768> Specify the LLDP PDU TX interval in unit of second. |
| **Default** | Default TX interval is 30 seconds |
| **Mode** | Global Configuration |
| **Usage** | Use "**lldp tx-interval**" command to configure the LLDP TX interval. It should be noticed that both "**lldp tx-interval**" and "**lldp tx-delay**" affects the LLDP PDU TX time. The larger value of the two configurations decides the TX interval. The configuration could be shown by "**show lldp**" command.<br><br>Use the **no** form of this command to restore the interval to default value. |
| **Example** | This example sets LLDP TX interval to 10 seconds.<br>`Switch(config)# lldp tx-interval 10`<br>`Switch# show lldp`<br>  |

```
Switch(config)# lldp tx-interval 10
Switch(config)# do  show lldp

State: Enabled
Timer: 10 Seconds
Hold multiplier: 4
Reinit delay: 2 Seconds
Tx delay: 2 Seconds
LLDP packet handling: Flooding

Port     |  State | Optional TLVs  | Address
-------- + ------ + -------------- + --------
     gi1 |  RX,TX |                |192.168.1.92
     gi2 |     TX |                |192.168.1.92
     gi3 |     RX |                |192.168.1.92
     gi4 |Disable |                |192.168.1.92
     gi5 |  RX,TX |                |192.168.1.92
     gi6 |  RX,TX |                |192.168.1.92
     gi7 |  RX,TX |                |192.168.1.92
     gi8 |  RX,TX |                |192.168.1.92
     gi9 |  RX,TX |                |192.168.1.92
    gi10 |  RX,TX |                |192.168.1.92
    gi11 |  RX,TX |                |192.168.1.92
    gi12 |  RX,TX |                |192.168.1.92
    gi13 |  RX,TX |                |192.168.1.92
    gi14 |  RX,TX |                |192.168.1.92
```

### 2.13.5 lldp reinit-delay

| | |
|---|---|
| **Syntax** | **lldp reinit-delay** <1-10><br>**no lldp reinit-delay** |
| **Parameter** | <1-10> Specify the LLDP re-initial delay time in unit of second. |
| **Default** | Default reinital delay is 2 seconds |
| **Mode** | Global Configuration |
| **Usage** | Use "**lldp reinit-delay**" to configure the LLDP re-initial delay. This delay avoids LLDP generate too many PDU if the port is up and down frequently. The delay starts to count when the port links down. The port would not generate LLDP PDU until the delay counts to zero. The configuration could be shown by "show lldp" command.<br><br>Use the **no** form of this command to restore the delay to default value. |
| **Example** | **This example sets LLDP re-initial delay to 5 seconds.**<br>`Switch(config)# lldp reinit-delay 5`<br>`Switch# show lldp`<br>  |

### 2.13.6 lldp holdtime-multiplier

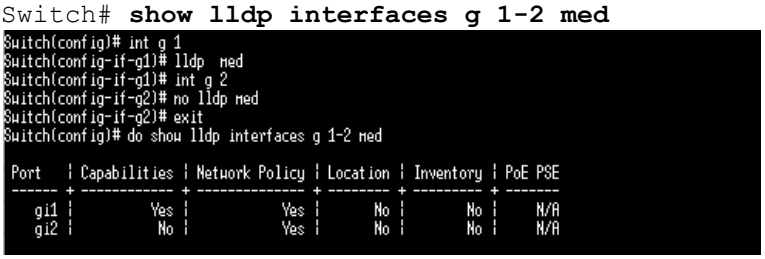
| | |
|---|---|
| **Syntax** | **lldp holdtime-multiplier** <2-10><br>**no holdtime-multiplier** |
| **Parameter** | <2-10> Specify the LLDP hold time multiplier. |
| **Default** | lldp holdtime-multiplier 4 |
| **Mode** | Global Configuration |
| **Usage** | Use “lldp holdtime-multiplier” command to configure the LLDP PDU hold multiplier that decides time-to-live (TTL) value sent in LLDP advertisements: TTL = (tx-interval * holdtime-multiplier). The configuration could be shown by “show lldp” command.<br><br>Use the no form of this command to restore the multiplier to default value. |
| **Example** | **This example sets LLDP hold time multiplier to 3.**<br>`Switch(config)# lldp holdtime-multiplier 3`<br>`Switch# show lldp`<br>  |

### 2.13.7 lldp lldpdu

| | | |
|---|---|---|
| **Syntax** | **lldp lldpdu (filtering\|flooding\|bridging)** | |
| **Parameter** | **Bridging** | When LLDP is globally disabled, LLDP packets are bridging (bridging LLDP PDU to VLAN member ports). |
| | **filtering** | When LLDP is globally disabled, LLDP packets are filtered (deleted). |
| | **flooding** | When LLDP is globally disable, LLDP packets are flooded(forward to all interfaces) |
| **Default** | Default LLDP PDU handling behavior when LLDP disabled is flooding | |
| **Mode** | Global Configuration | |
| **Usage** | Use "**lldp lldpdu**" command to configure the LLDP PDU handling behavior when LLDP is globally disabled. It should be noticed that if LLDP is globally enabled and per port LLDP RX status is configured to disabled, the received LLDP PDU would be dropped instead of taking the global disable behavior.<br>The configuration could be shown by "**show lldp**" command.<br>Use the **no** form of this command to restore the behavior to default. | |
| **Example** | This example sets LLDP disable action to bridging. | |

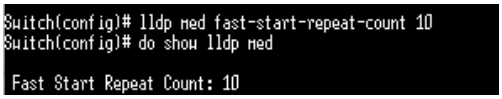
```
Switch(config)# lldp lldpdu bridging
Switch# show lldp
```

### 2.13.8 lldp med

| | |
|---|---|
| **Syntax** | **lldp med**<br>**no lldp med** |
| **Parameter** | N/A |
| **Default** | lldp med |
| **Mode** | Port Configuration |
| **Usage** | Use “lldp med” to configure the LLDP MED enable status. If LLDP MEDis enabled, LLDP MED capability TLV and other selected MED TLV would be attached. The configuration could be shown by “show lldp med” command.<br><br>Use the no form of this command to disable the LLDP MED status. |
| **Example** | This example sets port gi1 to enable LLDP MED, port gi2 to disable LLDP MED.<br><br>`Switch(config)# interface g 1`<br>`Switch(config-if)# lldp med`<br>`Switch(config)# interface g 2`<br>`Switch(config-if)# no lldp med`<br>`Switch# show lldp interfaces g 1-2 med`<br>  |

```
Switch(config)# int g 1
Switch(config-if-g1)# lldp  med
Switch(config-if-g1)# int g 2
Switch(config-if-g2)# no lldp med
Switch(config-if-g2)# exit
Switch(config)# do show lldp interfaces g 1-2 med

 Port   | Capabilities | Network Policy | Location | Inventory | PoE PSE
 ------ + ------------ + -------------- + -------- + --------- + -------
    gi1 |          Yes |            Yes |       No |        No |     N/A
    gi2 |           No |            Yes |       No |        No |     N/A
```

### 2.13.9 lldp med fast-start-repeat-count

| | |
|---|---|
| **Syntax** | **lldp med fast-start-repeat-count** <1-10><br>**no lldp med fast-start-repeat-count** |
| **Parameter** | <1-10> LLDP PDU fast start TX repeat counts. |
| **Default** | Default fast start TX repeat count is 3 |
| **Mode** | Global Configuration |
| **Usage** | Use "lldp med fast-start-repeat-count" command to configure the LLDP PDU fast start TX repeat count. When port links up, it will send LLDP PDU immediately to notify link partner. The number of LLDP PDU sends when it links up depends on fast-start-repeat-count configuration. The LLDP PDU fast-start transmits in interval of one second. The fast start behavior works no matter LLDP MED is enabled or not. The configuration could be shown by "**show lldp med**" command.<br>Use the **no** form of this command to restore count to default. |
| **Example** | This example sets fast start repeat count to 10.<br><br>`Switch(config)# lldp med fast-start-repeat-count 10`<br>`Switch# show lldp med`<br>  <br> |

### 2.13.10 lldp med location

| | | |
|---|---|---|
| **Syntax** | **lldp med location (coordination\|civic-address\|ecs-elin) ADDR**<br>**no lldp med location (coordination\|civic-address\|ecs-elin)** | |
| **Parameter** | **coordination**<br>**civic-address**<br>**ecs-elin** | Location type to be configured. “ecs-elin” is abbreviation of emergency call service – emergency location identifier number |
| | **ADDR** | Specify the location data. Input format is hexadecimal values without colon (for example: 1234AB). For coordination location type, the length of ADDR is 16 bytes. For civic-address, the length is 6 to 160 bytes.<br>For ecs-elin, the length is 10 to 25 bytes. |
| **Default** | Deafult is no location data. | |
| **Mode** | Port Configuration | |
| **Usage** | Use “**lldp med location**” command to configure the LLDP MED location data. The “coordinate”, “civic-address”, “ecs-elin” locations are independent, so at most three location TLVs could be sent if their data are not empty. The configuration of location could be shown by “**show lldp interface PORT med**” command.<br><br>Use the **no** form of this command to clear location data. | |

**Example** This example sets location data for interface g 1.

```
Switch(config)# interface g 1
Switch(config-if)# lldp med location coordinate
112233445566778899AABBCCDDEEFF00
Switch(config-if)# lldp med location civic-address
112233445566
Switch(config-if)# lldp med location ecs-elin
1122334455667788 99AA
Switch# show lldp interfaces g 1 med
```

```
Switch(config)# int g 1
Ked location coordinate 112233445566778899AABBCCDDEEFF00
Switch(config-if-g1)# lldp med location civic-address 112233445566
Switch(config-if-g1)# lldp med location ecs-elin 1122334455667788 99AA
Switch(config-if-g1)# exit
Switch(config)# do show lldp int g 1 med

Port    | Capabilities | Network Policy | Location | Inventory | PoE PSE
------ + ------------ + -------------- + -------- + --------- + -------
   gi1 |          Yes |            Yes |       No |        No |     N/A

Port ID: gi1
Network policies:
Location:
Coordinates: 112233445566778899AABBCCDDEEFF00
Civic-address: 112233445566
Ecs-elin: 1122334455667788 99AA
```

### 2.13.11 lldp med network-policy

**Syntax**

**lldp med network-policy** <1-32> **app (voice|voice-signaling|guest-voice|guest-voice-signaling|softphone-voice|video-conferencing|streaming- video|video-signaling) vlan** <1-4094> **vlan-type (tag|untag) priority** <0- 7> **dscp** <0-63>
**no lldp med network-policy <1-32>**

**Parameter**

| | |
|---|---|
| <1-32> | Specify the network policy index |
| voice<br>voice-signaling<br>guest-voice<br>guest-voice-signaling<br>softphone-voice<br>video-conferencing<br>streaming-video<br>video-signaling | Specify the network policy application type. |
| <1-4094> | Specify the L2 priority |
| Tag untag | Specify the VLAN tag status |
| <0-63> | Specify the DSCP value |

**Default**

No network policy is defined

**Mode**

Global Configuration

**Usage**

Use "**lldp med network-policy**" command to configure the LLDP MED network policy table and add a network policy entry that can be bind to ports. If LLDP MED network policy voice auto mode is enabled, "voice" type network policy can not be created since it is in auto mode. The network policy table configuration could be shown by "**show lldp med**" command.

Use the **no** form of this command to remove network policy entry of specific index. A network policy can be removed only when it is not bind to any port.

**Example**

**This example create 2 network policies.**

```
Switch(config)# lldp med network-policy 1 app voice-signaling vlan 2 vlan-type tag priority 3 dscp 4
Switch(config)# lldp med network-policy 32 app video-conferencing vlan 5 vlan-type tag priority 1 dscp 63
Switch# show lldp med
```

```
twork-policy 1 app voice-signaling vlan 2 vlan-type tag priority 3 dscp 4
k-policy 32 app video-conferencing vlan 5 vlan-type tag priority 1 dscp 63
Switch(config)# do show lldp med

 Fast Start Repeat Count: 10

Network policy 1
------------------
Application type: Voice Signaling
VLAN ID: 2 tagged
Layer 2 priority: 3
DSCP: 4

Network policy 32
------------------
Application type: Conferencing
VLAN ID: 5 tagged
Layer 2 priority: 1
DSCP: 63
```

### 2.13.12 lldp med network-policy(Interface)

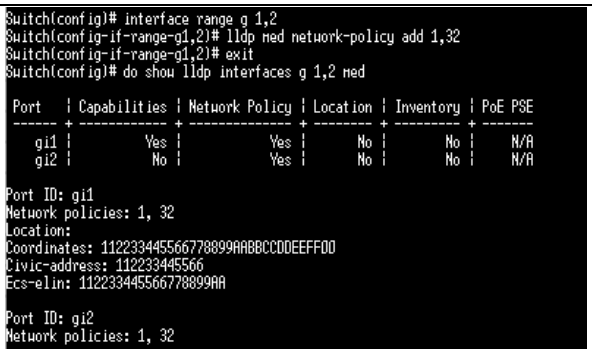
| | | |
|---|---|---|
| **Syntax** | **lldp med network-policy (add\|remove)** <1-32> | |
| **Parameter** | add | Add network policy binding for ports. |
| | remove | Remove network policy binding for ports. |
| | <1-32> | Specify the network policy index |
| **Default** | Default is no network policy binding to port. | |
| **Mode** | Port Configuration | |
| **Usage** | Use "**lldp med network-policy**" command to bind the network policy to port interface. The binded network policy of one port should be with different types. If network policy TLV is selected over a port, the binded network policies would be attached in LLDP MED PDU. The configuration of network policy binding could be shown by "**show lldp med**" command. | |

**Example** **This example binds network policy for interface gi1 and gi2.**

```
Switch# show lldp med
```

```
Switch(config)# do show lldp med

 Fast Start Repeat Count: 10

Network policy 1
------------------
Application type: Voice Signaling
VLAN ID: 2 tagged
Layer 2 priority: 3
DSCP: 4

Network policy 32
------------------
Application type: Conferencing
VLAN ID: 5 tagged
Layer 2 priority: 1
DSCP: 63
```

```
Switch(config)# interface range g 1,2
Switch(config-if-range)# lldp med network-policy add
                         1,32
Switch# show lldp interfaces g 1,2 med
```



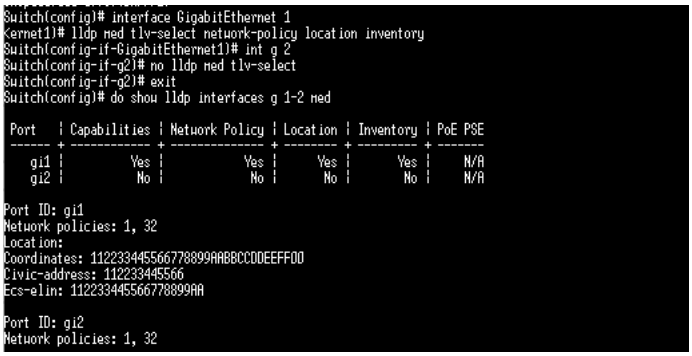

### 2.13.12 lldp med network-policy voice auto

| | |
|---|---|
| **Syntax** | **lldp med network-policy voice auto**<br>**no lldp med network-policy voice auto** |
| **Parameter** | N/A |
| **Default** | ldp med network-policy auto |
| **Mode** | Global Configuration |
| **Usage** | Use "**lldp med network-policy voice auto**" command to enable network policy voice auto mode. In voice auto mode, if network-policy TLV is selected, a voice type network policy would be attached to PDU that contents comes from voice VLAN configuration. This works for voice VLAN module to exchange voice VLAN information with link partner. If voice auto mode is enabled, user can not manually create an voice type network policy; if an voice type network policy is created, the voice auto mode can not be enabled. The configuration of network policy auto mode could be shown by "**show lldp med**" command.<br><br>Use the no form of this command to disable voice auto mode. |
| **Example** | This example sets network policy auto mode to enable and then disable.<br>`Switch (config)# lldp med network-policy auto`<br>`Switch (config)# no lldp med network-policy auto` |

### 2.13.13 lldp med tlv-select

| | |
|---|---|
| **Syntax** | **lldp med tlv-select MEDTLV [MEDTLV] [MEDTLV] [MEDTLV]**<br>**no lldp med tlv-select** |
| **Parameter** | MEDTLV MED optional TLV. Available optional TLVs are : network-policy, location, poe-pse, inventory. |
| **Default** | network-policy TLV |
| **Mode** | Port Configuration |
| **Usage** | Use “lldp med tlv-select” command to configure the LLDP MED TLV Selection. It should be noticed that even no MED TLV is selected, MED capability TLV would be attached if LLDP MED is enable. The configuration could be shown by “show lldp med” command.<br>Use the **no** form of this command to remove all selected MED TLV over the dedicated ports. |
| **Example** | This example sets port gi1-2 to select LLDP MED network policy, location, POE-PSE, inventory TLVs, and it sets port gi3-4 to un-select all LLDP MED TLVs. |

```
Switch(config)# interface gi1
Switch(config-if)# lldp med tlv-select network-policy location inventory
Switch(config)# interface gi2 Switch(config-if)# no lldp med tlv-select
Switch# show lldp interfaces gi1-2 med
```



### 2.13.14 lldp tlv-select

| | | |
|---|---|---|
| **Syntax** | **lldp tlv-select** TLV [TLV] [TLV] [TLV] [TLV] [TLV] [TLV] [TLV]<br>**no lldp tlv-select** | |
| **Parameter** | TLV | Specify the selected optional TLV. Available optional TLVs are : sys-name (system name), sys-desc (system description), sys-cap (system capability), mac-phy (802.3 MAC-PHY), lag (802.3 link aggregation), max-frame-size (802.3 max frame size), and management-add (management address). |
| **Default** | Default is no selected optional TLV. | |
| **Mode** | Port Configuration | |
| **Usage** | Use "**lldp tlv-select**" command to attach selected TLV in PDU. The configuration could be shown by "s**how lldp**" command.<br><br>Use the **no** form of this command to remove all selected TLV. | |

**Example** This example selects system name, system description, system capability, 802.3 MAC-PHY, 802.3 link aggregation, 802.3 max frame size, and management address TLVs for interface gi1 and gi3.

```
Switch(config)# interface range gi 1,3
Switch(config-if-range)# lldp tlv-select port-desc sys-
name sys-desc sys-cap mac-phy lag max-frame-size
management-addr Switch(config-if-range)# end
Switch# show lldp interfaces gi1,3
 State: Disabled
 Timer: 10 Seconds
 Hold multiplier: 3
 Reinit delay: 2 Seconds
 Tx delay: 2 Seconds
 LLDP packet handling: Flooding

 Port     |  State | Optional TLVs  | Address
 -------- + ------ + -------------- + --------
      gi1 |  RX,TX | PD, SN, SD, SC |192.168.1.254
      gi3 |  RX,TX | PD, SN, SD, SC |192.168.1.254

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: Enabled

Port ID: gi3
802.3 optional TLVs: 802.3-mac-phy, 802.3-lag, 802.3-max-
frame-size, management-addr
802.1 optional TLVs
PVID: Enabled
```

### 2.13.15 lldp tlv-select pvid

| | |
|---|---|
| **Syntax** | **lldp tlv-select pvid (disable\|enable)**<br>**no lldp tlv-select pvid** |
| **Parameter** | disable — Disable LLDP 802.1 PVID TLV attach state<br>enable — Enable LLDP 802.1 PVID TLV attach state |
| **Default** | Default is enabled |
| **Mode** | Port Configuration |
| **Usage** | Use "**lldp tlv-select pvid**" command to configure the 802.1 PVID TLV attach enable status. The configuration could be shown by "**show lldp**" command. Use the no form of this command to restore the pvid to default value. |
| **Example** | This example sets port gi1 PVID TLV attaches status to disable and port g 2 to enable. |

```
Switch(config)# interface g 1
Switch(config-if)# lldp tlv-select pvid disable
Switch(config-if)# interface g 2
Switch(config-if)# lldp tlv-select pvid enable
Switch# show lldp interfaces g 1, g 2
```

```
Switch(config)# interface g 1
Switch(config-if-g 1)# lldp tlv-select pvid disable
Switch(config-if-g 1)# int g 2
Switch(config-if-g2)# lldp tlv-select pvid enable
Switch(config-if-g2)# exit
Switch(config)# do show lldp interfaces g 1-2

State: Enabled
Timer: 10 Seconds
Hold multiplier: 3
Reinit delay: 5 Seconds
Tx delay: 2 Seconds
LLDP packet handling: Bridging

Port     | State | Optional TLVs  | Address
-------- + ----- + -------------- + --------
     gi1 | RX,TX |                |192.168.1.92
     gi2 |    TX |                |192.168.1.92

Port ID: gi1
802.3 optional TLVs:
802.1 optional TLVs
PVID: Disabled

Port ID: gi2
802.3 optional TLVs:
802.1 optional TLVs
PVID: Enabled
```

### 2.13.16 lldp tlv-select vlan-name

| | | |
|---|---|---|
| **Syntax** | **lldp tlv-select vlan-name (add\|remove)** VLAN-LIST | |
| **Parameter** | **add** VLAN-LIST | Add VLAN list for LLDP 802.1 VLAN-NAME TLV on the specific interface. The configured ports should be member of all the specified VLANs or the VLAN-LIST is not valid. |
| | **remove** VLAN-LIST | Remove VLAN list of LLDP 802.1 VLAN-NAME TLV from interface. |
| **Default** | Default is no VLAN added. | |
| **Mode** | Port Configuration | |
| **Usage** | Use "**lldp tlv-select vlan-name**" command to add or remove VLAN l list for 802.1 VLAN-NAME TLV. The configuration could be shown by "**show lldp**" command. | |
| **Example** | This example add VLAN 100 to VLAN-NAME TLV for port g 10. | |

```
Switch(config)# vlan 100
Switch(config-vlan)# exit
Switch(config)# interface gi1
Switch(config-if)# switchport trunk allowed vlan add all
Switch(config-if)# lldp tlv-select vlan-name add 100
Switch(config-if)# end
```

```
Switch# show lldp interfaces g 1

State: Enabled
Timer: 10 Seconds
Hold multiplier: 3
Reinit delay: 5 Seconds
Tx delay: 2 Seconds
LLDP packet handling: Bridging

Port     | State | Optional TLVs  | Address
-------- + ----- + -------------- + --------
     gi1 | RX,TX |                |192.168.1.92

Port ID: gi1
802.3 optional TLVs:
802.1 optional TLVs
PVID: Disabled
VLANs: 100
```

### 2.13.17 lldp tx

| | |
|---|---|
| **Syntax** | **lldp / tx no lldp tx** |
| **Parameter** | N/A |
| **Default** | Default is enable |
| **Mode** | Port Configuration |
| **Usage** | Use "**lldp tx**" command to enable the LLDP PDU TX ability. The configuration could be shown by "show lldp" command. Use the no form of this command to disable the TX ability. |
| **Example** | This example sets port g 1 to enable LLDP TX, port g 2 to disable RX but enable TX, port g 3 to enable RX but disable TX, port g 4 to disable RX and TX. |

```
Switch(config)# interface g 1
Switch(config-if)# lldp rx
Switch(config-if)# lldp tx
Switch(config)# interface g 2
Switch(config-if)# no lldp rx
Switch(config-if)# lldp tx
Switch(config)# interface g 3
Switch(config-if)# lldp rx
Switch(config-if)# no lldp tx
Switch(config)# interface g 4
Switch(config-if)# no lldp rx
Switch(config-if)# no lldp tx
Switch(config-if)# end
Switch# show lldp interfaces g 1-4
```

```
Switch# show lldp interfaces g 1-4

State: Enabled
Timer: 10 Seconds
Hold multiplier: 3
Reinit delay: 5 Seconds
Tx delay: 2 Seconds
LLDP packet handling: Bridging

Port     | State | Optional TLVs  | Address
-------- + ----- + -------------- + --------
     gi1 |  RX,TX |               |192.168.1.92
     gi2 |     TX |               |192.168.1.92
     gi3 |     RX |               |192.168.1.92
     gi4 |Disable |               |192.168.1.92
```

### 2.13.18 lldp tx-delay

| | |
|---|---|
| **Syntax** | **lldp tx-delay <1-8192>**<br>**no lldp tx-delay** |
| **Parameter** | <1-8192> Specify the LLDP tx delay in unit of seconds. |
| **Default** | Default TX delay is 2 seconds |
| **Mode** | Global Configuration |
| **Usage** | Use "**lldp tx-delay**" command to configure the delay in seconds between successive LLDP frame transmissions. The delay starts to count in any case LLDP PDU is sent such as by LLDP PDU advertise routine, LLDP PDU content change, port link up, etc. The configuration could be shown by "**show lldp**" command.<br><br>Use the **no** form of this command to restore the delay to default value |
| **Example** | This example sets LLDP PDU TX delay to 10 seconds.<br><br>`Switch(config)# lldp tx-delay 10`<br>`Switch# show lldp` |

### 2.13.19 show lldp

| | |
|---|---|
| **Syntax** | **show lldp**<br>**show lldp interface** IF_NMLPORTS |
| **Parameter** | IF_NMLPORTS Specify the ports to display information |
| **Default** | This command has no default value. |
| **Mode** | Privileged EXEC |
| **Usage** | Use “show lldp” and “show lldp interface” commands to display LLDP global information including LLDP enable status, LLDP PDU TX interval, hold time multiplier, re-initial delay, TX delay, and LLDP packet handling when LLDP is disabled. The per port information displayed includes port LLDP RX/TX enable status, selected TLV to TX and IP address. The abbreviations in optional TLVs are: port description (PD), system name (SN),system description (SD), and system capability (SC). |
| **Example** | This example displays lldp information of port gi1 and gi2 |

```
Switch# show lldp interfaces gi1,gi2
```

```
Switch(config)# do show lldp interfaces gi1,gi2

State: Enabled
Timer: 10 Seconds
Hold multiplier: 3
Reinit delay: 5 Seconds
Tx delay: 2 Seconds
LLDP packet handling: Bridging

Port     | State | Optional TLVs  | Address
-------- + ----- + -------------- + --------
     gi1 | RX,TX |                |192.168.1.92
     gi2 |    TX |                |192.168.1.92

Port ID: gi1
802.3 optional TLVs:
802.1 optional TLVs
PVID: Disabled
VLANs: 100

Port ID: gi2
802.3 optional TLVs:
802.1 optional TLVs
PVID: Enabled
```

## 2.13.20 show lldp local-device

| | |
|---|---|
| **Syntax** | **show lldp local-device**<br>**show lldp interfaces** IF_NMLPORTS **local-device** |
| **Parameter** | IF_NMLPORTS Specify the ports to display information |
| **Default** | There is no default configuration for this command |
| **Mode** | Privileged EXEC |
| **Usage** | Use “show lldp local-device” command to show the local configuration of LLDP PDU. By the commands, a user can view the contents of LLDP/ LLDP-MED TLVs that would be attached in LLDP PDU. |
| **Example** | This example displays the local device information. |

```
Switch# show lldp local-device
```

```
Switch(config)# do show lldp local-device

LLDP Local Device Information:
 Chassis Type : Mac Address
 Chassis ID   : 00:18:95:83:FB:AC
 System Name  : Switch
 System Description  : FR-9T448F
 System Capabilities Support : Bridge, Router
 System Capabilities Enable  : Bridge, Router
 Management Address : 0.0.0.0(IPv4)
```

```
Switch(config)# show lldp interfaces gi1 local-device
```

```
Switch(config)# do show lldp interfaces gi1 local-device

Device ID: 00:18:95:83:FB:AC
Port ID: gi1
System Name: Switch
Capabilities: Bridge, Router
System description: FR-9T448F
Port description:
Time To Live: 30
802.1 VLAN: 100
802.1 VLAN name: 100(VLAN0100)
LLDP-MED capabilities: Capabilities, Network Policy, Location, Inventory
LLDP-MED Device type: Network Connectivity
LLDP-MED Network policy
Application type: Voice Signaling
Flags: Defined
VLAN ID: 2
Layer 2 priority: 3
DSCP: 4
LLDP-MED Network policy
Application type: Video Conferencing
Flags: Defined
VLAN ID: 5
Layer 2 priority: 1
DSCP: 63
Hardware revision:
Firmware revision: 3.6.7.55090
Software revision: 1.0.0.12
Serial number:
Manufacturer Name: Default
Model name: GS9300-28
Asset ID:
LLDP-MED Location
Coordinates: 11:22:33:44:55:66:77:88:99:AA:BB:CC:DD:EE:FF:00
Civic-address: 11:22:33:44:55:66
Ecs-elin: 11:22:33:44:55:66:77:88:99:AA
```

## 2.13.21 show lldp med

| | |
|---|---|
| **Syntax** | **show lldp med**<br>**show lldp interfaces** IF_NMLPORTS **med** |
| **Parameter** | IF_NMLPORTS Specify the ports to display information |
| **Default** | There is no default configuration for this command |
| **Mode** | Privileged EXEC |
| **Usage** | Use “show lldp med” command to display the LLDP MED configuration information. |

**Example** **This example displays the local device information.**

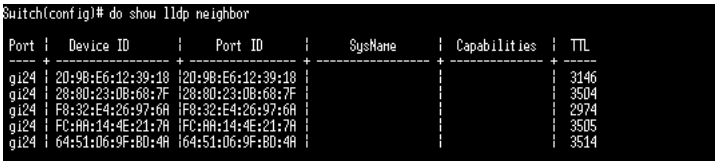
```
Switch# show lldp med
```

```
do show lldp med

 Fast Start Repeat Count: 10

Network policy 1
------------------
Application type: Voice Signaling
VLAN ID: 2 tagged
Layer 2 priority: 3
DSCP: 4

Network policy 32
------------------
Application type: Conferencing
VLAN ID: 5 tagged
Layer 2 priority: 1
DSCP: 63

 Port   | Capabilities | Network Policy | Location | Inventory | PoE PSE
 ------ + ------------ + -------------- + -------- + --------- + -------
    gi1 |          Yes |            Yes |      Yes |       Yes |     N/A
    gi2 |           No |             No |       No |        No |     N/A
    gi3 |          Yes |            Yes |       No |        No |     N/A
    gi4 |          Yes |            Yes |       No |        No |     N/A
    gi5 |          Yes |            Yes |       No |        No |     N/A
    gi6 |          Yes |            Yes |       No |        No |     N/A
    gi7 |          Yes |            Yes |       No |        No |     N/A
    gi8 |          Yes |            Yes |       No |        No |     N/A
    gi9 |          Yes |            Yes |       No |        No |      No
   gi10 |          Yes |            Yes |       No |        No |      No
   gi11 |          Yes |            Yes |       No |        No |      No
   gi12 |          Yes |            Yes |       No |        No |      No
   gi13 |          Yes |            Yes |       No |        No |      No
   gi14 |          Yes |            Yes |       No |        No |      No
   gi15 |          Yes |            Yes |       No |        No |      No
   gi16 |          Yes |            Yes |       No |        No |      No
   gi17 |          Yes |            Yes |       No |        No |      No
   gi18 |          Yes |            Yes |       No |        No |      No
   gi19 |          Yes |            Yes |       No |        No |      No
   gi20 |          Yes |            Yes |       No |        No |      No
   gi21 |          Yes |            Yes |       No |        No |      No
   gi22 |          Yes |            Yes |       No |        No |      No
   gi23 |          Yes |            Yes |       No |        No |      No
   gi24 |          Yes |            Yes |       No |        No |      No
    te1 |          Yes |            Yes |       No |        No |     N/A
    te2 |          Yes |            Yes |       No |        No |     N/A
    te3 |          Yes |            Yes |       No |        No |     N/A
    te4 |          Yes |            Yes |       No |        No |     N/A
```

## 2.13.22 show lldp neighbor

| | |
|---|---|
| **Syntax** | **show lldp neighbor**<br>**show lldp interfaces** IF_NMLPORTS **neighbor** |
| **Parameter** | IF_NMLPORTS Specify the ports to display information |
| **Default** | There is no default configuration for this command |
| **Mode** | Privileged EXEC |
| **Usage** | Use “show lldp neighbor” command to display the received neighbor LLDP PDU information. When LLDP PDU is received on LLDP RX enable ports, system would store the PDU information in database until time to live of the PDU counts down to zero. |
| **Example** | **This example displays the neighbor information.** |

```
Switch# show lldp neighbor
```




```
Switch# show lldp interfaces gi 3 neighbor
```

## 2.13.23 show lldp statistics

| | |
|---|---|
| **Syntax** | **show lldp statistics**<br>**show lldp interfaces** IF_NMLPORTS **statistics** |
| **Parameter** | IF_NMLPORTS Specify the ports to display information |
| **Default** | There is no default configuration for this command |
| **Mode** | Privileged EXEC |
| **Usage** | Use “show lldp statistics” command to display the LLDP RX/TX statistics. |
| **Example** | This example display the LLDP statistics. |

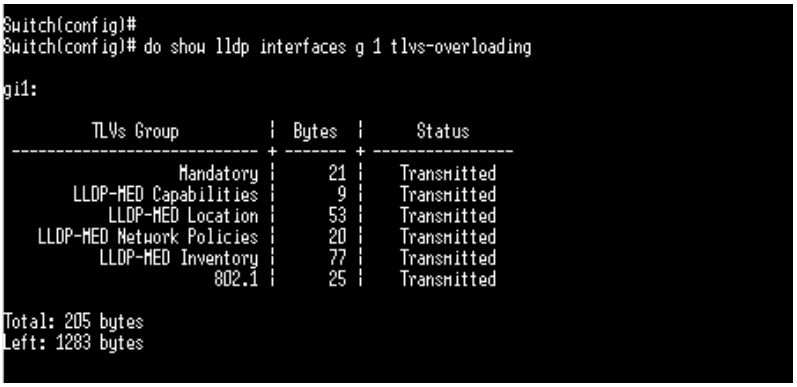
```
Switch# show lldp statistics
```

```
Switch(config)# do show lldp statistics

LLDP Global Statistics:
Insertions : 10
Deletions  : 5
Drops      : 0
Age Outs   : 1

       | TX Frames |        RX Frames          |         RX TLVs         | RX Ageouts
  Port |   Total   | Total | Discarded | Errors | Discarded | Unrecognized |   Total
-------+-----------+-------+-----------+--------+-----------+--------------+----------
   gi1 |         0 |     0 |         0 |      0 |         0 |            0 |         0
   gi2 |         0 |     0 |         0 |      0 |         0 |            0 |         0
   gi3 |         0 |     0 |         0 |      0 |         0 |            0 |         0
   gi4 |         0 |     0 |         0 |      0 |         0 |            0 |         0
   gi5 |         0 |     0 |         0 |      0 |         0 |            0 |         0
   gi6 |         0 |     0 |         0 |      0 |         0 |            0 |         0
   gi7 |         0 |     0 |         0 |      0 |         0 |            0 |         0
   gi8 |         0 |     0 |         0 |      0 |         0 |            0 |         0
   gi9 |         0 |     0 |         0 |      0 |         0 |            0 |         0
  gi10 |         0 |     0 |         0 |      0 |         0 |            0 |         0
  gi11 |         0 |     0 |         0 |      0 |         0 |            0 |         0
  gi12 |         0 |     0 |         0 |      0 |         0 |            0 |         0
  gi13 |         0 |     0 |         0 |      0 |         0 |            0 |         0
  gi14 |         0 |     0 |         0 |      0 |         0 |            0 |         0
  gi15 |         0 |     0 |         0 |      0 |         0 |            0 |         0
  gi16 |         0 |     0 |         0 |      0 |         0 |            0 |         0
  gi17 |         0 |     0 |         0 |      0 |         0 |            0 |         0
  gi18 |         0 |     0 |         0 |      0 |         0 |            0 |         0
  gi19 |         0 |     0 |         0 |      0 |         0 |            0 |         0
  gi20 |         0 |     0 |         0 |      0 |         0 |            0 |         0
  gi21 |         0 |     0 |         0 |      0 |         0 |            0 |         0
  gi22 |         0 |     0 |         0 |      0 |         0 |            0 |         0
  gi23 |         0 |     0 |         0 |      0 |         0 |            0 |         0
  gi24 |      1605 |   317 |         4 |      0 |         0 |            0 |         1
   te1 |         0 |     0 |         0 |      0 |         0 |            0 |         0
   te2 |         0 |     0 |         0 |      0 |         0 |            0 |         0
   te3 |         0 |     0 |         0 |      0 |         0 |            0 |         0
   te4 |         0 |     0 |         0 |      0 |         0 |            0 |         0
```

```
Switch# show lldp int g 1 statistics
```

```
Switch(config)# do show lldp interfaces g 1 statistics

LLDP Port Statistics:
       | TX Frames |        RX Frames          |         RX TLVs         | RX Ageouts
  Port |   Total   | Total | Discarded | Errors | Discarded | Unrecognized |   Total
-------+-----------+-------+-----------+--------+-----------+--------------+----------
   gi1 |         0 |     0 |         0 |      0 |         0 |            0 |         0
```

### 2.13.24 show lldp tlv-overloading

| | |
|---|---|
| **Syntax** | **show lldp interfaces** IF_NMLPORTS **tlvs-overloading** |
| **Parameter** | IF_NMLPORTS Specify the ports to display information |
| **Default** | There is no default configuration for this command |
| **Mode** | Privileged EXEC |
| **Usage** | The LLDP PDU is composed by TLVs and selected number TLVs may compose a large PDU that the system can not handle. The maximum PDU length is to take the smaller number of jumbo frame size minus 30 bytes (30 bytes kept for header) or 1488 bytes.<br><br>Use "**show lldp tlv-overloading**" command to display the length of LLDP TLVs and if the TLVs overload the PDU length. The TLVs with status marked "overload" would not be transmitted. |
| **Example** | **This example display the LLDP TLVs overloading status of port gi1.**<br>`Switch# show lldp interfaces gi1 tlvs-overloading`<br>  |

```
Switch(config)#
Switch(config)# do show lldp interfaces g 1 tlvs-overloading

gi1:

        TLVs Group          ¦  Bytes  ¦     Status
 ---------------------------+---------+---------------
                  Mandatory ¦     21 ¦   Transmitted
      LLDP-MED Capabilities ¦      9 ¦   Transmitted
          LLDP-MED Location ¦     53 ¦   Transmitted
   LLDP-MED Network Policies ¦     20 ¦   Transmitted
        LLDP-MED Inventory  ¦     77 ¦   Transmitted
                    802.1   ¦     25 ¦   Transmitted

Total: 205 bytes
Left: 1283 bytes
```

# 2.14 Logging

## 2.14.1 clear logging

| | |
|---|---|
| **Syntax** | **clear logging (buffered\|file)** |
| **Parameter** | **buffered** Clear the log messages stored in the RAM.<br>**file** Clear the log messages stored in the Flash. |
| **Default** | N/A |
| **Mode** | Privileged EXEC |
| **Usage** | To clear the log messages from the internal logging buffer and flash, use the command clear logging in the Privileged EXEC mode. |
| **Example** | **The following example clear the log messages stored in RAM and Flash.**<br>`Switch# clear logging buffered`<br>`Switch# clear logging file` |

## 2.14.2 logging

| | |
|---|---|
| **Syntax** | **logging / no logging** |
| **Parameter** | N/A |
| **Default** | Logging service is enabled. |
| **Mode** | Privileged EXEC |
| **Usage** | To enable logging service on the switch, use the command **logging** in the Global Configuration mode. Otherwise, use the **no** form of the command to disable the logging service on the switch.<br><br>The status of global logging server is available from the command **show logging** in the Privileged EXEC mode. When the logging service is enabled, logging on and off at each destination rule can be individually configured by the command **logging console, logging buffered, logging file**, and **logging host** in the Global Configuration mode. If the logging service is disabled, no messages will be sent to these destinations. |
| **Example** | The following example disables and enables the logging service on the switch.<br><br>`Switch(config)# no logging`<br>`Switch(config)# logging` |

### 2.14.3 logging host

**Syntax**

**logging host (**ip-addr|hostname**) [facility** facility**] [port** port**]**
**[severity** sev**]**
**no logging host (**ip-addr|hostname**)**

**Parameter**

| | |
|---|---|
| ipv4-addr | IPv4 address of the remote logging server. |
| hostname | Hostname of the remote logging server. |
| **facility** facility | Specify the facility of the logging messages. It can be on of the following value: local0, local1, local2, local3, local4, local5, local6, and local7. The default value of facility is local7. |
| **port** port | Specify the port number of the remote logging server.The valid range is from 0 to 65535, and the default value is 512. |
| **severity** sev | Specify the minimum severity of the logging messages. The valid range is from 0 to 7, and the number 0 to 7 represents emerg, alert, critical, error, warning, notice, info, and debug individually. The default value of minimum severity level is 5 (emerg, alert, crit, error, warning, notice). |

**Default**

No remote logging destination is configured.

**Mode**

Global Configuration

**Usage**

To define the logging server, use the command **logging host** to add the remote logging server in the Global Configuration mode. Otherwise, use the command **no logging host** to remove the remote logging rules.

For the host name configuration, logging service would try translating the host name to IP address directly. Add the logging host would be failed on the failure of host name translating.

**Example**

The following example adds the remote logging rules by IP and Hostname.

```
Switch(config)# logging host 1.2.3.4
Switch(config)# logging host SYSLOG
```

### 2.14.4 logging severity

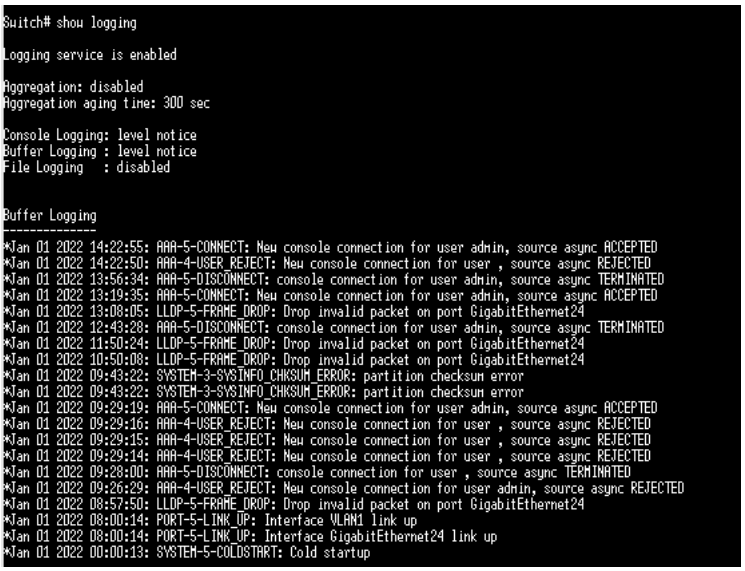
| | | |
|---|---|---|
| **Syntax** | **logging (buffered\|console\|file) [severity sev]**<br>**no logging (buffered\|console\|file)** | |
| **Parameter** | **Buffered** | Log Messages to RAM. |
| | **Console** | Log messages to console buffer. |
| | **file** | Log messages to Flash |
| | **severity** | Specify the minimum severity of the logging messages.The valid range is from 0 to 7, and the number 0 to 7 represents emerg, alert, critical, error, warning, notice, info, and debug individually. The default minimum severity of the logging severity configuration is 5 (emerg, alert, crit, error, warning, notice). |
| **Default** | Logging to buffered and console is enabled, and the default minimum severity level is 5 (emerg, alert, crit, error, warning, notice). | |
| **Mode** | Global Configuration | |
| **Usage** | To set the minimum severity for the messages that are logged to RAM, console, or Flash, use the command logging severity in the Global Configuration mode. Use the no form of the command to remove the mechanism of logging to RAM, console, or Flash individually. | |
| **Example** | The following example sets the minimum severity level of logging to RAM and Flash as debugging.<br>`Switch(config)# logging buffered 7`<br>`Switch(config)# logging flash 7` | |

## 2.14.5 show logging

| | |
|---|---|
| **Syntax** | **show logging [buffered\|file]** |
| **Parameter** | **Buffered** Display the log messages stored in the RAM.<br>**file** Display the log messages stored in the Flash. |
| **Default** | N/A |
| **Mode** | Previledged EXEC |
| **Usage** | To display the global logging configuration, and the logging messages stored in the RAM and Flash, use the command show logging in the Privileged EXEC mode. |

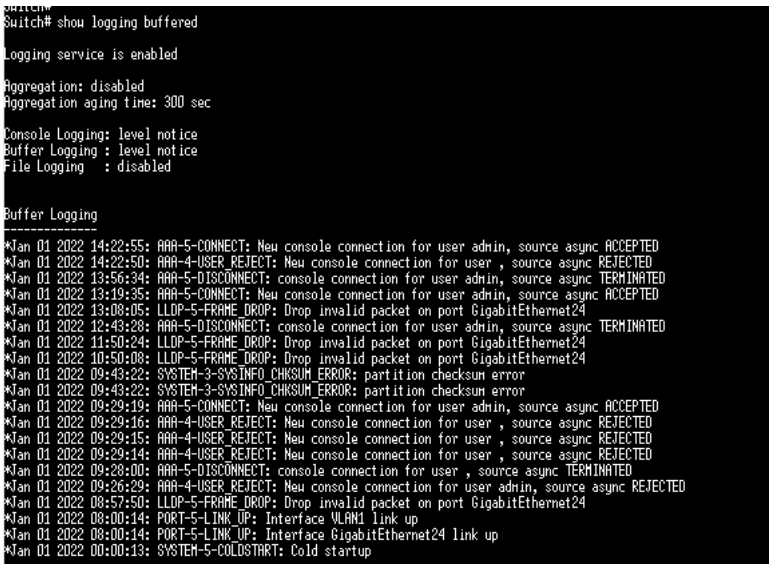
**Example** **The following example shows the global logging configuration.**

```
Switch# show logging
```




The following example shows the log messages stored in the RAM.

```
Switch# show logging buffered
```




## 2.15 MAC Address Table

### 2.15.1 clear mac address-table

| | | |
|---|---|---|
| **Syntax** | **clear mac address-table dynamic [interfaces** IF_PORTS**\|vlan** vlan-id**]** | |
| **Parameter** | **interfaces** IF_PORTS | Delete all dynamic addresses learned on the specific interface. |
| | **vlan** vlan-id | Delete all source addresses learned on the specific VLAN. |
| **Default** | N/A | |
| **Mode** | Privileged EXEC | |
| **Usage** | To clear the dynamic (learned) MAC entries from the MAC address table, the specific interface, or the specific VLAN, use the command clear mac address-table in the Priveleged EXEC mode. | |
| **Example** | The following example clears the learned MAC addresses on the interface gi1. | |

```
Switch# clear mac address-table dynamic interfaces gi1
```

### 2.15.2 mac address-table aging-time

| | | |
|---|---|---|
| **Syntax** | **mac accress-table aging-time** seconds | |
| **Parameter** | seconds | The time in seconds that an entry remains in the MAC address table. Its valid range is from 10 to 630 seconds,and the default value is 300 seconds. |
| **Default** | The default aging time is 300 seconds. | |
| **Mode** | Global Configuration | |
| **Usage** | To set the aging time of the MAC address table, use the command **mac address-table aging-time** in the Global Configuration mode. | |
| **Example** | The following example set the agimg time to 500 seconds.<br>`Switch(config)# mac address-table aging-time 500` | |

### 2.15.3 mac address-table static

| | | |
|---|---|---|
| **Syntax** | **mac address-table static** mac-addr **vlan** vlan-id **interfaces** IF_PORTS<br>**mac address-table static** mac-addr **vlan** vlan-id **drop**<br>**no mac address-table static** mac-addr **vlan** vlan-id | |
| **Parameter** | mac-addr | MAC address. |
| | **vlan** vlan-id | Specify the VLAN ID for the interface. |
| | **Interface** IF_PORTS | Specify the interface ID or a list of interface IDs. |
| | **drop** | Drop the packets with the specified source or destination unicast MAC address. |
| **Default** | No static addresses are configured | |
| **Mode** | Global Configuration | |
| **Usage** | To add a static address to the MAC address table, use the command **mac address-table static** in the Global Configuration mode. For the unicast MAC address filtering, use the command **mac address-table static** with parameter **drop** to drop the packets with the specified source or destination unist MAC address. To delete the static entry from the MAC address table, use the **no** form of the command. | |

**Example** The following example adds a static address into MAC address table.

```
Switch# mac address-table static 00:11:22:33:44:55 vlan
        1 interfaces g 5
```

The following example adds a rule of unist address filtering into MAC address table.

```
Switch# mac address-table static 00:11:22:33:44:55 vlan
        1 drop
```

### 2.15.4 show mac address-table

| | | |
|---|---|---|
| **Syntax** | **show mac address-table [dynamic\|static] [interface IF_PORTS] [vlan vlan-id] show mac address-table [mac-addr] [vlan vlan-id]** | |
| **Parameter** | dynamic | Display only dynamic MAC addresses |
| | static | Display only static MAC addresses |
| | **Interface** IF_PORTS | Display the MAC addresses entries for a specifc interface. |
| | **vlan** vlan-id | Display the MAC address entries for a specific VLAN. |
| | **mac-addr** | Display entries for a specific MAC address |
| **Default** | N/A | |
| **Mode** | Privileged EXEC | |
| **Usage** | To show the entry in the MAC address table, use the command show mac address-table in the Privilieged EXEC mode. | |

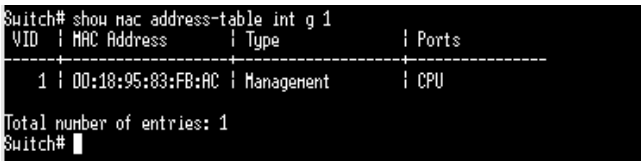
**Example** The following example displays the entire MAC addrss table.

```
Switch# show mac address-table
```

```
Switch# show mac address-table
 VID  | MAC Address       | Type           | Ports
------+-------------------+----------------+--------------
   1  | 00:08:AB:A9:FF:3F | Dynamic        | gi24
   1  | 00:18:95:83:FB:AC | Management     | CPU
   1  | 00:20:6B:66:5D:00 | Dynamic        | gi24
   1  | 00:E0:4C:36:01:AA | Dynamic        | gi24
   1  | 00:E0:4C:4B:E1:22 | Dynamic        | gi24
   1  | 08:26:AE:38:C2:8C | Dynamic        | gi24
   1  | 08:62:66:55:3D:3C | Dynamic        | gi24
   1  | 08:97:98:F3:77:26 | Dynamic        | gi24
   1  | 0E:44:32:3D:6D:3A | Dynamic        | gi24
   1  | 20:9B:E6:12:39:18 | Dynamic        | gi24
   1  | 28:8D:23:0B:68:7F | Dynamic        | gi24
   1  | 30:8D:99:15:A8:BA | Dynamic        | gi24
   1  | 34:29:8F:75:FF:24 | Dynamic        | gi24
   1  | 3C:2A:F4:D4:A4:C3 | Dynamic        | gi24
   1  | 3C:97:0E:B2:D9:DA | Dynamic        | gi24
   1  | 3C:A8:2A:86:9B:B1 | Dynamic        | gi24
   1  | 50:9A:4C:3E:CB:3F | Dynamic        | gi24
   1  | 50:E5:49:19:1D:87 | Dynamic        | gi24
   1  | 50:FA:84:CD:94:E9 | Dynamic        | gi24
   1  | 54:E1:AD:AB:63:E0 | Dynamic        | gi24
   1  | 5A:38:38:D0:D2:DF | Dynamic        | gi24
```

The following example displays the static MAC address configuration for the interface g 1.

```
Switch# show mac address-table static interfaces g 1
```




The following example displays address table entries containing the specified MAC address.

```
Switch# show mac address-table 00:11:22:33:44:55 vlan
```

### 2.15.5 show mac address-table counters

| | |
|---|---|
| **Syntax** | **show mac address-table counters** |
| **Parameter** | N/A |
| **Default** | N/A |
| **Mode** | **Privileged EXEC** |
| **Usage** | To display the total entries in the MAC addrss table, use the command show mac address-table counters in the Privilieged EXEC mode. |
| **Example** | The following example display numbers of addresses in the address table.<br><br>`Switch# show mac address-table counters` |

### 2.15.6 show mac address-table aging-time

| | |
|---|---|
| **Syntax** | **show mac address-table aging-time** |
| **Parameter** | **N/A** |
| **Default** | **N/A** |
| **Mode** | **Privileged EXEC** |
| **Usage** | To show MAC address aging time, use the command show mac address-table aging-time in the Privilieged EXEC mode. |
| **Example** | The following example displays aging time for the MAC address table.<br>`Switch# show mac address-table aging-time` |

## 2.16 MAC VLAN

### 2.16.1 vlan mac-vlan group(Global)

| | |
|---|---|
| **Syntax** | **vlan mac-vlan group** <1- 2147483647> **mac-address mask** <9-48><br>**no vlan mac-vlan group mac-address mask** <9-48> |
| **Parameter** | ***<1-2147483647>*** Specify the group ID<br>***Mac-address*** Specify the MAC address to be mapped.<br>***<9-48>*** Specify the mask length of MAC address. |
| **Default** | No MAC Groups are configured. |
| **Mode** | Global Configuration |
| **Usage** | Use the "**vlan mac-vlan group**" command to create MAC address group.<br>Use the **no** form of this command to delete specify group. |
| **Example** | The following example shows how to create a MAC group with group ID 3.<br>`Switch(config)# vlan mac-vlan group 333 22:33:44:55:66:77 mask 48` |

### 2.16.2 vlan mac-vlan group(Interface)

| | |
|---|---|
| **Syntax** | **vlan mac-vlan group** <1- 2147483647> **vlan** <1-4094><br>**no vlan mac-vlan [group** <1- 2147483647>**]** |
| **Parameter** | ***<1-2147483647>*** Specify the group ID. (optional in no form) Delete all mapping group if not specify.<br>***<1-4094>*** Specify the VLAN ID to give to match packet. |
| **Default** | No mappings are configured. |
| **Mode** | Interface Configuration |
| **Usage** | Use the "**vlan mac-vlan group**" to create mapping of group and VLAN ID of an interface. Use the **no** form of this command to delete mapping. |
| **Example** | The following example shows how to mapping group id 333 to VLAN 100 on interface g 1.<br>`Switch(config)# Interface g 1`<br>`Switch(config-if)# vlan mac-vlan group 333 VLAN 100` |

### 2.16.3 show vlan mac-vlan groups

| | |
|---|---|
| **Syntax** | **show vlan mac-vlan groups** |
| **Parameter** | N/A |
| **Default** | N/A |
| **Mode** | Privileged EXEC |
| **Usage** | Use the **show vlan mac-vlan groups** command to display mac groups configuration |
| **Example** | This following example shows how to display mac group.<br>`Switch# show vlan mac-vlan groups` |

### 2.16.4 show vlan mac-vlan interfaces

| | | |
|---|---|---|
| **Syntax** | **show vlan mac-vlan [interfaces** IF_PORTS**]** | |
| **Parameter** | IF_PORTS (Optional) | Specify interfaces mac vlan to display. Display all ports if not specify. |
| **Default** | N/A | |
| **Mode** | Privileged EXEC | |
| **Usage** | Use the show **vlan mac-vlan interface** command in EXEC mode to display the mac-vlan interfaces setting | |
| **Example** | The following example shows how to display the MAC-Based VLAN interfaces setting<br>`Switch# show vlan mac-vlan interfaces g 1` | |

## 2.17 Management ACL

### 2.17.1 management access-list

| | | |
|---|---|---|
| **Syntax** | **management access-list NAME**<br>**no management access-list NAME** | |
| **Parameter** | **NAME** | The name of management ACL |
| **Default** | No management ACL is configured. | |
| **Mode** | Global Configuration | |
| **Usage** | Use the management **access-list** command to create a management access list and to enter management access-list configuration mode. The name of ACL must be unique that cannot have same name with other management ACL. Use the no form of this command to delete | |
| **Example** | The following example shows how to add a management ACL with name “test”<br>`Switch(config)# management access-list test` | |

### 2.17.2 management access-class

| | |
|---|---|
| **Syntax** | **management access-class** NAME<br>**no management access-class** |
| **Parameter** | **NAME** The name of management ACL to be used |
| **Default** | Default is no management ACL restrictions |
| **Mode** | Global Configuration |
| **Usage** | Use the **management access-class** command to activate a management ACL. Use the no form of this command to delete |
| **Example** | The following example shows how to add a management ACL with name "test"<br>`Switch(config)# management access-list test` |

### 2.17.3 deny

| | |
|---|---|
| **Syntax** | **[sequence** <1-65535>**] deny interfaces** IF_PORTS **service (all\|http\|https\|snmp\|ssh\|telnet)**<br>**[sequence** <1-65535>**] deny ip** A.B.C.D/A.B.C.D **interfaces** IF_PORTS **service (all\|http\|https\|snmp\|ssh\|telnet)**<br>**[sequence** <1-65535>**] deny ipv6 X:X::X:X/<0-128> interfaces** IF_PORTS **service (all\|http\|https\|snmp\|ssh\|telnet)** |

**Parameter**

| | |
|---|---|
| ***<1-65535>*** | Optional) Specify sequence index of ACL entry, the sequence index represent the priority of an entry in ACL. If not specified, the switch assigns a number from 1 in ascending order. |
| **interfaces** IF_PORTS | Specify the interface ID or a list of interface IDs. |
| **ip** A.B.C.D/A.B.C.D | Specify the source IP address and mask of packet. |
| **ipv6** X:X::X:X/<0-128> | Specify the source IPv6 address and prefix length of packet. |
| **(all\|http\|https\|snmp\|ssh\|telnet)** | Specify the type of services. |

| | |
|---|---|
| **Default** | No rules are configured. |

| | |
|---|---|
| **Mode** | Management Access-List Configuration |
| **Usage** | Use the deny command to add deny rules that drop those packets hit the rule. |
| **Example** | The following example shows how to add a deny rule to drop all types of services packets that source ip is 1.1.1.1 from interface gi1.<br><br>`Switch(config)# management access-list test`<br>`Switch(config-macl)# sequence 1 deny ip 1.1.1.1/255.255.255.255 interfaces gi1 service all` |

### 2.17.4 permit

| | |
|---|---|
| **Syntax** | **[sequence** <1-65535>**] deny interfaces** IF_PORTS **service (all\|http\|https\|snmp\|ssh\|telnet)**<br>**[sequence** <1-65535>**] deny ip** A.B.C.D/A.B.C.D **interfaces** IF_PORTS **service (all\|http\|https\|snmp\|ssh\|telnet)**<br>**[sequence** <1-65535>**] deny ipv6 X:X::X:X/<0-128> interfaces** IF_PORTS**service (all\|http\|https\|snmp\|ssh\|telnet)** |

**Parameter**

| | |
|---|---|
| ***<1-65535>*** | (Optional) Specify sequence index of ACL entry, the sequence index represent the priority of an entry in ACL. If not specified, the switch assigns a number from 1 in ascending order. |
| **interfaces** IF_PORTS | Specify the interface ID or a list of interface IDs. |
| **ip** A.B.C.D/A.B.C.D | Specify the source IP address and mask of packet. |
| **ipv6** X:X::X:X/<0-128> | Specify the source IPv6 address and prefix length of packet. |
| **(all\|http\|https\|snmp\|ssh\|telnet)** | Specify the type of services. |

| | |
|---|---|
| **Default** | No rules are configured. |
| **Mode** | Management Access-List Configuration |
| **Usage** | Use the permit command to add deny rules that drop those packets hit the rule. |

**Example** The following example shows how to add a permit rule to bypass http service packets that source ip is 2.2.2.2 from interface gi1.

```
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
```

### 2.17.5 no sequence

| | |
|---|---|
| **Syntax** | **no sequence** <1-65535> |
| **Parameter** | <1-65535> Specify sequence index of ACL entry to delete. |
| **Default** | No rules are configured. |
| **Mode** | Management Access-List Configuration |
| **Usage** | Use the **no sequence** command to delete an entry in management ACL. |

**Example** The following example shows how to delete an entry.

```
Switch(config)# management access-list test
Switch(config-macl)# sequence 10 deny interfaces gi1
                      service all
Switch(config-macl)# no sequence 10
```

### 2.17.6 show management access-class

| | |
|---|---|
| **Syntax** | **show management access-class** |
| **Parameter** | N/A |
| **Default** | No default is defined |
| **Mode** | Privileged EXEC |
| **Usage** | Use the **show management access-class** command to show the active management access-list. |
| **Example** | The example shows how to show management access-class<br>`Switch# show management access-class` |

### 2.17.7 show management access-list

| | |
|---|---|
| **Syntax** | **show management access-list** [NAME] |
| **Parameter** | NAME Specify the name of management ACL to displayed |
| **Default** | No default is defined |
| **Mode** | Privileged EXEC |
| **Usage** | Use the show management access-list command to show management ACL. |
| **Example** | The example shows how to show management access-list<br>`Switch# show management access-list` |

## 2.18 Mirror

### 2.18.1 mirror session destination interface

| | |
|---|---|
| **Syntax** | **mirror session** <1-4> **destination interface** IF_NMLPORT **[allow-ingress]**<br>**no mirror session** <1-4> **destination interface** IF_NMLPORT<br>**no mirror session (**<1-4> **\| all)** |

**Parameter**

| | |
|---|---|
| *<1-4>* | Specify the mirror session to configure |
| *IF_NMLPORT* | Specify the SPAN destination. A destination must be a physical port |
| **allow-ingress** | Enable ingress traffic forwarding. |

**Default** No monitor sessions are configured.

**Mode** Global Configuration

**Usage** Use the **"mirror session destination interface**" command to start a destination interface of a port mirror session.

Use the **no** form of this command to stop a destination interface of a port mirroring session.

Use the "**no mirror session**" command to disable all mirror sessions or specific mirror session.

**Example** The following example shows how to create a local session 1 to monitor both sent and received traffic on source port g 1.

```
Switch(config)# mirror session 1 destination interface
                g 1
Switch# show mirror session 1 Session 1 Configuration
Source RX
```

## 2.18.2 mirror session source interface

| | |
|---|---|
| **Syntax** | **mirror session <1-4> source interfaces IF_PORTS (both \| rx \| tx)**<br>**no mirror session <1-4> source interfaces IF_PORTS (both \| rx \| tx)**<br>**no mirror session (<1-4> \| all)** |

**Parameter**

| | |
|---|---|
| *<1-4>* | Specify the mirror session to configure |
| *IF_PORTS* | Specify the source interface, Valid interfaces include physical ports and port channels. |
| **both** | Mirror tx and rx direction |
| **rx** | Mirror rx direction only |
| **tx** | Mirror tx direction only |

**Default** No monitor sessions are configured.

**Mode** Global Configuration

**Usage**

Use the "**mirror session source interface**" command to start a port mirror session.

Use the **no** form of this command to stop a port mirroring session.

Use the "**no mirror session**" command to disable all mirror sessions or specific mirror session.

**Example**

The following example shows how to create a local SPAN session 1 to monitor both sent and received traffic on source port fa1.

```
Switch(config)# mirror session 1 source interface g 2-5 both Switch(config)# mirror session 1 destination interface fa1 Switch(config)# show mirror session 1
```

```
Switch(config)# mirror session 1 source interfaces g 2-5 both
Switch(config)# mirror session 1 destination interface g 1
Switch(config)# do show mirror session 1

Session 1 Configuration
Source RX Port    : gi2-5
Source TX Port    : gi2-5
Destination port  : gi1
Ingress State: disabled
```

### 2.18.3 show mirror

| | |
|---|---|
| **Syntax** | **show mirror [session <1-4>]** |
| **Parameter** | <1-4> Specify the mirror session to display |
| **Default** | N/A |
| **Mode** | Privileged EXEC |
| **Usage** | Use the show mirror command to display mirror session configuration |
| **Example** | This following example shows how to display mirror session configuration<br>`Switch(config)# show mirror` |

## 2.19 MLD Snooping

### 2.19.1 Ipv6 mld snooping

| | |
|---|---|
| **Syntax** | **ipv6 mld / snooping no ipv6 / mld snooping** |
| **Parameter** | N/A |
| **Default** | Default is disabled |
| **Mode** | Global Configuration |
| **Usage** | Use the **ipv6 mld snooping** command to enable MLD snooping function. Use the **no** form of this command to disable. Disable will clear all ipv6 mld snooping dynamic group and dynamic router port, and make the static ipv6 mld group invalid. No more dynamic group and router port by mld message will be learned.<br>You can verify settings by the **show ipv6 mld snooping** command. |
| **Example** | The following example specifies that set ipv6 mld snooping test.<br>`Switch(config)# ipv6 mld snooping` |

### 2.19.2 ipv6 mld snooping report-suppression

| | |
|---|---|
| **Syntax** | **ipv6 mld snooping report-suppression**<br>**no ipv6 mld snooping report-suppression** |
| **Parameter** | N/A |
| **Default** | Default is enabled |
| **Mode** | Global Configuration |
| **Usage** | Use the **ipv6 mld snooping** command to enable MLD snooping function. Use the **no** form of this command to disable. Disable will clear all ipv6 mld snooping dynamic group and dynamic router port, and make the static ipv6 mld group invalid. No more dynamic group and router port by mld message will be learned.<br>You can verify settings by the **show ipv6 mld snooping** command. |
| **Example** | The following example specifies that disable ipv6 mld snooping report-suppression test.<br>`Switch(config)# no ipv6 mld snooping report-suppression` |

### 2.19.3 ipv6 mld snooping version

| | |
|---|---|
| **Syntax** | **ipv6 mld snooping version (1\|2)** |
| **Parameter** | (1\|2) Ipv6 mld snooping running version 1 or 2 |
| **Default** | Default is version 1 |
| **Mode** | Global Configuration |
| **Usage** | Use the **ipv6 mld snooping version** command to change MLD support version. Version 2 packet won't be processed if choose version 1.<br>You can verify settings by the **show ip igmp snooping** command. |

**Example** The following example specifies that disable ipv6 mld snooping report-suppression test.

Switch(config)# **no ipv6 mld snooping report-suppression**

### 2.19.4 ipv6 mld snooping unknown-multicast action

| | |
|---|---|
| **Syntax** | **ipv6 mld snooping unknown-multicast action (drop \| flood \|router-port)**<br>**no ipv6 mld snooping unknown-multicast action** |
| **Parameter** | (drop \| flood \| router- port) Drop、flood in vlan or forward to router port of unknown multicast packet |
| **Default** | Default is flood. |
| **Mode** | Global Configuration |
| **Usage** | When igmp and mld snooping disabled, it can't set action router-port. When disable igmp snooping & mld snooping, it set unknown multicast action flood. When action is router-port to flood or drop, it will delete the unknown multicast group entry.<br><br>Use the **ipv6 mld snooping unknown-multicast action** command to change action.<br>Use the **no** form of this command to restore to default.<br>You can verify settings by the **show ipv6 mld snooping** command. |
| **Example** | The following example specifies that set ipv6 mld unknown multicast action router-port test.<br>`Switch(config)# ipv6 mld snooping unknown-multicast action router-port` |

### 2.19.5 ipv6 mld snooping vlan

| | |
|---|---|
| **Syntax** | **ipv6 mld snooping vlan VLAN-LIST**<br>**no ipv6 mld snooping vlan VLAN-LIST** |
| **Parameter** | VLAN-LIST specifies VLAN ID list to set |
| **Default** | Default is disabled for all VLANs |
| **Mode** | Global Configuration |
| **Usage** | Disable will clear all ipv6 mld snooping dynamic group and dynamic router port and make all static ip igmp group invalid of this vlan. Will not learn dynamic group and router port by igmp message any more.<br>Use the **ipv6 mld snooping vlan** command to enable MLD on VLAN.<br>Use the no form of this command to disable<br>You can verify settings by the **show ipv6 mld snooping vlan** command. |
| **Example** | The following example specifies that set ipv6 mld snooping vlan test.<br>`Switch(config)# ipv6 mld snooping vlan 1` |

## 2.19.6 ipv6 mld snooping vlan parameters

**Syntax**

**ipv6 mld snooping vlan <VLAN-LIST> last-member-query-count <1-7>**
**no ipv6 mld snooping vlan <VLAN-LIST> last-member-query-count**
**ipv6 mld snooping vlan <VLAN-LIST> last-member-query-interval <1-60>**
**no ipv6 mld snooping vlan <VLAN-LIST> last-member-query-interval**
**[no] ipv6 mld snooping vlan <VLAN-LIST> router learn pim-dvmrp**
**[no] ipv6 mld snooping vlan <VLAN-LIST> fastleave**
**ipv6 mld snooping vlan <VLAN-LIST> query-interval <30-18000>**
**no ipv6 mld snooping vlan <VLAN-LIST> query-interval**
**ipv6 mld snooping vlan <VLAN-LIST> response-time <5-20>**
**no ipv6 mld snooping vlan <VLAN-LIST> response-time**
**ipv6 mld snooping vlan <VLAN-LIST> robustness-variable <1-7>**
**no ipv6 mld snooping vlan <VLAN-LIST> robustness-variable**

**Parameter**

| | |
|---|---|
| ***VLAN-LIST*** | specifies VLAN ID list to set |
| ***last-member-query- count <1-7>*** | specifies last member query count to set. Default is 2 |
| **last-member-query- interval <1-60>** | specifies last member query interval to set. Default is 1 |
| **query-interval <30-18000>** | specifies query interval to set. Default is125 |
| **response-time <5-20>** | specifies a response time to set. default is 10 |
| **robustness-variable <1-7>** | specifies a robustness value to set, default is 2 |

**Default**

**no ipv6 mld snooping vlan 1-4094 last-member-query-count no ipv6 mld snooping vlan 1-4094 last-member-query-interval ipv6 mld snooping vlan 1-4094 router learn pim-dvmrp**
**no ipv6 mld snooping vlan 1-4094 fastleave**
**no ipv6 mld snooping vlan 1-4094 query-interval no ipv6 mld snooping vlan 1-4094 response-time**
**no ipv6 mld snooping vlan 1-4094 robustness-variable**

**Mode**

Global Configuration

**Usage**

'no ipv6 mld snooping vlan 1 (last-member-query-count | last-member-query- interval | query-interval | response-time | robustness-variable)' will set the vlan parameters to default. The cli setting will change the ipv6 mld vlan parameters admin settings. The configure can use 'show ipv6 mld snooping vlan 1'.

**Example**

The following example specifies that set ipv6 mld snooping vlan parameters test.

```
Switch(config)# ipv6 mld snooping vlan 1 fastleave
Switch(config)# ipv6 mld snooping vlan 1 last-member-
                query-count 5
Switch(config)# ipv6 mld snooping vlan 1 last-member-
                query-interval 3
Switch(config)# ipv6 mld snooping vlan 1 query-interval
```

```
                    100
Switch(config)# ipv6 mld snooping vlan 1 response-time 12
Switch(config)# ipv6 mld snooping vlan 1 robustness-
                 variable 4
Switch# show ipv6 mld snooping vlan 1
```


### 2.19.7 ipv6 mld snooping vlan fastleave

| | |
|---|---|
| **Syntax** | **ipv6 mld snooping vlan <VLAN-LIST> fastleave**<br>**no ipv6 mld snooping vlan <VLAN-LIST> fastleave** |
| **Parameter** | VLAN-LIST specifies VLAN ID list to set |
| **Default** | Default is disabled |
| **Mode** | Global Configuration |
| **Usage** | Use the ipv6 mld snooping vlan fastleave command to enable fastleave function. Group will remove port immediately when receive leave packet. Use the no form of this command to disable.<br>You can verify settings by the show ipv6 mld snooping vlan command |
| **Example** | **The following example specifies that set ipv6 mld snooping vlan fastleave test.**<br>`Switch(config)# ipv6 mld snooping vlan 1 fastleave` |

### 2.19.8 ipv6 mld snooping vlan last-member-query-count

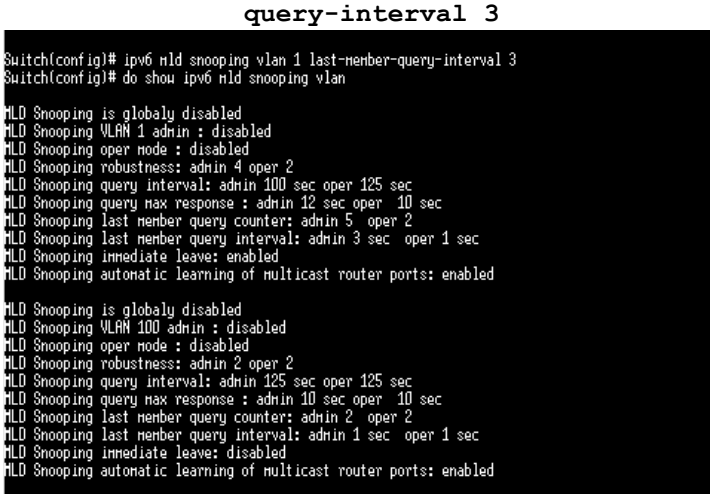
| | |
|---|---|
| **Syntax** | **ipv6 mld snooping vlan <VLAN-LIST> last-member-query-count <1-7>**<br>**no ipv6 mld snooping vlan <VLAN-LIST> last-member-query-count** |
| **Parameter** | ***VLAN-LIST*** specifies VLAN ID list to set<br>***last-member-query- count <1-7>*** specifies last member query count to set |
| **Default** | Default is 2 |
| **Mode** | Global Configuration |
| **Usage** | Use the ipv6 mld snooping vlan last-member-query-count command to change how many query packets will send.<br>Use the no form of this command to restore to default.<br>You can verify settings by the show ipv6 mld snooping vlan command |
| **Example** | The following example specifies that set ipv6 mld snooping vlan last-member-query-count test.<br>`Switch(config)# ipv6 mld snooping vlan 1 last-member-query-count 5` |

### 2.19.9 ipv6 mld snooping vlan last-member-query-interval

| | |
|---|---|
| **Syntax** | **ipv6 mld snooping vlan <VLAN-LIST> last-member-query-interval <1- 60>**<br>**no ipv6 mld snooping vlan <VLAN-LIST> last-member-query-interval** |
| **Parameter** | ***VLAN-LIST*** specifies VLAN ID list to set<br>***last-member-query- interval <1-60>*** specifies last member query interval to set |
| **Default** | Default is 1 |
| **Mode** | Global Configuration |
| **Usage** | Use the **ipv6 mld snooping vlan last-member-query-interval** command to set interval between each query packet.<br>Use the no form of this command to restore to default<br>You can verify settings by the **show ipv6 mld snooping vlan** command |
| **Example** | The following example specifies that set ipv6 mld snooping vlan last- |

member-query-interval test.

```
Switch(config)# ipv6 mld snooping vlan 1 last-member-query-interval 3
```




### 2.19.10 ipv6 mld snooping vlan query-interval

| | |
|---|---|
| **Syntax** | **ipv6 mld snooping vlan <VLAN-LIST> query-interval <30-18000>**<br>**no ipv6 mld snooping vlan <VLAN-LIST> query-interval** |
| **Parameter** | ***VLAN-LIST*** specifies VLAN ID list to set<br>***query-interval <30-18000>*** specifies query interval to set |
| **Default** | Default is 125 |
| **Mode** | Global Configuration |
| **Usage** | Use the **ipv6 mld snooping vlan query-interval** command to set interval between each query.<br>Use the **no** form of this command to restore to default<br>You can verify settings by the **show ipv6 mld snooping vlan** command |
| **Example** | The following example specifies that set ipv6 mld snooping vlan query-interval test.<br>`Switch(config)# ipv6 mld snooping vlan 1 query-interval 100` |

### 2.19.11 ipv6 mld snooping vlan response-time

| | |
|---|---|
| **Syntax** | **ipv6 mld snooping vlan <VLAN-LIST> response-time <5-20>**<br>**no ipv6 mld snooping vlan <VLAN-LIST> response-time** |
| **Parameter** | ***VLAN-LIST*** specifies VLAN ID list to set<br>***Response-time <5-20>*** specifies a response time to set |
| **Default** | Default is 10 |
| **Mode** | Global Configuration |
| **Usage** | Use the ipv6 mld snooping vlan response-time command to set response time.<br>Use the no form of this command to restore to default.<br>You can verify settings by the show ipv6 mld snooping vlan command |
| **Example** | The following example specifies that set ipv6 mld snooping vlan response- time test.<br>`Switch(config)# ipv6 mld snooping vlan 1 response-time 12` |

### 2.19.12 ipv6 mld snooping vlan robustness-variable

| | |
|---|---|
| **Syntax** | **ipv6 mld snooping vlan <VLAN-LIST> robustness-variable <1-7>**<br>**no ipv6 mld snooping vlan <VLAN-LIST> robustness-variable** |
| **Parameter** | ***VLAN-LIST*** specifies VLAN ID list to set<br>***robustness-variable <1-7>*** specifies a robustness value to set |
| **Default** | Default is 2 |
| **Mode** | Global Configuration |
| **Usage** | Use the **ipv6 mld snooping vlan robustness-variable** command to times to retry.<br>Use the no form of this command to restore to default<br>You can verify settings by the **show ipv6 mld snooping vlan** command |
| **Example** | The following example specifies that set ipv6 mld snooping vlan parameters test.<br>`Switch(config)# ip igmp snooping vlan 1 robustness-variable` |

### 2.19.13 ipv6 mld snooping vlan router

| | |
|---|---|
| **Syntax** | **ipv6 mld snooping vlan VLAN-LIST router learn pim-dvmrp**<br>**no ipv6 mld snooping vlan VLAN-LIST router learn pim-dvmrp** |
| **Parameter** | ***VLAN-LIST*** specifies VLAN ID list to set |
| **Default** | Default is enabled |
| **Mode** | Global Configuration |
| **Usage** | Use the **ipv6 mld snooping vlan router** command to enable learning router port by routing protocol packets such as PIM/PIMv2, DVMRP, MOSPF. Use the **no** form of this command to disable.<br>You can verify settings by the **show ipv6 mld snooping vlan** command |
| **Example** | The following example specifies that set ipv6 mld snooping vlan router test.<br>`Switch(config)# ipv6 mld snooping vlan 99 router` |

### 2.19.14 ipv6 mld snooping vlan static-port

| | |
|---|---|
| **Syntax** | **ipv6 mld snooping vlan <VLAN-LIST> static-port IF_PORTS**<br>**no ipv6 mld snooping vlan <VLAN-LIST> static-port IF_PORTS** |
| **Parameter** | *VLAN-LIST* specifies VLAN ID list to set<br>*IF_PORTS* specifies a port list to set or remove |
| **Default** | No static port by default |
| **Mode** | Global Configuration |
| **Usage** | Use the ipv6 mld snooping vlan static-port command to add static forwarding port, all known vlan 1 ipv6 group will add the static ports. Use the no form of this command to delete static port.<br>You can verify settings by the show ipv6 mld snooping forward-all command. |
| **Example** | The following example specifies that set ipv6 mld snooping static port test.<br>`Switch(config)# ipv6 mld snooping vlan 1 static-port g 1-2` |

### 2.19.15 ipv6 mld snooping vlan forbidden-router-port

| | |
|---|---|
| **Syntax** | **ipv6 mld snooping vlan <VLAN-LIST> forbidden-router-port IF_PORTS**<br>**no ipv6 mld snooping vlan <VLAN-LIST> forbidden-router-port IF_PORTS** |
| **Parameter** | *VLAN-LIST* specifies VLAN ID list to set<br>*IF_PORTS* specifies a port list to set or remove |
| **Default** | No forbidden router ports by default |
| **Mode** | Global Configuration |
| **Usage** | Use the ipv6 mld snooping vlan forbidden-router-port command to add static forbidden router port. This will also remove port from static router port. The forbidden router port will not forward received query packet.<br>Use the no form of this command to delete forbidden router port.<br>You can verify settings by the show ipv6 mld snooping router command. |
| **Example** | The following example specifies that set ipv6 mld snooping forbidden test.<br>`Switch(config)# ipv6 mld snooping vlan 1 forbidden router-port gi2` |

### 2.19.16 ipv6 mld snooping vlan static router port

| | |
|---|---|
| **Syntax** | **ipv6 mld snooping vlan <VLAN-LIST> static-router-port IF_PORTS**<br>**no ipv6 mld snooping vlan <VLAN-LIST> static-router-port IF_PORTS** |
| **Parameter** | *VLAN-LIST* specifies VLAN ID list to set<br>*IF_PORTS* specifies a port list to set or remove |
| **Default** | None static router ports by default |
| **Mode** | Global Configuration |
| **Usage** | Use the **ipv6 mld snooping vlan static-router-port** command to add static router port. All query packets will forward to this port.<br>Use the **no** form of this command to delete static router port.<br>You can verify settings by the show ipv6 mld snooping router command. |
| **Example** | The following example specifies that set ipv6 mld snooping static test.<br>`Switch(config)# ipv6 mld snooping vlan 1 static-router-port gi1-2` |

### 2.19.17 ipv6 mld snooping vlan static-group

| | |
|---|---|
| **Syntax** | **ipv6 mld snooping vlan <VLAN-LIST> static-group [<ipv6-addr>] interfaces IF_PORTS**<br>**no ipv6 mld snooping vlan <VLAN-LIST> static-group <ipv6-addr> interfaces IF_PORTS** |
| **Parameter** | *VLAN-LIST* — specifies VLAN ID list to set<br>*Ipv6-addr* — specifies multicast group ipv6 address<br>*IF_PORTS* — specifies port list to set or remove |
| **Default** | No static group by default |
| **Mode** | Global Configuration |
| **Usage** | Use the ipv6 mld snooping vlan static-group command to add a static group. The static group will not learn other dynamic ports. If the dynamic group exists, then the static group will overlap the dynamic group. The static group set to valid unless igmp snooping global and vlan enable.<br><br>Use the no form of this command to delete a port in static group. If remove the last member of static group, the static group will be delete.<br><br>You can verify settings by the show ipv6 mld snooping group command. |
| **Example** | The following example specifies that set ipv6 mld snooping static group test.<br>`Switch(config)# ipv6 mld snooping vlan 1 static-group ff13::1 interfaces gi1-2` |

### 2.19.18 ipv6 mld snooping vlan group

| | |
|---|---|
| **Syntax** | **no ipv6 mld snooping vlan <VLAN-LIST> group <ipv6-addr>** |
| **Parameter** | *VLAN-LIST* — specifies VLAN ID list to set<br>*Ipv6-addr* — specifies multicast group ipv6 address |
| **Default** | None |
| **Mode** | Global Configuration |
| **Usage** | Use the **no ipv6 mld snooping vlan group** command to delete a group which could be static or dynamic.<br>You can verify settings by the show **ipv6 mld snooping group** command. |
| **Example** | The following example specifies that set ip igmp snooping static group test.<br>`Switch(config)# no ip igmp snooping vlan 1 group ff13::1` |

### 2.19.19 profile range

| | | |
|---|---|---|
| **Syntax** | **profile range ipv6 <ipv6-addr> [ipv6-addr] action (permit \| deny)** | |
| **Parameter** | *<ipv6-addr>* | Start ipv6 multicast address |
| | *[ipv6-addr]* | End ipv6 multicast address |
| | *(permit \| deny)* | Permit: allow Multicast address range ip address learning<br>deny: do not allow Multicast address range ip address learning |
| **Default** | None | |
| **Mode** | mld profile configuration mode | |
| **Usage** | Use the profile command to generate MLD profile.<br>You can verify settings by the show ipv6 mld profile command | |
| **Example** | The following example specifies that set ipv6 mld profile test.<br>`Switch(config)# ipv6 mld profile 1`<br>`Switch(config-mld-profile)# profile range ipv6 ff13::1 ff13::10 action permit` | |

### 2.19.20 ipv6 mld profile

| | | |
|---|---|---|
| **Syntax** | **ipv6 mld profile <1-128> / no ipv6 mld profile <1-128>** | |
| **Parameter** | *<1-128>* | specifies profile ID |
| **Default** | No profie exist by default | |
| **Mode** | Global Configuration | |
| **Usage** | Use the **ipv6 mld profile** command to enter profile configuration Use the no form of this command to delete profile<br>You can verify settings by the **show ipv6 mld profile** command | |
| **Example** | The following example specifies that set ipv6 mld profile test.<br>`Switch(config)# ipv6 mld profile 1`<br>`Switch(config-mld-profile)# profile range ipv6 ff13::1 ff13::10 action permit` | |

### 2.19.21 ipv6 mld filter

| | |
|---|---|
| **Syntax** | **ipv6 mld filter <1-128> / no ipv6 mld filter** |
| **Parameter** | *<1-128>* specifies profile ID<br>*[interfaces IF_PORTS]* specifies interfaces to display |
| **Default** | None |
| **Mode** | Port Configuration |
| **Usage** | Use the ipv6 mld filter command to bind a profile for port. When the port bind a profile. Then the port learning group will update, if the group is not match the profile rule it will remove the port from the group. Static group is excluded.<br>Use the no form of this command to delete profile<br>You can verify settings by the show ipv6 mld filter command |
| **Example** | The following example specifies that set ipv6 mld filter test.<br>`Switch(config)# interface gi1`<br>`Switch(config-if)# ipv6 mld filter 1` |

### 2.19.22 ipv6 mld max-groups

| | |
|---|---|
| **Syntax** | **ipv6 mld max-groups <0-1024> / no ipv6 mld max-groups** |
| **Parameter** | *<1-128>* specifies profile ID |
| **Default** | Default is 1024 |
| **Mode** | Port Configuration |
| **Usage** | Use the **ipv6 mld max-groups** command to limit port learning max group number. When the port has reach limitation, new group will not add this port. Static group is excluded.<br>Use the **no** form of this command to restore to default<br>You can verify settings by the **show ipv6 mld max-groups** command. |
| **Example** | The following example specifies that set ipv6 mld max-groups test.<br>`Switch(config)# interface gi1`<br>`Switch(config-if)# ipv6 mld max-groups 10` |

### 2.19.23 ip igmp max-groups action

| | |
|---|---|
| **Syntax** | **ipv6 mld max-groups action (deny \| replace)** |
| **Parameter** | (deny \| replace) — Deny: current port igmp group arrived max-groups,don't add group. Replace: current port igmp group arrived max-groups,remove port for rand group, and add port to new group. |
| **Default** | Default action is deny |
| **Mode** | Interface mode |
| **Usage** | Use the **ipv6 mld max-groups action** command to set the action when the numbers of groups reach the limitation.<br>Use the **no** form of this command to restore to default<br>You can verify settings by the **show ipv6 mld max-groups** command. |
| **Example** | The following example specifies that set action replace test.<br>`Switch(config-if)#ipv6 mld max-groups action replace` |

### 2.19.24 clear ipv6 mld snooping groups

| | |
|---|---|
| **Syntax** | **clear ipv6 mld snooping groups [(dynamic \| static)]** |
| **Parameter** | None — Clear ipv6 mld groups include dynamic and static<br>(dynamic \| static) — ipv6 mld group type is dynamic or static |
| **Default** | None |
| **Mode** | Privileged EXEC |
| **Usage** | This command will **clear the ipv6 mld groups** for dynamic or static or all of type.<br>You can verify settings by the **show ipv6 mld snooping groups** command. |
| **Example** | The following example specifies that clear ipv6 mld snooping groups test.<br>`Switch# clear ipv6 mld snooping groups static` |

### 2.19.25 clear ipv6 mld snooping statistics

| | |
|---|---|
| **Syntax** | **clear ipv6 mld snooping statistics** |
| **Parameter** | None |
| **Default** | None |
| **Mode** | Privileged EXEC |
| **Usage** | This command will clear the igmp statistics.<br>You can verify settings by the **show ipv6 mld snooping** command. |
| **Example** | The following example specifies that clear ipv6 mld snooping statistics test.<br>`Switch# clear ipv6 mld snooping statistics` |

### 2.19.26 show ipv6 mld snooping groups counters

| | |
|---|---|
| **Syntax** | **show ipv6 mld snooping groups counters** |
| **Parameter** | None |
| **Default** | None |
| **Mode** | Privileged EXEC |
| **Usage** | This command will display the ipv6 mld group counter include static group. |
| **Example** | The following example specifies that display ipv6 mld snooping group counter test.<br>`Switch# show ipv6 mld snooping group counters` |

### 2.19.27 show ipv6 mld snooping groups

| | | |
|---|---|---|
| **Syntax** | **show ipv6 mld snooping groups [(dynamic \| static)]** | |
| **Parameter** | **None** | **Show ipv6 mld groups include dynamic and static** |
| | **(dynamic \| static)** | **Display ipv6 mld group type is dynamic or static** |
| **Default** | display all ipv6 mld groups | |
| **Mode** | Privileged EXEC | |
| **Usage** | This command will display the ipv6 mld groups for dynamic or static or all of type. | |
| **Example** | The following example specifies that show ipv6 mld snooping groups test.<br>`Switch# show ipv6 mld snooping groups` | |

### 2.19.28 show ipv6 mld snooping router

| | | |
|---|---|---|
| **Syntax** | **show ipv6 mld snooping router [(dynamic \| forbidden \|static )]** | |
| **Parameter** | **None** | **Show ipv6 mld groups include dynamic and static** |
| | **(dynamic \| forbidden \| static)** | **Display ipv6 mld router info for different type** |
| **Default** | None | |
| **Mode** | Privileged EXEC | |
| **Usage** | This command will display the ipv6 mld router info. | |
| **Example** | The following example specifies that show ipv6 mld snooping router test.<br>`Switch# show ipv6 mld snooping router` | |

## 2.19.29 show ipv6 mld snooping

| | |
|---|---|
| **Syntax** | **show ipv6 mld snooping** |
| **Parameter** | None |
| **Default** | None |
| **Mode** | Privileged EXEC |
| **Usage** | This command will display ipv6 mld snooping global info. |
| **Example** | The following example specifies that show ipv6 mld snooping test. |

```
Switch# show ipv6 mld snooping
```

```
Switch# show ipv6 mld snooping

              MLD Snooping Status
              -------------------

   Snooping                        : Disabled
   Report Suppression              : Enabled
   Operation Version               : v1
   Forward Method                  : mac
   Unknown IPv6 Multicast Action   : Flood


              Packet Statistics
   Total RX                        : 0
   Valid RX                        : 0
   Invalid RX                      : 0
   Other RX                        : 0
   Leave RX                        : 0
   Report RX                       : 0
   General Query RX                : 0
   Specail Group Query RX          : 0
   Specail Group & Source Query RX : 0
   Leave TX                        : 0
   Report TX                       : 0
   General Query TX                : 0
   Specail Group Query TX          : 0
   Specail Group & Source Query TX : 0
Switch#
```

### 2.19.30 show ipv6 mld snooping vlan

| | |
|---|---|
| **Syntax** | **show ipv6 mld snooping vlan [VLAN-LIST]** |

| **Parameter** | | |
|---|---|---|
| | **None** | Show all ipv6 mld snooping vlan info |
| | **[VLAN-LIST]** | Show specifies vlan ipv6 mld snooping info |

| | |
|---|---|
| **Default** | Show all ipv6 mld snooping vlan info |
| **Mode** | Privileged EXEC |
| **Usage** | This command will display ipv6 mld snooping vlan info. |

**Example** The following example specifies that show ipv6 mld snooping test.

```
Switch# show ipv6 mld snooping vlan 1
```

```
Switch# show ipv6 mld snooping vlan 1

MLD Snooping is globaly disabled
MLD Snooping VLAN 1 admin : disabled
MLD Snooping oper 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  oper 2
MLD Snooping last member query interval: admin 1 sec  oper 1 sec
MLD Snooping immediate leave: disabled
MLD Snooping automatic learning of multicast router ports: enabled
```

### 2.19.31 show ipv6 snooping forward-all

| | |
|---|---|
| **Syntax** | **show ipv6 mld snooping forward-all [vlan VLAN-LIST]** |

| **Parameter** | | |
|---|---|---|
| | **None** | Show all ipv6 mld snooping vlan forward-all info |
| | **[VLAN-LIST]** | Show specifies vlan of ipv6 mld forward info. |

| | |
|---|---|
| **Default** | Show all vlan ipv6 mld forward all info |
| **Mode** | Privileged EXEC |
| **Usage** | This command will display ipv6 mld snooping forward all info. |

**Example** The following example specifies that show ipv6 mld snooping forward-all test.

```
Switch# show ipv6 mld snooping forward-all
```

```
Switch# show ipv6 mld snooping forward-all

MLD Snooping VLAN          : 1
MLD Snooping static port   : None
MLD Snooping forbidden port : None
```

### 2.19.32 show ipv6 mld profile

| | | |
|---|---|---|
| **Syntax** | **show ipv6 mld profile [<1-128>]** | |
| **Parameter** | **None** | Show all ipv6 mld snooping profile info |
| | **[<1-128>]** | Show specifies index profile info |
| **Default** | Show all ipv6 mld profile info | |
| **Mode** | Privileged EXEC | |
| **Usage** | This command will display ipv6 mld profile info. | |
| **Example** | The following example specifies that show ipv6 mld profile test.<br>`Switch# show ipv6 mld profile` | |

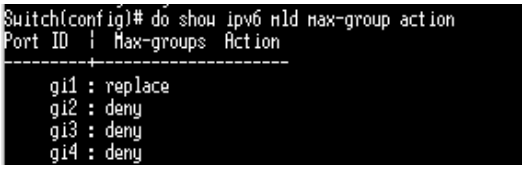
### 2.19.33 show ipv6 mld filter

| | | |
|---|---|---|
| **Syntax** | **show ipv6 mld filter [interfaces IF_PORTS]** | |
| **Parameter** | **None** | Show all port filter |
| | **[interfaces IF_PORTS]** | Show specifies ports filter |
| **Default** | None | |
| **Mode** | Privileged EXEC | |
| **Usage** | This command will display ipv6 mld port filter info. | |
| **Example** | The following example specifies that show ipv6 mld filter test.<br>`Switch# show ipv6 mld filter` | |

### 2.19.34 show ipv6 mld max-group

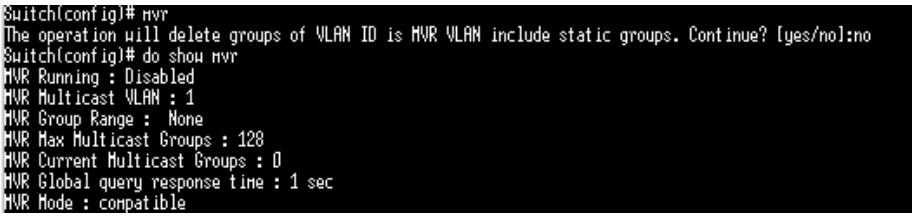
| | | |
|---|---|---|
| **Syntax** | **show ipv6 mld max-group [interfaces IF_PORTS]** | |
| **Parameter** | **None** | Show all port max-group |
| | **[interfaces IF_PORTS]** | Show specifies ports max-group |
| **Default** | None | |
| **Mode** | Privileged EXEC | |
| **Usage** | This command will display ipv6 mld port max-group. | |
| **Example** | The following example specifies that show ipv6 mld max-group test.<br>`Switch(config-if)# ipv6 mld max-groups 50`<br>`Switch# show ipv6 mld max-group` | |

### 2.19.35 show ipv6 mld port max-group action

| | | |
|---|---|---|
| **Syntax** | **show ipv6 mld max-group action [interfaces IF_PORTS]** | |
| **Parameter** | **None** | Show all port max-group action |
| | **[interfaces IF_PORTS]** | Show specifies ports max-group action |
| **Default** | Show all ports ipv6 mld max-group action | |
| **Mode** | Privileged EXEC | |
| **Usage** | This command will display ipv6 mld port max-group action. | |
| **Example** | The following example specifies that show ipv6 mld max-group action test.<br>`Switch(config-if)# ipv6 mld max-groups action replace`<br>`Switch# show ipv6 mld max-group action`<br>  | |

## 2.20 MVR

### 2.20.1 mvr

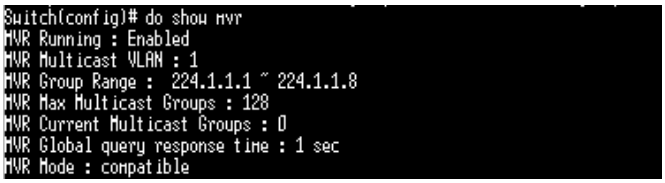
| | |
|---|---|
| **Syntax** | **mvr / no mvr** |
| **Parameter** | None |
| **Default** | Default is disabled |
| **Mode** | Global Configuration |
| **Usage** | Use the mvr command to enable MVR function. The command will clear all mvr VLAN ID multicast snooping group.<br>Use the **no** form of this command to disable. Disable will clear all mvr group. You can verify settings by the **show mvr** command. |
| **Example** | The following example specifies that set mvr test.<br>`Switch(config)# mvr`<br>`Switch(config)# no mvr`<br>`Switch# show mvr`<br>  |

```
Switch(config)# mvr
The operation will delete groups of VLAN ID is MVR VLAN include static groups. Continue? [yes/no]:no
Switch(config)# do 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
```

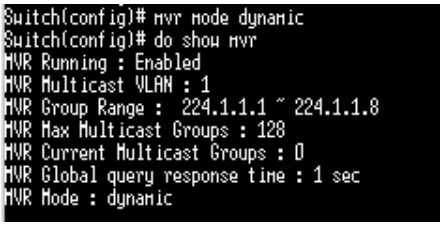
### 2.20.2 mvr vlan

| | |
|---|---|
| **Syntax** | **mvr vlan <VLAN-ID>** |
| **Parameter** | <VLAN-ID> The exist static vlan id |
| **Default** | Default mvr vlan id is 1 |
| **Mode** | Global Configuration |
| **Usage** | Use the **mvr vlan** command to modify mvr vlan id when the mvr status is enabled.<br>Change mvr vlan id will delete the old mvr vlan and new mvr vlan group.<br>If there have configure source or receiver port, there will check the source must only in the mvr vlan , and receiver port must not in the mvr vlan member.<br>You can verify settings by the **show mvr** command. |
| **Example** | The following example specifies that configure mvr vlan 2 test.<br>`Switch(config)# vlan 2`<br>`Switch(config)# mvr`<br>**The operation will delete groups of VLAN ID is MVR VLAN include static groups. Continue? [yes/no]:y**<br>`Switch(config)# mvr vlan 2`<br>**The operation will delete the old and new MVR VLAN groups include static MVR groups.Continue? [yes/no]:y**<br>`Switch# show mvr`<br>  <br> |

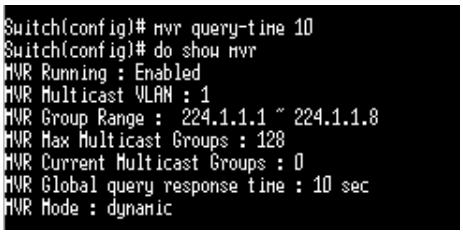
### 2.20.3 mvr group

| | |
|---|---|
| **Syntax** | **mvr group <ip-address> [<1-128>]** |
| **Parameter** | **< ip-address> Start MVR IP multicast address**<br>**[<1-128>] Contiguous series of IP addresses.** |
| **Default** | None |
| **Mode** | Global Configuration |
| **Usage** | Use the mvr group command to configure mvr group address range when mvr is enabled. The command will delete all mvr vlan ipv4 group entry You can verify settings by the **show mvr** command |
| **Example** | The following example specifies that set mvr group range is 224.1.1.1 ~ 224.1.1.8 test.<br>`Switch(config)# mvr`<br>`Switch(config)# mvr group 224.1.1.1 8`<br>`The operation will delete the MVR VLAN groups include static MVR groups.Continue? [yes/no]:y`<br>`Switch# show mvr`<br>  <br>Switch(config)# do show mvr<br>MVR Running : Enabled<br>MVR Multicast VLAN : 1<br>MVR Group Range : 224.1.1.1 ~ 224.1.1.8<br>MVR Max Multicast Groups : 128<br>MVR Current Multicast Groups : 0<br>MVR Global query response time : 1 sec<br>MVR Mode : compatible |

### 2.20.4 mvr mode

| | | |
|---|---|---|
| **Syntax** | **mvr mode (dynamic \| compatible)** | |
| **Parameter** | **(dynamic\|compatible)** | **dynamic: Allows dynamic MVR membership on source ports**<br>**compatible: does not support IGMP dynamic joins on source ports.** |
| **Default** | Default is compatible. | |
| **Mode** | Global Configuration | |
| **Usage** | Use the mvr mode command to change mvr mode when mvr is enabled.<br>You can verify settings by the show mvr command. | |
| **Example** | The following example specifies that set mvr mode dynamic test.<br>`Switch(config)#mvr`<br>`Switch(config)#mvr mode dynamic`<br>`Switch# show mvr`<br>  | |

### 2.20.5 mvr query-time

| | |
|---|---|
| **Syntax** | **mvr query-time <1-10> / no mvr query-time** |
| **Parameter** | <1-10> specifies query response time is 1~10 sec. |
| **Default** | Default is 1 sec |
| **Mode** | Global Configuration |
| **Usage** | Use the **mvr query-time** command to configure when mvr is enabled. Use the no form of this command to set query-time default value. You can verify settings by the **show mvr** command. |
| **Example** | The following example specifies that set mvr query-time 10 sec test.<br>`Switch(config)# mvr`<br>`Switch(config)# mvr query-time 10`<br>`Switch# show mvr`<br>  |

### 2.20.6 mvr port type

| | | |
|---|---|---|
| **Syntax** | **mvr type (source \| receiver) / no mvr type** | |
| **Parameter** | (source \| receiver) | Source: Configure uplink ports that receive and send multicast data as source ports. Subscribers cannot be directly connected to source ports. All source ports on a switch belong to the single multicast VLAN. Receiver: Configure a port as a receiver port if it is a subscriber port and should only receive multicast data. It does not receive data unless it becomes a member of the multicast group, either statically or by using IGMP leave and join messages. Receiver ports cannot belong to the multicast VLAN. |
| **Default** | None | |
| **Mode** | Port Configuration | |
| **Usage** | Use the **mvr type** command to configure mvr port type when mvr is enabled.<br>The source port must only belong to mvr vlan. The receiver port must not belong to mvr vlan, and port mode must be access mode.<br>Use the **no** form of this command to set mvr type none<br>You can verify settings by the **show mvr interface** command | |
| **Example** | The following example specifies that set gi1 is source port , gi2 is receiver port test.<br>`Switch(config)# vlan 2`<br>`Switch(config-vlan)#exit`<br>`Switch(config)# mvr`<br>`Switch(config)# mvr vlan 2`<br>`Switch(config)# mvr group 224.1.1.1 8`<br>`Switch(config)# interface gi1`<br>`Switch(config-if)# switchport trunk allowed vlan 2`<br>`Switch(config-if)# mvr type source Switch(config-if)#exit`<br>`Switch(config)# interface gi2`<br>`Switch(config-if)# switchport mode access`<br>`Switch(config-if)# mvr type receiver Switch# show mvr interface` | |

### 2.20.7 mvr port immediate

| | |
|---|---|
| **Syntax** | **mvr immediate / no mvr immediate** |
| **Parameter** | None |
| **Default** | Default is disabled |
| **Mode** | Port Configuration |
| **Usage** | Use the **mvr immediate** command to configure mvr support immediate leave when mvr is enabled.<br>**Note** This command applies to only receiver ports and should only be enabled on receiver ports to which a single receiver device is connected.<br>Use the **no** form of this command to disable immediate leave. You can verify settings by the **show mvr interface** command |
| **Example** | The following example specifies that set gi2 immediate enable test. The configure should configure mvr receiver port firstly.(eg. mvr port type)<br>`Switch(config)# interface gi2`<br>`Switch(config-if)#mvr immediate`<br>`Switch(config-if)#exit`<br>`Switch(config)# exit`<br>`Switch# show mvr interface` |

### 2.20.8 mvr static group

| | |
|---|---|
| **Syntax** | **mvr vlan <VLAN-ID> group <ip-addr> interfaces IF_PORTS no mvr vlan < VLAN-ID> group <ip-addr> interfaces IF_PORTS** |

**Parameter**

| | |
|---|---|
| VLAN-ID | specifies MVR VLAN ID for static group |
| ip-addr | specifies multicast MVR group address |
| IF_PORTS | specifies port list to set or remove |

| | |
|---|---|
| **Default** | None |
| **Mode** | Global Configuration |
| **Usage** | Use the **mvr vlan group** command to add a static group or configure static group member ports when mvr is enabled.<br>This command applies to only receiver ports.<br>In compatible mode, this command applies to only receiver ports. In dynamic mode, it applies to receiver ports and source ports.<br>When remove static mvr group all ports, the static group will be delete.<br>Or can use **no ip igmp vlan VLAN-ID group** to delete the mvr static group.<br>Static group can't learn dynamic port by igmp memesage.<br>Use the **no** form of this command to delete a port in static group. If remove the last member of static group, the static group will be delete.<br><br>You can verify settings by the **show mvr members** command. |
| **Example** | The following example specifies that set mvr static group test.<br>The configure must configure mvr receiver port firstly.(eg. mvr port type)<br>`Switch(config)# mvr vlan 2 group 224.1.1.1 interfaces gi2`<br>`Switch# show mvr members` |

### 2.20.9 clear mvr members

| | |
|---|---|
| **Syntax** | **clear mvr members [dynamic\|static]** |
| **Parameter** | dynamic — specifies MVR dynamic group<br>static — specifies MVR static group |
| **Default** | Clear all of mvr group |
| **Mode** | Privileged EXEC |
| **Usage** | This command will clear the mvr groups for selected type. |
| **Example** | The following example specifies that clear all mvr groups test.<br>`Switch# clear mvr members` |

### 2.20.10 show mvr members

| | |
|---|---|
| **Syntax** | **show mvr members** |
| **Parameter** | None |
| **Default** | None |
| **Mode** | Privileged EXEC |
| **Usage** | This command will display the mvr groups for all of type. |
| **Example** | The following example specifies that show mvr groups test.<br>`Switch# show mvr members` |

### 2.20.11 show mvr interface

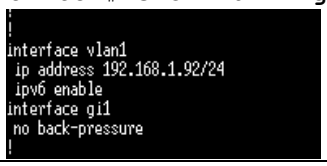
| | | |
|---|---|---|
| **Syntax** | **show mvr interface [IF_PORTS]** | |
| **Parameter** | IF_PORTS | Show specifies port list configuration |
| **Default** | None | |
| **Mode** | Privileged EXEC | |
| **Usage** | This command will display mvr port type and port immediate status. | |
| **Example** | The following example specifies that show mvr interface test.<br>`Switch# show mvr interface` | |

### 2.20.12 show mvr

| | |
|---|---|
| **Syntax** | **show mvr** |
| **Parameter** | None |
| **Default** | None |
| **Mode** | Privileged EXEC |
| **Usage** | This command will display mvr global information. |
| **Example** | The following example specifies that show mvr test.<br>`Switch# show mvr` |

# 2.21 Port

## 2.21.1 back-pressure

| | |
|---|---|
| **Syntax** | **back-pressure / back-pressure** |
| **Parameter** | None |
| **Default** | Default back pressure state is enabled. |
| **Mode** | Interface Configuration |
| **Usage** | Use "**back-pressure**" command to make port to enable back pressure feature.<br>Use **no** form of this command to disable back pressure feature.<br>The only way to show this configuration is using "**show running-config**" command. |
| **Example** | This example shows how to configure port g1 and g2 to be protected port.<br>`Switch(config)# interface g 1`<br>`Switch(config-if)# no back-pressure`<br><br>This example shows how to show current jumbo-frmae size<br>`Switch# show running-config interface g 1`<br>  |

### 2.21.2 clear interface

| | |
|---|---|
| **Syntax** | **clear interfaces** IF_PORTS **counters** |
| **Parameter** | IF_PORTS Specify port to clear counters. |
| **Default** | No default value for this command. |
| **Mode** | Privileged EXEC |
| **Usage** | Use "**clear interface**" command to clear statistic counters on specific ports. |
| **Example** | This example shows how to clear counters on port fa1.<br>`Switch(config)# clear interfaces g 1 counters`<br><br>This example shows how to show current counters<br>`Switch# show interfaces g 1` |

### 2.21.3 description

| | |
|---|---|
| **Syntax** | **description** WORD<1-32><br>**no description** |
| **Parameter** | WORD<1-32> Specifiy port description string. |
| **Default** | Default port description is empty. |
| **Mode** | Interface Configuration |
| **Usage** | Use "**description**" command to give the port a name to identify it easily.<br><br>If description includes space character, please use double quoted to wrap it. Use **no** form to restore description to empty string. |
| **Example** | This example shows how to modify port descriptions.<br>`Switch(config)# interface g 1`<br>`Switch(config-if)# description userport`<br>`Switch(config-if)# exit`<br>`Switch(config)# interface g 2`<br>`Switch(config-if)# description "uplink port"`<br>  |

```
Switch(config)# do show int g 1-2 status
Port  Name              Status      Vlan  Duplex  Speed        Type
gi1   userport          notconnect  1     auto    auto       Copper
gi2   uplinkport        notconnect  1     auto    auto       Copper
```

### 2.21.4 duplex

| | |
|---|---|
| **Syntax** | **duplex (auto \| full \| half)** |

**Parameter**

| | |
|---|---|
| auto | Specify port duplex to auto negotiation. |
| full | Specify port duplex to force full duplex |
| half | Specify port duplex to force half duplex |

**Default** Default port duplex is auto.

**Mode** Interface Configuration

**Usage** Use "**duplex**" command to change port duplex configuration.

**Example** This example shows how to modify port duplex configuration.

```
Switch(config)# interface g 1
Switch(config-if)# duplex full
Switch(config-if)# exit
Switch(config)# interface g 2
Switch(config-if)# duplex half
```

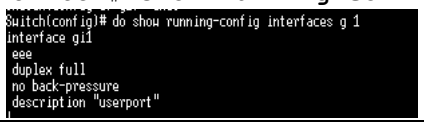
```
Switch(config)# do show running-config interfaces g 1-2
interface gi1
 duplex full
 no back-pressure
 description "userport"
!
interface gi2
 duplex half
 description "uplinkport"
!
```

This example shows how to show current interface link speed

```
Switch# show interfaces g 1-2 status
```

```
Switch(config)# do sho int g 1-2 status
Port  Name              Status      Vlan  Duplex  Speed          Type
gi1   userport          notconnect  1     full    auto         Copper
gi2   uplinkport        notconnect  1     half    auto         Copper
```

### 2.21.5 eee

| | |
|---|---|
| **Syntax** | **eee / no eee** |
| **Parameter** | None |
| **Default** | Default eee state is disabled. |
| **Mode** | Interface Configuration |
| **Usage** | Use "**eee**" command to make port to enable the energy efficient Ethernet feature.<br><br>Use no form of this command to disable eee.<br><br>The only way to show this configuration is using "**show running-config**" command. |
| **Example** | This example shows how to configure port fa1 and fa2 to be protected port.<br>`Switch(config)# interface g 1`<br>`Switch(config-if)# eee`<br><br>This example shows how to show current jumbo-frmae size<br>`Switch# show running-config interface g 1`<br>  <br> |

### 2.21.6 flowcontrol

| | | |
|---|---|---|
| **Syntax** | **flowcontrol (auto \| off \| on) / no flowcontrol** | |
| **Parameter** | auto | Automatically enables or disables flow control on the interface. |
| | off | Disable port flow control. |
| | on | Enable port flow control. |
| **Default** | Default port flow control is off. | |
| **Mode** | Interface Configuration | |
| **Usage** | Use "**flowcontrol**" command to change port flow control configuration.<br>Use **no** form to restore flow control to default (off) configuration. | |
| **Example** | This example shows how to modify port duplex configuration.<br>`Switch(config)# interface g 1`<br>`Switch(config-if)# flowcontrol on`<br>This example shows how to show current flow control configuration<br>`Switch# show interfaces g 1` | |

### 2.21.7 jumbo-frame

| | | |
|---|---|---|
| **Syntax** | **jumbo-frame** <1518-9216> | |
| **Parameter** | <1518-9216> | Specify the maximum frame size. |
| **Default** | Default maximum frame size is 1522. | |
| **Mode** | Global Configuration | |
| **Usage** | Use "**jumbo-frame**" command to modify maximum frame size. The only way to show this configuration is using "**show running-config**" command. | |
| **Example** | This example shows how to modify maximum frame size on fa1 to 9216 bytes.<br>`Switch(config)# jumbo-frame 9216`<br>This example shows how to show current jumbo-frmae size<br>`Switch# show running-config` | |

### 2.21.8 media-type

| | |
|---|---|
| **Syntax** | **media-type (auto-select \| rj45 \| sfp)**<br>**no media-type** |
| **Parameter** | Auto-select — Select media automatically<br>Rj45 — Select copper media<br>Sfp — Select fiber media |
| **Default** | Default media type is auto. |
| **Mode** | Interface Configuration |
| **Usage** | Use "**media-type**" command to change combo port media type.<br><br>Use **no** form of this command to restore media type to default. |
| **Example** | This example shows how to modify combo port media type to copper.<br>`Switch(config)# interface gi1`<br>`Switch(config-if)# media-type rj45` |

### 2.21.9 protected

| | |
|---|---|
| **Syntax** | **protected / no protected** |
| **Parameter** | Default protected state is no protected. |
| **Default** | Default media type is auto. |
| **Mode** | Interface Configuration |
| **Usage** | Use "**protected**" command to make port to be protected. Protected port is only allowed to communicate with unprotected port. In other words, protected port is not allowed to communicate with another protected port.<br><br>Use **no** form to make port unprotected. |
| **Example** | This example shows how to configure port fa1 and fa2 to be protected port.<br>`Switch(config)# interface range fa1-2`<br>`Switch(config-if-range)# protected`<br><br>This example shows how to show current protected port state.<br>`Switch# show interfaces fa1-2 protected` |

### 2.21.10 show interface

| | |
|---|---|
| **Syntax** | **show interfaces IF_PORTS**<br>**show interfaces IF_PORTS status**<br>**show interfaces IF_PORTS potected** |
| **Parameter** | IF_PORTS Specifiy port to show. |
| **Default** | No default value for this command. |
| **Mode** | Privileged EXEC |
| **Usage** | Use "**show interface**" command to show detail port counters, parameters and status.<br><br>Use "**show interface status**" command to show brief port status. Use "**show interface protected**" command to show protected status. |
| **Example** | This example shows how to show current counters<br>`Switch# show interfaces g 1`<br><br>This example shows how to show current protected port state.<br>`Switch# show interfaces fa1-2 protected`<br><br>`This example shows how to show current port status`<br>`Switch# show interfaces fa1-2 status` |

## 2.21.11 speed

**Syntax**

**speed (10 | 100 | 1000)**
**speed auto [(10 | 100 | 1000 | 10/100)]**

**speed negotiate**
**no speed negotiate**

**Parameter**

| | |
|---|---|
| 10 | Specify port speed to force 10Mbits/s or auto with 10Mbits/s ability. |
| 100 | Specify port speed to force 100Mbits/s or auto with 100Mbits/s ability. |
| 1000 | Specify port speed to force 1000Mbits/s or auto with 1000Mbits/s ability. |
| 10/100 | Specify port speed to auto with 10Mbits/s and 100Mbits/s |

**Default** Default port speed is auto with all available abilities.

**Mode** Interface Configuration

**Usage** Use “speed” command to change port speed configuration. The speed is only able to configure to the physical maximum speed. For example, in fast Ethernet port, speed 1000 is not available.

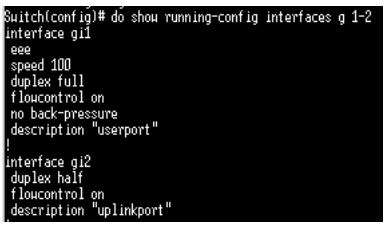
You cannot configure the speed on the SFP module ports, but you can configure the speed to not negotiate (nonegotiate) if it is connected to a device that does not support autonegotiation.

**Example** This example shows how to modify port speed configuration.

```
Switch(config)# interface g 1
Switch(config-if)# speed 100
Switch(config-if)# exit
Switch(config)# interface g 2
Switch(config-if)# speed auto
```

This example shows how to show current speed configuration

```
Switch# show running-config interfaces g 1-2
```



### 2.21.12 shutdown

| | |
|---|---|
| **Syntax** | **shutdown / no shutdown** |
| **Parameter** | None |
| **Default** | Default port admin state is no shutdown. |
| **Mode** | Interface Configuration |
| **Usage** | Use “shutdown” command to disable port and use “no shutdown” to enable port. If port is error disabled by some reason, use “no shutdown” command can also recovery the port manually. |
| **Example** | This example shows how to modify port duplex configuration.<br>`Switch(config)# interface g 1`<br>`Switch(config-if)# shutdown`<br><br>This example shows how to show current admin state configuration<br>`Switch# show running-config interfaces g 1` |

## 2.22 Port Error Disbale

### 2.22.1 errdisable recovery cause

**Syntax**

**errdisable recovery cause (all|acl|arp inspection| bpduguard| broadcast- flood|dhcp-rate-limit|psecure-violation |selfloop |unicast-flood|unknown-multicastflood)**
**no errdisable recovery cause (all|acl|arp-inspection |bpduguard |broadcast- flood|dhcp-rate-limit|psecure-violation |selfloop |unicast-flood|unknown- multicastflood)**

**Parameter**

| | |
|---|---|
| **all** | Enable the auto recovery for port error disabled from all causes. |
| **acl** | Enable the auto recovery for port error disabled from the ACL cause. |
| **arp-inspection** | Enable the auto recovery for port error disabled from the ARP inspection cause. |
| **bpduguard** | Enable the auto recovery for port error disabled from the STP BPDU Guard cause. |
| **broadcast-flood** | Enable the auto recovery for port error disabled from the broadcast flooging cause. |
| **dhcp-rate-limit** | Enable the auto recovery for port error disabled from the DHCP rate limit cause. |
| **psecure-violation** | Enable the auto recovery for port error disabled from the port security cause. |
| **selfloop** | Enable the auto recovery for port error disabled from the STP self-loop cause. |
| **unicast-flood** | Enable the auto recovery for port error disabled from the unicast flooding cause. |
| **unknown-multicastflood** | Enable the auto recovery for port error disabled from the unknown multicast flooding cause. |

**Default**

Error disable recovery is disabled for all cause.

**Mode**

Global Configuration

**Usage**

Ports would be disabled because of the invalid actions detected by protocols.
To enable the port error disable recovery from the specific cause, use the command errdisable recovery cause in the Global Configuration mode.

**Example**

The following example enables the port error disable recovery for the STP BPDU Guard and self-loog cause.

```
Switch(config)# errdisable recovery cause bpduguard
Switch(config)# errdisable recovery cause selfloop
```

### 2.22.2 errdisable recovery interval

| | |
|---|---|
| **Syntax** | **errdisable recovery interval seconds** |
| **Parameter** | **seconds** — The time in seconds to recover from a specific error-disable state. The vaild range is 0 to 86400 seconds, and the default value is 300 seconds. |
| **Default** | The default recovery time is 300 seconds. |
| **Mode** | Global Configuration |
| **Usage** | To set the recovery time of the error disabled ports, use the command errdisable recovert interval in the Global Configuration mode. |
| **Example** | The following example set the agimg time to 500 seconds. |

```
Switch(config)# errdisable recovery interval 60
```

### 2.22.3 show errdisable recovery

| | |
|---|---|
| **Syntax** | **show errdisable recovery** |
| **Parameter** | N/A |
| **Default** | N/A |
| **Mode** | Privileged EXEC |
| **Usage** | To show the error disable configuration and the interfaces in the error disabled state, use the command **show errdisable recovery** in the Privileged EXEC mode. |
| **Example** | The following example shows the error disable configuration, and the interfaces in the error disabled state. |

```
Switch# show errdisable recovery
```

```
Switch# show errdisable recovery
ErrDisable Reason        | Timer Status
-------------------------+--------------
              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 |  Error Disable Reason    | Time Left
```

## 2.23 Port Security

### 2.23.1 port security (Global)

| | |
|---|---|
| **Syntax** | **port-security / no port-security** |
| **Parameter** | N/A |
| **Default** | Default is disabled |
| **Mode** | Global Configuration |
| **Usage** | The "**port-security**" command enables the port security functionality globally.<br>Use the **no** form of this command to disable.<br>You can verify settings by the *show port-security* command. |
| **Example** | The following example shows how to enable port security<br>`switch(config)# port-security`<br>`switch# show port-security` |

### 2.23.2 port-security(Interface)

| | |
|---|---|
| **Syntax** | **port-security / no port-security** |
| **Parameter** | N/A |
| **Default** | Default is disabled |
| **Mode** | Port Configuration |
| **Usage** | The "**port-security**" command enables the port security functionality on this port.<br>Use the **no** form of this command to disable<br>You can verify settings by the **show port-security interface** command. |
| **Example** | The following example shows how to enable port security on interface g 1 |

```
switch(config)# interface g 1
switch(config-if)# port-security
switch(config)# show port-security interfaces g 1
```

```
Switch(config)# do show port-security int g 1
Port  Status      MaxAddr  TotalAddr  ConfigAddr  Violation   Action
----- ----------- -------- ---------- ----------- ----------- ---------
gi1   SecureDown  1        0          0           0           Protect
```

### 2.23.3 port-security address-limit

| | |
|---|---|
| **Syntax** | **port-security address-limit <1-256> action (forward \|discard \| shutdown)**<br>**no port-security address-limit** |
| **Parameter** | **<1-256>** — The learning-limit number. It specifies how many MAC addresses this port can learn.<br>**forward** — Forward this packet whose SMAC is new to system and exceed the learning-limit number.<br>**discard** — Discard this packet whose SMAC is new to system and exceed the learning-limit number.<br>**shutdown** — Shutdown this port when receives a packet whose SMAC is new to system and exceed the learning limit number. |
| **Default** | The address-limit default is 1 and action is “drop”. |
| **Mode** | Port Configuration |
| **Usage** | Use the “**port-security address-limit**” command to set the learning-limit number and the violation action.<br>Use the **no** form of this command to restore the default settings.<br>You can verify settings by the s**how port-security interface** command. |
| **Example** | The following example shows how to enable port security on port 1 and set the learning limit number to 10.<br>`switch(config)# interface g 1`<br>`switch(config-if)# port-security address-limit 10 action discard`<br>`switch(config-if)# port-security`<br>`switch(config)# show port-security interfaces g 1` |

### 2.23.4 show port-security

| | |
|---|---|
| **Syntax** | **show port-security** |
| **Parameter** | N/A |
| **Default** | No default value for this command. |
| **Mode** | Privileged EXEC |
| **Usage** | Use “show port-security” command to show port-security global information. |
| **Example** | This example shows how to show port-security configurations.<br>`Switch# show port-security` |

### 2.23.5 show port-security interface

| | |
|---|---|
| **Syntax** | **show port-security interface** IF_PORTS |
| **Parameter** | IF_PORTS Select port to show port-security configurations. |
| **Default** | No default value for this command. |
| **Mode** | Privileged EXEC |
| **Usage** | Use “**show port-security interfaces**” command to show port-security information of the specified port. |
| **Example** | This example shows how to show port-security configurations on interface g 1.<br>`Switch# show port-security interfaces fa1` |

## 2.24 Protocol VLAN

### 2.24.1 vlan protocol-vlan group (Global)

**Syntax**

**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**

| | |
|---|---|
| **<1-8>** | Specify protocol vlan group to configure |
| **(ethernet_ii \|llc_other\|snap_1042)** | Specify protocol based frame type |
| **VALUE** | Specify protocol value to configure |

**Default**

no protocol vlan group are configured

**Mode**

Global Configuration

**Usage**

Use the **vlan protocol-vlan group** Global Configuration mode command to add protocol vlan group with spefied proto type and value.
Use the **no** form of this command to remove protocol vlan group setting.
You can verify your setting by entering the **show vlan proto-vlan Privileged** EXEC command

**Example**

The following example show how to configure 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
Switch# show vlan protocol-vlan
```

```
Switch# configure
<vlan group 1 frame-type ethernet_ii  protocol-value 0x806
<ol-vlan group 2 frame-type llc_other protocol-value 0x800
Switch(config)# do show vlan protocol

  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    |      --      |        --
```

### 2.24.2 vlan protocol-vlan group (Interface)

| | |
|---|---|
| **Syntax** | **vlan protocol-vlan group** <1-8> **vlan** <1-4094><br>**no vlan protocol-vlan group** <1-8> |
| **Parameter** | **<1-8>** Specify protocol vlan group to binding<br>**<1-4094>** Specifies the Proto VLAN ID to configure. |
| **Default** | In default all group are not binding to any interface. |
| **Mode** | Interface configuration |
| **Usage** | Use the **vlan protocol-vlan binding** Interface Configuration mode command to binding protocol VLAN Group on specified interfaces, Use the no form of this command to cancel protocol VLAN Group Binding. You can verify your setting by entering the **show vlan protocol-vlan interfaces IF_PORTS Privileged EXEC** command |
| **Example** | The following example how to configure Protocol VLAN function on specified interfaces..<br>`Switch(config)# interface g 1`<br>`Switch(config-if)# vlan protocol-vlan group 1 vlan 2`<br>`Switch(config-if)# vlan protocol-vlan group 2 vlan 3`<br>`Switch# show vlan protocol-vlan interfaces g 1` |

### 2.24.3 show vlan protocol-vlan

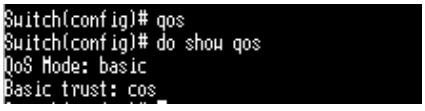
| | |
|---|---|
| **Syntax** | **show vlan protocol-vlan [group <1-8>]** |
| **Parameter** | **<1-8>** Specify protocol vlan group to binding |
| **Default** | N/A |
| **Mode** | Privileged EXEC |
| **Usage** | Use the show vlan proto-vlan command in EXEC mode to display Proto VLAN group configuration. |
| **Example** | The following example how to display Proto VLAN group configuration<br>`Switch# show vlan protocol-vlan` |

### 2.24.4 show vlan protocol-vlan interfaces

| | |
|---|---|
| **Syntax** | **show vlan protocol-vlan interfaces** IF_PORTS |
| **Parameter** | **IF_PORTS** Specify interfaces protocol vlan to display |
| **Default** | N/A |
| **Mode** | Privileged EXEC |
| **Usage** | Use the show vlan protocol-vlan interface command in EXEC mode to display the Protocol VLAN interfaces setting |
| **Example** | The following example shows how to display the Protocol VLAN interfaces setting<br>`Switch# show vlan protocol-vlan interfaces g 1` |

## 2.25 QoS

### 2.25.1 qos

| | |
|---|---|
| **Syntax** | **qos / no qos** |
| **Parameter** | N/A |
| **Default** | Default qos is disabled. |
| **Mode** | Privileged EXEC |
| **Usage** | Use "**qos**" command to enable quality of service which according to basic trust type to assign queue for packets, and packets with higher priority are able to send first.<br><br>Use no form of this command to disable quality of service. |
| **Example** | This example shows how to change qos to basic mode.<br>`Switch(config)# qos`<br><br>This example shows how to check current qos mode.<br>`Switch# show qos`<br>  |

### 2.25.2 qos cos

| | |
|---|---|
| **Syntax** | **qos cos** <0-7> |
| **Parameter** | cos <0-7> Specify the CoS value for the interface. |
| **Default** | Default CoS value for interface is 0. |
| **Mode** | Interface Configuration |
| **Usage** | Sometimes, there is no qos information in the packets, such as CoS, DSCP, IP Precedence. But we still can give the priority for packets by configuring the interface default cos value. If there is no qos information in the packets, the device will use this default cos value and find the cos-queue map to get the final destination queue.<br><br>Use "**qos cos**" command to assign port default cos value. |
| **Example** | **This example shows how to configure default cos value 7 on interface g 1.**<br>`Switch(config)# interface GigabitEthernet 1`<br>`Switch(config-if)# qos cos 7`<br>`Switch(config-if)# end`<br>`Switch# show qos interface GigabitEthernet 1` |

```
Switch(config)# int g 1
Switch(config-if-g1)# qos cos 7
Switch(config-if-g1)# exit
Switch(config)# do show qos int g 1
   Port   |  CoS   |  Trust State  | Remark Cos | Remark DSCP | Remark IP Prec
----------+--------+---------------+------------+-------------+---------------
    gi1   |   7    |      enabled  |   disabled |    disabled |      disabled |
```

### 2.25.3 qos map

**Syntax**

**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 or show CoS to queue map |
| **dscp-queue** | Configure or show DSCP to queue map |
| **precedence -queue** | Configure or show IP Precedence to queue map. |
| **queue-cos** | Configure or show queue to CoS map |
| **queue-dscp** | Configure or show queue to DSCP map |
| **queue-precedence** | Configure or show queue to IP Precedence map |
| **SEQUENCE** | Specify the cos, dscp, precedence or queue with one or multiple values. |
| <1-8> | Specify th queue id |
| <0-7> | Specify the cos or precedence values |
| <0-63> | Specify the dscp values |

**Default**

The default values of cos-queue are showing in the following table.

| CoS | Queue ID |
|---|---|
| 0 | 2 |
| 1 | 1 |
| 2 | 3 |
| 3 | 4 |
| 4 | 5 |
| 5 | 6 |
| 6 | 7 |
| 7 | 8 |

The default values of dscp-queue are showing in the following table.

| 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 |

The default values of ip precedence are showing in the following table.

| IP Precedence | Queue ID |
|---|---|
| 0 | 1 |
| 1 | 2 |
| 2 | 3 |
| 3 | 4 |
| 4 | 5 |
| 5 | 6 |
| 6 | 7 |
| 7 | 8 |

The default values of queue-cos are showing in the following table.

| Queue ID | CoS |
|---|---|
| 1 | 1 |
| 2 | 0 |
| 3 | 2 |
| 4 | 3 |
| 5 | 4 |
| 6 | 5 |
| 7 | 6 |
| 8 | 7 |

The default values of queue-dscp are showing in the following table.

| Queue ID | DSCP |
|---|---|
| 1 | 0 |
| 2 | 8 |
| 3 | 16 |
| 4 | 24 |
| 5 | 32 |
| 6 | 40 |
| 7 | 48 |
| 8 | 56 |

The default values of queue-precedence are showing in the following table.

| Queue ID | IP Precedence |
|---|---|
| 1 | 0 |
| 2 | 1 |
| 3 | 2 |
| 4 | 3 |
| 5 | 4 |
| 6 | 5 |
| 7 | 6 |
| 8 | 7 |

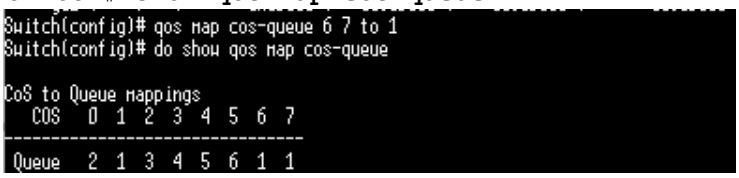
**Mode** Global Configuration

**Usage** According to different trust type, packets will be assigned to different queue based on the specific qos map. For example, if the trust type is trust cos, the device will get the cos value in packet and reference the cos-queue mapping to assign the correct queue.

The queue to cos, dscp or precedence maps are used by remarking function. If the port remarking feature is enabled, the remarking function will reference these 3 tables to remark packets.

**Example** This example shows how to map cos 6 and 7 to queue 1

```
Switch(config)# qos map cos-queue 6 7 to 1
Switch# show qos map cos-queue
```




This example shows how to map queue 4 and 5 to cos 7.

```
Switch(config)# qos map queue-cos 4 5 to 7
Switch# show qos map queue-cos
```

### 2.25.4 qos queue

**Syntax**

**qos queue strict-priority-num <0-8>**
**qos queue weight SEQUENCE**
**show qos queueing**

**Parameter**

| | |
|---|---|
| **strict-priority-num <0-8>** | Specify the strict priority queue number |
| **weight SEQUENCE** | Specify the non-strict priority queue weight value. The valid queue weight value is from 1 to 127. |

**Default**

Default strict priority queue number is 8, it means all queues are strict priority queue.

The default queue weight for each queue is shown in following table.

| Queue ID | Queue Weight |
|---|---|
| 1 | 1 |
| 2 | 2 |
| 3 | 3 |
| 4 | 4 |
| 5 | 5 |
| 6 | 9 |
| 7 | 13 |
| 8 | 15 |

**Mode**

Global Configuration

**Usage**

The device support total 8 queues for QoS queueing. It is able to set the queue to be strict priority queue or weighted queue to prevent starvation. The queue with higher id value has higher priority.
First, you need to decide how many strict priority queue you need. The strict priority queue will always occupy the higher priority queue. For example, if you specify the strict priority number to be 2, then the queue 7 and 8 will be the strict priority queues and the others are weighted queues.

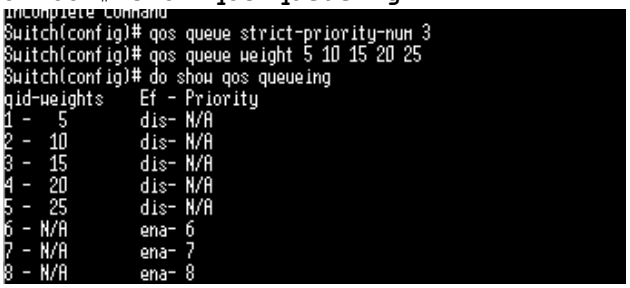
After you setup the number of strict priority queue, you need to setup the weight for the weighted queues by using “qos queue weight” command. And the bandwidth will shared by the weight you configured between these weighted queues.

**Example**

This example shows how to setup device with 3 strict priority queues

and give other weighted queues with weight 5, 10, 15, 20, 25.

```
Switch(config)# qos queue strict-priority-num 3
Switch(config)# qos queue weight 5 10 15 20 25
Switch# show qos queueing
```




### 2.25.5 qos remark

| | |
|---|---|
| **Syntax** | **qos remark (cos \| dscp \| precedence)**<br>**no qos remark (cos \| dscp \| precedence)** |
| **Parameter** | **cos** Enable/Disable cos remarking.<br>**dscp** Enable/Disable dscp remarking.<br>**precedence** Enable/Disable precedence remarking. |
| **Default** | Default CoS remarking is disabled.<br>Default DSCP remarking is disabled.<br>Default IP Precedence remarking is disabled. |
| **Mode** | Interface Configuration |
| **Usage** | QoS remarking feature allow you to change priority information in packets based on egress queue. For example, you want all packets egress from interface fa1 queue 1 to remark the cos value to be 5 for next tier of device, you can enable the cos remarking feature on fa1 and configure the queue-cos map for queue 1 map to cos 5.<br><br>Use "**qos remark**" command to enable remarking feature on specific type.<br>And use "**no qow remark**" command to disable it. |
| **Example** | This example shows how to enable remarking features on interface fa1.<br>`Switch(config)# interface GigabitEthernet 1`<br>`Switch(config-if)# qos remark cos`<br>`Switch(config-if)# qos remark dscp`<br>`Switch(config-if)# qos remark precedence`<br>`Switch(config-if)# end`<br>`Switch# show qos interface GigabitEthernet 1` |

### 2.25.6 qos trust

| | | |
|---|---|---|
| **Syntax** | **qos trust (cos \| cos-dscp \| dscp \| precedence)** | |
| **Parameter** | cos | Specify the device to trust CoS |
| | cos-dscp | Specify the device to trust DSCP for IP packets, and trust CoS for non-IP packets. |
| | dscp | Specify the device to trust DSCP |
| | precedence | Specify the device to trust IP Precedence |
| **Default** | Default QoS trust type is cos. | |
| **Mode** | Global Configuration | |
| **Usage** | In QoS basic mode, there are 4 trust types for device to judge the appropriate queue of the packets. This command is able to switch between these trust types.<br>**CoS:**<br>IEEE 802.1p defined 3bits priority value in vlan tag. Trust this value in packets and assign queue according to cos-queue map.<br>**DSCP:**<br>IETF RFC2474 defined 6bits priority value in IP packet (highest 6bits in ToS field). Trust this value in packets and assign queue according to dscp-queue map.<br>**IP Precedence:**<br>The highest 3bits priority value in IP packet ToS field. Trust this value in packets and assign queue according to precedence-queue map.<br>**CoS-DSCP:**<br>Trust DSCP for IP packets and assign queue according to dscp-queue map. Trust CoS for non-IP packets and assign queue according to cos-queue map. | |
| **Example** | This example shows how to change qos basic mode trust types.<br>`Switch(config)# qos trust cos`<br>`Switch(config)# qos trust cos-dscp`<br>`Switch(config)# qos trust dscp`<br>`Switch(config)# qos trust precedence`<br><br>This example shows how to check current qos trust type.<br>`Switch# show qos` | |

### 2.25.7 qos trust(Interface)

| | |
|---|---|
| **Syntax** | **qos trust / no qos trust** |
| **Parameter** | N/A |
| **Default** | Default interface qos trust state is enabled. |
| **Mode** | Interface Configuration |
| **Usage** | After QoS function is enabled in basic mode, the device also support per interface enable/disable the qos function. If the trust state on interface is enabled, all ingress packets of this interface will remap according to the trust type and the qos maps. Otherwise, all ingress packets will assign to queue 1.<br><br>Use "**qos trust**" to enable trust state on interface and use "**no qos trust**" to disable trust state on interface. |
| **Example** | This example shows how to disable qos trust state on interface fa1.<br>`Switch(config)# interface GigabitEthernet 1`<br>`Switch(config-if)# no qos trust`<br>`Switch(config-if)# end`<br>`Switch# show qos interface GigabitEthernet 1` |

### 2.25.8 show qos

| | |
|---|---|
| **Syntax** | **show qos** |
| **Parameter** | N/A |
| **Default** | No default value for this command. |
| **Mode** | Privileged EXEC |
| **Usage** | Use "**show qos**" command to show qos state and trust type. |
| **Example** | This example shows how to check current qos mode.<br>`Switch# show qos` |

### 2.25.9 show qos interface

| | |
|---|---|
| **Syntax** | **show qos interface** IF_PORTS |
| **Parameter** | IF_PORTS Select port to show qos configurations. |
| **Default** | No default value for this command. |
| **Mode** | Privileged EXEC |
| **Usage** | Use "**show qos interfaces**" command to show port default cos ,remarking state and remarking type state informations. |
| **Example** | This example shows how to show qos configurations on interface g 1.<br>`Switch# show qos interface GigabitEthernet 1` |

### 2.25.10 show qos map

| | |
|---|---|
| **Syntax** | **show qos map [(cos-queue \| dscp-queue \| precedence-queue \| queue-cos \|queue-dscp \| queue-precedence)]** |
| **Parameter** | **cos-queue** Show CoS to queue map.<br>**dscp-queue** Show DSCP to queue map.<br>**precedence-queue** Show IP Precedence to queue<br>map. **queue-cos** Show queue to CoS map.<br>**queue-dscp** Show queue to DSCP map.<br>**queue-precedence** Show queue to IP Precedence map. |
| **Default** | No default value for this command. |
| **Mode** | Privileged EXEC |
| **Usage** | Use "s**how qos map**" command to show all kinds of mapping for qos remapping and remarking features. |
| **Example** | This example shows how to show all qos maps.<br>`Switch(config)# show qos map` |

### 2.25.11 show qos queueing

| | |
|---|---|
| **Syntax** | **show qos queueing** |
| **Parameter** | No default value for this command. |
| **Default** | No default value for this command. |
| **Mode** | Privileged EXEC |
| **Usage** | Use "**show qos queueing**" command to show qos queueing information. |
| **Example** | This example shows how to check current qos queueing information.<br>`Switch# show qos queueing` |

## 2.26 Rate Limit

### 2.26.1 rate limit egress

| | |
|---|---|
| **Syntax** | **rate-limit egress** <16-1000000><br>**no rate-limit egress** |
| **Parameter** | <16-1000000> Specify the committed information rate. |
| **Default** | Default rate limit is disabled. |
| **Mode** | Interface configuration |
| **Usage** | Use the "**rate-limit egress**" command to configure the egress port shaper. Use the **no** form of this command to disable the shaper. You can verify your setting by entering the **show running-config interfaces** command. |
| **Example** | The following example show how to configure ingress port rate limit and egress port shaper.<br>`Switch(config)# interfaces gi1`<br>`Switch(config-if)# rate-limit egress 2048`<br>`Switch# show running-config interfaces gi1`<br>  <br> |

### 2.26.2 rate limit egress queue

| | |
|---|---|
| **Syntax** | **rate-limit egress queue** <1-8> <16-1000000><br>**no rate-limit egress queue** <1-8> |
| **Parameter** | <1-8> Specify the egress shaper queue number<br>*<16-1000000>* Specify the queue rate. |
| **Default** | Default queue rate limit is disabled. |
| **Mode** | Interface configuration |
| **Usage** | Use the "**rate-limit egress queue**" command to configure the egress queue shaper. Use the **no** form of this command to disable the queue shaper.You can verify your setting by entering the s**how running-config interfaces** command. |
| **Example** | The following example show how to configure ingress port rate limit and egress port shaper.<br>`Switch(config)# interfaces gi1`<br>`Switch(config-if)# rate-limit egress queue 3 2048`<br>`Switch# show running-config interfaces gi1`<br>`Switch(config)# do show running-config interfaces g 1`<br>`interface gi1`<br>` rate-limit egress 2048`<br>` rate-limit egress queue 3 2048` |

### 2.26.3 rate limit ingress

| | |
|---|---|
| **Syntax** | **rate-limit ingress <16-1000000>**<br>**no rate-limit ingress** |
| **Parameter** | <1-8> Specify the egress shaper queue number<br>*<16-1000000>* Specify the ingress limit rate |
| **Default** | Rate limiting is disabled. |
| **Mode** | Interface configuration |
| **Usage** | Use the "**rate-limit ingress**" command to limit the incoming traffic rate on a port. Use the **no** form of this command to disable the rate limit. You can verify your setting by entering the **show running-config interfaces** command |
| **Example** | The following example show how to configure ingress port rate limit.<br>`Switch(config)# interfaces gi1`<br>`Switch(config-if)# rate-limit ingress 128`<br>`Switch# show running-config interfaces gi1`<br>`Switch(config)# show running-config int g 1`<br>`interface gi1`<br>` rate-limit ingress 128`<br>` rate-limit egress 2048`<br>` rate-limit egress queue 3 2048` |

## 2.27 RMON

### 2.27.1 rmon event

| | |
|---|---|
| **Syntax** | **rmon event <1-65535> [log] [trap COMMUNITY] [description DESCRIPTION] [owner NAME]**<br>**no rmon event <1-65535>** |

**Parameter**

| | |
|---|---|
| **<1-65535>** | Specify event index to create or modify. |
| **[log]** | (Optional)Specify to show syslog. |
| **[trap COMMUNITY]** | (Optional)Specify SNMP community to show SNMP trap. |
| **[description DESCRIPTION]** | (Optional)Specify description of event |
| **[owner NAME]** | (Optional)Specify owner of event. |

| | |
|---|---|
| **Default** | No default is defined. |
| **Mode** | Global Configuration |
| **Usage** | Use the **rmon event** command to add or modify a RMON evnet entry.<br>Use the no form of this command to delete.<br>You can verify settings by the **show rmon event** command. |

**Example**

The example shows how to add RMON event entry with log and trap action and then modify it action to log only.

```
switch(config)# rmon event 1 log trap public
                description test owner admin
switch(config)# show rmon event 1
```

```
Switch(config)# rmon event 1 log trap public description test owner admin
Switch(config)# do 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   :
Rmon Event Owner       : admin
```

### 2.27.2 rmon alarm

**Syntax**

**rmon alarm <1-65535> interface IF_PORT (drop-events|octets|pkts|broadcast-pkts| multicast-pkts|crc-align-errors|undersize-pkts|oversizepkts|fragments|jabbers|collisions|pkts64octets|pkts65to127octets|pkts128to255octets|pkts256to511octets|pkts512to1023octets|pkts1024to1518octets) <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>** | Specify alarm index to create or modify |
| **IF_PORT** | Specify the interface to sample |
| **(variable)** | Specify a mib object to sample |
| **<1-2147483647>** | Specify the time in seconds that the alarm monitors the MIB variable. |
| **(absolute\|delta)** | Specify absolute to compare sample counter absolutely.<br>Specify delta to compare delta counter between samples |
| **<0-2147483647>** | Specify a number which the alarm trigger rising<br>event |
| **<0-65535>** | Specify event index when the rising threshold exceeds. |
| **<0-2147483647>** | Specify a number which the alarm trigger falling<br>event |
| **<0-65535>** | Specify event index when the falling threshold exceeds. |
| **(rising\|rising-falling\|falling)** | Specify only to how rising or falling startup event. Or show either rising or falling startup event. |
| **[owner NAME]** | (Optional) Specify owner of alarm. |

**Default**

No default is defined.

**Mode**

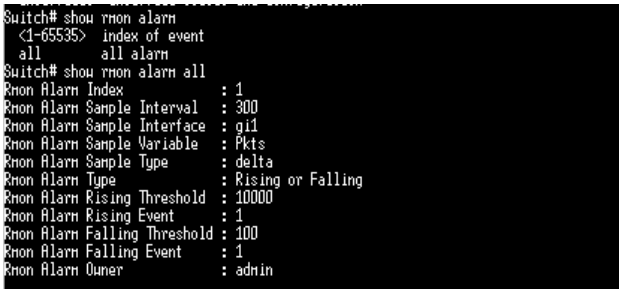
Global Configuration

**Usage**

Use the **rmon alarm** command to add or modify a RMON alarm entry. Before add alarm entry, at least one event entry must be added. Use the **no** form of this command to delete.
You can verify settings by the **show rmon alarm** command.

**Example** The example shows how to add RMON alarm entry that sample interface fa1 packets delta count every 300 seconds. Trigger event index 1 if over than rising threshold 10000, trigger event index 2 if lower than falling threshold.

```
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
```




### 2.27.3 rmon history

**Syntax** **rmon history <1-65535> interface IF_PORT [buckets <1-65535>] [interval <1-3600>] [owner NAME]**
**no rmon history <1-65535>**

**Parameter**

| | |
|---|---|
| **<1-65535>** | Specify history index to create or modify. |
| **IF_PORT** | Specify the interface to sample |
| **[bucket <1-65535>]** | (Optional) Specify the maximum number of buckets. |
| **[interval <>1-3600]** | (Optional) Specify time interval for each sample |
| **[owner NAME]** | (Optional)Specify owner of history |

**Default** No default is defined.

**Mode** Global Configuration

**Usage** Use the **rmon history** command to add or modify a RMON history entry. Use the **no** form of this command to delete. You can verify settings by the **show rmon history** command.

**Example** The example shows how to add RMON history entry that monitor interface gi1 every 60 seconds and then modify it to monitor every 30

seconds.

```
switch(config)# rmon history 1 interface gi1 interval
                60 owner admin
switch(config)# show rmon history 1
```


### 2.27.4 clear rmon interfaces statistics

| | |
|---|---|
| **Syntax** | **clear rmon interfaces IF_PORTS statistics** |
| **Parameter** | **IF_PORTS** specifies ports to clear |
| **Default** | No default is defined. |
| **Mode** | Privileged EXEC |
| **Usage** | Use the **clear rmon interfaces statistics** command to clear RMON etherStat statistics those are recorded on interface.<br>You can verify results by the **show rmon interface statistics** command. |
| **Example** | The example shows how to clear RMON etherStat statistics on interface gi1.<br><br>`switch# clear rmon interfaces gi1 statistics`<br>`switch# show rmon interfaces gi1 statistics` |

### 2.27.5 show rmon interfaces statistics

| | |
|---|---|
| **Syntax** | **show rmon interfaces IF_PORTS statistics** |
| **Parameter** | IF_PORTS — specifies ports to show |
| **Default** | No default is defined. |
| **Mode** | Privileged EXEC |
| **Usage** | Use the **show rmon interfaces statistics** command to show RMON etherStatstatistics of interface. |
| **Example** | The example shows how to show RMON etherStat statistics of interface gi1.<br>`switch(config)# show rmon interfaces gi1 statistics` |

### 2.27.6 show rmon event

| | |
|---|---|
| **Syntax** | **show rmon event <1-65535> log** |
| **Parameter** | <1-65535> — specifies event index to show<br>all — Show all existed event |
| **Default** | No default is defined. |
| **Mode** | Privileged EXEC |
| **Usage** | Use the **show rmon event** command to show existed RMON event entry. |
| **Example** | The example shows how to show rmon event entry.<br>`switch(config)# rmon event 1 log trap public description test owner admin`<br>`switch(config)# show rmon event 1` |

```
Switch(config)# rmon event 1 log trap public description test owner admin
Switch(config)# 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   :
Rmon Event Owner       : admin
```

### 2.27.7 show rmon event log

| | |
|---|---|
| **Syntax** | **show rmon event (<1-65535> \| all)** |
| **Parameter** | **<1-65535>** specifies event index to show event log |
| **Default** | No entry and log is exist |
| **Mode** | Privileged EXEC |
| **Usage** | Use the **show rmon event log** command to show log triggered by RMON alarm. |
| **Example** | The example shows how to show rmon event log.<br>`switch(config)# show rmon event 1 log` |

### 2.27.8 show rmon alarm

| | |
|---|---|
| **Syntax** | **show rmon alarm (<1-65535> \| all)** |
| **Parameter** | **<1-65535>** specifies alarm index to show<br>**All** Show all existed alarm |
| **Default** | No alarm is defined |
| **Mode** | Privileged EXEC |
| **Usage** | Use the **show rmon alarm** command to show existed RMON alarm entry. |
| **Example** | The example shows how to show rmon alarm entry.<br>`Switch(config)# rmon alarm 1 interface gi1 pkts 300 delta rising 10000 1 falling 100 1 startup rising-falling owner admin` |

```
Switch(config)# show rmon alarm all
Rmon Alarm Index            : 1
Rmon Alarm Sample Interval  : 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 Alarm Rising Event     : 1
Rmon Alarm Falling Threshold : 100
Rmon Alarm Falling Event    : 1
Rmon Alarm Owner            : admin
```

### 2.27.9 show rmon history

| | |
|---|---|
| **Syntax** | **show rmon history (<1-65535> \| all)** |
| **Parameter** | **<1-65535>** specifies history index to show<br>**All** Show all existed history |
| **Default** | No history is defined |
| **Mode** | Privileged EXEC |
| **Usage** | Use the **show rmon history** command to show existed RMON history entry. |
| **Example** | The example shows how to show RMON history entry.<br>`switch(config)# rmon history 1 interface gi1 interval 30 owner admin`<br>`switch(config)# show rmon history 1`<br>  |



### 2.27.10 show rmon history statistic

| | |
|---|---|
| **Syntax** | **show rmon history <1-65535> statistic** |
| **Parameter** | **<1-65535>** specifies history index to show history statistic |
| **Default** | No history is defined |
| **Mode** | Privileged EXEC |
| **Usage** | Use the show **rmon history statistic** command to show statistics that are recorded by RMON history. |
| **Example** | The example shows how to show RMON history statistics<br>`switch(config)# show rmon history 1 statistics` |

## 2.28 SNMP

### 2.28.1 show snmp

| | |
|---|---|
| **Syntax** | **show snmp** |
| **Parameter** | N/A |
| **Default** | N/A |
| **Mode** | Privileged EXEC |
| **Usage** | To show the status of Simple Network Management Protocol (SNMP), use the command **show snmp** in the Privileged EXEC mode. |
| **Example** | The following example shows the SNMP status.<br><br>`Switch# show snmp` |

### 2.28.2 show snmp community

| | |
|---|---|
| **Syntax** | **show snmp community** |
| **Parameter** | N/A |
| **Default** | N/A |
| **Mode** | Privileged EXEC |
| **Usage** | To show the configuration of snmp communities, use the command **show snmp community** in the Privileged EXEC mode. |
| **Example** | The following example shows the SNMP communities configuration.<br><br>`Switch# show snmp community` |

### 2.28.3 show snmp engineid

| | |
|---|---|
| **Syntax** | **show snmp engineid** |
| **Parameter** | N/A |
| **Default** | N/A |
| **Mode** | Privileged EXEC |
| **Usage** | To show the SNMPv3 engine IDs defined on the switch, use the command **show snmp engineid** in the Privileged EXEC mode. |
| **Example** | The following example shows the SNMP engind id information.<br><br>`Switch# show snmp engineid` |

### 2.28.4 show snmp group

| | |
|---|---|
| **Syntax** | **show snmp group** |
| **Parameter** | N/A |
| **Default** | N/A |
| **Mode** | Privileged EXEC |
| **Usage** | To show the SNMP group configuration on the switch, use the command show snmp group in the Privileged EXEC mode. |
| **Example** | The following example shows the SNMP group configuration.<br><br>`Switch# show snmp group` |

### 2.28.5 show snmp host

| | |
|---|---|
| **Syntax** | **show snmp host** |
| **Parameter** | N/A |
| **Default** | N/A |
| **Mode** | Privileged EXEC |
| **Usage** | To show the SNMP trap notification recipients defined on the switch, use the command **show snmp host** in the Privileged EXEC mode. |
| **Example** | The following example shows the configuration of SNMP notification recipients on the switch.<br><br>`Switch# show snmp host` |

### 2.28.6 show snmp trap

| | |
|---|---|
| **Syntax** | **show snmp trap** |
| **Parameter** | N/A |
| **Default** | N/A |
| **Mode** | Privileged EXEC |
| **Usage** | To show the status of SNMP traps on the switch, use the command **show snmp trap** in the Privileged EXEC mode. |
| **Example** | The following example shows the status of SNMP traps.<br><br>`Switch# show snmp trap`<br>  <br> |

### 2.28.7 show snmp view

| | |
|---|---|
| **Syntax** | **show snmp view** |
| **Parameter** | N/A |
| **Default** | N/A |
| **Mode** | Privileged EXEC |
| **Usage** | To show the SNMP view defined on the switch, use the command **show snmp view** in the Privileged EXEC mode. |
| **Example** | The following example shows the configuration of SNMP view.<br><br>`Switch# show snmp view` |

### 2.28.8 show snmp user

| | |
|---|---|
| **Syntax** | **show snmp user** |
| **Parameter** | N/A |
| **Default** | N/A |
| **Mode** | Privileged EXEC |
| **Usage** | To show the SNMP users defined on the switch, use the command **show snmp user** in the Privileged EXEC mode. |
| **Example** | The following example shows the configuration of SNMP user.<br><br>`Switch# show snmp user` |

### 2.28.9 snmp

| | |
|---|---|
| **Syntax** | **snmp** |
| **Parameter** | N/A |
| **Default** | SNMP is disabled by default |
| **Mode** | Global Configuration |
| **Usage** | To enable the SNMP on the switch, use the command snmp in the Global Configuration mode. Otherwise, use the no form of the command to disable to SNMP. |
| **Example** | The following example enables the SNMP.<br>`Switch(config)# snmp` |

### 2.28.10 snmp community

| | |
|---|---|
| **Syntax** | **snmp community community-name [view view-name] (ro\|rw)**<br>**snmp community community-name group group-name**<br>**no snmp community community-name** |
| **Parameter** | **community-name** The SNMP community name. Its maximum length is 20 characters.<br>**view** view-name Specify the SNMP view configured by the command **snmp view** to define the object available to the community.<br>**ro** Read only access (default)<br>**rw** Writable access<br>**group** group-name Specify the SNMP group configured by the command snmp group to define the object available to the community. |
| **Default** | No SNMP community is configured |
| **Mode** | Global Configuration |
| **Usage** | To define the SNMP community that permit access for SNMP v1 and v2, use the command **snmp community** in the Global Configuration mode. |
| **Example** | The following example defines the SNMP community named private with the default view all, and the access right is read-only.<br><br>Switch(config)# **snmp community private ro** |

### 2.28.11 snmp engineid

| | | |
|---|---|---|
| **Syntax** | **snmp engineid (default\|ENGINEID)** | |
| **Parameter** | **default** | Default engine ID generated on the basis of the switch MAC address. |
| | ENGINEID | Specify SNMP engine ID. The engine ID is the 10 to 64 hexadecimal characters, and the hexadecimal number must be divided by 2. |
| **Default** | The default SNMP engine ID on the switch is based on switch MAC address. | |
| **Mode** | Global Configuration | |
| **Usage** | To define the SNMP engine on the switch, use the command **snmp engineid** in the Global Configuration mode. | |
| **Example** | The following example configure the switch SNMP engine ID<br>`Switch(config)# snmp engineid 00036D001122` | |

### 2.28.12 snmp engineid remote

| | | |
|---|---|---|
| **Syntax** | **snmp engineid remote (ip-addr\|ipv6-addr) ENGINEID**<br>**no snmp engineid remote (ip-addr\|ipv6-addr)** | |
| **Parameter** | **ENGINEID** | Specify SNMP engine ID. The engine ID is a 10 to 64 hexadecimal characters, and the hexadecimal number must be divided by 2. |
| | ip-addr | IP address of the remote host |
| | ipv6-addr | IPv6 address of the remote host |
| **Default** | N/A | |
| **Mode** | Global Configuration | |
| **Usage** | To define the remote host for SNMP engine, use the command snmp engineid remote in the Global Configuration mode; and use the no form of the command to delete the remote host from the SNMP engine. | |
| **Example** | The following example adds the remote 192.168.1.11 into SNMP engine<br>`Switch(config)# snmp engineid remote 192.168.1.11 00036D10000A` | |

### 2.28.13 snmp group

**Syntax**

**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** | Specify SNMP group name, and the maximum length is 30 characters. |
| **(1\|2c\|3)** | Specify the SNMP version. |
| **noauth** | Specify that no packet authentication is performed. |
| **auth** | Specify that no packet authentication without entryption is performed. It is applicable only to the SNMPv3 security mode. |
| **priv** | Specify that no packet authentication with entryption is performed. It is applicable only to the SNMPv3 security mode. |
| **read-view** read- view | Set the view name that enables configuring the agent, and its maximum length is 30 characters. |
| **write-view** write- view | Set the view name that enables viewing only, and its maximum length is 30 characters. |
| **notify-view** notify- view | Sets the view name that sends only traps with contents that is included in SNMP view selected for notification. The maximum length is 30 characters |

**Default**

No group entry is existed.

**Mode**

Global Configuration

**Usage**

To define the SNMP group, use the command **snmp group** in the Glocal Configuration mode, and use the no form of the command to delete the configuration.

SNMP group configuration is used in the command **snmp use** to map SNMP users to the SNMP group. These users would be automatically maped to the SNMP views defined in this command.

The securety level for SNMP v1 or v2 is always **noauth**.

**Example**

The following example adds SNMPv3 group

```
Switch(config)# snmp group v3 version 3 auth read-view
                all write-view all notify-view all
```

## 2.28.14 snmp host

**Syntax**

**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 IP adderss of recipet. |
| ipv6-addr | The IPv6 adderss of recipet. |
| hostname | The host name of recipet. |
| **traps** | Send SNMP traps to the host. It is the default action. |
| **informs** | Send SNMP informs to the host. |
| **version (1\|2c\|3)** | Specify the SNMP version. |
| **noauth** | Specify that no packet authentication is performed. It is applicable only to the SNMPv3 security mode. |
| **auth** | Specify that no packet authentication without entryption is performed. It is applicable only to the SNMPv3 security mode. |
| **priv** | Specify that no packet authentication with entryption is performed. It is applicable only to the SNMPv3 security mode. |
| community-name | The SNMP community sent with the notification. |
| **udp-port** udp-port | Specify the UDP port number. |
| **timeout** timeout | Specify the SNMP informs timeout |
| **retries** retries | Specify the retry counter of the SNMP informs. |

**Default**

No SNMP host is configured.
The default SNMP version for the command is SNMPv1.

**Mode**

Global Configuration

**Usage**

To configure the hosts to receive SNMP notificatons, use the command snmp host in the Global Configuration mode; and use the no form of the command to delete the configuration.

**Example**

The following example adds the recipet 192.168.1.11 for the SNMP traps notification.

```
Switch(config)# snmp host 192.168.1.11 private
```

### 2.28.15 snmp trap

| | |
|---|---|
| **Syntax** | **snmp trap (auth\|cold-start\|linkUpDown\|port-security\|warm-start)**<br>**no snmp trap (auth\|cold-start\|linkUpDown\|port-security\|warm-start)** |
| **Parameter** | **auth** Enable the SNMP authentication failure trap.<br>**cold-start** Enable the SNMP cold start-up failure trap.<br>**linkUpDown** Enable the SNMP link up and down failure trap.<br>**port-security** Enable the SNMP port security trap.<br>**warm-start** Enable the SNMP warm start-up failure trap. |
| **Default** | All the SNMP traps are enabled. |
| **Mode** | Global Configuration |
| **Usage** | To send the SNMP traps, use the command snmp trap in the Global Configuration mode; and use the no form of the command to disable the SNMP traps. |
| **Example** | The following example disables and enables the SNMP link up and down traps individually.<br><br>`Switch(config)# no snmp trap linkUpDown`<br>`Switch(config)# snmp trap linkUpDown` |

### 2.28.16 snmp user

| | |
|---|---|
| **Syntax** | **snmp user username group-name [auth (md5\|sha) AUTHPASSWD]**<br>**snmp user username group-name auth (md5\|sha) AUTHPASSWD priv PRIVPASSWD**<br>**no snmp user username** |
| | username Specify the SNMP user name on the host that connects to the SNMP agent. The max character is 30 characters. For the SNMP v1 or v2c, the user name must match the community name by the command snmp host.<br>group-name Specify the SNMP group to which the SNMP user belongs. The SNMP group should be SNMPv3 and configured by the command snmp group.<br>**auth (md5\|)** Specify the HMAC-MD5-96 authentication protocol as the user authentication.<br>**auth (sha\|)** Specify the HMAC-SHA-96 authentication protocol as the user authentication.<br>AUTHPASSWD The password for authentication and the range of length is from 8 to 32 characters. |

| | | |
|---|---|---|
| **Parameter** | **Priv** PRIVPASSWD | The private password for the privacy key, and the range of length is from 8 to 64 characters. |
| **Default** | N/A | |
| **Mode** | Global Configuration | |
| **Usage** | To define a SNMP user, use the command snmp user in the Global Configuration mode; and use the no form to delete the SNMP user. | |
| **Example** | The following example adds SNMP user v3 into the group v3 by the MD5 authentication.<br><br>`Switch(config)# snmp user v3 v3 auth md5 12345678` | |

### 2.28.17 snmp view

| | | |
|---|---|---|
| **Syntax** | **snmp view view-name subtree oid-tree oid-mask (all\|oid-mask) viewtype(included\|excluded)**<br>**no snmp view view-name subtree (all\|oid-tree)** | |
| **Parameter** | view-name | The SNMP view name. Its maximum length is 30 characters. |
| | **subtree** oid-tree | Specify the ASN.1 subtree object identifier (OID) to be included or excluded from the SNMP view. |
| | **oid-mask (all\|**oid- mask**)** | Specify the OID family mask. It is used to define a family of view subtrees. For example, OID mask FA.80 is is 11111010.10000000. The length of the OID mask must be less than the length of subtree OID. |
| | **iewtype (included\|excluded)** | Include or exclude the selected MIBs in the view. |
| **Default** | N/A | |
| **Mode** | Global Configuration | |
| **Usage** | To configure the SNMP view, use the command snmp view in the Global Configuration mode; and use the no form of the command to delete the SNMP view.<br><br>The default SNMP view cannot be deleted and modified by users. By default, the maximum numbers of SNMP view is limited to 16. | |

**Example** The following example defines the SNMP view.

```
Switch(config)# snmp view private subtree 1.3.3.1 oid-
                mask all viewtype included
```

## 2.29 Spanning Tree

### 2.29.1 instance (MST)

**Syntax**

**instance instance-id vlan vlan-list**
**no instance instance-id vlan vlan-list**

**Parameter**

| | |
|---|---|
| instance-id | The MSTP instance ID from 0 to 15. |
| **vlan** vlan-list | Add the VLAN list to the MSTP instance. |

**Default** All VLANs are mapped to the Common and Internal Spanning Tree (CIST) instance (instance 0).

**Mode** MST Configuration

**Usage**

To map the VLAN to the Multiple Spanning Tree (MSTP) instances, use the command instance in the MST Configuration mode; and use the no form of the command to restore its default configuration.

All VLANs that are not explicility configured to an MSTP instance are mapped to the CIST instance (instance 0).

For two or more switches in the samp MSTP regiom, their VLAN mapping, name and revision number configuration, must be the same.

**Example** The following example maps the vlan 10-20 to the MSTP instance 1, and VLAN 100 to instance 2.

```
Switch(config)# spanning-tree mst configuration
Switch(config-mst)# instance 1 vlan 10-20
Switch(config-mst)# instance 2 vlan 100
```

### 2.29.2 name(MST)

| | |
|---|---|
| **Syntax** | **name name-str**<br>**no name** |
| **Parameter** | name-str — The MSTP instance name. Its maximum length is 32 characters. |
| **Default** | The default MSTP name is the switch MAC address. |
| **Mode** | MST Configuration |
| **Usage** | To define the name for MSTP instance, use the command name in the MST Configuration mode; and use the no form to restore the default name configuration. |
| **Example** | The following example configures the name of MST instance to fiberroad |

```
Switch(config)# spanning-tree mst configuration
Switch(config-mst)# name fiberroad
```

### 2.29.3 revision(MST)

| | |
|---|---|
| **Syntax** | **revision rev**<br>**no revision** |
| **Parameter** | rev — The MSTP revision number. Its valid rage is from 0 to 65535. |
| **Default** | The default revision number is 0. |
| **Mode** | MST Configuration |
| **Usage** | To define the revision for the MSTP configuration, use the command revision in the MST Configuration mode; and use the no form of the command to restore it default configuration. |
| **Example** | The following example defines the revision MSTP configuration to 1. |

```
Switch(config)# spanning-tree mst configuration
Switch(config-mst)# revision 1
```

### 2.29.4 show spanning-tree

| | |
|---|---|
| **Syntax** | **show spanning-tree** |
| **Parameter** | N/A |
| **Default** | N/A |
| **Mode** | Privileged EXEC |
| **Usage** | To display the spanning tree configuration, use the command spanning-tree in the Privileged EXEC mode |
| **Example** | The following example shows the spanning tree configuration.<br><br>`Switch# show spanning-tree` |

### 2.29.5 show spanning-tree interface

| | | |
|---|---|---|
| **Syntax** | **show spanning-tree interface** IF_PORTS **[statistic]** | |
| **Parameter** | **interface** IF_PORTS | An interface ID or the list of interface IDs. |
| | **statistic** | Display the STP statistic for an interface. |
| **Default** | N/A | |
| **Mode** | Privileged EXEC | |
| **Usage** | To show the STP configuration and statistics for an interface, use the command **show spanning-tree interface** in the Privileged EXEC mode. | |
| **Example** | The following example shows the STP configuration for the interface g23.<br><br>`Switch# show spanning-tree interfaces g 23`<br><br>The following example shows the STP statistic for the interface fa23.<br><br>`Switch# show spanning-tree interfaces g 23 statistic` | |

### 2.29.6 show spanning-tree mst

| | |
|---|---|
| **Syntax** | **show spanning-tree mst** instace-id |
| **Parameter** | **instance-id** The MSTP instance ID. Its valid range is from 0 to 15. |
| **Default** | N/A |
| **Mode** | Privileged EXEC |
| **Usage** | To show the information for a specific MSTP instance, use the command show **spanning-tree mst** in the Privileged EXEC mode. |
| **Example** | The following example displays the information for the MSTP instance 0 and 1 individually.<br>`Switch# show spanning-tree mst 0`<br>`Switch# show spanning-tree` |

### 2.29.7 show spanning-tree mst configuration

| | |
|---|---|
| **Syntax** | **show spanning-tree mst configuration** |
| **Parameter** | N/A |
| **Default** | N/A |
| **Mode** | Privileged EXEC |
| **Usage** | To show the global MST configuration, use the command **show spanning-tree mst configuration** in the Privileged EXEC mode. |
| **Example** | The following example shows the global MST configuration.<br>`Switch# show spanning-tree mst configuration` |

### 2.29.8 show spanning-tree mst interface

| | | |
|---|---|---|
| **Syntax** | **show spanning-tree mst** instance-id **interface** IF_PORTS | |
| **Parameter** | instance-id | The MSTP instance ID. Its valid range is from 0 to 15. |
| | **Interface IF_PORTS** | An interface ID or the list of interface IDs. |
| **Default** | N/A | |
| **Mode** | Privileged EXEC | |
| **Usage** | To show the MSTP instance information on the specific interface, use the command **show spanning-tree mst interface** in the Privileged EXEC mode. | |
| **Example** | The following example shows the MSTP 0 and 1 information individually on the interface g 23.<br><br>`Switch# show spanning-tree mst 0 interfaces g 23` | |

### 2.29.9 spanning-tree

| | |
|---|---|
| **Syntax** | **spanning-tree**<br>**no spanning-tree** |
| **Parameter** | N/A |
| **Default** | Spanning-Tree is enabled by default. |
| **Mode** | Global Configuration |
| **Usage** | To enable the spanning tree, use the command spanning-tree in the Global Configuration mode; and use the no form of the command to disable the spanning tree on the switch. |
| **Example** | The following example disables and enables the spanning tree individually.<br><br>`Switch(config)# no spanning-tree` |

### 2.29.10 spanning-tree bpdu

| | |
|---|---|
| **Syntax** | **spanning-tree bpdu (filtering\|flooding)**<br>**no spanning-tree bpdu** |
| **Parameter** | **filtering** Filter the BPDU when STP is diabled.<br>**flooding** Flood the BPDU when the STP is disabled. |
| **Default** | The default configuration is flooding. |
| **Mode** | Global Configuration |
| **Usage** | To configure the action of Bridge Protocol Data Unit (BPDU) handlring when STP is disabled, use the command spanning-tree bpdu in the Global Configuration mode. To restore the configuration to the default action, use the no form of the command. |
| **Example** | The following example configures the action of BPDU handling to fliter when the STP is disabled.<br>`Switch(config)# spanning-tree bpdu filtering` |

### 2.29.11 spanning-tree bpdu-filter

| | |
|---|---|
| **Syntax** | **spanning-tree bpdu-filter**<br>**no spanning-tree bpdu-filter** |
| **Parameter** | N/A |
| **Default** | BPDU filter is disabled. |
| **Mode** | Interface Configuration |
| **Usage** | To enable the BPDU filter, use the command spanning-tree bpdu-filter in the Interface Configuration mode; and use no form of the command to disable the BPDU filter. |
| **Example** | The following example enables the BPDU filter for interface fa1.<br>`Switch(config)# interface fa1`<br>`Switch(config-if)# spanning-tree bpdu-filter` |

### 2.29.12 spanning-tree bpdu-guard

| | |
|---|---|
| **Syntax** | **spanning-tree bpdu-guard**<br>**no spanning-tree bpdu-guard** |
| **Parameter** | N/A |
| **Default** | BPDU guard is disabled |
| **Mode** | Interface Configuration |
| **Usage** | To enable the BPDU filter, use the command spanning-tree bpdu-guard in the Interface Configuration mode; and use no form of the command to disable the BPDU filter. |
| **Example** | The following example enables the BPDU guard for interface gi1.<br>`Switch(config)# interface gi1`<br>`Switch(config-if)# spanning-tree bpdu-guard` |

### 2.29.13 spanning-tree cost

| | |
|---|---|
| **Syntax** | **spanning-tree cost** cost<br>**no spanning-tree cost** |
| **Parameter** | cost — The port path cost. For the long path cost method, its valid range is from 0 to 200000000; and the valid range is from 0 to 65535 for the short path cost method. The value 0 indicates AUTO, which the port path cost is determined by the port speed and the path cost method. |
| **Default** | The default port path cost is 0, and it is determined by the port speed and the 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 |
| **Usage** | To configure the STP path cost for an interface, use the command spanning-tree cost in the Interface Configuration mode; and use the |

no form of the command to restore it to the default configuration.

**Example** The following example configures port path cost to 30000 for interface g 2.

```
Switch(config)# interface gi1
Switch(config-if)# spanning-tree cost 30000
```

### 2.29.14 spanning-tree forward-time

**Syntax**

**spanning-tree forward-time seconds**
**no spanning-tree forward-time**

**Parameter**

| | |
|---|---|
| seconds | STP forward delay time. Its valid range is from 4 to 10 seconds. |

**Default** The default forward delay time is 15 seconds.

**Mode** Global Configuration

**Usage** To configure the STP bridge forward delay time, which is the amount of time that a port remains in the Listening and Learning states before it enters the Forwarding state, use the command spanning-tree forward-time in the Global Configuration mode. To restore it to the default configuration, use the **no** form of the command.

When the forward delay time is configured, the following relationship shold be maintained:

2 * (forward-time - 1) >= Max-Age

**Example** The following example configures STP forward delay time to 25.

```
Switch(config)# spanning-tree forward-time 25
```

### 2.29.15 spanning-tree hello-time

| | |
|---|---|
| **Syntax** | **spanning-tree hello-time** seconds<br>**no spanning-tree hello-time** |
| **Parameter** | seconds — STP hello time in second. Its valid range is from 1 to 10 seconds. |
| **Default** | The default STP hello time is 2 seconds. |
| **Mode** | Global Configuration |
| **Usage** | STP hello time is the time interval to broadcast its hello message to other bridges. To configure the STP hello time, use the command spanning-tree hello-time in the Global Configuration mode; and use the no form of the command to restore the hello time to default configuration.<br><br>When the hello time is configured, the following relationship should be maintained:<br><br>Max-Age >= 2 * (hello-time + 1) |
| **Example** | The following example configures BPDU hello time to 4.<br>`Switch(config)# spanning-tree hello-time 4` |

### 2.29.16 spanning-tree edge

| | |
|---|---|
| **Syntax** | **spanning-tree edge**<br>**no spanning-tree edge** |
| **Parameter** | N/A |
| **Default** | The default configuration is disabled. |
| **Mode** | Interface Configuration |
| **Usage** | To enable the edge mode for an interface, use the command spanning-tree edge in the Interface Configuration mode; and use the no form of the command to restore it to the default configuration. In the edge mode, the interface would be put into the Forwarding state immediately upon link up. If the edge mode is enabled for the interface and there are BPDUs received on the interface, the loop might be occurred in the short time. |
| **Example** | The following example enables the edge mode for the interface g 1.<br>`Switch(config)# interface g 1`<br>`Switch(config-if)# spanning-tree edge` |

### 2.29.17 spanning-tree link-type

| | |
|---|---|
| **Syntax** | **spanning-tree link-type (point-to-point\|shared)**<br>**no spanning-tree link-type** |
| **Parameter** | point-to-point — Specify the port link type is point to point.<br>shared — Specify the port link type is shared. |
| **Default** | The default configuration link type is **point-to-point** for the ports with full duplex configuration, and **shared** for the ports with half duplex settings. |
| **Mode** | Interface Configuration |
| **Usage** | To set the RSTP link-type for an interface, use the command spanning-tree link in the Interface Configuration mode. For the default configuration, use the no form of the command. |
| **Example** | The following example configures the link-type to point-to-point for the interface g 1.<br>`Switch(config)# interface g 1`<br>`Switch(config-if)# spanning-tree link-type point-to-point` |

### 2.29.18 spanning-tree maximum-age

| | |
|---|---|
| **Syntax** | **spanning-tree maximum-age seconds**<br>**no spanning-tree maximum-age** |
| **Parameter** | seconds — The interval in seconds for a switch to wait the configuration messages, without attempting to redefine its own configuration. |
| **Default** | The default maximum age is 20 seconds. |
| **Mode** | Global Configuration |
| **Usage** | To set the interval in seconds that the switch can wait without receiving the configuration messages, before attempting to redefine its own configuration, use the command spanning-tree maximum-age in the Global Configuratio mode. For the default configuration, use the no form of the commands.<br>When the maximum age is configured, the following relationship should be maintained:<br>2 * (forward-time - 1)>= Max-Age >= 2 * (hello-time + 1) |

| | |
|---|---|
| **Example** | The following example configures STP maximum age to 10.<br><br>`Switch(config)# spanning-tree maximum-age 10` |

### 2.29.19 spanning-tree mcheck

| | |
|---|---|
| **Syntax** | **spanning-tree mecheck** |
| **Parameter** | N/A |
| **Default** | N/A |
| **Mode** | Interface Configuration |
| **Usage** | To restart the Spanning Tree Protocol (STP) migration process (re-negotiate forcely with its neighborhood) on the specific interface, use the command spanning-tree mcheck in the Interface Configuration mode |
| **Example** | The following example restarts the STP negotiation on the interface g 1.<br><br>`Switch(config)# interface g 1`<br>`Switch(config-if)# spanning-tree mecheck` |

### 2.29.20 spanning-tree mode

| | |
|---|---|
| **Syntax** | **spanning-tree mode (mstp\|rstp\|stp)**<br>**no spanning-tree force-version** |
| **Parameter** | mstp — Enable the Multiple Spanning Tree (MSTP) operation.<br>rstp — Enable the Rapid Spanning Tree (RSTP) operation.<br>stp — Enable the Spanning Tree (STP) operation. |
| **Default** | The default mode is rstp. |
| **Mode** | Global Configuration |
| **Usage** | To specify the spanning tree operation mode, use the command of spanning- tree mode in the Global Configuration mode. For the default configuration, use the command no spanning-tree force-version in the Global Configuration mode.<br><br>When the switch is configured as MSTP mode, it can use STP and RSTP for the backward compatibility with switches working in STP and RSTP mode individually. For the RSTP configuration, the switch can also use STP for the switches working in the STP operation. |
| **Example** | The following example sets the STP operation to MSTP.<br><br>`Switch(config)# spanning-tree mode mstp` |

### 2.29.21 spanning-tree mst configuration

| | |
|---|---|
| **Syntax** | **spanning-tree mst configuration** |
| **Parameter** | N/A |
| **Default** | N/A |
| **Mode** | Global Configuration |
| **Usage** | To enter the MST configuration mode for the MSTP configuration modification, use the command spanning-tree mst configuration in the Global Configuration mode. |
| **Example** | The following example modifies the MSTP configuration in the MST Configuration mode. |

```
Switch(config)# spanning-tree mst configuration
Switch(config-mst)# instance 1 vlan 10-20
Switch(config-mst)# name fiberroad
Switch(config-mst)# revision 1
```

### 2.29.22 spanning-tree mst cost

| | |
|---|---|
| **Syntax** | **spanning-tree mst** instance-id **cost** cost<br>**no spanning-tree mst** instance-id **cost** cost |

**Parameter**

| | |
|---|---|
| instance-id | Specify the instance ID. The valid range is from 0 to 15. |
| cost | Specify the path cost for the interfaces on the specific MSTP instance. For the long path cost method, its valid range is from 0 to 200000000; and the valid range is from 0 to 65535 for the short path cost method. The value 0 indicates AUTO, which the port path cost is determined by the port speed and the path cost method. |

**Default** The default port path cost is 0, and it is determined by the port speed and the 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 |
| **Usage** | To configure the path cost for MSTP calculations, use the command spanning-tree mst cost in the Interface Configuration mode. If the loop occurs, the MSTP considers the path cost when selecting the interface into the Forwarding state. For the default configuration, use the no form of the command.<br>When configuring the path cost on the CIST (instance 0), it is equal to the command spanning-tree cost in the Interface Configuration mode. |
| **Example** | The following example configures the path cost of interface fa1 on the instance 1 to 30000<br><br>`Switch(config)# interface gi1`<br>`Switch(config-if)# spanning-tree mst 1 cost 30000` |

### 2.29.23 spanning-tree mst port-priority

| | |
|---|---|
| **Syntax** | **spanning-tree mst** instance-id **port-priority** priority<br>**no spanning-tree mst** instance-id **port-priority** |
| **Parameter** | instance-id — Specify the instance ID. The valid range is from 0 to 15.<br>priority — Specify the interface priority on the specific instance. |
| **Default** | The default port priority on each instance is 128 |
| **Mode** | Interface Configuration |
| **Usage** | To configure the interface priority on the specific instances, use the command spanning-tree mst port-priority in the Interface Configuration mode. For the default configuration, use the no form of the command.<br><br>The priority value must be the multiple of 16. When the port priority on the CIST (instance 0) is configured, it is equal to the command spanning-tree port-priority in the Interface Configuration mode. |
| **Example** | The following example sets the port priority of gi1 on the instance 1 to 144; and set the port priority of gi1 on the CIST (instance 0) to 96<br><br>`Switch(config)# interface gi1`<br>`Switch(config-if)# spanning-tree mst 1 port-priority 144`<br>`Switch(config-if)# spanning-tree mst 0 port-priority 96` |

### 2.29.24 spanning-tree mst priority

| | |
|---|---|
| **Syntax** | **spanning-tree mst instance** instance-id **priority** priority<br>**no spanning-tree mst instance** instance-id **priority** |
| **Parameter** | instance-id: Specify the instance ID. The valid range is from 0 to 15.<br>priority: Specify the bridge priority on the specific instance. The valid range is from 0 to 61440. It nsures the probility that the switch is selected as the root bridge, and the lower values has the higher priority for the switch to be selected as the root bridge. |
| **Default** | The default priority on each instance is 32768. |
| **Mode** | Global Configuration |
| **Usage** | To configure the bridge priority on the specific instance, use the command spanning-tree mst priority in the Global Configuration mode. To restore the default configuration, use the no form of the command.<br><br>The value of bridge priority must be the multiple of 4096. A switch with the lowest priority is the root of the STP topology. For the configuration of bridge priority on the CIST (instance 0), it is equal to the command spanning-tree priority in the Global Configuration mode. |
| **Example** | The following example modifies the bridge priority to 4096 on instance 0 and instance 1 individually.<br><br>`Switch(config)# spanning-tree mst 0 priority 4096`<br>`Switch(config)# spanning-tree mst 1 priority 4096` |

### 2.29.25 spanning-tree pathcost method

| | |
|---|---|
| **Syntax** | **spanning-tree pathcost method (long\|short)** |
| **Parameter** | long — The range for the path cost is from 1 to 200000000.<br>short — The range for the path cost is from 1 to 65535. |
| **Default** | The default path cost method is long. |
| **Mode** | Global Configuration |
| **Usage** | To set the spanning tree path cost method, use the command **spanning-tree pathcost method** in the Global Configuration mode.<br><br>If the short method is specified, the switch calculates the path cost in the range 1 throuth 65535; Otherwise, it calculates the path cost in the range 1 to 200000000. |
| **Example** | The following example modifies path cost method to short.<br><br>`Switch(config)# spanning-tree pathcost method short` |

### 2.29.26 spanning-tree port-priority

| | |
|---|---|
| **Syntax** | **spanning-tree port-priority priority**<br>**no spanning-tree port-priority priority** |
| **Parameter** | priority — Specify the priority for an interface. The valid range is from 0 to 240. |
| **Default** | The default priority for each interface is 128. |
| **Mode** | Interface Configuration |
| **Usage** | To configure the STP priority for an interface, use the command spanning- tree port-priority in the Interface Configuration mode. For the default configuration, use the no form of the command.<br><br>The priority value must be the multiple of 16. |
| **Example** | The following example modifies the port priority to 96 for the interface gi2 .<br><br>`Switch(config)# interface gi2`<br>`Switch(config-if)# spanning-tree port-priority 96` |

### 2.29.27 spanning-tree priority

| | |
|---|---|
| **Syntax** | **spanning-tree priority priority**<br>**no spanning-tree priority** |
| **Parameter** | instance-id — Specify the instance ID. The valid range is from 0 to 15.<br>priority — Specify the bridge STP priority. The valid range is from 0 to 61440. It nsures the probility that the switch is selected as the root bridge, and the lower values has the higher priority for the switch to be selected as the root bridge of SFP topology |
| **Default** | The default priority for the switch 32768. |
| **Mode** | Global Configuration |
| **Usage** | To configure the bridge priority, use the command **spanning-tree mst priority** in the Global Configuration mode. To restore the default configuration, use the no form of the command.<br><br>The value of bridge priority must be the multiple of 4096. A switch with the lowest priority is the root of the STP topology. When swithes with the same priority configuration in the environment, the switch with lowest MAC address would be selected as the root bridge. |
| **Example** | The following example modifies the bridge priority to 4096.<br><br>`Switch(config)# spanning-tree priority 4096` |

### 2.29.28 spanning-tree tx-hold-count

| | |
|---|---|
| **Syntax** | **spanning-tree tx-hold-count count**<br>**no spanning-tree tx-hold-count** |
| **Parameter** | count — Specify the tx-hold-count used to limit the maximum numbers of packets transmission per second. The valid range is from 1 to 10. |
| **Default** | The default value is 6. |
| **Mode** | Global Configuration |
| **Usage** | To limit the maximum numbers of packets transmission per second, use the command spanning-tree tx-hold-count in the Global Configuration mode. For the default configuration, use the no form of the command. |
| **Example** | The following example sets the tx-hold-count to 4.<br><br>`Switch(config)# spanning-tree tx-hold-count 4` |

## 2.30 Storm Control

### 2.30.1 show storm-control

| | |
|---|---|
| **Syntax** | **show storm-control**<br>**show storm-control interface IF_PORTS** |
| **Parameter** | IF_PORTS Specify port to show. |
| **Default** | No default value for this command |
| **Mode** | Privileged EXEC |
| **Usage** | Use "**show storm-control**" command to show all storm control related configurations including global configuration and per port configurations.<br><br>Use "**show storm-control interface**" command to show selected port storm control configurations. |
| **Example** | This example shows how to show storm control global configuration.<br>`Switch# show storm-control` |

```
Switch# show storm-control
  Storm control preamble and IFG: Excluded
  Storm control unit: bps

  Port    | State |  Broadcast  |  Unkown-Multicast  | Unknown-Unicast |   Action
          |       |     kbps    |        kbps        |      kbps       |
----------+-------+-------------+--------------------+-----------------+-----------
  gi1       disable Off(  10000)   Off(  10000)         Off(  10000)          Drop
  gi2       disable Off(  10000)   Off(  10000)         Off(  10000)          Drop
  gi3       disable Off(  10000)   Off(  10000)         Off(  10000)          Drop
```

### 2.30.2 storm-control

**Syntax**

**storm-control**
**no storm-control**

**storm-control (broadcast | unknown-unicast | unknown-multicast)**
**no storm-control (broadcast | unknown-unicast | unknown-multicast)**

**Parameter**

| | |
|---|---|
| broadcast | Select broadcast storm control type |
| unknown-unicast | Select unknown unicast storm control type |
| unknown-multicast | Select unknown multicast storm control type |

**Default**

Default storm control is disabled.
Default broadcast storm control is disabled.
Default unknown multicast storm control is disabled
Default unknown unicast storm control is disabled

**Mode**

Interface Configuration

**Usage**

Storm control function is able to enable/disable on each single port. Use the "**storm control**" command to enable storm control feature on the selected ports. And use "**no storm control**" command to disable storm control feature. Not only port is able to enable/disable on the port. Each storm control type is also able to enable/disable on each single port.

Use the "**storm-control (broadcast|unknown-unicast|unknown-multicast**)" command to enable the storm control type you need and use no form to disable it.

**Example**

This example shows how to enable storm control on interface gi1.

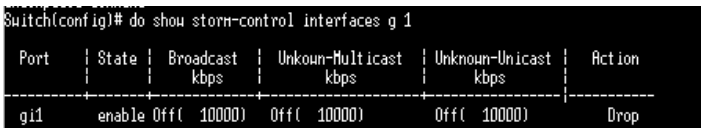
```
Switch(config)# interface gi1
Switch(config-if)# storm-control
```

This example shows how to enable broadcast storm control and configure broadcast storm control rate to 200.

```
Switch(config)# interface gi1
Switch(config-if)# storm-control broadcast
```

This example shows how to show current storm control configuration on interface gi1

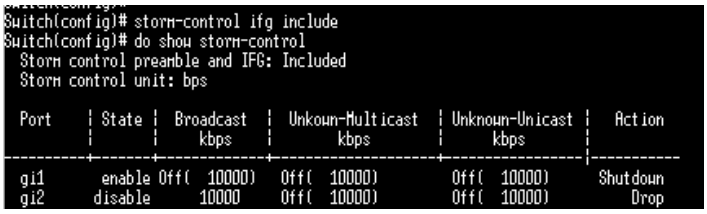
```
Switch# show storm-control interfaces gi1
```




### 3.30.3 storm-control action

| | |
|---|---|
| **Syntax** | **storm-control action (drop \| shutdown)**<br>**no storm-control action** |
| **Parameter** | drop Storm control rate calculates by octet-based<br>shutdown |
| **Default** | Default storm control action is drop. |
| **Mode** | Interface Configuration |
| **Usage** | Use "**storm-control action**" command to set the action when the received storm control packets exceed the maximum rate on an interface. Use **no** form to restore to default action. |
| **Example** | This example shows how to configure storm control action to shutdown port on interface gi1.<br>`Switch(config)# interface gi1`<br>`Switch(config-if)# storm-control action shutdown`<br><br>This example shows how to show storm control action on interface gi1.<br>`Switch# show storm-control interfaces gi1` |

### 2.30.4 storm-control ifg

| | | |
|---|---|---|
| **Syntax** | **storm-control ifg (include \| exclude)** | |
| **Parameter** | include | Include preamble & IFG (20 bytes) when count ingress storm control rate. |
| | exclude | Exclude preamble & IFG (20 bytes) when count ingress storm control rate |
| **Default** | Default storm control inter frame gap is excluded. | |
| **Mode** | Global Configuration | |
| **Usage** | Storm control mechanism will try to calculate ingress packets is exceed configured rate or not and do corresponding action.<br><br>Use storm-control ifg command to include/exclude the preamble and inter frame gap into the calculating. | |
| **Example** | This example shows how to configure storm inter frame gap to include.<br>`Switch(config)# storm-control ifg include`<br><br>This example shows how to show storm control global configuration.<br>`Switch# show storm-control`<br>  | |

```
Switch(config)# storm-control ifg include
Switch(config)# do show storm-control
  Storm control preamble and IFG: Included
  Storm control unit: bps

  Port     | State |  Broadcast  |  Unkown-Multicast  | Unknown-Unicast |   Action
           |       |     kbps    |        kbps        |      kbps       |
-----------+-------+-------------+--------------------+-----------------+-----------
  gi1        enable Off(  10000)   Off(  10000)         Off(  10000)      Shutdown
  gi2       disable      10000     Off(  10000)         Off(  10000)          Drop
```

### 2.30.5 storm-control level

| | |
|---|---|
| **Syntax** | **storm-control (broadcast \| unknown-unicast \| unknown-multicast) level<1-1000000>**<br>**no storm-control (broadcast \| unknown-unicast \| unknown multicast) level** |

**Parameter**

| | |
|---|---|
| broadcast | Select broadcast storm control type |
| unknown-unicast | Select unknown unicast storm control type |
| unknown-multicast | Select unknown multicast storm control type |
| **level** <1-1000000> | Specify the storm control rate for selected type.<br>For bps, range is 16-1000000<br>For pps, range is 1-262143 |

| | |
|---|---|
| **Default** | Default broadcast storm control rate is 10000.<br>Default unknown multicast storm control rate is 10000.<br>Default unknown unicast storm control rate is 10000. |
| **Mode** | Interface Configuration |
| **Usage** | Each control type is allowed to have different storm control rate.<br><br>Use **"storm-control (broadcast\|unknown-unicast\|unknown-multicast) level"** command to configure it<br><br>Use no form to restore to default rate. |

**Example**

This example shows how to enable broadcast storm control and configure broadcast storm control rate to 200.

```
Switch(config)# interface gi1
Switch(config-if)# storm-control broadcast
Switch(config-if)# storm-control broadcast level 200
```

This example shows how to show current storm control configuration on interface gi1

```
Switch# show storm-control interfaces gi1
```

```
Switch(config-if-gi1)# storm-control broadcast level 200
Switch(config-if-gi1)# exit
Switch(config)# eixt
Incomplete command
Switch(config)# show storm-control int g 1

 Port     | State |  Broadcast  |  Unkown-Multicast  | Unknown-Unicast |   Action
          |       |     kbps    |        kbps        |      kbps       |
----------+-------+-------------+--------------------+-----------------+----------
 gi1        enable       208      Off(  10000)         Off(  10000)      Shutdown
```

### 2.30.6 storm-control unit

| | |
|---|---|
| **Syntax** | **storm-control unit (bps \| pps)** |
| **Parameter** | bps — Storm control rate calculates by octet-based<br>pps — Storm control rate calculates by packet-based |
| **Default** | Default storm control unit is bps. |
| **Mode** | Global Configuration |
| **Usage** | Storm control mechanism will try to calculate ingress packets is exceed configured rate or not and do corresponding action.<br><br>Use **storm-control unit** command to change the unit of calculating method. |
| **Example** | This example shows how to configure storm control rate unit as pps.<br>`Switch(config)# storm-control unit pps`<br><br>This example shows how to show storm control global configuration.<br>`Switch# show storm-control` |

# 2.31 System File

## 2.31.1 boot system

| | |
|---|---|
| **Syntax** | **boot system (image0 \| image1)** |
| **Parameter** | image0 Boot from flash image partition 0<br>image1 Boot from flash image partition 1 |
| **Default** | Default boot image is image. |
| **Mode** | Global Configuration |
| **Usage** | Dual image allow user to have a backup image in the flash partition. Use **"boot system"** command to select the active firmware image. And another firmware image will become a backup one. |
| **Example** | This example shows how to select image1 as active image.<br>`Switch(config)# boot system image1`<br>`Select "image1" Success`<br><br>This example shows how to show active image partition.<br>Switch# **show flash** |

## 2.31.2 copy

| | |
|---|---|
| **Syntax** | **copy (flash:// \| tftp://) (flash:// \| tftp://)**<br>**copy tftp:// (backup-config \| running-config \| startup-config)**<br>**copy (backup-config \| running-config \| startup-config) tftp://**<br><br>**copy (backup-config \| startup-config) running-config copy (backup-config \| running-config) startup-config copy (running-config \| startup-config) backup-config** |
| **flash://** | Specify the file stored in flash to operation.<br>Available files are:<br>flash://startup-config<br>flash://backup-config<br>flash://rsa1<br>flash://rsa2<br>flash://dsa2<br>flash://image0<br>flash://image1<br>flash://ram.log<br>flash://flash.log |

| | | |
|---|---|---|
| **Parameter** | **tftp://** | Specify remote tftp server and remote file name. The format is "tftp://192.168.1.111/remote_file_name" |
| | **running-config** | Running configuration file |
| | **startup-config** | Startup configuration file |
| | **backup-config** | Backup configuration file |

**Default** No default value for this command.

**Mode** Privileged EXEC

**Usage** There are many types of files in system. These files are very important for administrator to manage the switch. The most common file operation is copy. By using these copy commands, we can upgrade, backup following type of files.

- Firmware Image
- Configuration Files
- Syslog Files
- Language Files
- Security Certificate

**Example** This example shows how to copy running configuration to startup configuration.

```
Switch# copy running-config startupst-config
```

This example shows how to backup running configuration to remote tftp server 192.168.111 with file name test1.cfg.

```
Switch# copy running-config tftp://192.168.1.111/
        test1.cfg
Uploading file...Please Wait... Uploading Done
```

This example shows how to upgrade startup configuration from remote tftp server 192.168.1.111 with file name test2.cfg.

```
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
```

This example shows how to backup security file dsa2 to remote tftp server 192.168.1.111 with file name dsa2.

```
Switch# copy flash://dsa2 tftp://192.168.1.111/dsa2
```

```
Uploading file...Please Wait...
Uploading Done
```

### 2.31.3 delete

| | |
|---|---|
| **Syntax** | **delete (startrup-config \| backup-config \| flash://)**<br>**delete system (image0 \| image1)** |
| **Parameter** | **flash://** Specify the configuration file stored in flash to delete. Available files are:<br>flash://startup-config<br>flash://backup-config<br>**startup-config** Delete startup configuration file<br>**backup-config** Delete backup configuration file<br>**image0** Delete flash image0.<br>**image1** Delete flash image1. |
| **Default** | No default value for this command. |
| **Mode** | Privileged EXEC |
| **Usage** | Use "**delete**" command to delete configuration files or use "delete system" command to delete firmware image stored in flash.<br>The "**delete startup-config**" command is using to restore factory default and it is equal to command "**restore-defaults**". |
| **Example** | This example shows how to delete backup configuration file.<br>`Switch# delete backup-config`<br><br>This example shows how to delete backup firmware image from flash.<br>`Switch# delete system image1`<br><br>This example shows how to show file status in flash.<br>`Switch# show flash` |

### 2.31.4 restore-defaults

| | |
|---|---|
| **Syntax** | **restore-defaults [interfaces** IF_PORTS**]** |
| **Parameter** | **interfaces IF_PORTS** — Specify port to restore its' ruuning config |
| **Default** | No default value for this command. |
| **Mode** | Privileged EXEC |
| **Usage** | Use "restore-defaults" command to restore factory default of all system. The command is equal to "delete startup-config", |
| **Example** | This example shows how to restore factory defaults.<br>`Switch# restore-defaults` |

### 2.31.5 save

| | |
|---|---|
| **Syntax** | **save** |
| **Parameter** | N/A |
| **Default** | No default value for this command. |
| **Mode** | Privileged EXEC |
| **Usage** | Privileged EXEC |
| **Example** | Use "**save**" command to save running configuration to startup configuration file. This command is equal to "**copy running-config startup-config**".<br><br>`Switch# save` |

### 2.31.6 show bootvar

| | |
|---|---|
| **Syntax** | **show bootvar** |
| **Parameter** | N/A |
| **Default** | No default value for this command. |
| **Mode** | Privileged EXEC |
| **Usage** | Use "**show bootvar**" command to show image information in both flash partitions. It also shows current active image and active image on next booting |
| **Example** | This example shows how to show dual image information<br>Switch# show bootvar |

### 2.31.7 show config

| | | |
|---|---|---|
| **Syntax** | **show (running-config \| startrup-config \| backup-config)**<br>**show running-config interfaces** *IF_PORTS* | |
| **Parameter** | **running-config** | Show running configuration on terminal |
| | **startup-config** | Show startup configuration on terminal |
| | **backup-config** | Show backup configuration on terminal |
| | IF_PORTS | Specify port to show its' ruuning config |
| **Default** | No default value for this command. | |
| **Mode** | Privileged EXEC | |
| **Usage** | Our configuration file is text based. Therefore, we can show the configuration on terminal and read it by this command.<br>Use "**show config**" command to show configuration files stored in system. Use "**show config interfaces**" command to show specific port configurations. | |
| **Example** | This example shows how to show startup configuration<br>`Switch# show startup-config`<br><br>This example shows how to show running configuration<br>`Switch# show running-config`<br><br>This example shows how to display running configuraiton on specific port.<br>`Switch# show running-config interfaces gi1` | |

### 2.31.8 show flash

| | |
|---|---|
| **Syntax** | **show flash** |
| **Parameter** | N/A |
| **Default** | No default value for this command. |
| **Mode** | Privileged EXEC |
| **Usage** | Use "**show flash**" command to show all files' status which stored in flash. |
| **Example** | This example shows how to show all files status stored in flash.<br>`Switch# show flash` |

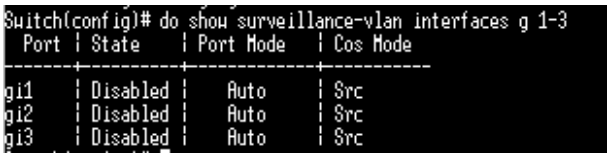
## 2.32 Surveillance VLAN

### 2.32.1 surveillance-vlan(Global)

| | |
|---|---|
| **Syntax** | **surveillance-vlan**<br>**no surveillance -vlan** |
| **Parameter** | N/A |
| **Default** | Surveillance VLAN is disabled |
| **Mode** | Global Configuration |
| **Usage** | Use the **surveillance vlan** global configuration command to enable the functional Surveillance VLAN on the device.<br>Use the no form of this command to disable Surveillance VLAN function. You can verify your setting by entering the **show surveillance vlan Privileged EXEC** command. |
| **Example** | The following example shows how to enable Surveillance VLAN.<br>`Switch(config)# surveillance -vlan`<br>`Switch# show surveillance -vlan`<br>  |

```
Switch(config)# surveillance-vlan
  <cr>
  aging-time  Surveillance VLAN aging time settings
  cos         Surveillance VLAN Class Of Service settings
  oui-table   OUI-Table configuration
  vlan        VLAN configuration
Switch(config)# surveillance-vlan
A Default VLAN can not be configured as Surveillance VLAN
Switch(config)# do show surveillance-vlan
Administrate Surveillance VLAN state   : disabled
Surveillance VLAN ID       : none (disable)
Surveillance VLAN Aging    : 1440 minutes
Surveillance VLAN CoS      : 6
Surveillance VLAN 1p Remark: disabled

OUI table
  OUI MAC   |  Description
------------+---------------
```

### 2.32.2 surveillance-vlan(Interface)

| | |
|---|---|
| **Syntax** | **surveillance-vlan**<br>**no surveillance-vlan** |
| **Parameter** | N/A |
| **Default** | Disable by default. |
| **Mode** | Interface Configuration |
| **Usage** | Use the **surveillance vlan** Interface configuration command to enable OUI surveillance VLAN configuration on an interface<br>Use the **no** form of this command to disable Surveillance VLAN on an interfaces<br>You can verify your setting by entering the **show surveillance vlan** Privileged EXEC command |
| **Example** | The following example how to enable Surveillance VLAN function in oui mode on an interface<br>`Switch(config)#interface range g 1-3`<br>`Switch(config-if)#surveillance-vlan`<br>`Switch# show surveillance-vlan interfaces g 1-3`<br>  |

```
Switch(config)# do show surveillance-vlan interfaces g 1-3
  Port | State    | Port Mode   | Cos Mode
-------+----------+-------------+----------
gi1    | Disabled |    Auto     | Src
gi2    | Disabled |    Auto     | Src
gi3    | Disabled |    Auto     | Src
```

### 2.32.3 surveillance-vlan vlan

| | |
|---|---|
| **Syntax** | **surveillance-vlan vlan <1-4094>**<br>**no surveillance-vlan vlan** |
| **Parameter** | <1-4094> Specify the Surveillance VLAN ID |
| **Default** | The default Surveillance VLAN ID is None. |
| **Mode** | Global Configuration |
| **Usage** | Use the **surveillance vlan** id global configuration command to configure the VLAN identifier of the surveillance VLAN statically. Use the **no** form of this command to restore surveillance VLAN id to default. You can verify your setting by entering the **show surveillance vlan Privileged EXEC** command |
| **Example** | The following example shows how to set Surveillance VLAN id. The VLAN id must be created first.<br>`Switch(config)# surveillance-vlan vlan 128`<br>`Switch# show surveillance-vlan` |

### 2.32.4 surveillance-vlan oui-table

| | |
|---|---|
| **Syntax** | **surveillance-vlan oui-table** A:B:C [DESCRIPTION]<br>**no surveillance-vlan oui-table** [A:B:C] |
| **Parameter** | **A:B:C** Specify OUI Mac address to add or remove<br>**startup-config** Specify description of the specified MAC address to the surveillance VLAN OUI table |
| **Default** | Default has no pre-defined OUI. |
| **Mode** | Global Configuration |
| **Usage** | Use the **surveillance vlan oui-table** global configuration command to add OUI mac address to OUI Table<br>Use the **no** form of this command to remove all or specified OUI mac address.<br>You can verify your setting by entering the show surveillance vlan Privileged EXEC command |
| **Example** | This following example shows how to add OUI Mac.<br>`Switch(config)# surveillance-vlan oui-table 00:01:02 "Test"`<br>`Switch# show surveillance-vlan interfaces g 1-3` |

### 2.32.5 surveillance-vlan cos (Global)

| | |
|---|---|
| **Syntax** | **surveillance-vlan cos** <0-7> [remark]<br>**no surveillance-vlan cos** |
| **Parameter** | <0-7> — Specify the surveillance VLAN Class of Service value in telephone OUI mode<br>remark — Specify that the L2 user priority is remarked with the CoS value |
| **Default** | The default cos value is 6, remark is disabled. |
| **Mode** | Global Configuration |
| **Usage** | Use the **surveillance vlan cos** global configurations command to configure the surveillance VLAN cos value and 1p remark function. Use the "**no**" form to restore to default mode.<br>You can verify your setting by entering the **show surveillance vlan** Privileged EXEC command |
| **Example** | The following example show how to set cos value and enable 1p remark function<br>`Switch(config)# surveillance-vlan cos 7 remark`<br>`Switch# show surveillance-vlan` |

### 2.32.6 surveillance-vlan cos (Interface)

| | |
|---|---|
| **Syntax** | **surveillance-vlan cos ( src \| all )**<br>**no surveillance-vlan cos** |
| **Parameter** | src — Specify QoS attributes are applied to packets with OUIs in the source MAC address.<br>All — Specify QoS attributes are applied to packets that are classified to the Surveillance VLAN. |
| **Default** | The default all port in Src mode. |
| **Mode** | Global Configuration |
| **Usage** | Use the surveillance vlan cos mode Interface configuration command to configure OUI surveillance VLAN cos mode configuration on an interface. Use the "no" form to restore to default mode.<br>You can verify your setting by entering the show surveillance-vlan interfaces Privileged EXEC command |
| **Example** | The following example how to configure surveillance packet QoS attributes on an interface |

```
Switch(config)#interface range g 1-3
Switch(config-if)#surveillance-vlan cos all
Switch# show surveillance-vlan interfaces g 1-3
Switch# show surveillance-vlan
```

### 2.32.7 surveillance-vlan mode

| | |
|---|---|
| **Syntax** | **surveillance-vlan**<br>**mode (auto\|manual)**<br>**no surveillance-vlan mode** |
| **Parameter** | **auto** — Specifies that the port is identified as a candidate to join the surveillance VLAN. When a packet with a source OUI MAC address that identifies the remote equipment as surveillance equipment is seen on the port, the port joins the surveillance VLAN as a tagged port.<br>**manual** — Specifies that the port is manually assigned to the surveillance VLAN. |
| **Default** | The default is auto mode. |
| **Mode** | Interface Configuration |
| **Usage** | Use the **surveillance-vlan mode** global configuration command to configure the surveillance VLAN mode for interface.<br>Use the "**no**" form to restore to default mode.<br>You can verify your setting by entering the **show surveillance-vlan interfaces** Privileged EXEC command. |
| **Example** | The following example how to configure surveillance mode to manual<br>`Switch(config)#interface range fa1-3`<br>`Switch(config-if)#surveillance-vlan mode manaul`<br>`Switch# show surveillance-vlan interfaces g 1-3` |

### 2.32.8 surveillance-vlan aging-time

| | |
|---|---|
| **Syntax** | **surveillance-vlan aing-time <30-65536>**<br>**no surveillance-vlan aing-time** |
| **Parameter** | **<30-65536>** Specify the Surveillance VLAN aging timeout interval in minutes |
| **Default** | The default aging-timeout value is 1440 minutes |
| **Mode** | Global Configuration |
| **Usage** | Use the **surveillance vlan aging-time** global configuration command to configure the surveillance VLAN aging timeout.<br>Use the "**no**" form to restore to default time.<br>You can verify your setting by entering the **show surveillance vlan** Privileged EXEC command |
| **Example** | The following example shows how to set aging time.<br>`Switch(config)# surveillance-vlan aging-time 720`<br>`Switch# show surveillance-vlan`<br>`Switch(config)# do show surveillance-vlan`<br>`Administrate Surveillance VLAN state : disabled`<br>`Surveillance VLAN ID : none (disable)`<br>`Surveillance VLAN Aging : 720 minutes`<br>`Surveillance VLAN CoS : 6`<br>`Surveillance VLAN 1p Remark: disabled` |

### 2.32.9 show surveillance-vlan

| | |
|---|---|
| **Syntax** | **show surveillance-vlan**<br>**show surveillance-vlan interfaces** [IF_PORTS] |
| **Parameter** | **IF_PORTS** Specifies interfaces to display surveillance VLAN settings in OUI mode |
| **Default** | N/A |
| **Mode** | Privileged EXEC |
| **Usage** | Use the **show surveillance vlan** command in EXEC mode to display the surveillance VLAN status for all interfaces or for a specific interface if the surveillance VLAN type is OUI |
| **Example** | The following example show how to display surveillance vlan OUI mode settings<br>`Switch# show surveillance-vlan` |

# 2.33 Time

## 2.33.1 clock set

| | |
|---|---|
| **Syntax** | **clock set HH:MM:SS (jan \|feb \|mar \|apr \|may \|jun \|jul \|aug \|sep\|oct\|nov\|dec) <1-31> <2000-2035>** |
| **Parameter** | **H:MM:SS** — Specify static time of year, month, day, hour, minute, second<br>**(jan\|feb\|mar\|apr \|may\|jun\|jul\|aug\| sep\|oct\|nov\|dec)** — Specify static time of year, month, day, hour, minute, second<br>**<1-31>** — Specify static time of year, month, day, hour, minute, second<br>**<2000-2035>** — Specify static time of year, month, day, hour, minute, second |
| **Default** | No default is defined.<br>The clock set to 2000/01/01 08:00:00 by default at startup. |
| **Mode** | Privileged EXEC |
| **Usage** | Use the clock set command to set static time. The static time won't save to configuration file.<br>You can verify your setting by entering the show clock Privileged EXEC command. |
| **Example** | The example shows how to set static time of switch.<br>`switch# clock set 11:03:00 sep 21 2012`<br><br>`switch# show clock` |

## 2.33.2 clock timezone

| | |
|---|---|
| **Syntax** | **clock timezone ACRONYM HOUR-OFFSET [minutes <0-59>]**<br>**no clock timezone** |
| **Parameter** | **ACRONYM** — Specify acronym name of time zone<br>**HOUR-OFFSET** — Specify hour offset of time zone<br>**Minutes <1-59>** — Specify minute offset of time zone |
| **Default** | Default time zone is UTC+8. |
| **Mode** | Global Configuration |
| **Usage** | Use the clock timezone command to set timezone setting.<br>Use the **no** form of this command to restore to default setting.<br>You can verify your setting by entering the **show clock detail** Privileged EXEC command. |
| **Example** | The example shows how to set time zone of switch and then restore to default time zone.<br>`switch(config)# clock timezone test +5`<br>`switch(config)# show clock detail` |

### 2.33.3 clock source

| | |
|---|---|
| **Syntax** | **clock source (local\|sntp)** |
| **Parameter** | **local** Specify to use static time<br>**sntp** Specify to use sntp time |
| **Default** | Default is using local time. |
| **Mode** | Global Configuration |
| **Usage** | Use the clock source command to set the source of time.<br>Use the no form of this command to restore to default setting.<br>You can verify your setting by entering the show clock detail Privileged EXEC command. |
| **Example** | The example shows how to set clock source of switch.<br>`switch(config)# clock source sntp`<br>`switch(config)# show clock detail` |

### 2.33.4 clock summer-time

| | |
|---|---|
| **Syntax** | **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>]**<br>**clock summer-time ACRONYM recurring (usa\|eu) [<1-1440>]**<br>**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>]**<br>**no clock summer-time** |
| | **ACRONYM** Specify acronym name of time zone |
| | **(jan\|feb\|mar\|apr\|may\|jun\|jul\|aug\|sep\|oct\|nov\|dec) <1-31><2000-2037> HH:MM** Specify non-recurring daylight saving time duration. |
| | **(jan\|feb\|mar\|apr\|may\|jun\|jul\|aug\|sep\|oct\|nov\|dec) <1-31> <2000-2037> HH:MM** |

| | | |
|---|---|---|
| **Parameter** | **<1-1440>** | Specify adjust offset of daylight saving time |
| | **usa** | Using daylight saving time in the United States that starts on the second Sunday of March and ends on the first Sunday of November |
| | **eu** | Using daylight saving time in the Europe that starts on the last Sunday in March and ending on the last Sunday in October |
| | **(<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** | Specify ecurring daylight saving time duration. |
| **Default** | No default daylight saving time is defined. | |
| **Mode** | Global Configuration | |
| **Usage** | Use the **clock summer-time** command to set daylight saving time for system time. The "**usa**" or "**eu**" means that use the global daylight saving policy which defined by international organization. In both the "**date**"and "**recurring**", the first part of the command specifies when summer time begins, and the second part specifies when it ends. All times are relative to the local time zone. The "**recurring**" means that adjust time every year within the month. Use the no form of this command to default setting.<br>You can verify your setting by entering the **show clock detail** Privileged EXEC command. | |
| **Example** | The example shows how to set clock summer time of switch. You can verify settings by the following show show clock command.<br><br>`switch(config)# clock summer-time test recurring usa`<br>`switch(config)# show clock detail` | |

### 2.33.5 show clock

| | |
|---|---|
| **Syntax** | **show clock [detail]** |
| **Parameter** | **detail** Show more detail information of clock |
| **Default** | No default is defined |
| **Mode** | Privileged EXEC |
| **Usage** | Use the **show clock** command to show clock of switch. The "**detail**" means that show more information of clock such as time zone and daylight saving time. |
| **Example** | The example shows how to show clock of switch and detail information. |

```
Switch(config)# clock source sntp
Switch(config)# clock summer-time DLS recurring usa
Switch(config)# sntp host 192.168.1.100
Switch(config)# show clock

Switch(config)# show clock detail
```

### 2.33.6 sntp

| | |
|---|---|
| **Syntax** | **sntp host HOSTNAME [port <1-65535>]**<br>**no sntp** |
| **Parameter** | **HOSTNAME** Specify ip address or hostname of sntp server<br>**sntp** Specify server port of sntp server |
| **Default** | No default SNTP server defined. Default server port is 123 when server created. |
| **Mode** | Global Configuration |
| **Usage** | Use the sntp command to set remote SNTP server. Use the no form of this command to default setting.<br>You can verify your setting by entering the **show sntp** Privileged EXEC command. |
| **Example** | The example shows how to set remote SNTP server of switch. |

```
switch(config)# clock source sntp
switch(config)# sntp host 192.168.1.100
switch(config)# show sntp
```

```
Switch(config)# do show sntp
SNTP is Enabled
SNTP Server address: 192.168.1.100
SNTP Server port: 123
```

### 2.33.7 show sntp

| | |
|---|---|
| **Syntax** | **show sntp** |
| **Parameter** | None |
| **Default** | No default is defined |
| **Mode** | Privileged EXEC |
| **Usage** | Use the show sntp command to remote SNTP server information. |
| **Example** | The example shows how to show remote SNTP server.<br>Switch (config)# show sntp |

## 2.34 UDLD

### 2.34.1 errdisable recovery cause udld

| | |
|---|---|
| **Syntax** | **errdisable recovery cause udld**<br>**no errdisable recovery cause udld** |
| **Parameter** | N/A |
| **Default** | Error disable auto recovery is disabled by default. |
| **Mode** | Global EXEC |
| **Usage** | Use the **errdisable recovery cause udld** to enable auto recovery of UniDirectional Link Detection (UDLD).<br>Use the "**no**" to disable it. |
| **Example** | The example shows how to enable auto recovery of UniDirectional Link Detection (UDLD).<br><br>`switch(config)# errdisable recovery cause udld`<br>`switch# show errdisable recovery`<br>  |

### 2.34.2 udld

| | |
|---|---|
| **Syntax** | **udld**<br>**no udld** |
| **Parameter** | N/A |
| **Default** | UDLD is disabled by default. |
| **Mode** | Interface Configuration |
| **Usage** | Use the udld command to enable UniDirectional Link Detection (UDLD) normal mode of interface.<br>Use the **no** form of this command to restore to default setting.<br>You can verify your setting by entering the **show udld interface** Privileged EXEC command. |
| **Example** | The example shows how to enable UniDirectional Link Detection (UDLD) normal mode in interface gi 1.<br><br>`switch(config)# interface gi1`<br>`switch(config-if)# udld` |

### 2.34.3 udld aggressive

| | |
|---|---|
| **Syntax** | **udld / aggressive no / udld / aggressive** |
| **Parameter** | N/A |
| **Default** | UDLD aggressive mode is disabled by default. |
| **Mode** | Interface Configuration |
| **Usage** | Use the **udld aggressive** command to enable UniDirectional Link Detection (UDLD) aggressive mode of interface.<br>Use the no form of this command to restore to default setting.<br>You can verify your setting by entering the **show udld interface** Privileged EXEC command. |
| **Example** | The example shows how to enable udld aggressive mode in interface gi1.<br><br>`switch(config)# interface gi1`<br>`switch(config-if)# udld` |

### 2.34.3 udld message time

| | |
|---|---|
| **Syntax** | **udld message time** message-time-interval |
| **Parameter** | **message-time-interval** Specify the interval for sending message. Range is 1 -90 seconds. |
| **Default** | Default interval is 15 seconds. |
| **Mode** | Global Configuration |
| **Usage** | Use the udld message time to set interval of UniDirectional Link Detection (UDLD) sent message. |
| **Example** | The example shows how to set interval of UniDirectional Link Detection (UDLD) message.<br>`switch(config)# udld message time 30` |

### 2.34.4 udld reset

| | |
|---|---|
| **Syntax** | **udld reset** |
| **Parameter** | N/A |
| **Default** | No default is defined |
| **Mode** | Privileged EXEC |
| **Usage** | Use the **udld reset** command to reset all interfaces disabled by the UniDirectional Link Detection (UDLD) and permit traffic to begin passing through them again.<br>If the interface configuration is still enabled for UDLD, these ports begin to run UDLD again and are disabled for the same reason if the problem has not been corrected. |
| **Example** | The example shows how to reset all interfaces disabled by UDLD<br>`Switch# udld reset` |

### 2.34.5 show udld

| | |
|---|---|
| **Syntax** | **show udld**<br>**show udld interfaces** IF_NMLPORTS |
| **Parameter** | **IF_NMLPORTS** — Specify the normal interfaces to display udld information |
| **Default** | No default is defined |
| **Mode** | Privileged EXEC |
| **Usage** | Use the show udld command to to display UniDirectional Link Detection (UDLD) administrative and operational status for all ports or the specified port. |
| **Example** | The example shows how to show UniDirectional Link Detection (UDLD) settings and operational status of interface gi1.<br>`Switch(config)# show udld interfaces gi1` |

## 2.35 VLAN

### 2.35.1 vlan

| | |
|---|---|
| **Syntax** | **vlan / no vlan** |
| **Parameter** | N/A |
| **Default** | VLAN 1 created by default |
| **Mode** | Global Configuration |
| **Usage** | Use the vlan global configuration command to create VLAN. Use the no form of this command to remove exist VLAN.<br>You can verify your setting by entering the show vlan Privileged EXEC command. |
| **Example** | The following example creates and removes a VLAN entry (100).<br><br>`Switch# configure`<br>`Switch (config)# vlan 100`<br>`Switch# show vlan` |

### 2.35.2 Name(vlan)

| | |
|---|---|
| **Syntax** | **name NAME** |
| **Parameter** | NAME Specify the name of the VLAN (Max. 32 chars). |
| **Default** | Default name of new vlan is VLANxxxx. Xxxx is 4-digit vlan number. |
| **Mode** | VLAN Configuration |
| **Usage** | Use the vlan global configuration command to create VLAN. Use the no form of this command to remove exist VLAN.<br>You can verify your setting by entering the show vlan Privileged EXEC command. |
| **Example** | This example sets the VLAN name of VLAN 100 to be `VLAN-fiberroad`.<br><br>`Switch(config)# vlan 100`<br>`Switch(config-vlan)# name VLAN-fiberroad`<br>`Switch# show vlan` |

### 2.35.3 switchport mode

| | |
|---|---|
| **Syntax** | **switchport mode ( access \| hybrid \| trunk [uplink] \| tunnel )** |

**Parameter**

| | |
|---|---|
| access | Specify the VLAN mode to Access port. |
| hybrid | Specify the VLAN mode to Hybrid port. |
| trunk | Specify the VLAN mode to Trunk port. |
| uplink | Specify the Uplink property on this Trunk port. |
| tunnel | Specify the VLAN mode to Dot1Q Tunnel port. |

| | |
|---|---|
| **Default** | Default is trunk mode of all interfaces |
| **Mode** | Port Configuration |
| **Usage** | The VLAN mode is used to configure the port for different port role. **Access port**: Accepts only untagged frames and join an untagged VLAN. **Hybrid port**: Support all functions as defined in IEEE 802.1Q specification. **Trunk port**: An untagged member of one VLAN at most, and is a tagged member of zero or more VLANs. If it is an uplink port, it can recognize double tagging on this port.<br>**Tunnel port**: Port-based Q-in-Q mode.<br><br>Use the **switch mode** port configuration command to set mode of interface You can verify your setting by entering the **show interfaces switchport Privileged EXEC** command. |
| **Example** | This example sets VLAN mode to Access port.<br><br>`Switch(config)# interface g 12`<br>`Switch(config-if)# switchport mode access`<br>`Switch# show interfaces switchport g12` |

### 2.35.4 switchport hybrid pvid

| | |
|---|---|
| **Syntax** | **switchport hybrid pvid <1-4094>** |
| **Parameter** | <1-4094> Specify the port-based VLAN ID on the Hybrid port. |
| **Default** | Default pivd is 1. |
| **Mode** | Port Configuration |
| **Usage** | Use the **switch hybrid pivd** port configuration command to set pvid of interface.<br>You can verify your setting by entering the **show interfaces switchport** Privileged EXEC command. |
| **Example** | This example sets PVID to 100.<br>`Switch(config)# interface g 10`<br>`Switch(config-if)# switchport mode hybrid`<br>`Switch(config-if)# switchport hybrid pvid 100`<br>`Switch# show interfaces switchport g 10` |

### 2.35.5 switchport hybrid ingress-filtering

| | |
|---|---|
| **Syntax** | **switchport bybrid ingress-filtering no switchport hybrid ingress-filtering** |
| **Parameter** | Default is enabled |
| **Default** | Port Configuration |
| **Mode** | Port Configuration |
| **Usage** | Use the switchport hybrid ingress-filtering port configuration command to enable vlan ingress filter.<br>Use the no form of this command to disable.<br><br>You can verify your setting by entering the s show interfaces switchport Privileged EXEC command. |
| **Example** | This example sets ingress-filtering to disable.<br>`Switch(config)# interface g 10`<br>`Switch(config-if)# switchport mode hybrid`<br>`Switch(config-if)# no switchport hybrid ingress-filtering`<br>`Switch# show interfaces switchport g 10` |

### 2.35.6 switchport hybrid acceptable-frame-type

| | |
|---|---|
| **Syntax** | **switchport hybrid acceptable-frame-type ( all \| tagged-only \| untagged- only )** |
| **Parameter** | all — Specify to accept all frames.<br>tagged-only — Specify to only accept tagged frames.<br>untagged-only — Specify to only accept untagged frames. |
| **Default** | Default is accept all frames |
| **Mode** | Port Configuration |
| **Usage** | Use the **switchport hybrid accept-frame-type** port configuration command to choose which type of frame can be accepted.<br><br>You can verify your setting by entering the **show interfaces switchport** Privileged EXEC command |
| **Example** | This example sets acceptable-frame-type to tagged-only.<br>`Switch(config)# interface g 10`<br>`Switch(config-if)# switchport mode hybrid`<br>`Switch(config-if)# switchport hybrid acceptable-frame-type tagged- only`<br>`Switch# show interfaces switchport g 10` |

### 2.35.7 switchport hybrid allowed vlan

| | |
|---|---|
| **Syntax** | **switchport hybrid allowed vlan add VLAN-LIST [(tagged\|untagged)]**<br>**switchport hybrid allowed vlan remove VLAN-LIST** |
| **Parameter** | VLAN-LIST — Specifies the VLAN list to be added or remove.<br>( tagged \| untagged ) — Specifies the member type is tagged or untagged. |
| **Default** | Only vlan 1 is untagged member by default. Default is tagged member when added. |
| **Mode** | Port Configuration |
| **Usage** | Use the switchport hybrid allow vlan add port configuration command to allow vlan on interface.<br>Use the switchport hybrid allow vlan remove port configuration command to remove vlan on interface.<br>You can verify your setting by entering the s show interfaces switchport Privileged EXEC command. |
| **Example** | This example sets port fa10 VLAN to join the VLAN 100 as tagged member. |

```
Switch (config)# interface fa10
Switch (config-if)# switchport hybrid allowed vlan
                    add 100-105
Switch (config-if)# switchport hybrid allowed vlan
                    remove 105
Switch# show interfaces switchport fa10
```

### 2.35.8 switchport access vlan

| | |
|---|---|
| **Syntax** | **switchport access vlan <1-4094> No switchport access vlan** |
| **Parameter** | <1-4094> Specifies the access VLAN ID. |
| **Default** | Default is vlan 1 |
| **Mode** | Port Configuration |
| **Usage** | Use the **switchport access vlan** port configuration command to set native vlan on interface. The vlan will be pvid on interface as well.<br>Use the no form of this command to restore to default vlan<br>You can verify your setting by entering the s show interfaces switchport Privileged EXEC command. |
| **Example** | This example sets Access port g 10 native VLAN ID to 100.<br><br>`Switch(config)# interface g 10`<br>`Switch(config-if)# switchport mode access`<br>`Switch(config-if)# switchport access vlan 100`<br>`Switch# show interfaces switchport g 10` |

### 2.35.9 switchport tunnel vlan

| | |
|---|---|
| **Syntax** | **switchport tunnel vlan <1-4094>**<br>**no switchport tunnel vlan** |
| **Parameter** | <1-4094> Specifies the tunnel VLAN ID. |
| **Default** | Default is vlan 1 |
| **Mode** | Port Configuration |
| **Usage** | Use the switchport tunnel vlan port configuration command to set dot1q tunnel vlan on interface. The vlan will be pvid on interface as well.<br>Use the no form of this command to remove vlan on interface. The tunnel vlan id will set to reserve vlan 4095.<br>You can verify your setting by entering the s show interfaces switchport Privileged EXEC command. |
| **Example** | This example sets Tunnel port g 10 native VLAN to 100.<br><br>`Switch(config)# interface fa10`<br>`Switch(config-if)# switchport mode tunnel`<br>`Switch(config-if)# switchport tunnel vlan 100`<br>`Switch# show interfaces switchport` |

### 2.35.10 switchport trunk native vlan

| | |
|---|---|
| **Syntax** | **switchport trunk native vlan <1-4094>**<br>**no switchport trunk native vlan** |
| **Parameter** | <1-4094> Specifies the tunnel VLAN ID. |
| **Default** | Default is vlan 1 |
| **Mode** | Port Configuration |
| **Usage** | Use the switchport trunk native vlan port configuration command to set native vlan on interface.<br>Use the no form of this command to restore to default vlan.<br>You can verify your setting by entering the s show interfaces switchport Privileged EXEC command. |

**Example** This example sets Trunk port g 10 native VLAN to 100.

```
Switch(config)# interface g 10
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport trunk native vlan 100
Switch# show interfaces switchport g 10
```

### 2.35.11 switchport trunk allowed vlan

| | | |
|---|---|---|
| **Syntax** | **switchport trunk allowed vlan ( add \| remove ) ( VLAN-LIST \| all )** | |
| **Parameter** | ( add \| remove ) | Specify the action to add or remove the allowed VLAN list. |
| | ( VLAN-LIST \| all ) | Specify the VLAN list or all VLANs to be added or removed. |
| **Default** | N/A | |
| **Mode** | Port Configuration | |
| **Usage** | Use the s**witchport trunk allow vlan add** port configuration command to allow vlan on interface.<br>Use the **switchport trunk allow vlan remove** port configuration command to remove vlan on interface.<br>You can verify your setting by entering the **show interfaces switchport** Privileged EXEC command. | |

**Example** This example sets Trunk port g10 to add the allowed VLAN 100.

```
Switch(config)# interface g 10
Switch(config-if)# switchport trunk allowed vlan add
                    100
Switch# show interfaces switchport g 10
```

### 2.35.12 switchport trunk allow vlan

| | |
|---|---|
| **Syntax** | **switchport trunk allowed vlan ( add \| remove ) ( VLAN-LIST \|all )** |
| **Parameter** | ( add \| remove ) — Specify the action to add or remove the allowed VLAN list.<br>( VLAN-LIST \| all ) — Specify the VLAN list or all VLANs to be added or removed. |
| **Default** | N/A |
| **Mode** | Port Configuration |
| **Usage** | Use the **switchport trunk allow vlan** add port configuration command to allow vlan on interface.<br>Use the **switchport trunk allow vlan** remove port configuration command to remove vlan on interface.<br>You can verify your setting by entering the **show interfaces switchpor**t Privileged EXEC command. |
| **Example** | This example sets Trunk port fa10 to add the allowed VLAN 100. |

```
Switch(config)# interface g 10
Switch(config-if)# switchport trunk allowed vlan
                   add 100
Switch# show interfaces switchport g 10
```

### 2.35.13 switchport default-vlan tagged

| | |
|---|---|
| **Syntax** | **switchport default-vlan tagged**<br>**no switchport default-vlan tagged** |
| **Parameter** | None |
| **Default** | Default is untagged |
| **Mode** | Port Configuration |
| **Usage** | Use the **switchport default vlan tagged** port configuration command to become default vlan tagged member.<br>Use the **no switchport default vlan tagged** port configuration command to restore to default<br>You can verify your setting by entering the **show interfaces switchport** Privileged EXEC command |
| **Example** | This example sets Trunk port fa10 membership with the default VLAN to tag. |

```
Switch(config)# interface g 10
Switch(config-if)# switchport default-vlan tagged
Switch# show interfaces switchport g 10
```

### 2.35.14 switchport forbidden default-vlan

| | |
|---|---|
| **Syntax** | **switchport forbidden default-vlan**<br>**no switchport forbidden default-vlan** |
| **Parameter** | None |
| **Default** | Default is allowed |
| **Mode** | Port Configuration |
| **Usage** | Use the **switchport forbidden default-vlan** port configuration command to forbid default-vlan on interface.<br>Use the **no switchport forbidden default-vlan** port configuration c command to restore to default<br>You can verify your setting by entering the **show interfaces switchport** Privileged EXEC command |
| **Example** | This example sets the membership of the default VLAN with port g 10 to forbidden.<br><br>`Switch(config)# interface g 10`<br>`Switch(config-if)# switchport forbidden default-vlan`<br>`Switch# show interfaces switchport g 10` |

### 2.35.15 switchport forbidden vlan

| | |
|---|---|
| **Syntax** | **switchport forbidden vlan ( add \| remove ) VLAN-LIST** |
| **Parameter** | ( add \| remove ) Add or remove forbidden membership.<br>( VLAN-LIST \| all ) Specify the VLAN list. |
| **Default** | No vlan is forbidden by default |
| **Mode** | Port Configuration |
| **Usage** | Use the **switchport forbidden vlan add** port configuration command to forbid vlan on interface.<br>Use the **switchport forbidden vlan** remove port configuration command to accpet vlan on interface.<br>You can verify your setting by entering the **show interfaces switchport** Privileged EXEC command |
| **Example** | This example sets the membership of the VLAN 100 with port fa10 to forbidden.<br><br>`Switch(config)# interface g 10`<br>`Switch (config-if)# switchport forbidden vlan add 100`<br>`Switch# show interfaces switchport g 10` |

### 2.35.16 switchport vlan tpid

| | |
|---|---|
| **Syntax** | **switchport vlan tpid (0x8100\|0x88a8\|0x9100\|0x9200)** |
| **Parameter** | (0x8100\|0x88a8\|0x9100\|0x9200) Select TPID to set. |
| **Default** | Default TPID is 0x8100 |
| **Mode** | Port Configuration |
| **Usage** | Use the **switchport vlan tpid** port configuration command to set TPID on interface.<br>You can verify your setting by entering the **show running-config** Privileged EXEC command |
| **Example** | This example sets the TPID to 0x9100 on interface fa10.<br>`Switch(config)# interface fa10`<br>`Switch(config-if)# switchport vlan tpid 0x9100` |

### 2.35.17 management-vlan

| | |
|---|---|
| **Syntax** | **management-vlan vlan <1-4094>**<br>**no management-vlan** |
| **Parameter** | <1-4094> Specify the VLAN ID of management-vlan. |
| **Default** | Default management vlan is 1. |
| **Mode** | Global Configuration |
| **Usage** | Use the management vlan Global Configuration mode command to set management vlan id. Vlan id must be created first.<br>Use the **no** form of this command to restore to default setting.<br>You can verify your setting by entering the show management-vlan Privileged EXEC command |
| **Example** | (1)The following example specifies that management vlan 2 is created Switch(config)#vlan 2<br>`Switch(config)# management-vlan vlan 2`<br>(2) The following example specifies that management-vlan is restored to be default VLAN.<br>`Switch(config)# no management-vlan` |

### 2.35.18 show vlan

| | |
|---|---|
| **Syntax** | **show vlan [(VLAN-LIST\|dynamic\|static)]** |
| **Parameter** | (VLAN-LIST\| dynamic\|static) — Specify vlan id to show information or show all static or dynamic vlan entries. |
| **Default** | None |
| **Mode** | Privileged EXEC |
| **Usage** | Display information about vlan entry |
| **Example** | The following example specifies that show vlan Switch# show vlan<br>`Switch# show vlan` |

### 2.35.19 show vlan interface membership

| | |
|---|---|
| **Syntax** | **show vlan VLAN-LIST interfaces IF_PORTS membership** |
| **Parameter** | <VLAN-List> — Specify vlan to show<br>IF_PORTS — Specify interface is to show |
| **Default** | None |
| **Mode** | Privileged EXEC |
| **Usage** | Display information about vlan membership on interfaces. |
| **Example** | The following example specifies that show vlan interface membership.<br>`Switch# show vlan 100 interfaces fa10 membership` |

### 2.35.20 show interface switchport

| | |
|---|---|
| **Syntax** | **show interface switchport interfaces** IF_PORTS |
| **Parameter** | IF_PORTS — Specify interfaces protocol vlan to display |
| **Default** | None |
| **Mode** | Privileged EXEC |
| **Usage** | Display information about default vlan |
| **Example** | The following example specifies that show interfacce switchport. |

```
Switch(config)# interface g 10
Switch(config-if)# switchport trunk allowed vlan
                   add 100
Switch# show interfaces switchport fa10
```

### 2.35.21 show management-vlan

| | |
|---|---|
| **Syntax** | **show management-vlan** |
| **Parameter** | None |
| **Default** | None |
| **Mode** | Privileged EXEC |
| **Usage** | Display information about management vlan |
| **Example** | The following example specifies that show management vlan<br>`Switch(config)# show management-vlan` |

## 2.36 Voice VLAN

### 2.36.1 voice-vlan(Global)

| | |
|---|---|
| **Syntax** | **voice-vlan / no voice-vlan** |
| **Parameter** | None |
| **Default** | Voice VLAN is disabled |
| **Mode** | Global Configuration |
| **Usage** | Use the voice vlan global configuration command to enable the functional Voice VLAN on the device.<br>Use the no form of this command to disable voice vlan function.<br>You can verify your setting by entering the show voice vlan Privileged EXEC command. |
| **Example** | The following example shows how to enable voice vlan.<br>`Switch(config)# voice-vlan`<br>`Switch# show voice-vlan` |

### 2.36.2 voice-vlan(Interface)

| | |
|---|---|
| **Syntax** | **voice-vlan / no voice-vlan** |
| **Parameter** | None |
| **Default** | The default all port admin-staus is disabled. |
| **Mode** | Interface Configuration |
| **Usage** | Use the **voice vlan** Interface configuration command to enable OUI voice VLAN configuration on an interface<br>Use the **no** form of this command to disable voice vlan on an interfaces You can verify your setting by entering the **show voice vlan** Privileged EXEC command |
| **Example** | The following example how to enable voice VLAN function in oui mode on an interface<br>`Switch(config)#interface range g 1-3`<br>`Switch(config-if)#voice-vlan`<br>`Switch# show voice-vlan interfaces g 1-3` |

### 2.36.3 voice-vlan vlan

| | |
|---|---|
| **Syntax** | **voice-vlan vlan <1-4094>**<br>**no voice-vlan vlan** |
| **Parameter** | <1-4094> Specify the voice VLAN ID |
| **Default** | The default Voice VLAN ID is None. |
| **Mode** | Global Configuration |
| **Usage** | Use the voice vlan id global configuration command to configure the VLAN identifier of the voice VLAN statically.<br>Use the no form of this command to restore voice vlan id to default. You can verify your setting by entering the show voice vlan Privileged EXEC command |
| **Example** | The following example shows how to set Voice vlan id. The vlan id must be created first.<br>`Switch(config)# voice-vlan vlan 128`<br>`Switch# show voice-vlan` |

### 2.36.4 voice-vlan oui-table

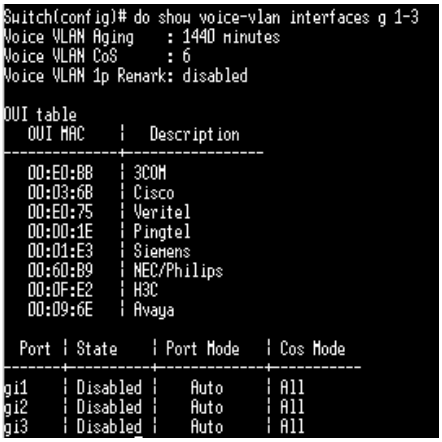
| | |
|---|---|
| **Syntax** | **voice-vlan oui-table** A:B:C [DESCRIPTION]<br>**no voice-vlan oui-table** [A:B:C] |
| **Parameter** | IF_PORTS — Specify interfaces protocol vlan to display<br>DESCRIPTION — Specify description of the specified MAC address to the voice VLAN OUI table |
| **Default** | The system default has 8 oui addresses. |
| **Mode** | Global Configuration |
| **Usage** | Use the voice vlan oui-table global configuration command to add oui mac address to OUI Table<br>Use the no form of this command to remove all or specified oui mac address.. You can verify your setting by entering the show voice vlan Privileged EXEC command |
| **Example** | This following example shows how to add OUI Mac.<br>`Switch(config)# voice-vlan oui-table 00:01:02 "Test"`<br>`Switch# show voice-vlan interfaces all` |

### 2.36.5 voice-vlan cos(Global)

| | |
|---|---|
| **Syntax** | **voice-vlan cos** <0-7> [remark]<br>**no voice-vlan cos** |
| **Parameter** | <0-7> — Specify the voice VLAN Class of Service value in telephone oui mode<br>remark — Specify that the L2 user priority is remarked with the CoS value |
| **Default** | The default cos value is 6, remark is disabled. |
| **Mode** | Global Configuration |
| **Usage** | Use the **voice vlan cos** global configuration command to configure the voice VLAN cos value and 1p remark function<br>Use the "**no**" form to restore to default mode.<br>You can verify your setting by entering the s**how voice vlan** Privileged EXEC command |
| **Example** | The following example show how to set cos value and enable 1p remark function<br>`Switch(config)# voice-vlan cos 7 remark`<br>`Switch# show voice-vlan` |

### 2.36.6 voice-vlan cos(Interface)

| | | |
|---|---|---|
| **Syntax** | **voice-vlan cos ( src \| all )**<br>**no voice-vlan cos** | |
| **Parameter** | src | Specify QoS attributes are applied to packets with OUIs in the source MAC address. |
| | All | Specify QoS attributes are applied to packets that are classified to the Voice VLAN. |
| **Default** | The default all port in Src mode. | |
| **Mode** | Interface Configuration | |
| **Usage** | Use the **voice vlan cos Interface configuration** command to configure OUI voice VLAN cos mode configuration on an interface<br>Use the "**no**" form to restore to default mode.<br>You can verify your setting by entering the s**how voice-vlan interfaces** Privileged EXEC command | |
| **Example** | The following example how to configure voice packet QoS attributes on an interface<br>`Switch(config)#interface range g 1-3`<br>`Switch(config-if)#voice-vlan cos all`<br>`Switch# show voice-vlan interfaces g 1-3` | |

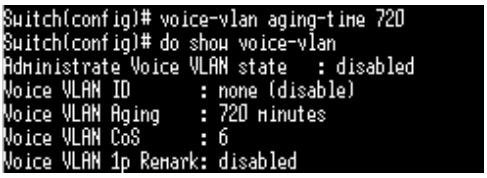


## 2.36.7 voice-vlan mode

| | | |
|---|---|---|
| **Syntax** | **voice-vlan mode (auto\|manual)**<br>**no voice-vlan mode** | |
| **Parameter** | auto | Specifies that the port is identified as a candidate to join the voice VLAN. When a packet with a source OUI MAC address that identifies the remote equipment as voice equipment is seen on the port, the port joins the voice VLAN as a tagged port. |
| | manual | Specifies that the port is manually assigned to the voice VLAN. |
| **Default** | The default is auto mode. | |
| **Mode** | Interface Configuration | |
| **Usage** | Use the **voice-vlan mode** global configuration command to configure the voice VLAN mode for interface.<br>Use the "**no**" form to restore to default mode.<br>You can verify your setting by entering the **show voice-vlan interfaces** Privileged EXEC command. | |
| **Example** | The following example how to configure voice mode to manual<br>`Switch(config)#interface range g 1-3`<br>`Switch(config-if)#voice-vlan mode manaul`<br>`Switch# show voice-vlan interfaces g 1-3` | |

```
Switch(config)# do show voice-vlan int g 1-3
Voice VLAN Aging   : 1440 minutes
Voice VLAN CoS     : 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

  Port | State    | Port Mode   | Cos Mode
-------+----------+-------------+----------
gi1    | Disabled |  Manual     | All
gi2    | Disabled |  Manual     | All
gi3    | Disabled |  Manual     | All
```

### 2.36.8 voice-vlan aging-time

| | |
|---|---|
| **Syntax** | **voice-vlan aing-time** <30-65536><br>**no voice-vlan aing-time** |
| **Parameter** | <30-65536> Specify the voice VLAN aging timeout interval in minutes |
| **Default** | The default aging-timeout value is 1440 minutes |
| **Mode** | Global Configuration |
| **Usage** | Use the **voice vlan aging-time** global configuration command to configure the voice VLAN aging timeout.<br>Use the "no" form to restore to default time.<br>You can verify your setting by entering the **show voice vlan** Privileged EXEC command |
| **Example** | The following example shows how to set aging time.<br>`Switch(config)# voice-vlan aging-time 720`<br>`Switch# show voice-vlan`<br>  |



### 2.36.9 show voice-vlan

| | |
|---|---|
| **Syntax** | **show voice-vlan**<br>**show voice-vlan interfaces** [IF_PORTS] |
| **Parameter** | IF_PORTS Specifies intefaces to display voice VLAN settings in oui mode |
| **Default** | N/A |
| **Mode** | Privileged EXEC |
| **Usage** | Use the show voice vlan command in EXEC mode to display the voice VLAN status for all interfaces or for a specific interface if the voice VLAN type is OUI |
| **Example** | The following example show how to display voice vlan oui mode settings<br>`Switch# show voice-vlan` |

## 2.37 Static Routing

### 2.37.1 IPv4 Interface

**Syntax**

**interface vlan**
**ip address** ipaddr mask
**no interface vlan**
**no ip address**

**Parameter**

| | |
|---|---|
| ipaddr | Specify IPv4 address for switch |
| mask | Specify net mask address for switch |

**Default**

The vlan interface and ip address are not configured by default.

**Mode**

Global configuration and vlan interface configuration.

**Usage**

Use the **interface vlan** global configuration command to config ip interface on the device.
Use the **ip address** command in vlan interface mode to configure the device's ip address.
Use the **no ip address** command to delete the configured ip address.
Use the **no interface vlan** command to delete ip interface on the device.
You can verify your setting by entering the **show ip interface vlan** Privileged EXEC command.

**Example**

The following example shows how to config ip interface.

```
Switch(config)# interface vlan 2
Switch(config-if)# ip address 192.168.3.1
                              255.255.255.0
Switch# show ip interface vlan 2
```

```
Switch# show ip interface vlan 2

IP Address        I/F       I/F Status Type    Status    Roles
                            admin/oper
----------------- --------- ---------- ------- --------- ---------
192.168.3.1/24    VLAN 2    UP/DOWN    Static  Valid     primary
```

### 2.37.2 IPv4 Routes

**Syntax**

**ip route** dest-ipaddr mask router-ipaddr
**no ip route** dest-ipaddr mask router-ipaddr

**Parameter**

| | |
|---|---|
| Dest-ipaddr | Destination ip address prefix |
| mask | Destination ip address prefix mask |
| router-ipaddr | Forwarding router's ip address |

**Default**

Static route is not configured by default.

**Mode**

Global configuration

**Usage**

Use the **ip route** command in global mode to configure a static route rule.
Use the **no ip route** command to delete a static routing rule.
You can verify your setting by entering the **show ip route** Privileged EXEC command

**Example**

The following example shows how to configure a static route.

```
Switch(config)# vlan 2
Switch(config)# interface GigabitEthernet 4
Switch(config-if)# switchport trunk allowed vlan
                    add 2
Switch(config)# interface vlan 2
Switch(config-if)# ip address 192.168.3.1
                  255.255.255.0
Switch(config)# ip route 1.1.1.1 255.0.0.0
                192.168.3.11
Switch# show ip route
```

### 2.37.3 IPv4 ARP

| | |
|---|---|
| **Syntax** | **arp ip-addr mac-addr vlan vlanid**<br>**no arp ip-addr mac-addr vlan vlanid** |
| **Parameter** | ip-addr — IP address of ARP entry<br>mac-addr — MAC address of ARP entry<br>vlanid — Vlan ID of this arp entry |
| **Default** | The device contains ARP entries of the vlan interface. |
| **Mode** | Global configuration |
| **Usage** | Use the **arp** command to add a static arp entry.<br>Use the **no arp** command to delete a static arp entry.<br>You can verify your setting by entering the **show arp** Privileged EXEC command |
| **Example** | The following example shows how to configure and view a static arp entry.<br>`Switch(config)# arp 192.168.3.22 00:00:11:11:11:11 vlan 2`<br>`Switch# show arp` |

### 2.37.4 IPv6 Interface

| | |
|---|---|
| **Syntax** | **interface vlan vlanid**<br>**ipv6 enable**<br>**no interface vlan vlanid**<br>**no ipv6 enable** |
| **Parameter** | vlanid — Vlan id for vlan interface |
| **Default** | The vlan interface are not configured by default.Ipv6 is disabled. |
| **Mode** | Global configuration and vlan interface configuration. |
| **Usage** | Use the **interface vlan** global configuration command to config ip interface on the device.<br>Use the **ipv6 enable** command in vlan interface mode to enable ipv6 function.<br>Use the **no ipv6 enable** command to disable ipv6 function.<br>Use the **no interface vlan** command to delete ip interface on the device.<br>You can verify your setting by entering the **show ipv6 interface vlan** Privileged EXEC command. |
| **Example** | The following example shows how to config ip interface.<br>`Switch(config)# interface vlan 2`<br>`Switch(config-if)# ipv6 enable`<br>`Switch# show ipv6 interface vlan 2` |

### 2.37.5 IPv6 Address

| | |
|---|---|
| **Syntax** | **ipv6 address ipv6-addr**<br>**no ipv6 address** |
| **Parameter** | ipv6-addr Manually configured ipv6 address |
| **Default** | The vlan interface are not configured by default.Ipv6 is disabled. |
| **Mode** | Global configuration and vlan interface configuration. |
| **Usage** | Use the **ipv6 address** command in vlan interface mode to config a manual ipv6 address.<br>Use the **no ipv6 address** command in vlan interface mode to delete all manual ipv6 addresses on this vlan interface.<br>You can verify your setting by entering the **show ipv6 interface vlan** Privileged EXEC command. |
| **Example** | The following example shows how to config ip interface.<br>`Switch(config)# interface vlan 2`<br>`Switch(config-if)# ipv6 address 2001:01::01:01/64`<br>`Switch# show ipv6 interface vlan 2`<br>  |

```
Switch(config-if-vlan2)# ipv6 address 2001:01::01:01/64
Switch(config-if-vlan2)# exit
Switch(config)# do show ipv6 int vlan 2
VLAN 2 is up/down
IPv6 is enabled, link-local address is fe80::218:95ff:fe83:fbac (TENTA
IPv6 Forwarding is disabled
Global unicast address(es):
IPv6 Global Address                     Type
2001:1::1:1/64 (TEN)                    Manual
ND DAD is enabled, number of DAD attempts: 1
Stateless autoconfiguration is enabled
```

### 2.37.6 IPv6 Routes

| | |
|---|---|
| **Syntax** | **ipv6 route** ipv6-addr/length route-ipv6-addr<br>**no ipv6 address** ipv6-addr/length |
| **Parameter** | ipv6-addr/length — Destination ipv6 prefix and length<br>route-ipv6-addr — Forwarding router's ipv6 address |
| **Default** | The ipv6 routing entry is not configured by default. |
| **Mode** | Global configuration and vlan interface configuration. |
| **Usage** | Use the **ipv6 route** command to configure a static ipv6 routing entry.<br>Use the **no ipv6 address** command to delete a static ipv6 routing entry.<br>You can verify your setting by entering the **show ipv6 route static** Privileged EXEC command. |
| **Example** | The following example shows how to configure an ipv6 routing entry.<br>`Switch(config)# ipv6 route 2002:01::01:01/96 2001:01::01:02`<br>`Switch# show ipv6 route static` |

### 2.37.7 IPv6 Neighbors

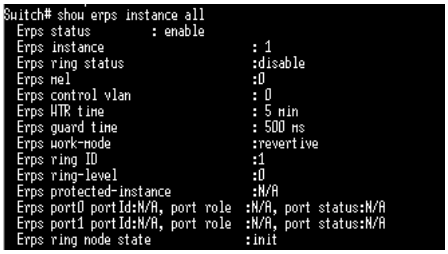
| | |
|---|---|
| **Syntax** | **ipv6 neighbor ipv6-addr vlan vlanid macaddr**<br>**no ipv6 neighbor** |
| **Parameter** | ipv6-addr — Neighbor ipv6 address<br>vlanid — Vlan interface number<br>macaddr — MAC address of ipv6 neighbor entry |
| **Default** | No ipv6 neighbor address by default. |
| **Mode** | Global configuration |
| **Usage** | Use the **ipv6 neighbor** command to configure a static ipv6 neighbor entry.<br>Use the **no ipv6 neighbor** command to delete ipv6 neighbor entry.<br>You can verify your setting by entering the **show ipv6 neighbors** Privileged EXEC command. |
| **Example** | The following example shows how to configure an ipv6 neighbor entry.<br>`Switch(config)# ipv6 neighbor 2001:01::01:11 vlan 2 00:00:00:11:11:12`<br>`Switch# show ipv6 neighbors` |

# 2.38 ERPS

## 2.38.1 erps global

| | |
|---|---|
| **Syntax** | **erps**<br>**no erps** |
| **Parameter** | N/A |
| **Default** | Default is disable |
| **Mode** | Global configuration |
| **Usage** | Use the **erps** command to configure erps enable.<br>You can verify your setting by entering the **show running-configuration** Privileged EXEC command. |
| **Example** | The following example shows how to configure enable erps in global configuration.<br>`Switch(config)# erps` |

## 2.38.2 erps instance(Global)

| | |
|---|---|
| **Syntax** | **erps instance <0-15>**<br>**no erps instance <0-15>** |
| **Parameter** | <0 -15> erps instance number |
| **Default** | N/A |
| **Mode** | Global configuration |
| **Usage** | Use the **erps instance** command to configure erps instance.<br>You can verify your setting by entering the **show erps instance(\|0-15\|all\|)>**Privileged EXEC command. |
| **Example** | The following example shows how to configure erps instance in global configuration.<br>`Switch(config)# erps instance 1`<br>`Switch # show erps instance all`<br>  |

```
Switch# show erps instance all
  Erps status        : enable
  Erps instance                  : 1
  Erps ring status               :disable
  Erps mel                       :0
  Erps control vlan              : 0
  Erps WTR time                  : 5 min
  Erps guard time                : 500 ms
  Erps work-mode                 :revertive
  Erps ring ID                   :1
  Erps ring-level                :0
  Erps protected-instance        :N/A
  Erps port0 portId:N/A, port role  :N/A, port status:N/A
  Erps port1 portId:N/A, port role  :N/A, port status:N/A
  Erps ring node state           :init
```

### 2.38.3 control-vlan

| | | |
|---|---|---|
| **Syntax** | **control-vlan <1-4094>**<br>**no control-vlan** | |
| **Parameter** | <1-4094> | Specify the control vlan ID. The valid range is from 1 to 4094 |
| **Default** | N/A | |
| **Mode** | erps instance configuration | |
| **Usage** | Use the **erps control-vlan** command to configure the control vlan to the erps instance .<br>You can verify your setting by entering the **show erps instance** Privileged EXEC command. | |
| **Example** | The following example shows how to configure control vlan in erps instance global configuration.<br>`Switch(config)# erps instance 1`<br>`Switch(config-erps-inst)# control-vlan 2`<br>`Switch(config)# do show erps instance 1`<br>  | |

```
Switch(config)# do show erps instance 1
  Erps instance                    : 1
  Erps ring status                 :disable
  Erps mel                         :0
  Erps control vlan                : 2
  Erps WTR time                    : 5 min
  Erps guard time                  : 500 ms
  Erps work-mode                   :revertive
  Erps ring ID                     :1
  Erps ring-level                  :0
  Erps protected-instance          :N/A
  Erps port0 portId:N/A, port role :N/A, port status:N/A
  Erps port1 portId:N/A, port role :N/A, port status:N/A
  Erps ring node state             :init
```

### 2.38.4 wtr-timer

| | | |
|---|---|---|
| **Syntax** | **wtr-timer <1-12>**<br>**no wtr-timer** | |
| **Parameter** | <1-12> | Specify the wtr-timer 1-12. The valid range is from 1 to 12 |
| **Default** | Default is 5 min | |
| **Mode** | erps configuration | |
| **Usage** | Use the **wtr-timer** command to configure the WTR to the erps instance .<br>You can verify your setting by entering the **show erps instance** Privileged EXEC command. | |
| **Example** | The following example shows how to configure erps **wtr-timer** in erps instance.<br>Switch(config)# **erps instance 1**<br>Switch(config-erps-inst)# **wtr-timer 6**<br>Switch(config)# **do show erps instance 1** | |

```
Switch(config)# do show erps instance 1
  Erps instance                    : 1
  Erps ring status                 :disable
  Erps mel                         :0
  Erps control vlan                : 2
  Erps WTR time                    : 6 min
  Erps guard time                  : 500 ms
  Erps work-mode                   :revertive
  Erps ring ID                     :1
  Erps ring-level                  :0
  Erps protected-instance          :N/A
  Erps port0 portId:N/A, port role  :N/A, port status:N/A
  Erps port1 portId:N/A, port role  :N/A, port status:N/A
  Erps ring node state             :init
```

### 2.38.5 guard-timer

| | |
|---|---|
| **Syntax** | **guard-timer <100-2000>**<br>**no guard-timer** |
| **Parameter** | <100-2000> Specify the guard-timer 100-2000 ms. |
| **Default** | Default is 500 ms |
| **Mode** | erps configuration |
| **Usage** | Use the **guard-timer** command to configure the guard-timer to the erps instance .<br>You can verify your setting by entering the **show erps instance** Privileged EXEC command. |
| **Example** | The following example shows how to configure erps **guard-timer** in erps instance.<br>Switch(config)# **erps instance 1**<br>Switch(config-erps-inst)# **guard-timer 6**<br>Switch(config)# **do show erps instance 1** |

```
Switch(config)# erps instance 1
Switch(config-erps-inst)# guard-timer
  <100-2000>  Valid range is 100-2000 ms. Default is 500 ms.
Switch(config-erps-inst)# guard-timer 100
Switch(config-erps-inst)# exit
Switch(config)# do show erps instance 1
  Erps instance                    : 1
  Erps ring status                 :disable
  Erps mel                         :0
  Erps control vlan                : 2
  Erps WTR time                    : 6 min
  Erps guard time                  : 100 ms
  Erps work-mode                   :revertive
  Erps ring ID                     :1
  Erps ring-level                  :0
  Erps protected-instance          :N/A
  Erps port0 portId:N/A, port role  :N/A, port status:N/A
  Erps port1 portId:N/A, port role  :N/A, port status:N/A
  Erps ring node state             :init
```

### 2.38.6 work-mode

| | |
|---|---|
| **Syntax** | **work-mode (revertive\|non_revertive)** |
| **Parameter** | N/A |
| **Default** | Default is revertive |
| **Mode** | erps configuration |
| **Usage** | Use the **work-mode** command to configure the (revertive\|non_revertive) to the erps instance .<br>You can verify your setting by entering the **show erps instance** Privileged EXEC command. |
| **Example** | The following example shows how to configure erps **work-mode** in erps instance.<br>`Switch(config)# erps instance 1`<br>`Switch(config-erps-inst)# word-mode revertive`<br>`Switch(config)# do show erps instance 1` |

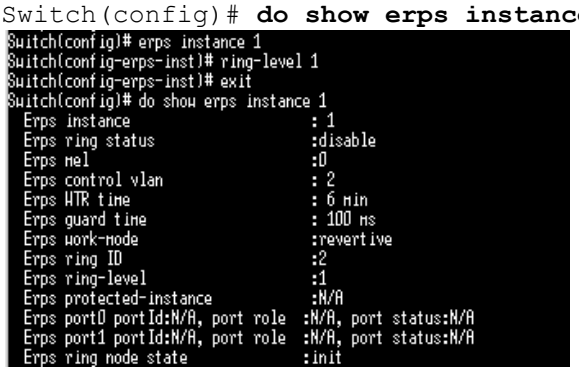
```
Switch(config-erps-inst)# work-mode revertive
Switch(config-erps-inst)# exit
Switch(config)# do show erps instance 1
  Erps instance                    : 1
  Erps ring status                 :disable
  Erps mel                         :0
  Erps control vlan                : 2
  Erps WTR time                    : 6 min
  Erps guard time                  : 100 ms
  Erps work-mode                   :revertive
  Erps ring ID                     :1
  Erps ring-level                  :0
  Erps protected-instance          :N/A
  Erps port0 portId:N/A, port role  :N/A, port status:N/A
  Erps port1 portId:N/A, port role  :N/A, port status:N/A
  Erps ring node state             :init
```

### 2.38.7 ring<ID>

| | |
|---|---|
| **Syntax** | **ring(1-239)** |
| **Parameter** | <1-239> Specify the ring ID 1-239. |
| **Default** | Default Ring ID is 1 |
| **Mode** | erps configuration |
| **Usage** | Use the **ring<1-239>** command to configure the ring ID to the erps instance .<br>You can verify your setting by entering the **show erps instance** Privileged EXEC command. |
| **Example** | The following example shows how to configure erps **ring id** in erps instance.<br>`Switch(config)# erps instance 1`<br>`Switch(config-erps-inst)# ring 2`<br>`Switch(config)# do show erps instance 1` |

```
Switch(config)# erps instance 1
Switch(config-erps-inst)# ring 2
Switch(config-erps-inst)# exit
Switch(config)# do show erps instance 1
  Erps instance                    : 1
  Erps ring status                 :disable
  Erps mel                         :0
  Erps control vlan                : 2
  Erps WTR time                    : 6 min
  Erps guard time                  : 100 ms
  Erps work-mode                   :revertive
  Erps ring ID                     :2
  Erps ring-level                  :0
  Erps protected-instance          :N/A
  Erps port0 portId:N/A, port role  :N/A, port status:N/A
  Erps port1 portId:N/A, port role  :N/A, port status:N/A
  Erps ring node state             :init
```

### 2.38.8 ring level

| | | |
|---|---|---|
| **Syntax** | **ring-level<0-1>** | |
| **Parameter** | <0-1> | Specify the ring level. Major ring is ring level 0, sub-ring is ring level 1. |
| **Default** | Default ring level is 0 | |
| **Mode** | erps configuration | |
| **Usage** | Use the **ring level** command to configure the ring level to the erps instance .<br>You can verify your setting by entering the **show erps instance** Privileged EXEC command. | |
| **Example** | The following example shows how to configure erps **ring level** in erps instance.<br>`Switch(config)# erps instance 1`<br>`Switch(config-erps-inst)# ring-level 1`<br>`Switch(config)# do show erps instance 1`<br>  | |

```
Switch(config)# erps instance 1
Switch(config-erps-inst)# ring-level 1
Switch(config-erps-inst)# exit
Switch(config)# do show erps instance 1
  Erps instance                    : 1
  Erps ring status                 :disable
  Erps mel                         :0
  Erps control vlan                : 2
  Erps WTR time                    : 6 min
  Erps guard time                  : 100 ms
  Erps work-mode                   :revertive
  Erps ring ID                     :2
  Erps ring-level                  :1
  Erps protected-instance          :N/A
  Erps port0 portId:N/A, port role  :N/A, port status:N/A
  Erps port1 portId:N/A, port role  :N/A, port status:N/A
  Erps ring node state             :init
```

### 2.38.9 port

| | |
|---|---|
| **Syntax** | **port0 IF_PORTS** (owner\|neihbour\|next-neighbour)<br>**port1 IF_PORTS** (owner \| neihbour \| next-neighbour) |
| **Parameter** | IF_PORTS Specify the port number. |
| **Default** | Default is port1 |
| **Mode** | erps configuration |
| **Usage** | Use the **port0 IF_PORTS (owner\|neihbour\|next-neighbour)** command to configure the specific port role the erps instance . You can verify your setting by entering the **show erps instance** Privileged EXEC command. |
| **Example** | The following example shows how to configure the specific port role in erps instance.<br>Switch(config)# **erps instance 1**<br>Switch(config-erps-inst)# **port0 GigabitEthernet 2 owner**<br>Switch(config)# **do show erps instance 1** |

```
Switch(config)# do show erps instance 1
  Erps instance                    : 1
  Erps ring status                 :disable
  Erps mel                         :0
  Erps control vlan                : 2
  Erps WTR time                    : 6 min
  Erps guard time                  : 100 ms
  Erps work-mode                   :revertive
  Erps ring ID                     :2
  Erps ring-level                  :1
  Erps protected-instance          :N/A
  Erps port0 portId:gi2, port role  :owner, port status:disabled
  Erps port1 portId:N/A, port role  :N/A, port status:N/A
```

## 2.38.10 mel

| | |
|---|---|
| **Syntax** | **<0-7>** |
| **Parameter** | <0-7> Specify the mel value. |
| **Default** | Default is 0 |
| **Mode** | erps configuration |
| **Usage** | Use the **mel <0-7>** command to configure the level erps instance . You can verify your setting by entering the **show erps instance** Privileged EXEC command. |
| **Example** | The following example shows how to configure the mel value in erps instance.<br>Switch(config)# **erps instance 1**<br>Switch(config-erps-inst)# **mel 2**<br>Switch(config)# **do show erps instance 1** |

```
Switch(config)# do show erps instance 1
  Erps instance                      : 1
  Erps ring status                   :disable
  Erps mel                           :2
  Erps control vlan                  : 2
  Erps WTR time                      : 6 min
  Erps guard time                    : 100 ms
  Erps work-mode                     :revertive
  Erps ring ID                       :2
  Erps ring-level                    :1
  Erps protected-instance            :N/A
  Erps port0 portId:gi2, port role   :owner, port status:disabled
  Erps port1 portId:N/A, port role   :N/A, port status:N/A
  Erps ring node state               :init
```

### 2.38.11 ring enable

| | |
|---|---|
| **Syntax** | **ring (enable|disable)** |
| **Parameter** | N/A |
| **Default** | Default is disable |
| **Mode** | erps configuration |
| **Usage** | Use the **ring (enable|disable)** command to configure the ring status in erps instance .<br>You can verify your setting by entering the **show erps instance** Privileged EXEC command. |
| **Example** | The following example shows how to configure the ring status in erps instance.<br>`Switch(config)# erps instance 1`<br>`Switch(config-erps-inst)# ring enable`<br>`Switch(config)# do show erps instance 1` |

```
Switch(config-erps-inst)# ring enable
Switch(config-erps-inst)# exit
Switch(config)# do show erps instance 1
  Erps instance                      : 1
  Erps ring status                   :enable
  Erps mel                           :2
  Erps control vlan                  : 2
  Erps WTR time                      : 6 min
  Erps guard time                    : 100 ms
  Erps work-mode                     :revertive
  Erps ring ID                       :2
  Erps ring-level                    :1
  Erps protected-instance            :N/A
  Erps port0 portId:gi2, port role  :owner, port status:disabled
  Erps port1 portId:N/A, port role  :N/A, port status:N/A
  Erps ring node state               :protection
```

### 2.38.12 show erps instance

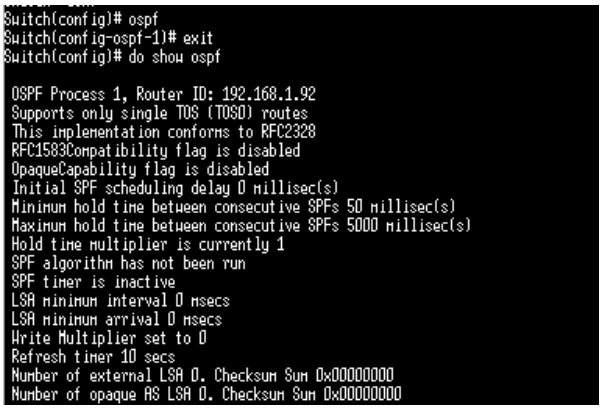
| | |
|---|---|
| **Syntax** | **show erps instance (all \| <0-15>)** |
| **Parameter** | (all \| <0-15>) Specify the erps instance number |
| **Default** | N/A |
| **Mode** | erps configuration |
| **Usage** | Use the **show erps instance** command to show the specific erps instance |
| **Example** | The following example shows how to configure to show the erps instance.<br><br>Switch# show erps instance 1 |

```
Switch# show erps instance 1
  Erps instance                    : 1
  Erps ring status                 :enable
  Erps mel                         :2
  Erps control vlan                : 2
  Erps WTR time                    : 6 min
  Erps guard time                  : 100 ms
  Erps work-mode                   :revertive
  Erps ring ID                     :2
  Erps ring-level                  :1
  Erps protected-instance          :N/A
  Erps port0 portId:gi2, port role  :owner, port status:disabled
  Erps port1 portId:N/A, port role  :N/A, port status:N/A
  Erps ring node state             :protection
```

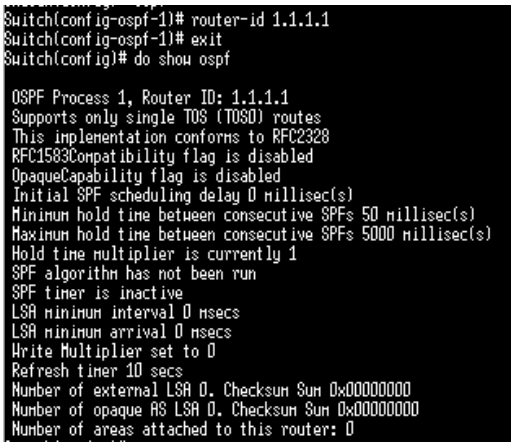
## 2.39 OSPF

### 2.39.1 ospf(global)

| | |
|---|---|
| **Syntax** | **ospf**<br>**no ospf** |
| **Parameter** | process id The process id only support 1 |
| **Default** | Default is disable |
| **Mode** | Global Configuration |
| **Usage** | Use the **ospf** command to enable ospf running, You can verify your setting by entering the **show ospf** Privileged EXEC command. |
| **Example** | The following example shows how to configure to ospf process 1.<br>`Switch(config)# ospf`<br>`Switch(config-ospf-1)#`<br>`Switch# show ospf` |



### 2.39.2 router-id

| | |
|---|---|
| **Syntax** | **router-id A.B.C.D**<br>**no router-id** |
| **Parameter** | A.B.C.D Specify the router id |
| **Default** | N/A |
| **Mode** | OSPF Configuration Mode |
| **Usage** | Use the **router-id 1.1.1.1** command to configure OSFP process 1 router ID is 1.1.1.1, You can verify your setting by entering the **show ospf** Privileged EXEC command. |
| **Example** | The following example shows how to configure ospf process 1 router-id.<br>`Switch(config)# ospf`<br>`Switch(config-ospf-1)#router-id 1.1.1.1`<br>`Switch# show ospf`<br>  |

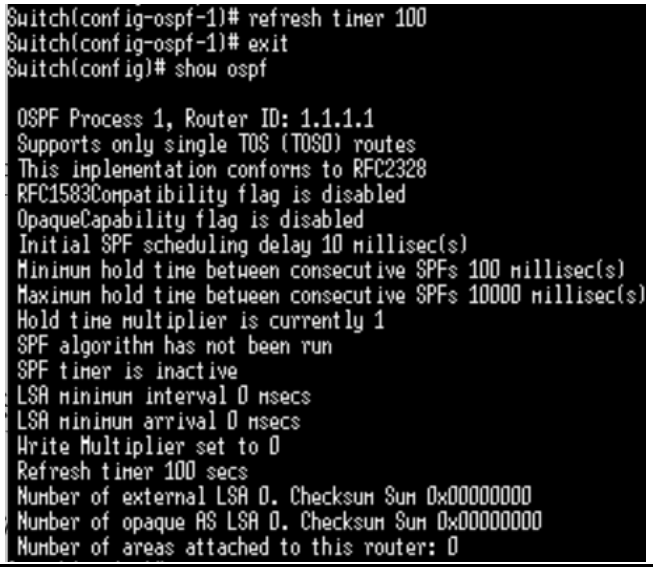
```
Switch(config-ospf-1)# router-id 1.1.1.1
Switch(config-ospf-1)# exit
Switch(config)# do show ospf

OSPF Process 1, Router ID: 1.1.1.1
Supports only single TOS (TOS0) routes
This implementation conforms to RFC2328
RFC1583Compatibility flag is disabled
OpaqueCapability flag is disabled
Initial SPF scheduling delay 0 millisec(s)
Minimum hold time between consecutive SPFs 50 millisec(s)
Maximum hold time between consecutive SPFs 5000 millisec(s)
Hold time multiplier is currently 1
SPF algorithm has not been run
SPF timer is inactive
LSA minimum interval 0 msecs
LSA minimum arrival 0 msecs
Write Multiplier set to 0
Refresh timer 10 secs
Number of external LSA 0. Checksum Sum 0x00000000
Number of opaque AS LSA 0. Checksum Sum 0x00000000
Number of areas attached to this router: 0
```

### 2.39.3 timers throttle spf

| | |
|---|---|
| **Syntax** | **timers throttle spf <0-600000> <0-600000> <0-600000>**<br>**no timers throttle spf** |
| **Parameter** | **Delay time <0-60000>** — Initial SPF scheduling delay<br>**Hold time <0-60000>** — Minimum hold time between consecutive SPFs<br>**Max hold time <0-60000>** — Maximum hold time between consecutive SPFs |
| **Default** | delay time 0, hlod time 50, max hold time 5000 |
| **Mode** | OSPF Process Configuration Mode |
| **Usage** | Use the **timers throttle spf 10 100 10000** command to configure OSFP process 1 timer throttle spf, You can verify your setting by entering the **show ospf** Privileged EXEC command. |
| **Example** | The following example shows how to configure to ospf timers throttle spf.<br>`Switch(config)# ospf`<br>`Switch(config-ospf-1)# timers throttle spf 10 100 10000`<br>`Switch# show ospf` |

```
Switch(config-ospf-1)# timers throttle spf 10 100 10000
Switch(config-ospf-1)# exit
Switch(config)# do show ospf

 OSPF Process 1, Router ID: 1.1.1.1
 Supports only single TOS (TOS0) routes
 This implementation conforms to RFC2328
 RFC1583Compatibility flag is disabled
 OpaqueCapability flag is disabled
 Initial SPF scheduling delay 10 millisec(s)
 Minimum hold time between consecutive SPFs 100 millisec(s)
 Maximum hold time between consecutive SPFs 10000 millisec(s)
 Hold time multiplier is currently 1
 SPF algorithm has not been run
 SPF timer is inactive
 LSA minimum interval 0 msecs
 LSA minimum arrival 0 msecs
 Write Multiplier set to 0
 Refresh timer 10 secs
 Number of external LSA 0. Checksum Sum 0x00000000
 Number of opaque AS LSA 0. Checksum Sum 0x00000000
 Number of areas attached to this router: 0
```

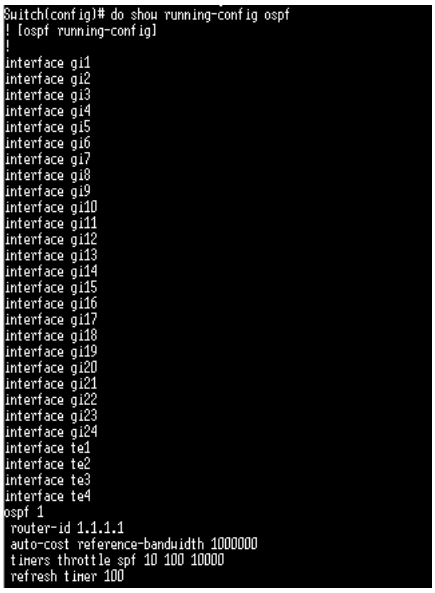
### 2.39.4 refresh timer

| | |
|---|---|
| **Syntax** | **refresh timers <10-1800>**<br>**no refresh timers** |
| **Parameter** | <0-60000> The refresh time interval |
| **Default** | Default is 10 secs |
| **Mode** | OSPF Process Configuration Mode |
| **Usage** | Use the **refresh timers** command to configure OSFP process 1 refresh time interval, You can verify your setting by entering the **show ospf** Privileged EXEC command. |
| **Example** | The following example shows how to configure to ospf refresh t timer.<br>`Switch(config)# ospf`<br>`Switch(config-ospf-1)# refresh timer 100`<br>`Switch# show ospf`<br>  |

## 2.39.5 auto-cost reference-bandwidth

| | |
|---|---|
| **Syntax** | **auto-cost reference-bandwidth <1-4294967>**<br>**no auto-cost reference-bandwidth** |
| **Parameter** | <1-429467> The value ranges from 1 to 4,294,967 in megabits |
| **Default** | Default is 100000 |
| **Mode** | OSPF Process Configuration Mode |
| **Usage** | Use the **auto-cost reference-bandwidth** command to configure OSFP process 1 referebce-bandwidth, You can verify your setting by entering the **show running-config ospf** Privileged EXEC command. |
| **Example** | The following example shows how to configure to ospf auto-cost reference-bandwidth. |

```
Switch(config)# ospf
Switch(config-ospf-1)# auto-cost reference-
                       bandwidth 1000000
Switch(config-ospf-1)# exit
Switch(config)# do show running-config ospf
```



### 2.39.6 default-metric

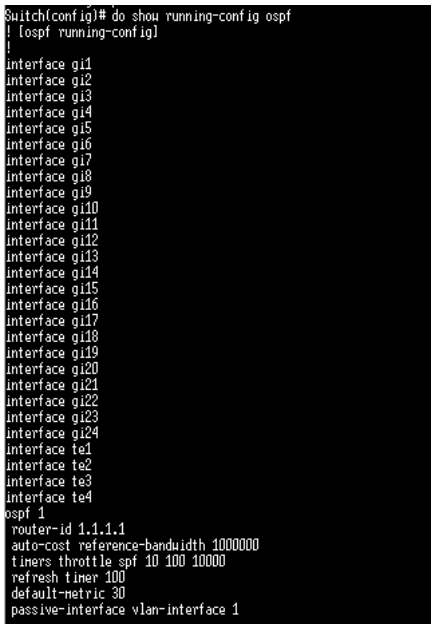
| | |
|---|---|
| **Syntax** | **default-metric <0-16777214>**<br>**no default-metric** |
| **Parameter** | <0-16777214> Set the default metric for importing routes. |
| **Default** | Default metric 20 |
| **Mode** | OSPF Process Configuration Mode |
| **Usage** | Use the **default-metric** command to configure OSFP process 1 metric, You can verify your setting by entering the **show running-config ospf** Privileged EXEC command. |
| **Example** | The following example shows how to configure to ospf default-metric.<br>Switch(config)# **ospf**<br>Switch(config-ospf-1)# **default-metric 30**<br>Switch(config-ospf-1)# **exit**<br>Switch(config)# **do show running-config ospf** |

```
Switch(config)# do show running-config ospf
[ [ospf running-config]
!
interface gi1
interface gi2
interface gi3
interface gi4
interface gi5
interface gi6
interface gi7
interface gi8
interface gi9
interface gi10
interface gi11
interface gi12
interface gi13
interface gi14
interface gi15
interface gi16
interface gi17
interface gi18
interface gi19
interface gi20
interface gi21
interface gi22
interface gi23
interface gi24
interface te1
interface te2
interface te3
interface te4
ospf 1
 router-id 1.1.1.1
 auto-cost reference-bandwidth 1000000
 timers throttle spf 10 100 10000
 refresh timer 100
 default-metric 30
```

### 2.39.7 passive-interface vlan-interface

| | |
|---|---|
| **Syntax** | **passive-interface vlan-interface <1-4094>**<br>**no passive-interface vlan-interface** |
| **Parameter** | <1-4094> Specify vlan-interface id |
| **Default** | N/A |
| **Mode** | OSPF Process Configuration Mode |
| **Usage** | Use the **passive-interface vlan-interface** configure the mode of OSPF process 1 on the specified interface, This parameter is used together with passive-interface default. You can verify your setting by entering the **show running-config ospf** Privileged EXEC command. |
| **Example** | The following example shows how to configure OSPF process 1 vlan interface 1 does not send hello packets |

```
Switch(config)# ospf
Switch(config-ospf-1)# passive-interface vlan-
                       interface 1
Switch(config)# do show running-config ospf
```



### 2.39.8 passive-interface default

| | |
|---|---|
| **Syntax** | **passive-interface default**<br>**no passive-interface default** |
| **Parameter** | N/A |
| **Default** | Default is disabled passive-interface default |
| **Mode** | OSPF Process Configuration Mode |
| **Usage** | Use the **passive-interface default** configure the passive-interface default on OSPF process 1 .You can verify your setting by entering the **show running-config ospf** Privileged EXEC command. |
| **Example** | The following example shows how to configure passive-interface default on OSPF process 1.<br>`Switch(config)# ospf`<br>`Switch(config-ospf-1)# passive-interface default`<br>`Switch(config)# do show running-config ospf` |

```
Switch(config)# show running-config ospf
! [ospf running-config]
!
interface gi1
interface gi2
interface gi3
interface gi4
interface gi5
interface gi6
interface gi7
interface gi8
interface gi9
interface gi10
interface gi11
interface gi12
interface gi13
interface gi14
interface gi15
interface gi16
interface gi17
interface gi18
interface gi19
interface gi20
interface gi21
interface gi22
interface gi23
interface gi24
interface te1
interface te2
interface te3
interface te4
ospf 1
 router-id 1.1.1.1
 auto-cost reference-banduidth 1000000
 timers throttle spf 10 100 10000
 refresh timer 100
 default-metric 30
 passive-interface default
```

## 2.39.9 area

| | |
|---|---|
| **Syntax** | **area (A.B.C.D\|<0-4294967295>)**<br>**no area (A.B.C.D\|<0-4294967295>)** |
| **Parameter** | **A.B.C.D** — Area ID, ip address format<br>**<0-4294967295>** — Area ID, The value is a decimal integer ranging from 0 to 4294967295. The system will process it as an IP address. |
| **Default** | N/A |
| **Mode** | OSPF Process Configuration Mode |
| **Usage** | Use the **area** configure OSPF process 1 area and enter area mode. You can verify your setting by entering the **show running-config ospf** Privileged EXEC command. |
| **Example** | The following example shows how to configure OSPF area and ID on OSPF process 1.<br>Switch(config)# **ospf**<br>`Switch(config-ospf-1)#area 0`<br>`Switch(config)# ospf`<br>`Switch(config-ospf-1)# area 0`<br>`Switch(config-ospf-1-area-0.0.0.0)#`<br>`Switch(config)# do show running-config ospf`<br>`auto-cost reference-banduidth 1000000`<br>`timers throttle spf 10 100 10000`<br>`refresh timer 100`<br>`default-metric 30`<br>`passive-interface default`<br>`area 0`<br>`exit` |

### 2.39.10 network

| | |
|---|---|
| **Syntax** | **network A.B.C.D/Mask**<br>**no network A.B.C.D/Mask** |
| **Parameter** | A.B.C.D/M IP Address and Mask |
| **Default** | By default, the interface does not belong to any area and the OSPF function is disabled. |
| **Mode** | OSPF area Configuration Mode |
| **Usage** | Use the **"network A.B.C.D/M"** command to enable OSPF in the OSPF area of each network interface of the device**.** You can verify your setting by entering the **show running-config ospf** Privileged EXEC command. |
| **Example** | The following example shows how to specify the IP address of the interface 10.1.1.0/24. OSPF is running in area 0. |

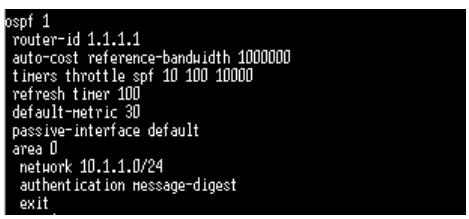
```
Switch(config)# ospf
Switch(config-ospf-1)#area 0
Switch(config-ospf-1-area-0.0.0.0)# network
                                        10.1.1.0/24
Switch(config)# do show running-config ospf
```

```
ospf 1
 router-id 1.1.1.1
 auto-cost reference-banduidth 1000000
 timers throttle spf 10 100 10000
 refresh timer 100
 default-metric 30
 passive-interface default
 area 0
  network 10.1.1.0/24
  exit
```

### 2.39.11 default-cost

| | |
|---|---|
| **Syntax** | **default-cost <0-16777215>**<br>**no default-cost** |
| **Parameter** | <0-16777215> Default cost |
| **Default** | Default is 1 |
| **Mode** | OSPF area Configuration Mode |
| **Usage** | Run the "default-cost <0-16777215>" command to configure the default cost of importing the default route to the stub/nssa area. This command only applies to the ABR router that is connected to the stub area or NSSA area. You can verify your setting by entering the show running-config ospf Privileged EXEC command. |
| **Example** | The following example shows how to configure default-cost on ospf area 1<br><br>`Switch(config)# ospf`<br>`Switch(config-ospf-1)#area 1`<br>`Switch(config-ospf-1-area-0.0.0.1)#default-cost 10` |

### 2.39.12 authentication

| | |
|---|---|
| **Syntax** | **authentication [message-digest]**<br>**no authentication** |
| **Parameter** | Message-digest: MD5 authentication mode. This parameter is optional. If this parameter is not selected, this parameter is simple authentication mode. |
| **Default** | Default is enabled |
| **Mode** | OSPF area Configuration Mode |
| **Usage** | Run the authentication command to configure the authentication mode for OSPF packets in an OSPF area. You can verify your setting by entering the show running-config ospf Privileged EXEC command. |
| **Example** | The following example shows how to configure authentication message-digest on area 0.<br><br>Switch(config)# **ospf**<br>Switch(config-ospf-1)#**area 0**<br>`Switch(config-ospf-1-area-0.0.0.0)#authentication message-digest`<br>  |

### 2.39.13 ospf authentication

| | |
|---|---|
| **Syntax** | **ospf authentication [(null \| message-digest)]**<br>**no ospf authentication** |
| **Parameter** | Message-digest: MD5 authentication mode. This parameter is optional. If this parameter is not selected, this parameter is simple authentication mode.(The password is in plaintext.)<br>null: no ospf authentication |
| **Default** | Default is disabled |
| **Mode** | Interface Configuration |
| **Usage** | Run the *ospf authentication* command to configure the interface to authenticate OSPF packets and the authentication mode.<br><br>Using the ospf authentication null and no ospf authentication commands, you can cancel the authentication mode configured on the related interface. |
| **Example** | The following example shows how to configure ospf authentication on vlan 1.<br><br>`Switch(config)# interface vlan 1`<br>`Switch(config-if-vlan1)# ospf authentication simple` |

### 2.39.14 ospf authentication-key

| | |
|---|---|
| **Syntax** | **ospf authentication-key WORD<1-64>**<br>**no ospf authentication-key** |
| **Parameter** | <1-64>: Plaintext password |
| **Default** | Default is no ospf authentication-key |
| **Mode** | Interface Configuration |
| **Usage** | Run the ospf authentication-key command to configure the plaintext password for the interface to authenticate OSPF packets. |
| **Example** | The following example shows how to configure ospf authentication -key on vlan 1.<br>`Switch(config)# interface vlan 1`<br>`Switch(config-if-vlan1)# ospf authenticatio-key 123456` |

### 2.39.15 ospf cost

| | |
|---|---|
| **Syntax** | **ospf cost <1-65535>**<br>**no ospf cost** |
| **Parameter** | <1-65535> OSPF Path Cost |
| **Default** | Default is 10 |
| **Mode** | Interface Configuration |
| **Usage** | Run the ospf cost command to set the cost for running OSPF on an interface |
| **Example** | The following example shows how to configure ospf cost on vlan 1.<br>`Switch(config)# interface vlan 1`<br>`Switch(config-if-vlan1)# ospf cost 20` |

### 2.39.16 ospf priority

| | |
|---|---|
| **Syntax** | **ospf priority <0-255>**<br>**no ospf priority** |
| **Parameter** | <0-255> The interface DR priority value |
| **Default** | Default is 1 |
| **Mode** | Interface Configuration |
| **Usage** | The **ospf priority** command is used to set the cost required for running OSPF on an interface.<br><br>The DR Priority of an interface determines the qualification of the interface in the DR/BDR election. A larger value indicates a higher priority. Those with higher priority are considered first in the event of a conflict over voting rights. If a device has a priority of 0, it is not elected as a DR Or BDR. |
| **Example** | The following example shows how to configure ospf priority on vlan 1.<br>`Switch(config)# interface vlan 1`<br>`Switch(config-if-vlan1)# ospf priority 10` |

### 2.39.17 ospf hello-interval

| | |
|---|---|
| **Syntax** | **ospf hello-interval <1-65535>**<br>**no ospf hello-interval** |
| **Parameter** | <1-65535> Interval for the interface to send Hello packets. The value ranges from 1 to 65535, in seconds |
| **Default** | Default is 10 seconds |
| **Mode** | Interface Configuration |
| **Usage** | Run the **ospf hello-interva**l command to set the interval for sending Hello packets on an interface. |
| **Example** | The following example shows how to configure ospf hello-interval on vlan 1.<br>`Switch(config)# interface vlan 1`<br>`Switch(config-if-vlan1)# ospf hello-interval 30` |

### 2.39.18 ospf dead-interval

| | |
|---|---|
| **Syntax** | **ospf dead-interval <1-65535>**<br>**no ospf dead-interval** |
| **Parameter** | <1-65535> Interval of interface neighbor failure The value ranges from 1 to 65535, in seconds |
| **Default** | By default, the invalid interval of OSPF neighbors on P2P and Broadcast interfaces is 40 seconds. The invalid time of the OSPF neighbor on the P2MP or NBMA interface is 120 seconds. |
| **Mode** | Interface Configuration |
| **Usage** | Run the ospf dead-interval command to set the dead interval of the OSPF neighbors on the interface |
| **Example** | The following example shows how to configure ospf dead-interval on vlan 1.<br>`Switch(config)# interface vlan 1`<br>`Switch(config-if-vlan1)# ospf dead-interval 30` |

### 2.39.19 ospf retransmit-interval

| | |
|---|---|
| **Syntax** | **ospf retransmit-interval <1-65535>**<br>**no ospf retransmit-interval** |
| **Parameter** | <1-65535> Interval for retransmitting LSA on an interface. The value ranges from 1 to 65535, in seconds |
| **Default** | Default is 5 seconds |
| **Mode** | Interface Configuration |
| **Usage** | Run the **ospf retransmit-interval** command to set the invalid time of the OSPF neighbor on the interface. |
| **Example** | The following example shows how to configure ospf retransmit-interval on vlan 1.<br>`Switch(config)# interface vlan 1`<br>`Switch(config-if-vlan1)# ospf retransmit-interval 10` |

### 2.39.20 ospf transmit-delay

| | |
|---|---|
| **Syntax** | **ospf transmit-delay <1-65535>**<br>**no ospf transmit-delay** |
| **Parameter** | <1-65535> Delay for transmitting LSA on an interface<br>The value ranges from 1 to 65535, in seconds |
| **Default** | Default is 1 seconds |
| **Mode** | Interface Configuration |
| **Usage** | Run the **ospf transmit-delay** command to set the time for the OSPF neighbor failure on the interface |
| **Example** | The following example shows how to configure ospf transmit-delay on vlan 1.<br>`Switch(config)# interface vlan 1`<br>`Switch(config-if-vlan1)# ospf transmit-delay 2` |

### 2.39.21 ospf network

| | |
|---|---|
| **Syntax** | **ospf network (broadcast\|non-broadcast\|point-to-multipoint\|point-to-point)**<br>**no ospf network** |
| **Parameter** | broadcast — The OSPF network type of the interface is broadcast<br>non-broadcast — The OSPF network type of the interface is NBMA<br>Point-to-multipoint — The OSPF network type of the interface is PTMP<br>point-to-point — The OSPF network type of the interface is PTP |
| **Default** | Default is broadcast |
| **Mode** | Interface Configuration |
| **Usage** | Run the ospf transmit-delay command to configure the OSPF network type of the interface |
| **Example** | The following example shows how to configure ospf network on vlan 1.<br>`Switch(config)# interface vlan 1`<br>`Switch(config-if-vlan1)# ospf network point-to-point` |

### 2.39.22 ospf mtu-ignore

| | |
|---|---|
| **Syntax** | **ospf mtu-ignore**<br>**no ospf mtu-ignore** |
| **Parameter** | N/A |
| **Default** | Default to check the MTU |
| **Mode** | Interface Configuration |
| **Usage** | Run the **ospf mtu-ignore** command to configure the interface not to check the MTU size during DD switching. |
| **Example** | The following example shows how to configure ospf mtu-ignore on vlan 1.<br>`Switch(config)# interface vlan 1`<br>`Switch(config-if-vlan1)# ospf mtu-ignore` |

# 2.40 RIP

## 2.40.1 distance

| | |
|---|---|
| **Syntax** | **distance num**<br>**no distance num** |
| **Parameter** | <1-255> — A decimal value from 1 through 255 that designates the administrative distance for all RIP routes. |
| **Default** | N/A |
| **Mode** | RIP Router configuration mode |
| **Usage** | Routes with lower administrative distance are more likely to be used when administrative distance is used for route comparison. |
| **Example** | The following example sets the administrative distance for RIP routes to 150.<br>`Switch(config)# rip`<br>`Switch(config-rip)# distance 150`<br>`Switch(config-rip)# exit` |

## 2.40.2 distribute-list in

| | |
|---|---|
| **Syntax** | **ip rip distribute-list access access-list-name in**<br>**no ip rip distribute-list in** |
| **Parameter** | access-list-name — Standard IP access list name, up to 32 characters. The list defines which routes in incoming RIP update messages are to be accepted and which are to be suppressed. |
| **Default** | No filtering |
| **Mode** | RIP Configuration mode |
| **Usage** | The **ip rip distribute-list in** rip configuration mode command enables filtering of routes in incoming RIP update messages. The **no** format of the command disables the filtering.<br><br>Each network from a received RIP update message is evaluated by the access list and it is accepted only if it is permitted by the list. See the ip access-list (IP standard) and ip prefix-list commands for details. |

**Example** The following example shows how to define input filtering:

```
Switch(config)#rip
switch(config-rip)# distribute-list 5 in interface
                                    vlan 1
switch(config-route-map)# exit
```

```
Switch(config)# do show rip

  Rip status      : on
  Rip version     : V2 (send V2, receive V1/2)
  Updates time    : 30 sec
  Age  time       : 180 sec
  Garbage-collect time  : 120 sec
  Default redistribution metric : 1
  Routing for Networks:

distribute list:
    intfv0 incoming filtered by 5
```

### 2.40.3 ip rip distribute-list out

**Syntax** **rip distribute-list access access-list-name out**
**no rip distribute-list out**

**Parameter**

| | |
|---|---|
| access-list-name | Standard IP access list name, up to 32 characters. The list defines which routes in outgoing RIP update messages are to be sent and which are to be suppressed. |

**Default** No filtering

**Mode** RIP Configuration mode

**Usage** The **rip distribute-list out** IP configuration mode command enables filtering of routes in outgoing RIP update messages. The **no** format of the command disables the filtering.

Each network from the IP Forwarding table is evaluated by the list and it is included in the RIP update message only if it is permitted by the list. See the ip access-list (IP standard) and ip prefix-list commands.

**Example** The following example shows how to define outgoing filtering:

```
switch(config)# interface ip 1.1.1.1
switch(config-rip)# distribute-list 5 out int vlan
                                    2
switch(config-route-map)# exit
```

### 2.40.4 network

| | |
|---|---|
| **Syntax** | **network** ip-address<br>**no network** ip-address |
| **Parameter** | **ip-address** An IP address of a switch IP interface.<br>A.B.C.D/M |
| **Default** | N/A |
| **Mode** | RIP Configuration mode |
| **Usage** | RIP can be defined only on manually-configured IP interfaces, meaning that RIP cannot be defined on an IP address defined by DHCP or on a default IP address.<br><br>Use the no network CLI command to remove RIP on an IP Interface and remove its interface configuration. |
| **Example** | The following example shows how to enable RIP on IP interface 1.1.1.1 with the default interface configuration:<br><br>`switch(config)# router rip`<br>`switch(config-rip)# network 192.168.1.88/24`<br>`switch(config-rip)# exit` |

### 2.40.5 route

| | |
|---|---|
| **Syntax** | **route** <A.B.C.D/M><br>**no router rip** <A.B.C.D/M> |
| **Parameter** | N/A |
| **Default** | Default is disabled |
| **Mode** | RIP Configuration mode |
| **Usage** | If a value of the RIP global state is disabled (default value), RIP is not operational and cannot be configured. When this state is set, the RIP configuration is removed. The state may be set by the no router rip CLI command from any RIP global state. |

| | |
|---|---|
| **Example** | The following example shows how to enable RIP globally:<br>`switch(config)# rip`<br>`switch(config-rip)# route 10.0.0.0/8` |

## 2.41 PoE

### 2.41.1 PoE Port Setting

| | |
|---|---|
| **Syntax** | **poe**<br>**no poe** |
| **Parameter** | N/A |
| **Default** | All ports are enabled for poe power supply by default.<br>( Poe-enabled device) |
| **Mode** | Interface Configuration mode |
| **Usage** | Use the poe command in interface mode to enable port poe power supply.<br>Use the no poe command in interface mode to disable port poe power supply.<br>You can check the port poe working status by using the show poe Privileged EXEC command. |
| **Example** | The following example shows how to config poe.<br>`Switch(config)# interface GigabitEthernet 1`<br>`Switch(config-if)# poe`<br>`Switch# show poe` |

### 2.41.2 PoE Port Schedule Setting

| | | |
|---|---|---|
| **Syntax** | **poe schedule week** days **hour** hours<br>**no poe schedule week** days **hour** hours | |
| **Parameter** | days | Port poe power supply days |
| | hours | Port poe power supply hours |
| **Default** | All ports open POE function all day by default.<br>( PoE-enabled device) | |
| **Mode** | Interface Configuration mode | |
| **Usage** | Use the **poe schedule** command in interface mode to set port | |

poe power supply time.
Use the **no poe schedule** command in interface mode to clear port poe power supply time..
You can check the port poe work time setting view through the web.

**Example**

The following example shows how to config poe schedule.

```
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.