COMMANDO IE2000 Series Switches Command Line Interface (CLI)

Note:

The software for all Soldier 2000 series switches are similar. This means, the GUI and the CLI of any 2000 series are interchangeably applicable to each other.

So, the model nos. and pictorial representation in this document may differ but it applicable. It may show Solider C2000 or E2000 Series, yet it is applicable to IE2000 Series as well.

INTRODUCTION

COMMANDO Solider IE2000 Series Industrial Ethernet, Managed Switches are fully managed, PoE+ Gigabit Ethernet switch with network resiliency and high availability, delivering robust performance and intelligent switching for growing networks. This series switches are easy to deploy, use, manage and designed exclusively for the networking needs of growing businesses and provide PoE+/PoE++ power on all ports. The security features equipped with today's advance networking hardware and software technology. This Series switches can be deployed in harsh environments to deliver hassle free mission-critical network services and surveillance requirements.

COMMANDO Solider IE2000 Series Industrial Ethernet, Managed Switches Series are fixed-configuration, with flexible uplinks Gigabit Ethernet switches that provide enterprise-class access for campus and branch applications. These Gigabit Ethernet switch enables home and office users to easily connect and supply power to high power wireless access points, PTZ (Pan Tilt Zoom) IP cameras, Surveillance cameras, VoIP telephony systems, kiosks, POS terminals, thin client, 802.11ac and 802.11ax access points, small cells, and connected LED lighting. It also provides the opportunity to add additional Ethernet devices like computers, printers, and Network Attached Storage (NAS) onto a network. This compact PoE+/PoE++ switch operates quietly, making it ideal for use in virtually any room or office. These switches are powerful and flexible enough for users to deploy wireless access points, surveillance cameras, IP phones and other PoE supported devices over longer distances up to 250 meters and support temperature range -40 C to 80° C. COMMANDO Solider IE2000 Series Industrial Ethernet, Managed provide easy device rack and wall mounting, on boarding, configuration, monitoring, and troubleshooting. These fully managed switches can provide advanced Layer 2+ and basic Layer 3 features as well as supports IEEE 802.3bt type-4 compliant PoE++ (Power over Ethernet Plus Plus)and 802.3at-compliant PoE+ (Power over Ethernet plus). Each switchport is capable to deliver 90 W PoE++ or 30 W PoE+ power on all ports along with automated power (ON/OFF) scheduling. All Switches are PoE+/PoE++ capable to provide power across all access ports for wireless APs, security cameras, and other IoT devices. Designed for operational simplicity to lower total cost of ownership, they enable scalable, secure, and energy-efficient business operations with intelligent and automated services.

COMMANDO Solider IE2000 Series Industrial Ethernet, Managed Switches Series provides a convenient and cost-effective wired access rack and wall mountable solution that can be quickly set up with Zero Touch Provisioning. Theses switches deliver

enhanced application, visibility, network reliability, and network resiliency and high availability.

COMMANDO Solider IE2000 Series Industrial Ethernet, Managed Switches has wire-speed back haul bandwidth capacity with flexible up to 1 Gigabit Ethernet copper/Fiber uplinks. This series also offers robust QoS, To optimize traffic on your Business Network, these switches provide (Port-based/802.1p/DSCP) QoS to keep latency-sensitive video and voice traffic jitter-free moving smoothly. Additionally, port-based, tag-based VLAN, Voice Vlans can improve security and meet more network segmentation requirements. This series switches also have provisioning of QOS, Static routing, IPV6 features. Moreover, with its innovative energy-efficient technology, can save up to 58% of power consumption, making it an eco-friendly perfect solution for your business network.

The COMMANDO SoldierOS IP Base switches provides CLI and WEBUI based PoE/PoE+ scheduling Premium feature. PoE/PoE+ Scheduling is a feature which allows you to specify the amount of time at scheduled time that power is delivered to a PoE/PoE+ port automatically making Switch intelligent . This not only can be used to save power when devices are not in use, but as a security feature to prevent wireless access from being available outside of business hours.It is possible to set a schedule for PoE/PoE+, a start time, an end time and which ports the PoE/PoE+ schedule applies to.

Intended Audience:

This document is intended for:

Network Device configuration and Troubleshooting Engineers

Internetworking Professionals and Experts

System maintenance engineers

Command Symbols

The command symbols that may be found in this document are defined as follows.

Table 1. General command symbols

Symbols	Description

Boldface	The keywords of a command line are in **boldface**. These Keywords are command syntax.
Italic	Command arguments are in *italics.*
[ ]	Items (keywords or arguments) in brackets [ ] are optional.
< >	Compulsory input.
{ }	Optional items.
|	Separated by vertical bars. One item is selected.
#	# sign is comments.

Management Access Modes

COMMANDO SoldierOS IP Base switches Management is made easy via a web-based Graphical User Interface (WEBUI) access via HTTP/HTTPS or industry-standard Command Line Interface (CLI) via Console/Telnet with administration traffic protected via , SNMP v1/v2C/v3, SSH v1/v2, RMON v1/v2 which enables the switch to be polled for valuable status information and allows it to send traps when abnormal events occur.

Simplified Configuration and Management

Zero-Touch Provisioning (ZTP) simplifies installation of the switch. Easy to manage via Console/web-Based Management (WEBUI)/Telnet/SSH/ HTTPS.

Remote Manageability

Remote management is the process that allows the administrators to take full control of all operations using a remote. This remote management via WEBUI / Telnet/ SSH/ HTTPS will reduce time and money spent on management and maintenance and physical presence of Network Engineer.

Management by CLI- Console, Telnet (RFC854) up to 3 sessions

Management by WebUI- HTTP, HTTPS for management Based on Remote Configuration and maintenance Using Telnet.

In this CLI guide we will understand Management by Command Line Interface(CLI) through console port, telnet management mode.

Accessing the Switch via console port

How to Login COMMANDO Series IE2000 via console port?

The console interface is used by connecting the Switch to an VT100–compatible terminal or a computer running an ordinary terminal emulator program (e.g., the HyperTerminal program included with the Windows operating system) using an RS–232C serial cable. Your terminal parameters will need to be set to:

• VT–100 compatible

• 115200 baud

• 8 data bits

• No parity

• One stop bit

• No flow control

Users may also access the same functions over a Telnet interface. Once you have set an IP address for your Switch, you can use a Telnet program (in VT–100 compatible terminal mode) to access and control the Switch. All of the screens are identical, whether accessed from the console port or from a Telnet interface.

Step 1 :Connect the Switch console port with PC/Laptop via console cable.

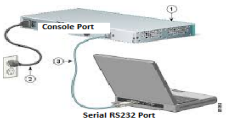


Fig-1. Connection of console port with PC/Laptop via console cable.

Step 2 The communication parameters configuration of the Putty Terminal with console is shown below Baud rate (Speed):**115200**

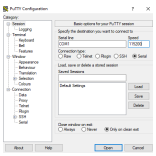


Fig-2. Putty configuration in PC for console port access

Step 3 : Click on **“Open”.** You will get following window.

With the console port properly connected to a management computer, the following screen should be visible.

Fig-3. COMMANDO Series IE2000 Switch CLI access via console port

How to Login COMMANDO Series IE2000 WEBUI and Enable Telnet?

Before Accessing Command Line Interface via telnet you have to login to WEBUI of COMMANDO IE2000 Switch. Connect one Ethernet port to your system with RJ45 LAN cable.

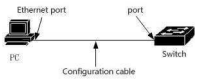


Fig-4. COMMANDO Series IE2000 Switch port connected with PC via RJ45 LAN cable.

In PC following LAN setting required.

• Open **Network and sharing center**.

• Click **change Adapter** settings.

• Double click on **Local Area Connection**.

• Click P**roperties**.

• Double click on **Internet Protocol Version 4(TCP/IPv4)** option and set default IP as shown below.

IP Address: : 192.168.0.(2-254)

Subnet Mask: 255.255.255.0

Default Gateway: **192.168.0.1**

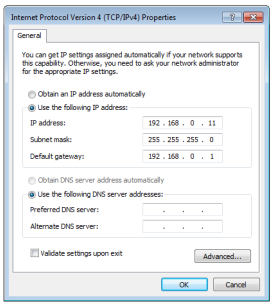


Fig-5. Local Area Connection properties for Web Interface

Now Open any web browser type http://192.168.0.1 and hit **“Enter”** following window will appear.

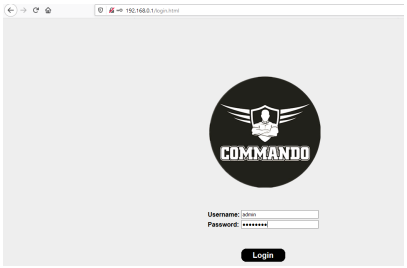


Fig-6. COMMANDO IE2000 Switch WEBUI Administrator Login Page

Use following login details to enter in WEBUI mode,

Username: **admin**

Password: **********

(Note:- Password is mentioned on backside of device)

Enter the login button. COMMANDO IE2000 series switch starting Page appears .

Following steps are required to access CLI via telnet lines.

Click on **"Management"**

Click on **"Management Access**

Click on **"Management Services**

Telnet Click on

Image not found or type unknown

“Apply” and **“Save”** the configuration.

This is required stage before accessing COMMANDO IE2000 Switch Command Line Interface (CLI) to enable **“Telnet”.** By default **“Telnet”** service is disabled so you have to enable it.

To view and configure Telnet, SSH,HTTP,HTTPS, SNMP along with , Session Timeout,Password Retry Count,Silent Time click on **Management >>Management Access>>Management Service**

Note:- By default HTTP access is enabled.

Now you will be able to login through Telnet by using any putty software.

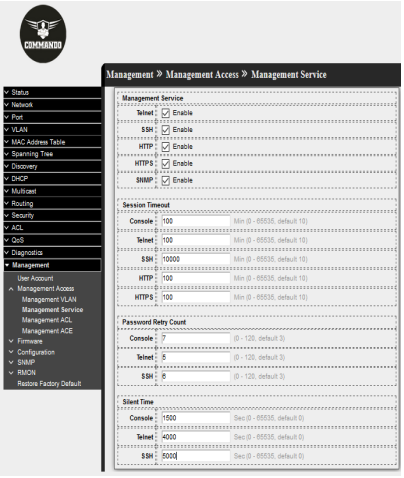


Fig-7. COMMANDO IE2000 Switch Management Access service.

Users access CLI through TELNET

Following are the steps to access CLI via telnet.

Step 1 : Connect the LAN port of PC/Laptop with any Ethernet port of the switch by LAN cable.

Step 2 The communication parameters configuration of the Putty Terminal with TELNET is shown below

IP Address: **192.168.0.1**

Port: **23**

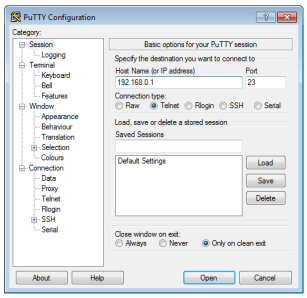


Fig-8. Putty configuration in PC for Telnet access

Step 3: Click on **“Open”**. You will get following window.

Username: **admin**

Password: **********

(Note:- Password is mentioned on backside of device)

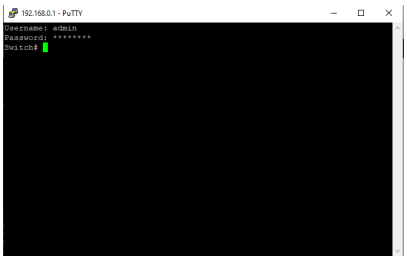


Fig-9. COMMANDO Series IE2000 Switch CLI access via telnet

ADMINISTRATION

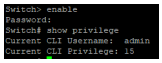
Syntax	**clear (authentication|gvrp|interfaces|ip|ipv6 |lacp|line|lldp|logging|mac|mvr|port-security|rmon|spanning-tree)**
Mode	Privileged EXEC
Example	This example shows how to clear interfaces, Switch# **clear interfaces GigabitEthernet 1 counters** 

1.4 ENABLE

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. 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#”.**

Switch>**enable [**<*1-15*>**]**

Switch#**disable [**<*1-14*>**]**

Syntax	**enable [***<1-15>***]** **disable [***<1-14>***]**
Parameter	*<1-15>* Specify privileged level to enable *<1-14>* Specify privileged level to disable
Default	Default privilege level is 15 if no privilege level is specified on enable command. Default privilege level is 1 if no privilege level is specified on disable command.
Mode	User EXEC
Example	This example shows how to enter privileged EXEC mode and show current privilege level. Switch>**enable** Password: Switch# **show privilege**  Switch# **disable** Switch>

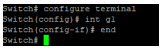
1.5 END

Use **“end”** command to return to privileged EXEC mode directly. Every mode except User EXEC mode has the **“end”** command.

Switch#**configure terminal**

Switch(config)# **interface GigabitEthernet 1**

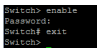
Switch(config-if)# **end**

Syntax	**end**
Mode	Privileged EXEC Global Configuration Interface Configuration Line Configuration
Example	This example shows how to enter Interface Configuration mode and use end command to go back to privileged EXEC mode Switch#**configure terminal** Switch(config)# **interface GigabitEthernet 1** Switch(config-if)# **end** Switch# 

1.6 EXIT

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.

Switch# **exit**

Syntax	**exit**
Mode	User EXEC Privileged EXEC Global Configuration Interface Configuration Line Configuration
Example	This example shows how to enter privileged EXEC mode and use exit command to go back to user EXEC mode. Switch>**enable** Switch# **exit** Switch> 

1.7 HISTORY

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.

Switch#**configure terminal**

Switch(config)# **line console**

Switch(config-line)# **history 100**

Switch(config-line)# **exit**

Syntax	**history** *<1-256>* **no history**
Parameter	*<1-256>*Specify maximum CLI history entry number.
Default	Default maximum history entry number is 128.
Mode	Line Configuration

This example shows how to change console history number to 100, telnet history number to 150 and ssh history number to 200.

Switch#**configure terminal**

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**

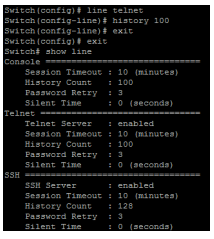
Switch(config)# **line ssh**

Switch(config-line)# **history 200**

Switch(config-line)# **exit**

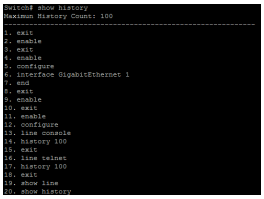
This example shows how show line information.

Switch# **show line**



This example shows how show history commands.

Switch# **show history**

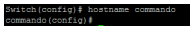


1.8 HOSTNAME

Use **“hostname”** command to modify hostname of the switch. The system name is also used to be CLI prompt.

Switch#**configure terminal**

Switch(config)# **hostname** *{WORD}*

Syntax	**hostname** *{WORD}*
Parameter	*WORD* Specify the hostname of the switch.
Default	Default name string is **“Switch”**.
Mode	Global Configuration
Example	This example shows how to modify contact information Switch#**configure terminal** Switch(config)# **hostname commando** commando(config)# 

1.9 INTERFACE

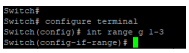
Some configurations are port based. In order to configure these configurations, we need to enter Interface Configuration mode to configure them. Use **“interface”** command to enter the Interface Configuration mode and select the port to be configured. In Interface Configuration mode, the prompt will show as **“Switch(config- if)#”**

Switch#**configure terminal**

Switch(config)# **interface** *{IF_PORTS}*

Switch(config)# **interface range** *{IF_PORT starting - IF_PORT ending }*

Syntax	**interface** *{IF_PORTS}* **interface range** *{IF_PORTS}*
Parameter	*IF_PORTS*Specify the port to select. This parameter allows partial port name and ignore case. For Example: GigabitEthernet 1, GigabitEthernet2, GigabitEthernet3 and so on If port range is specified, the list format is also available. For Example: gi1,3,5 gi2,gi1-3
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 terminal** Switch(config)# **interface GigabitEthernet 1** Switch(config-if)#  Switch#**configure terminal** Switch(config)# **interface range GigabitEthernet 1-3** Switch(config-if-range)# 

1.10 IP ADDRESS

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 IE2000 series switches.

Note:- By default Switch is having 192.168.0.1 as access IP.

Switch#**configure terminal**

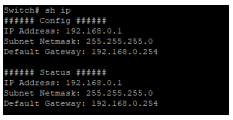
Switch(config)# **ip address** *{A.B.C.D}* **[mask** *{A.B.C.D}***]**

Syntax	**ip address A.B.C.D [mask A.B.C.D]**
Parameter	address A.B.C.D Specify IPv4 address for switch mask A.B.C.D Specify net mask address for switch
Default	Default IP address is 192.168.0.1 and default net mask is 255.255.255.0.
Mode	Global Configuration

Example

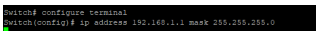
This example shows how to modify the ipv4 address of the switch.

Default setting of IE2000 series Switches



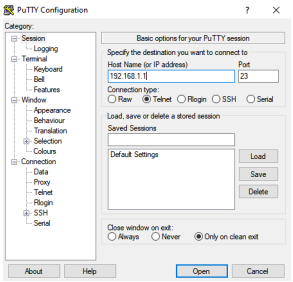
Switch#**configure terminal**

Switch(config)# **ip address 192.168.1.1 mask 255.255.255.0**

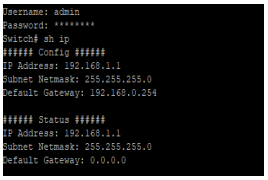


After this configuration you can access Switch with 192.168.1.1 IP address.

Accessing New IP address with Telnet.



This way to access with newly set IP address.



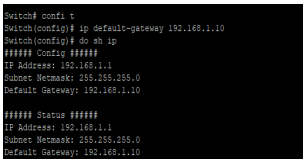
1.11 DEFAULT-GATEWAY

Use **“ip default-gateway”** command to modify default gateway address. And use **“no ip default-gateway”** to restore default gateway address to factory default.

Switch#**configure terminal**

Switch(config)# **ip default-gateway** *{A.B.C.D}*

Switch(config)# **no ip default-gateway**

Syntax	**ip default-gateway** *{A.B.C.D}* **no ip default-gateway**
Parameter	*A.B.C.D* Specify default gateway IPv4 address for switch
Default	Default IP address of default gateway is 192.168.0.254.
Mode	Global Configuration
Example	This example shows how to modify the ipv4 address of the switch. Switch#**configure terminal** Switch(config)# **ip default-gateway 192.168.1.10** This example shows how to show current ipv4 default gateway of the switch.  Switch# confi t Switch(config)# ip default-gateway 192.168.1.10 Switch(config)# do sh ip ##### Config ##### IP Address: 192.168.1.1 Subnet Netmask: 255.255.255.0 Default Gateway: 192.168.1.10 ##### Status ##### IP Address: 192.168.1.1 Subnet Netmask: 255.255.255.0 Default Gateway: 192.168.1.10

1.12 IP DHCP

Use **“ip dhcp”** command to enabled dhcp client to get IP address from remote DHCP server.

Use **“no ip dhcp”** command to disabled dhcp client and use static ip address.

Switch#**configure terminal**

Switch(config)# **ip dhcp**

Switch(config)# **no ip dhcp**

Syntax	**ip dhcp** **no ip dhcp**
Default	Default DHCP client is disabled.
Mode	Global Configuration
Example	This example shows how to enable dhcp client. Switch#**configure terminal** Switch(config)# **ip dhcp** This example shows how to show current dhcp client state of the switch. Switch# **show ip dhcp** 

1.13 IPV6 AUTOCONFIG

Use **“ipv6 autoconfig”** command to enabled IPv6 auto configuration feature. Use **“no ipv6 autoconfig”**command to disabled IPv6 auto configuration feature.

Switch#**configure terminal**

Switch(config)# **ipv6 autoconfig**

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

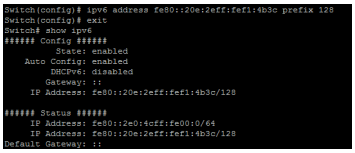
Syntax	**ipv6 autoconfig** **no ipv6 autoconfig**
Default	Default IPv6 auto config is enabled.
Mode	Global Configuration
Example	This example shows how to enable IPv6 auto config. Switch#**configure terminal** Switch(config)# **ipv6 autoconfig** This example shows how to show current IPv6 auto config state. Switch# **show ipv6** 

1.14 IPV6 ADDRESS

Use **“ipv6 address”** command to specify static IPv6 address.

Switch#**configure terminal**

Switch(config)# **ipv6 address** *{X:X::X:X}* **prefix** *<0-128>*

Syntax	**ipv6 address** *X:X::X:X* **prefix** *<0-128>*
Parameter	**address***X:X::X:X* Specify IPv6 address for switch **prefix***<0-128>* Specify IPv6 prefix length for switch
Mode	Global Configuration
Example	This example shows how to add static ipv6 address of the switch. Switch#**configure terminal** Switch(config)# **ipv6 address fe80::20e:2eff:fef1:4b3c prefix 128** This example shows how to show current ipv6 address of the switch. Switch# **show ipv6** 

```
Switch(config)# ipv6 address fe80::20e:2eff:fef1:4b3c prefix 128
Switch(config)# exit
Switch# show ipv6
###### Config ######
        State: enabled
    Auto Config: enabled
        DHCPv6: disabled
       Gateway: ::
    IP Address: fe80::20e:2eff:fef1:4b3c/128

###### Status ######
    IP Address: fe80::2e0:4cff:fe00:0/64
    IP Address: fe80::20e:2eff:fef1:4b3c/128
Default Gateway: ::
```

1.15 IPV6 DEFAULT-GATEWAY

Use **“ipv6 default-gateway”** command to modify default gateway IPv6.

Switch#**configure terminal**

Switch(config)# **ipv6 default-gateway** *{X:X::X:X}*

Syntax	**ipv6 default-gateway** *{X:X::X:X}*
Parameter	*X:X::X:X* Specify default gateway IPv6 address for switch
Mode	Global Configuration
Example	This example shows how to modify the ipv6 default gateway address of the switch. Switch#**configure terminal** Switch(config)# **ipv6 default-gateway fe80::dcad:beff:feef:103** Switch# **show ipv6** 

```
Switch(config)# ipv6 default-gateway fe80::dcad:beff:feef:103
Switch(config)# exit
Switch# show ipv6
##### Config #####
          State: enabled
    Auto Config: enabled
         DHCPv6: disabled
        Gateway: fe80::dcad:beff:feef:103
     IP Address: fe80::20e:2eff:fef1:4b3c/128

##### Status #####
     IP Address: fe80::2e0:4cff:fe00:0/64
     IP Address: fe80::20e:2eff:fef1:4b3c/128
Default Gateway: ::
```

1.16 IPV6 DHCP

Use **“ipv6 dhcp”** command to enabled dhcpv6 client to get IP address from remote DHCPv6 server.Use **“no ipv6 dhcp”** command to disabled dhcpv6 client and use static ipv6 address or ipv6 auto config address.

Switch#**configure terminal**

Switch(config)# **ipv6 dhcp**

Switch(config)# **no ipv6 dhcp**

Syntax	**ipv6 dhcp** **no ipv6 dhcp**
Default	Default DHCPv6 client is disabled.
Mode	Global Configuration
Example	This example shows how to enable dhcp client. Switch#**configure terminal** Switch(config)# **ipv6 dhcp** This example shows how to show current dhcpv6 client state of the switch. Switch# **show ipv6** 

```
Switch(config)# ipv6 dhcp
Switch(config)# exit
Switch# show ipv6
###### Config ######
          State: enabled
    Auto Config: enabled
         DHCPv6: enabled
        Gateway: fe80::dcad:beff:feef:103
     IP Address: fe80::20e:2eff:fef1:4b3c/128

###### Status ######
     IP Address: fe80::2e0:4cff:fe00:0/64
     IP Address: fe80::20e:2eff:fef1:4b3c/128
Default Gateway: ::
Switch#
```

1.17 IP SERVICE

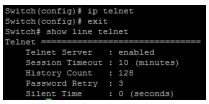
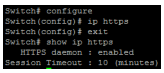
This is one of very important command to enable/disable management access via CLI. Use **“ip (telnet | ssh | http | https)”** command to enable all kinds of management services. Such as telnet, ssh, http and https from CLI.

Switch#**configure terminal**

Switch(config)# **ip (telnet | ssh | http | https)**

Switch(config)# **no ip (telnet | ssh | http | https)**

Syntax	**ip (telnet | ssh | http | https)** **no ip (telnet | ssh | http | https)**
Parameter	telnet Enable/Disable telnet service ssh Enable/Disable ssh service http Enable/Disable http service https Enable/Disable https service
Default	Default telnet service is disabled. Default ssh service is disabled. Default http service is enabled. Default https service is disabled.
Mode	Global Configuration

Example	This example shows how to enable telnet service and show current telnet service status. Switch#**configure terminal** Switch(config)# **ip telnet** Telnet daemon enabled. Switch(config)# **exit** Switch# **show line telnet**  This example shows how to enable https service and show current https service status. Switch#**configure terminal** Switch(config)# **ip https** Switch(config)# **exit** Switch# **show ip https** 

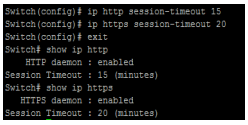
1.18 IP SESSION-TIMEOUT

Use **“ip session-timeout”** command to specify the session timeout value for http or https service. When user login into WEBGUI and do not do any action after session timeout will be logged out.

Switch#**configure terminal**

Switch(config)# **ip (http | https) session-timeout** *<0-86400>*

Syntax	**ip (http | https) session-timeout** *<0-86400>*
Parameter	httpSpecify 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

Example	This example shows how to change http session timeout to 15min and https session timeout to 20min Switch#**configure terminal** Switch(config)# **ip http session-timeout 15** Switch(config)# **ip https session-timeout 20** This example shows how to enable https service and show current https service status. Switch# **show ip http** Switch# **show ip https** 

1.19 IP SSH

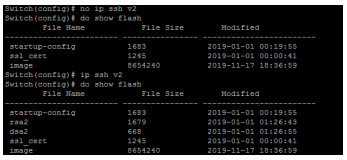
Use **“ip ssh”** command to generate the key files for ssh connection.

Switch#**configure terminal**

Switch(config)# **ip ssh (v1|v2|all)**

Switch(config)# **no ip ssh (v1|v2|all**)

Syntax	**ip ssh (v1|v2|all)** **no ip ssh (v1|v2|all**)

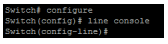
Parameter	v1 Generate/Delete version 1 key files v2 Generate/Delete version 2 key files all Generate/Delete version 1 and 2 key files
Default	Version 2 key files will be generated by default
Mode	Global Configuration
Example	This example shows how to delete and re-generate ssh version 2 key files. Switch#**configure terminal** Switch(config)# **no ip ssh v2** Switch(config)# **do show flash** Switch(config)# **ip ssh v2** Switch(config)# **do show flash** 

1.20 LINE

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.In Line Configuration mode, the prompt will show as **“Switch(config-line)#”**

Switch#configure terminal

Switch(config)# **line (console | telnet | ssh)**

Syntax	**line (console | telnet | ssh)**
Parameter	console Select console line to configure. Telnet Select telnet line to configure. Ssh Select ssh line to configure.
Mode	Global Configuration
Example	This example shows how to enter Interface Configuration mode Switch# **configure** Switch(config)# **line console** Switch(config-line)# 

1.21 REBOOT

Use **“reboot”** command to make system hot restart. Switch will be Power OFF and again ON (Restart) with this command.

Switch#**reboot**

Syntax	**reboot**
Mode	Privileged EXEC
Example	This example shows how to restart the system Switch# **reboot**

1.22 ENABLE PASSWORD

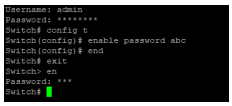
Use **“enable password”** command to edit password for each privilege level for enable authentication. Use **“no enable”** command to restore enable password to default empty value. The only way to show this configuration is using **“show running-config”** command.

Switch#**configure terminal**

Switch(config)# **enable [privilege** <*1-15*>**] (password UNENCRYPY-PASSWORD | secret UNENCRYPY-PASSWORD | secret encrypted ENCRYPT-PASSWORD)**

Switch(config)# **no enable [privilege** <*0-15*>**]**

Syntax	**enable [privilege** <*1-15*>**] (password UNENCRYPT-PASSWORD | secret** **UNENCRYPT-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 UNENCRYPT**-Specify password string and make it not encrypted. **secret UNENCRYPT- 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	No default enable password for all privilege levels.
Mode	Global Configuration
Example	This example shows how to edit enable password for privilege level 15 Switch#configure terminal Switch(config)# **enable password** abc  Configuration of privileged level for enable passwords This example shows how to set privilege level for enable password. Switch#configure terminal Switch(config)# **enable privilege 15 secret xyz** 

1.23 EXEC-TIMEOUT

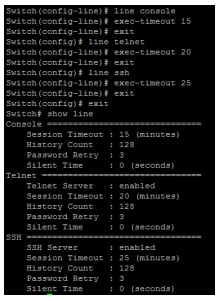
Use **“exec-timeout”** command to specify the session timeout value for CLI running on console, telnet or ssh service. When user login into CLI and do not do any action after session timeout will be logged out from the CLI session.

Switch#**configure terminal**

Switch(config)# **line console**

Switch(config-line)# **exec-timeout** <*0-65535*>

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

Example	This example shows how to change console session timeout to 15min, telnet session timeout to 20min and ssh session timeout to 25min. Timeout after specified minutes (0 means no timeout) Switch#**configure terminal** Switch(config)# **line console** Switch(config-line)# **exec-timeout 15** Switch(config-line)# **exit** Switch(config)# **line telnet** Switch(config-line)# **exec-timeout 20** Switch(config-line)# **exit** Switch(config)# **line ssh** Switch(config-line)# **exec-timeout 25** Switch(config-line)# **exit** This example shows how show line information. Switch# **show line** 

1.24 PASSWORD-THRESH

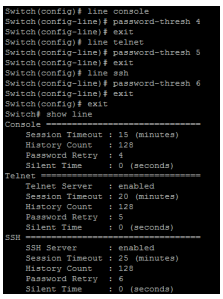
Use **“password-thresh”** command to specify the password fail retry number for CLI running on console, telnet or ssh service. When user input password to login and authenticate failed, the fail retry number will increase one. After fail retry number exceed configured one, the CLI will block login for the period of silent time which configured by the command **“silent-time”.**

Switch#**configure terminal**

Switch(config)# **line console**

Switch(config-line)# **password-thresh 4**

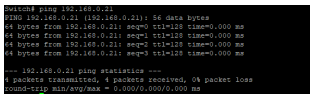
Syntax	**password-thresh** *<0-120>*
Parameter	*<0-120>*Specify password fail retry number. 0 means no limit.
Default	Default password fail retry number is 3.
Mode	Line Configuration

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. The number of allowed password attempts. (Range: 0-120; 0: no threshold) Switch#**configure terminal** Switch(config)# **line console** Switch(config-line)# **password-thresh 4** Switch(config-line)# **exit** Switch(config)# line **telnet** Switch(config-line)# **password-thresh 5** Switch(config-line)# **exit** Switch(config)# **line ssh** Switch(config-line)# **password-thresh 6** Switch(config-line)# **exit** This example shows how show line information. Switch# **show line**  Switch(config)# line console Switch(config-line)# password-thresh 4 Switch(config-line)# exit Switch(config)# line telnet Switch(config-line)# password-thresh 5 Switch(config-line)# exit Switch(config)# line ssh Switch(config-line)# password-thresh 6 Switch(config-line)# exit Switch(config)# exit Switch# show line Console ========== Session Timeout : 15 (minutes) History Count : 128 Password Retry : 4 Silent Time : 0 (seconds) Telnet ========== Telnet Server : enabled Session Timeout : 20 (minutes) History Count : 128 Password Retry : 5 Silent Time : 0 (seconds) SSH ========== SSH Server : enabled Session Timeout : 25 (minutes) History Count : 128 Password Retry : 6 Silent Time : 0 (seconds)

1.25 PING

Ping (Packet Internet Groper) tests the connection between two network nodes by sending packets to a host and measure the round-trip time. Use **“ping”** command to do network ping diagnostic.

Switch# **ping** *HOSTNAME* **[count** <*1-999999999*>**]**

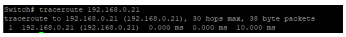
Syntax	**ping** *HOSTNAME* **[count** <*1-999999999*>**]**
Parameter	*HOSTNAME* Specify IPv4/IPv6 address or domain name to ping. count<*1-999999999*> Specify how many times to ping.
Mode	User EXEC Privileged EXEC
Example	This example shows how to ping remote host 192.168.0.21 Switch# **ping 192.168.0.21** 

1.26 TRACEROUTE

Traceroute discovers the IP routes along which packets were forwarded by sending an IP packet to the target host and back to the device. The Trace route page shows each hop between the device and a target host, and the round-trip time to each such hop.

Use **“traceroute”** command to do network trace route diagnostic.

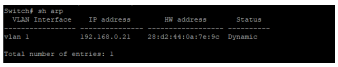
Switch# **traceroute** *{A.B.C.D}* **[max_hop**<*2-255*>**]**

Syntax	**Traceroute** *{A.B.C.D}* **[max_hop**<*2-255*>**]**
Parameter	*A.B.C.D* Specify IPv4 to trace. **max_hop**<*2-255*>Specify maximum hop to trace.
Mode	User EXEC Privileged EXEC
Example	This example shows how to trace route host 192.168.0.21. Switch# **traceroute 192.168.0.21** 

1.27 SHOW ARP

Use **“show arp”** command to show all arp entries.

Switch# **show arp**

Syntax	**show arp**
Mode	User EXEC Privileged EXEC
Example	This example shows how to show arp entries. Switch# **show arp** 

1.28 SHOW CPU UTILIZATION

Use **“show cpu utilization”** command to show current CPU utilization.

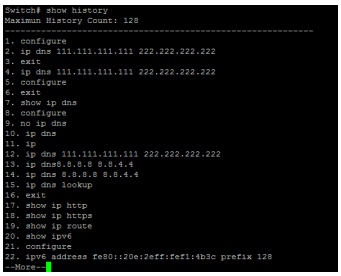
Switch# **show cpu utilization**

Syntax	**show cpu utilization**
Mode	Privileged EXEC
Example	This example shows how to show current CPU utilization. Switch# **show cpu utilization** 

1.29 SHOW HISTORY

Use **“show history”** to show commands we input before.

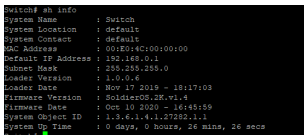
Switch# **show history**

Syntax	**show history**
Mode	User EXEC Privileged EXEC Global Configuration
Example	This example shows how show history commands. Switch# **show history** 

1.30 SHOW INFO

Use **“show info”** command to show system summary information.

Switch#**show info**

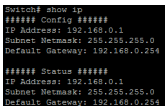
Syntax	**show info**
Mode	User EXEC Privileged EXEC
Example	This example shows how to show system version. Switch# **show info** 

```
Switch# sh info
System Name       : Switch
System Location   : default
System Contact    : default
MAC Address       : 00:E0:4C:00:00:00
Default IP Address : 192.168.0.1
Subnet Mask       : 255.255.255.0
Loader Version    : 1.0.0.6
Loader Date       : Nov 17 2018 - 18:17:03
Firmware Version  : SoldierOS.2K.v1.4
Firmware Date     : Oct 10 2020 - 16:45:59
System Object ID  : 1.3.6.1.4.1.27282.1.1
System Up Time    : 0 days, 0 hours, 26 mins, 26 secs
```

1.31 SHOW IP

Use **“show ip”** command to show system IPv4 address, net mask and default gateway.

Switch#**show ip**

Syntax	**show ip**
Mode	User EXEC Privileged EXEC
Example	This example shows how to show current ipv4 address of the switch. Switch# **show ip** 

1.32 SHOW IP DHCP

Use **“show ip dhcp”** command to show IPv4 dhcp client enable state.

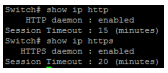
Switch#**show ip dhcp**

Syntax	**show ip dhcp**
Mode	User EXEC Privileged EXEC
Example	This example shows how to show current dhcp client state of the switch. Switch# **show ip dhcp** Switch# show ip dhcp DHCP Status : Enabled

1.33 SHOW IP HTTP

Use **“show ip http”** command to show HTTP/HTTPS information.

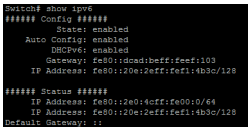
Switch#**show ip (http|https)**

Syntax	**show ip (http|https)**
Mode	Privileged EXEC
Example	This example shows how to show current ipv4 address of the switch. Switch# **show ip http** Switch# **show ip https** 

1.34 SHOW IPV6

Use **“show ipv6”** command to show system IPv6 address, net mask, default gateway and auto config state.

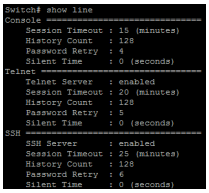
Switch#**show ipv6**

Syntax	**show ipv6**
Mode	User EXEC Privileged EXEC
Example	This example shows how to show current ipv6 address of the switch. Switch# **show ipv6** 

1.35 SHOW LINE

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.

Switch#**show line [(console | telnet | ssh)]**

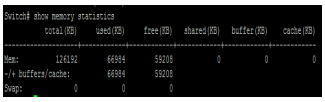
Syntax	**show line [(console | telnet | ssh)]**
Parameter	**console** Select console line to show. **telnet** Select telnet line to show. **Ssh** Select ssh line to show.
Mode	Privileged EXEC
Example	This example shows how show all lines’ information. Switch# **show line** 

```
Switch# show line
Console ==========================
    Session Timeout : 15 (minutes)
    History Count   : 128
    Password Retry  : 4
    Silent Time     : 0 (seconds)
Telnet ===========================
    Telnet Server   : enabled
    Session Timeout : 20 (minutes)
    History Count   : 128
    Password Retry  : 5
    Silent Time     : 0 (seconds)
SSH ==============================
    SSH Server      : enabled
    Session Timeout : 25 (minutes)
    History Count   : 128
    Password Retry  : 6
    Silent Time     : 0 (seconds)
```

1.36 SHOW MEMORY STATISTICS

Use **“show memory statistics”** command to show current memory utilization.

Switch#**show memory statistics**

Syntax	**show memory statistics**
Mode	Privileged EXEC
Example	This example shows how to show current system memory statistics. Switch# **show memory statistics** 

1.37 SHOW PRIVILEGE

Use **“show privilege”** command to show the privilege level of the current user.

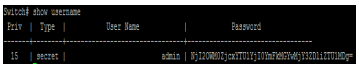
Switch#**show privilege**

Syntax	**show privilege**
Mode	User EXEC Privileged EXEC
Example	This example shows how to show arp entries. Switch# **show privilege** 

1.38 SHOW USERNAME

Use **“show username”**command shows all user accounts in local database.

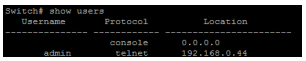
Switch#**show username**

Syntax	**show username**
Mode	Privileged EXEC
Example	This example shows how to show existing user accounts. Switch# **show username** 

1.39 SHOW USERS

Use **“show users”** command show information of all active users.

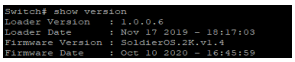
Switch#**show users**

Syntax	**show users**
Mode	Privileged EXEC
Example	This example shows how to show existing user accounts. Switch# **show users** 

1.40 SHOW VERSION

Use **“show version”** command to show loader and firmware version and build date.

Switch#**show version**

Syntax	**show version**
Mode	User EXEC Privileged EXEC
Example	This example shows how to show system version. Switch# **show version** 

1.41 SILENT-TIME

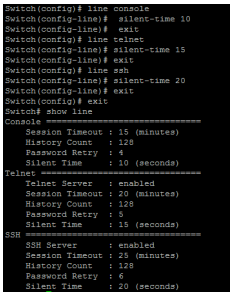
Use **“silent time”** command to specify the silent time for CLI running on console, telnet or ssh service. When user input password to login and authenticate failed, the fail retry number will increase one. After fail retry number exceed configured one, the CLI will block login for the period of silent time which configured by the command **“silent-time”**.

Switch#**configure terminal**

Switch(config)# **line {console|telnet|ssh|http}**

Switch(config-line)# **silent-time** <*0-65535*>

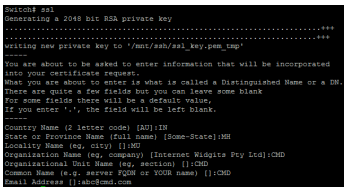
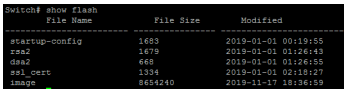
Syntax	**silent-time** <*0-65535*>
Parameter	<*0-65535*>Specify silent time with unit seconds. 0 means do not salient.
Default	Default silent time is 0.
Mode	Line Configuration

Example	This example shows how to change console silent time to 10, telnet silent time to 15 and ssh silent time to 20. Switch#**configure terminal** Switch(config)# **line console** Switch(config-line)# **silent-time 10** Switch(config-line)# **exit** Switch(config)# **line telnet** Switch(config-line)# **silent-time 15** Switch(config-line)# **exit** Switch(config)# **line ssh** Switch(config-line)# **silent-time 20** Switch(config-line)# **exit** This example shows how show line information. Switch# **show line**  Switch(config)# line console Switch(config-line)# silent-time 10 Switch(config-line)# exit Switch(config)# line telnet Switch(config-line)# silent-time 15 Switch(config-line)# exit Switch(config)# line ssh Switch(config-line)# silent-time 20 Switch(config-line)# exit Switch(config)# exit Switch# show line Console ========== Session Timeout : 15 (minutes) History Count : 128 Password Retry : 4 Silent Time : 10 (seconds) Telnet ========== Telnet Server : enabled Session Timeout : 20 (minutes) History Count : 128 Password Retry : 5 Silent Time : 15 (seconds) SSH ========== SSH Server : enabled Session Timeout : 25 (minutes) History Count : 128 Password Retry : 6 Silent Time : 20 (seconds)

1.42 SSL

Use **“ssl”** command to generate security certificate files such as RSA, DSA.

Switch#**ssl**

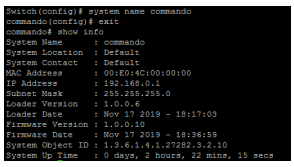
Syntax	**ssl**
Mode	Global Configuration
Example	This example shows how to generate certificate files. Switch# **ssl**  Switch# **show flash** 

1.43 SYSTEM NAME

Use **“system name”** command to modify system name information of the switch. The system name is also used to be CLI prompt.

Switch#**configure terminal**

Switch(config)#**system name** *{NAME}*

Syntax	**system name** *{NAME}*
Parameter NAME	*NAME* Specify system name string.
Default	Default name string is **“Switch”**.
Mode	Global Configuration
Example	This example shows how to modify contact information Switch#**configure terminal** Switch(config)# **system name** commando commando(config)# commando# **show info** 

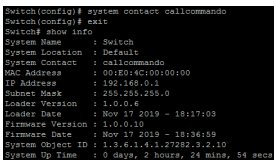
```
Switch(config)# system name commando
commando(config)# exit
commando# show info
System Name      : commando
System Location  : Default
System Contact   : Default
MAC Address      : 00:E0:4C:00:00:00
IP Address       : 192.168.0.1
Subnet Mask      : 255.255.255.0
Loader Version   : 1.0.0.6
Loader Date      : Nov 17 2019 - 18:17:03
Firmware Version : 1.0.0.10
Firmware Date    : Nov 17 2019 - 18:36:59
System Object ID : 1.3.6.1.4.1.27282.3.2.10
System Up Time   : 0 days, 2 hours, 22 mins, 15 secs
```

1.44 SYSTEM CONTACT

Use **“system contact”** command to modify contact information of the switch.

Switch#**configure terminal**

Switch(config)# **system contact** *{CONTACT}*

Syntax	**system contact** *{CONTACT}*
Parameter	*CONTACT* Specify contact string.
Default	Default contact string is **“Default Contact”**.
Mode	Global Configuration
Example	This example shows how to modify contact information Switch#**configure terminal** Switch(config)# **system contact callcommando** Switch# **show info** 

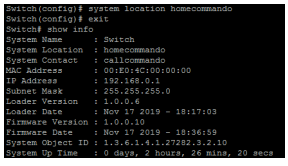
```
Switch(config)# system contact callcommando
Switch(config)# exit
Switch# show info
System Name      : Switch
System Location  : Default
System Contact   : callcommando
MAC Address      : 00:E0:4C:00:00:00
IP Address       : 192.168.0.1
Subnet Mask      : 255.255.255.0
Loader Version   : 1.0.0.6
Loader Date      : Nov 17 2019 - 18:17:03
Firmware Version : 1.0.0.10
Firmware Date    : Nov 17 2019 - 18:36:59
System Object ID : 1.3.6.1.4.1.27282.3.2.10
System Up Time   : 0 days, 2 hours, 24 mins, 54 secs
```

1.45 SYSTEM LOCATION

Use **“system location”** command to modify location information of the switch.

Switch#**configure terminal**

Switch(config)# **system location** *{LOCATION}*

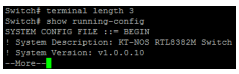
Syntax	**system location** *{LOCATION}*
Parameter	*LOCATION* Specify location string.
Default	Default location string is “**Default Location”.**
Mode	Global Configuration
Example	This example shows how to modify contact information Switch#**configure terminal** Switch(config)# **system location home** This example shows how to show system location information Switch# **show info** 

```
Switch(config)# system location homecommando
Switch(config)# exit
Switch# show info
System Name      : Switch
System Location  : homecommando
System Contact   : callcommando
MAC Address      : 00:E0:4C:00:00:00
IP Address       : 192.168.0.1
Subnet Mask      : 255.255.255.0
Loader Version   : 1.0.0.6
Loader Date      : Nov 17 2019 - 18:17:03
Firmware Version : 1.0.0.10
Firmware Date    : Nov 17 2019 - 18:36:59
System Object ID : 1.3.6.1.4.1.27282.3.2.10
System Up Time   : 0 days, 2 hours, 26 mins, 20 secs
```

1.46 TERMINAL LENGTH

Use **“terminal length”** command to specify the maximum line number the terminal is able to print.

Switch#**terminal length** *<0-24>*

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 Privileged EXEC
Example	This example shows how to change terminal length. Switch# **terminal length 3** Switch# **show running-config** 

1.47 USERNAME

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.

Switch#**configure terminal**

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

Switch(config)# **no username** *WORD<0-32>*

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

Parameter	**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 **“commando”** with privilege 15.
Mode	Global Configuration

<table>
<tr>
<td>Example</td>
<td>

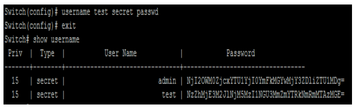
This example shows how to add a new user account.

Switch#configure terminal

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

This example shows how to show existing user accounts.

Switch# **show username**

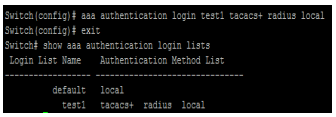
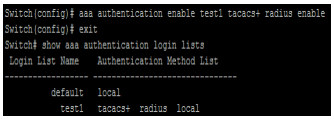


```
Switch(config)# username test secret passwd
Switch(config)# exit
Switch# show username
 Priv  |  Type  |          User Name          |           Password
-------+--------+-----------------------------+--------------------------------
  15   | secret |                       admin | NjI2OWM0ZjcxYTU1YjI0YmFkMGYwMjY3ZDliZTU1MDg=
  15   | secret |                        test | NzZhMjE3M2JlNjM5MzI1NGU3MmZmYTRkNmRmMTAzMGE=
```

</td>
</tr>
</table>

AAA (Authentication, Authorization, Accounting)

Syntax	**aaa authentication (login | enable) (default |** *listname* **)** *methodlist [methodlist] [methodlist] [methodlist]* **no aaa authentication (login | enable)** {listname}
Parameter	**login** Add/Edit login authentication list
	enable Add/Edit enable authentication list
	default Edit 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"**. Default authentication list name for type enable is **"default"** and default method is **"enable"**
Mode	Global Configuration

Example	This example shows how to add a login authentication list to authenticate with order tacacs+, radius, local. Switch(config)# **aaa authentication login test1 tacacs+ radius local** This example shows how to show existing login authentication lists Switch# **show aaa authentication login lists**  Switch(config)# **aaa authentication enable test1 tacacs+ radius enable** This example shows how to show existing enable authentication lists Switch# **show aaa authentication login lists Enable** 

2.1 LOGIN AUTHENTICATION

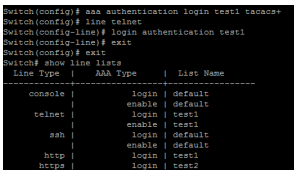
Different access methods are allowed to bind different login authentication lists. Use **“login authentication”** command to bind the list to specific line (console, telnet, ssh).

Switch#**configure terminal**

Switch(config-line)# **login authentication** {listname}

Switch(config-line)# **no login authentication**

Syntax	**login authentication** {listname} **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

Example	This example shows how to create a new login authentication list and bind to telnet line. Switch(config)# **aaa authentication login test1 (tacacs+| radius | local | none |enable)** Switch(config)# **line telnet** Switch(config-line)# **login authentication test1** This example shows how to show line binding lists. Switch# **show line lists** 

```
Switch(config)# aaa authentication login test1 tacacs+
Switch(config)# line telnet
Switch(config-line)# login authentication test1
Switch(config-line)# exit
Switch(config)# exit
Switch# show line lists
  Line Type  |    AAA Type      |  List Name
-------------+------------------+-----------
     console |            login | default
             |          enable | default
      telnet |            login | test1
             |          enable | test1
         ssh |            login | default
             |          enable | default
        http |            login | test1
       https |            login | test2
```

2.2 IP HTTP LOGIN AUTHENTICATION

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.

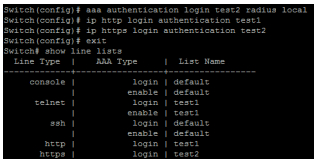
Switch#**configure terminal**

Switch(config)# **ip (http | https) login authentication** *{listname}*

Switch(config)# **no ip (http | https) login authentication**

Syntax	**ip (http | https) login authentication** *{listname}* **no ip (http | https) login authentication**

Parameter	**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

Example	This example shows how to create two new login authentication lists and bind to http and https. Switch#**configure terminal** Switch(config)# **aaa authentication login test1 tacacs+ radius local** Switch(config)# **aaa authentication login test2 radius local** Switch(config)# **ip http login authentication test1** Switch(config)# **ip https login authentication test2** This example shows how to show line binding lists. Switch# **show line lists** 

2.3 ENABLE AUTHENTICATION

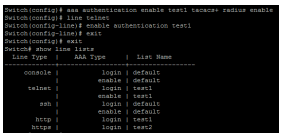
Different access methods are allowed to bind different enable authentication lists. Use **“enable authentication”** command to bind the list to specific line (console, telnet, ssh).

Switch#**configure terminal**

Switch(config-line)# **enable authentication** {listname}

Switch(config-line)# **no enable authentication**

Syntax	**enable authentication** {listname} **no enable authentication**
Parameter	listname Specify the enable authentication list name to use.
Default	Default enable authentication list for each line is **“default”**.
Mode	Line Configuration

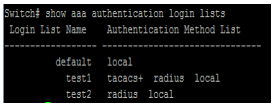
Example	This example shows how to create a new enable authentication list and bind to telnet line. Switch#**configure terminal** Switch(config)# **aaa authentication enable test1 tacacs+ radius enable** Switch(config)# **line telnet** Switch(config-line)# **enable authentication test1** 

2.4 SHOW AAA AUTHENTICATION

Use **“show aaa authentication”** command to show login authentication or Enable authentication method lists.

Switch#**show aaa authentication (login | enable) lists**

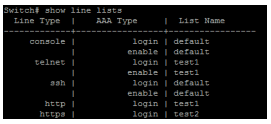
Syntax	**show aaa authentication (login | enable) lists**
Parameter	**login** Show login authentication list. **enable** Show enable authentication list.
Mode	Privileged EXEC

Example	This example shows how to show existing login authentication lists. Switch# **show aaa authentication login lists**  This example shows how to show existing enable authentication lists Switch# **show aaa authentication login lists** 

2.5 SHOW LINE LISTS

Use **“show line lists”** command to show all lines binding list of all.

Switch#**show line lists**

Syntax	**show line lists**
Mode	Privileged EXEC
Example	This example shows how to show line binding lists. Switch# **show line lists** 

```
Switch# show line lists
  Line Type  |    AAA Type      |  List Name
-------------+------------------+---------------
     console |            login | default
             |           enable | default
      telnet |            login | test1
             |           enable | test1
         ssh |            login | default
             |           enable | default
        http |            login | test1
       https |            login | test2
```

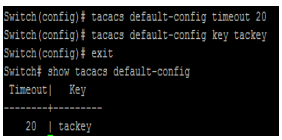
2.6 TACACS DEFAULT-CONFIG

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.

Switch#**configure terminal**

Switch(config)#**tacacs default-config [key TACACSKEY] [timeout** <*1-30*>**]**

Syntax	**tacacs default-config [key TACACSKEY] [timeout** <*1-30*>**]**
Parameter	**key TACACSKEY** Specify default tacacs+ server key string. **timeout**<*1-30*> Specify default tacacs+ server timeout value.
Default	Default tacacs+ key is **“********”**. Default tacacs+ timeout is 5 seconds.
Mode	Global Configuration

Example	This example shows how modify default tacacs+ configuration Switch#**configure terminal** Switch(config)# **tacacs default-config timeout 20** Switch(config)# **tacacs default-config key tackey** This example shows how to show default tacacs+ configurations. Switch# **show tacacs default-config** 

2.7 TACACS HOST

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.

Switch#**configure terminal**

Switch(config)# **tacacs host** *{HOSTNAME }*[**port** *<0-65535>*] **[key TACPLUSKEY] [priority***<0-65535>*]**[timeout** *<1-30>]*

Switch(config)#**no tacacs [host** *{HOSTNAME }*]

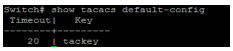
Syntax	**tacacs host** *HOSTNAME* **[port** *<0-65535>* **] [key TACPLUSKEY] [priority***<0-65535>* **] [timeout** *<1-30>*] **no tacacs [host** *{HOSTNAME }*]
Parameter	*HOSTNAME* Specify tacacs+ server host name, both IP address and domain name are available. **port** *<0-65535>* Specify tacacs+ server 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 **“********”.** Default tacacs+ timeout is 5 seconds.

Mode	Global Configuration
Example	This example shows command execution, 

2.8 SHOW TACACS DEFAULT-CONFIG

Use **“show tacacs default-config”** command to show tacacs+ default.

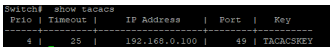
Switch#**show tacacs default-config**

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

2.9 SHOW TACACS

Use **“show tacacs”** command to show existing tacacs+ servers.

Switch#**show tacacs**

Syntax	**show tacacs**
Mode	Privileged EXEC
Example	This example shows how to show existing tacacs+ server. Switch# **show tacacs** 

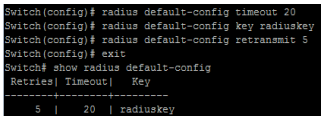
2.10 SHOW Default-config

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.

Switch#**configure terminal**

Switch(config)#**radius default-config [key RADIUSKEY] [retransmit** <*1-10*>**] [timeout** <*1-30*>**]**

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 seconds
Mode	Global Configuration

Example	This example shows how modify default radius configuration, Switch#**configure terminal** 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** 

2.11 RADIUS HOST

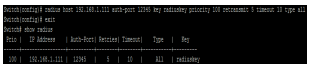
Use **“radius host”** command to add or edit an existing radius server. Use **“no”** form to delete one or all radius servers from database.

Switch#**configure terminal**

Switch(config)# **radius host** *{HOSTNAME }* **[auth-port** *<0-65535>***] [key RADIUSKEY][priority** *<0-65535>***] [retransmit** *<1-10>***] [timeout** *<1-30>***] [type (login|802.1x|all)]**

Switch(config)# **no radius [host** *{HOSTNAME }***]**

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	*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

Default	Default radius timeout is 3 seconds.
Mode	Global Configuration
Example	This example shows how to create a new radius server Switch(config)# **radius host 192.168.1.111 auth-port 12345 key radiuskey priority100 retransmit 5 timeout 10 type all** This example shows how to show existing radius server. Switch# **show radius** 

2.12 SHOW RADIUS Default-config

Use **“show radius default-config”** command to show radius default configurations.

Switch#**show radius default-config**

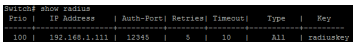
Syntax	**show radius default-config**
Mode	Privileged EXEC

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

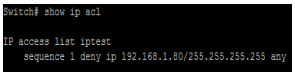
2.13 SHOW RADIUS

Use **“show radius”** command to show existing radius servers.

Switch#**show radius**

Syntax	**show radius**
Mode	Privileged EXEC
Example	This example shows how to show existing radius server. Switch# **show radius** 

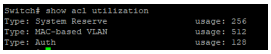
ACL (ACCESS CONRTOL LIST)

Syntax	**show acl** **show (mac|ip|ipv6) acl** **show (mac|ip|ipv6) acl NAME**
Parameter	**(mac|ip|ipv6)**Specify a type of ACL to show *NAME* Specify the name of ACL
Mode	Global Configuration Context Configuration
Example	The example shows how to show all IP ACL. Switch# **show ip acl** 

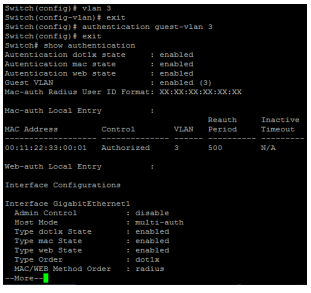
3.12 SHOW ACL UTILIZATION

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.

Switch#**show acl utilization**

Syntax	**show acl utilization**
Mode	Global Configuration
Example	The example shows how to show utilization Switch# **show acl utilization** 

AUTHENTICATION MANAGER

Syntax	**authentication guest-vlan** *<1-4094>* **no authentication guest-vlan**
Parameter	*<1-4094>*Guest VLAN ID
Default	Default guest VLAN is disabled
Mode	Global Configuration
Example	The following example shows how to create guest VLAN. Switch#**configure terminal** Switch(config)# **vlan 3** Switch(config-vlan)# **exit** Switch(config)# **authentication guest-vlan 3** Switch# **show authentication** 

```
Switch(config)# vlan 3
Switch(config-vlan)# exit
Switch(config)# authentication guest-vlan 3
Switch(config)# exit
Switch# 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        N/A

Web-auth Local Entry          :

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
--More--
```

4.7 AUTHENTICATION GUEST-VLAN (INTERFACE)

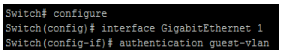
Use **“authentication guest-vlan”** command to enable the port setting of guest VLAN. Use the **“no”** form of this command to disable guest VLAN.

Switch#**configure terminal**

Switch(config)# **interface** {interface-name}

Switch(config-if)#**authentication guest-vlan**

Switch(config-if)#**no authentication guest-vlan**

Syntax	**authentication guest-vlan** **no authentication guest-vlan**
Default	Default guest VLAN is disabled
Mode	Interface Configuration
Example	The following example shows how to enable guest VLAN. Switch#configure terminal Switch(config)# **interface** GigabitEthernet1 Switch(config-if)# **authentication guest-vlan** 

4.8 AUTHENTICATION HOST-MODE

Use **“authentication host-mode”** command to configure the port, Authentication host mode. Use the **“no”** form of this command to restore default value.

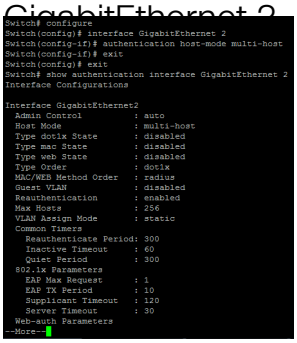
Switch#**configure terminal**

Switch(config)# **interface** {interface-name}

Switch(config)#**authentication host-mode (multi-auth|multi-host|single-host)**

Switch(config)#**no authentication host-mode**

Syntax	**authentication host-mode (multi-auth|multi-host|single-host)** **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

Example	The following example shows how to modify port host mode to multi-host. Switch#**configure terminal** Switch(config)# **interface** GigabitEthernet 2 Switch(config-if)# **authentication host-mode multi-host** Switch# **show authentication interface** GigabitEthernet 2 

```
Switch# configure
Switch(config)# interface GigabitEthernet 2
Switch(config-if)# authentication host-mode multi-host
Switch(config-if)# exit
Switch(config)# exit
Switch# show authentication interface GigabitEthernet 2
Interface Configurations

Interface GigabitEthernet2
  Admin Control          : auto
  Host Mode              : multi-host
  Type dot1x State       : disabled
  Type mac State         : disabled
  Type web State         : disabled
  Type Order             : dot1x
  MAC/WEB Method Order   : radius
  Guest VLAN             : disabled
  Reauthentication       : enabled
  Max Hosts              : 256
  VLAN Assign Mode       : static
  Common Timers
    Reauthenticate Period: 300
    Inactive Timeout     : 60
    Quiet Period         : 300
  802.1x Parameters
    EAP Max Request      : 1
    EAP TX Period        : 10
    Supplicant Timeout   : 120
    Server Timeout       : 30
  Web-auth Parameters
--More--
```

4.9 AUTHENTICATION MAX-HOSTS

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. Use **“no”** form of this command to restore default value.

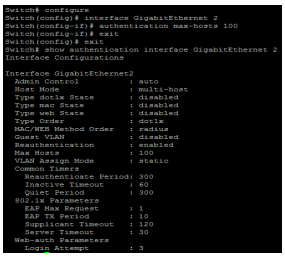
Switch#**configure terminal**

Switch(config)# **interface** {interface-name}

Switch(config-if)#**authentication max-hosts** <*1-256*>

Switch(config-if)#**no authentication max-hosts**

Syntax	**authentication max-hosts** <*1-256*> **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

Example	The following example shows how to change port max hosts number. Switch#**configure terminal** Switch(config)# **interface** GigabitEthernet 2 Switch(config-if)# **authentication max-hosts 100** Switch# **show authentication interface GigabitEthernet 2**  Switch# configure Switch(config)# interface GigabitEthernet 2 Switch(config-if)# authentication max-hosts 100 Switch(config-if)# exit Switch(config)# exit Switch# show authentication interface GigabitEthernet 2 Interface Configurations Interface GigabitEthernet2 Admin Control : auto Host Mode : multi-host Type dot1x State : disabled Type mac State : disabled Type web State : disabled Type Order : dot1x MAC/WEB Method Order : radius Guest VLAN : disabled Reauthentication : enabled Max Hosts : 100 VLAN Assign Mode : static Common Timers Reauthenticate Period: 300 Inactive Timeout : 60 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 : 3

4.10 AUTHENTICATION METHOD

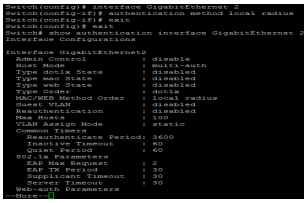
Use **“authentication method”** command to configure the port authentication method order.

Switch#**configure terminal**

Switch(config)# **interface** {interface-name}

Switch(config-if)# **authentication method local radius**

Syntax	**authentication method (local [radius] | radius [local])** **no authentication order**
Parameter	Local Use local account to authenticate Radius Use remote RADIUS server to authenticate
Default	Default is RADIUS method in first place and no other method.
Mode	Interface Configuration

Example	The following example shows how to modify port authentication order to local and then RADIUS. Switch#**configure terminal** Switch(config)# **interface GigabitEthernet 2** Switch(config-if)# **authentication method local radius** Switch# **show authentication interface GigabitEthernet 2** 

4.11 AUTHENTICATION ORDER

Use **“authentication order”** command to configure the port authentication type order. Use the **“no”** form of this command to restore default value.

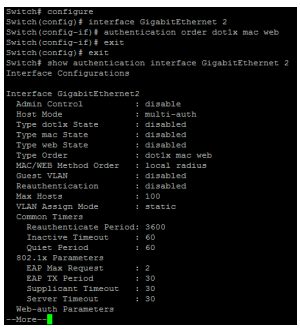
Switch#**configure terminal**

Switch(config)# **interface** {interface-name}

Switch(config-if)# **authentication order (dot1x [mac] [web] | mac [dot1x] [web] | web)**

Switch(config-if)# **no authentication order**

Syntax	**authentication order (dot1x [mac] [web] | mac [dot1x] [web] | web)** **no authentication order**

Parameter	**dot1x** Authenticating user by IEEE 802.1X **mac** Authenticating user by mac based authentication **web** Authenticating user by web based authentication
Default	Default is dot1x type in first place and no other types.
Mode	Interface Configuration
Example	The following example shows how to modify port authentication order to dot1x, mac and web. Switch#**configure terminal** Switch(config)# **interface** GigabitEthernet 2 Switch(config-if)# **authentication order dot1x mac web** Switch# **show authentication interface GigabitEthernet 2** 

```
Switch# configure
Switch(config)# interface GigabitEthernet 2
Switch(config-if)# authentication order dot1x mac web
Switch(config-if)# exit
Switch(config)# exit
Switch# show authentication interface GigabitEthernet 2
Interface Configurations

Interface GigabitEthernet2
  Admin Control           : disable
  Host Mode               : multi-auth
  Type dot1x State        : disabled
  Type mac State          : disabled
  Type web State          : disabled
  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
    Inactive Timeout     : 60
    Quiet Period         : 60
  802.1x Parameters
    EAP Max Request      : 2
    EAP TX Period        : 30
    Supplicant Timeout   : 30
    Server Timeout       : 30
  Web-auth Parameters
--More--
```

4.12 AUTHENTICATION PORT-CONTROL

Use **“authentication port-control”** command to enable the port authentication control mode. Use the **“no”** form of this command to disable authentication port control

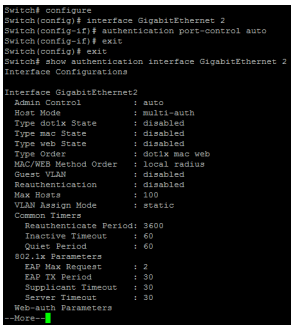
Switch#**configure terminal**

Switch(config)# **interface** {interface-name}

Switch(config-if)# **authentication port-control (auto|force-auth|force-unauth)**

Switch(config-if)# **no authentication port-control**

Syntax	**authentication port-control (auto|force-auth|force-unauth)** **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.
Mode	Interface Configuration

Example	The following example shows how to configure port control to auto mode. Switch#**configure terminal** Switch(config)# **interface** GigabitEthernet 2 Switch(config-if)# **authentication port-control auto** Switch# **show authentication interface GigabitEthernet 1** 

```
Switch# configure
Switch(config)# interface GigabitEthernet 2
Switch(config-if)# authentication port-control auto
Switch(config-if)# exit
Switch(config)# exit
Switch# show authentication interface GigabitEthernet 2
Interface Configurations

Interface GigabitEthernet2
  Admin Control          : auto
  Host Mode              : multi-auth
  Type dot1x State       : disabled
  Type mac State         : disabled
  Type web State         : disabled
  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
    Inactive Timeout     : 60
    Quiet Period         : 60
  802.1x Parameters
    EAP Max Request      : 2
    EAP TX Period        : 30
    Supplicant Timeout   : 30
    Server Timeout       : 30
  Web-auth Parameters
--More--
```

4.13 AUTHENTICATION RADIUS-ATTRIBUTES VLAN

Use **“authentication radius-attributes vlan”** command to configure the port RADIUS VLAN assign mode. Use the **“no”** form of this command to disable the port RADIUS VLAN assign.

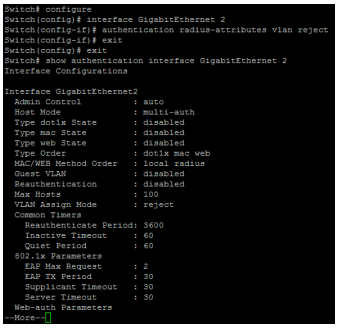
Switch#**configure terminal**

Switch(config)# **interface** {interface-name}

Switch(config-if)# **authentication radius-attributes vlan (reject | static)**

Switch(config-if)# **no authentication radius-attributes vlan**

Syntax	**authentication radius-attributes vlan (reject | static)** **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

Example	The following example shows how to configure port VLAN assign to reject mode. Switch#**configure terminal** Switch(config)# **interface** GigabitEthernet 2 Switch(config-if)# **authentication radius-attributes vlan reject** Switch# **show authentication interface** GigabitEthernet 2 

```
Switch# configure
Switch(config)# interface GigabitEthernet 2
Switch(config-if)# authentication radius-attributes vlan reject
Switch(config-if)# exit
Switch(config)# exit
Switch# show authentication interface GigabitEthernet 2
Interface Configurations

Interface GigabitEthernet2
  Admin Control          : auto
  Host Mode              : multi-auth
  Type dot1x State       : disabled
  Type mac State         : disabled
  Type web State         : disabled
  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
    EAP Max Request      : 2
    EAP TX Period        : 30
    Supplicant Timeout   : 30
    Server Timeout       : 30
  Web-auth Parameters
--More--
```

4.14 AUTHENTICATION REAUTH

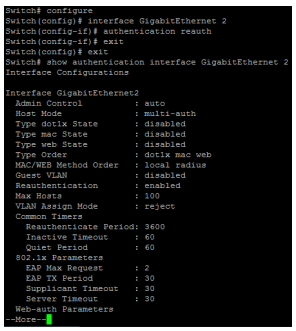
Use **“authentication reauth”** command to enable the port reauthentication.Use the **“no”** form of this command to disable reauthentication.

Switch#**configure terminal**

Switch(config)# **interface** {interface-name}

Switch(config-if)# **authentication reauth**

Switch(config-if)# **no authentication reauth**

Syntax	**authentication reauth** **no authentication reauth**
Mode	Interface Configuration
Example	The following example shows how to enable port reauthentication. Switch#**configure terminal** Switch(config)# **interface** GigabitEthernet 2 Switch(config-if)# **authentication reauth** Switch# **show authentication interface** GigabitEthernet 2 

```
Switch# configure
Switch(config)# interface GigabitEthernet 2
Switch(config-if)# authentication reauth
Switch(config-if)# exit
Switch(config)# exit
Switch# show authentication interface GigabitEthernet 2
Interface Configurations

Interface GigabitEthernet2
  Admin Control          : auto
  Host Mode              : multi-auth
  Type dot1x State       : disabled
  Type mac State         : disabled
  Type web State         : disabled
  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     : 60
    Quiet Period         : 60
  802.1x Parameters
    EAP Max Request      : 2
    EAP TX Period        : 30
    Supplicant Timeout   : 30
    Server Timeout       : 30
  Web-auth Parameters
--More--
```

4.15 AUTHENTICATION TIMER INACTIVE

Use **“authentication timer inactive”** command to configure the port inactive timeout value.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. Use **“no”** form of this command to restore default value.

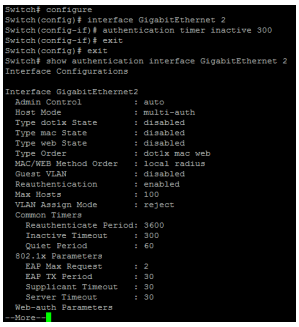
Switch#**configure terminal**

Switch(config)# **interface** {interface-name}

Switch(config-if)# **authentication timer inactive** *<60-65535>*

Switch(config-if)# **no authentication timer inactive**

Syntax	**authentication timer inactive** *<60-65535>* **no authentication timer inactive**
Parameter	<60-65535>Interval in seconds after which if there is no activity from the client then it will beunauthorized
Default	Default inactive timeout is 60 seconds.
Mode	Interface Configuration

Example	The following example shows how to configure port inactive period. Switch#**configure terminal** Switch(config)# **interface** GigabitEthernet 2 Switch(config-if)# **authentication timer inactive** 300 Switch# **show authentication interface** GigabitEthernet 2 

4.16 AUTHENTICATION TIMER QUIET

Use **“authentication timer quiet”** command to configure the port quiet period value. 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. Use **“no”** form of this command to restore default value.

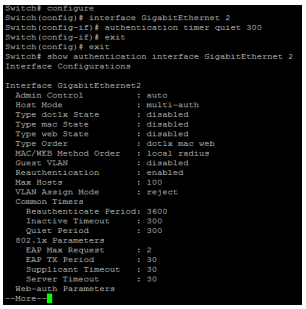
Switch#**configure terminal**

Switch(config)# **interface** {interface-name}

Switch(config-if)# **authentication timer quiet** <*0-65535*>

Switch(config-if)# **no authentication timer quiet**

Syntax	**authentication timer quiet** <*0-65535*> **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

Example	The following example shows how to configure port quiet period. Switch#**configure terminal** Switch(config)# **interface** GigabitEthernet 2 Switch(config-if)# **authentication timer quiet** 300 Switch# **show authentication interface** GigabitEthernet 2  Switch# configure Switch(config)# interface GigabitEthernet 2 Switch(config-if)# authentication timer quiet 300 Switch(config-if)# exit Switch(config)# exit Switch# show authentication interface GigabitEthernet 2 Interface Configurations Interface GigabitEthernet2 Admin Control : auto Host Mode : multi-auth Type dot1x State : disabled Type mac State : disabled Type web State : disabled 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 Supplicant Timeout : 30 Server Timeout : 30 Web-auth Parameters --More--

4.17 AUTHENTICATION TIMER REAUTH

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. Use **“no”** form of this command to restore default value.

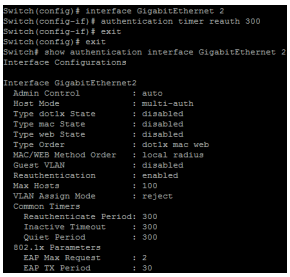
Switch#**configure terminal**

Switch(config)# **interface** {interface-name}

Switch(config-if)# **authentication timer reauth***<300-4294967294>*

Switch(config-if)# **no authentication timer reauth**

Syntax	**authentication timer reauth***<300-4294967294>* **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

Example	The following example shows how to configure port reauthentication period. Switch#**configure terminal** Switch(config)# **interface** GigabitEthernet 2 Switch(config-if)# **authentication timer reauth** 300 Switch# **show authentication interface** GigabitEthernet 2 

4.18 AUTHENTICATION WEB LOCAL

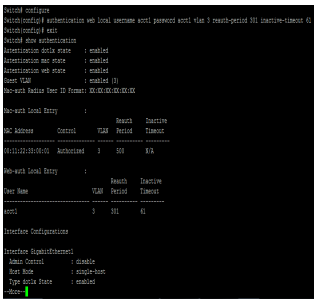
Use **“authentication web local”** command to add local account in database. This local account database is used when web authentication method is configured as **“local”** . The web authentication module will find account in this local database and authenticated it. Use the **“no”** form of this command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

Switch#**configure terminal**

Switch(config)# **authentication web local username USERNAME password (encryptedCRYPT-PASSWORD | PASSWORD) [vlan** *<1-4094>***] [reauth-period** *<300-4294967294>***] [inactive-timeout** *<60-65535>***]**

Switch(config)# **no authentication web local username USERNAME**

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 **Re-authentication period** *<300-4294967294>* of this local account inactive-timeout. **Inactive timeout** *<60-65535>* of this local account.
Mode	Global Configuration
Example	The following example shows how to add/delete a new local account. Switch#**configure terminal** Switch(config)# **authentication web local username acct1 password acct1 vlan 3reauth-period 301 inactive-timeout 61** Switch# **show authentication** 

4.19 AUTHENTICATION WEB MAX-LOGIN-ATTEMPTS

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.Use **“no”** form of this command to restore default value.

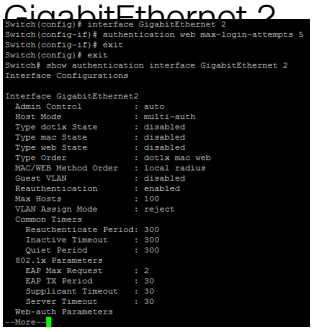
Switch#**configure terminal**

Switch(config)# **interface** {interface-id}

Switch(config-if)# **authentication web max-login-attempts (infinite|**<*3-10*>**)**

Switch(config-if)# **no authentication web max-login-attempts**

Syntax	**authentication web max-login-attempts (infinite|**<*3-10*>**)** **no authentication web max-login-attempts**
Parameter	**infinite** Do not care user login fail number <*3-10*> Allow user login fail number
Default	Default max login attempt number is 3.
Mode	Interface Configuration

Example	The following example shows how to configure port max login attempt number. Switch#**configure terminal** Switch(config)# **interface** GigabitEthernet 2 Switch(config-if)# **authentication web max-login-attempts** 5 Switch# **show authentication interface** GigabitEthernet 2 

```
Switch(config)# interface GigabitEthernet 2
Switch(config-if)# authentication web max-login-attempts 5
Switch(config-if)# exit
Switch(config)# exit
Switch# show authentication interface GigabitEthernet 2
Interface Configurations

Interface GigabitEthernet2
  Admin Control          : auto
  Host Mode              : multi-auth
  Type dot1x State       : disabled
  Type mac State         : disabled
  Type web State         : disabled
  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
--More--
```

4.20 CLEAR AUTHENTICATION SESSIONS

Use **“clear authentication sessions”** command to delete existing authentication sessions. If no parameter is specified, all sessions will be deleted.After authentication session is deleted, host need to do authentication procedure again.

Switch# **clear authentication sessions**

Switch# **clear authentication sessions interfaces** *{IF_PORTS}*

Switch# **clear authentication sessions mac** *{mac-addr}*

Switch# **clear authentication sessions session-id** *{WORD}*

Switch# **clear authentication sessions type (dot1x|mac|web)**

Syntax	**clear authentication sessions** **clear authentication sessions interfaces** *{IF_PORTS}* **clear authentication sessions mac** *{mac-addr}* **clear authentication sessions session-id** *{WORD}* **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)type** Clear session with specific authentication

Mode	Privileged EXEC
Example	The following example shows how to clear all authentication sessions. Switch# **clear authentication sessions** Switch# **show authentication sessions**

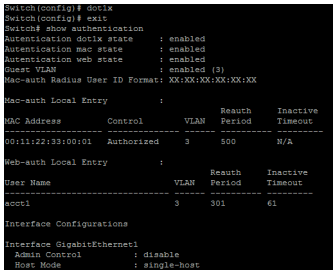
4.21 DOT1X

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 802.1 x authentications.

Switch#**configure terminal**

Switch(config)# **dot1x**

Switch(config)# **no dot1x**

Syntax	**dot1x** **no dot1x**
Default	Default 802.1x is disabled
Mode	Global Configuration
Example	The following example shows how to enable 802.1 x authentications. Switch#**configure terminal** Switch(config)# **dot1x** Switch# **show authentication** 

```
Switch(config)# dot1x
Switch(config)# exit
Switch# 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        N/A

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

Interface Configurations

Interface GigabitEthernet1
  Admin Control       : disable
  Host Mode           : single-host
```

4.22 DOT1X GUEST-VLAN

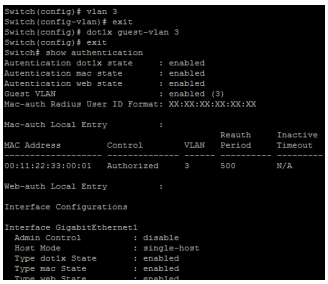
Use **“dot1x guest-vlan”** command to enable the global setting of guest VLAN and specify guest VLAN ID. Use the **“no”** form of this command to disable guest VLAN.

Switch#**configure terminal**

Switch(config)# **dot1x guest-vlan** *<1-4094>*

Switch(config)# **no dot1x guest-vlan**

Syntax	**dot1x guest-vlan** *<1-4094>* **no dot1x guest-vlan**
Parameter	*<1-4094>*Guest VLAN ID
Default	Default guest VLAN is disabled
Mode	Global Configuration

Example	The following example shows how to create guest VLAN. Switch#**configure terminal** Switch(config)# **vlan 3** Switch(config-vlan)# **exit** Switch(config)# **dot1x guest-vlan 3** Switch# **show authentication** 

```
Switch(config)# vlan 3
Switch(config-vlan)# exit
Switch(config)# dot1x guest-vlan 3
Switch(config)# exit
Switch# 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        N/A

Web-auth Local Entry          :

Interface Configurations

Interface GigabitEthernet1
  Admin Control         : disable
  Host Mode             : single-host
  Type dot1x State      : enabled
  Type mac State        : enabled
  Type web State        : enabled
```

4.23 DOT1X MAX-REQ

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. Use **“no”** form of this command to restore default value.

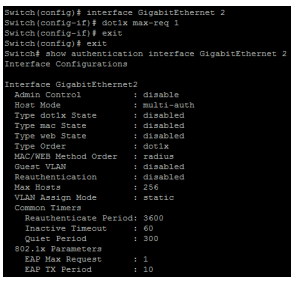
Switch#**configure terminal**

Switch(config)# **interface** {interface-id}

Switch(config-if)# **dot1x max-req**<*1-10*>

Switch(config-if)# **no dot1x max-req**

Syntax	**dot1x max-req**<*1-10*> **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

Example	The following example shows how to configure port 802.1x EAP TX period. Switch#**configure terminal** Switch(config)# **interface** GigabitEthernet 2 Switch(config-if)# **dot1x max-req 1** Switch# **show authentication interface** GigabitEthernet 2 

```
Switch(config)# interface GigabitEthernet 2
Switch(config-if)# dot1x max-req 1
Switch(config-if)# exit
Switch(config)# exit
Switch# show authentication interface GigabitEthernet 2
Interface Configurations

Interface GigabitEthernet2
  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              : 256
  VLAN Assign Mode       : static
  Common Timers
    Reauthenticate Period: 3600
    Inactive Timeout     : 60
    Quiet Period         : 300
  802.1x Parameters
    EAP Max Request      : 1
    EAP TX Period        : 10
```

4.24 DOT1X PORT-CONTROL

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.

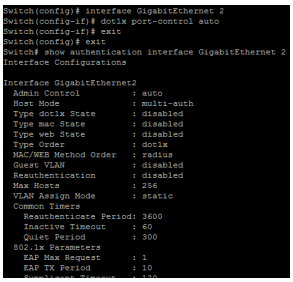
Switch#**configure terminal**

Switch(config)# **interface** {interface-id}

Switch(config-if)# **dot1x port-control (auto|force-auth|force-unauth)**

Switch(config-if)# **no dot1x port-control**

Syntax	**dot1x port-control (auto|force-auth|force-unauth)** **no dot1x 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.
Mode	Interface Configuration

Example	The following example shows how to configure port control to auto mode. Switch#**configure terminal** Switch(config)# **interface** GigabitEthernet 2 Switch(config-if)# **dot1x port-control auto** Switch# **show authentication interface** GigabitEthernet 2  Switch(config)# interface GigabitEthernet 2 Switch(config-if)# dot1x port-control auto Switch(config-if)# exit Switch(config)# exit Switch# show authentication interface GigabitEthernet 2 Interface Configurations Interface GigabitEthernet2 Admin Control : auto 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 : 256 VLAN Assign Mode : static Common Timers Reauthenticate Period: 3600 Inactive Timeout : 60 Quiet Period : 300 802.1x Parameters EAP Max Request : 1 EAP TX Period : 10

4.25 DOT1X REAUTH

Use **“dot1x reauth”** command to enable the port reauthentication. The **“authentication reauth”** command has the same effect, it is a backward compatible command

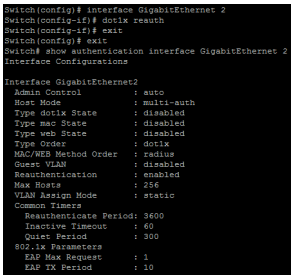
Switch#**configure terminal**

Switch(config)# **interface** {interface-id}

Switch(config-if)# **dot1x reauth**

Switch(config-if)# **no dot1x reauth**

Syntax	**dot1x reauth** **no dot1x reauth**
Mode	Interface Configuration

Example	The following example shows how to enable port reauthentication. Switch#**configure terminal** Switch(config)# **interface** {interface-id} Switch(config-if)# **interface** GigabitEthernet 2 Switch(config-if)# **dot1x reauth** Switch# **show authentication interface** GigabitEthernet 2 

4.26 DOT1X TIMEOUT REAUTH-PERIOD

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. The **“authentication timer reauth”** command has the same effect and it is a backward compatible command. Use **“no”** form of this command to restore default value.

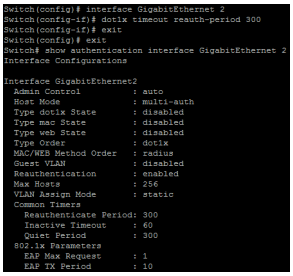
Switch#**configure terminal**

Switch(config)# **interface** {interface-id}

Switch(config-if)# **dot1x timeout reauth-period** *<300-4294967294>*

Switch(config-if)# **no dot1x timeout reauth-period**

Syntax	**dot1x timeout reauth-period <**300-4294967294**>** **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
Mode	Interface Configuration

Example	The following example shows how to configure port 802.1x reauthentication period. Switch#**configure terminal** Switch(config)# **interface** GigabitEthernet 2 Switch(config-if)# **dot1x timeout reauth-period** 300 Switch# **show authentication interface** GigabitEthernet 2 

```
Switch(config)# interface GigabitEthernet 2
Switch(config-if)# dot1x timeout reauth-period 300
Switch(config-if)# exit
Switch(config)# exit
Switch# show authentication interface GigabitEthernet 2
Interface Configurations

Interface GigabitEthernet2
  Admin Control          : auto
  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       : enabled
  Max Hosts              : 256
  VLAN Assign Mode       : static
  Common Timers
    Reauthenticate Period: 300
    Inactive Timeout     : 60
    Quiet Period         : 300
  802.1x Parameters
    EAP Max Request      : 1
    EAP TX Period        : 10
```

4.27 DOT1X TIMEOUT QUIET-PERIOD

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.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. Use **“no”** form of this command to restore default value.

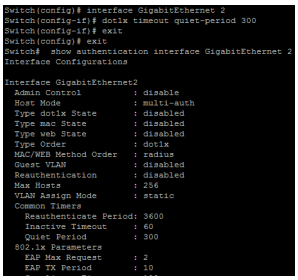
Switch#**configure terminal**

Switch(config)# **interface** {interface-id}

Switch(config-if)# **dot1x timeout quiet-period** <*0-65535*>

Switch(config-if)# **no dot1x timeout quiet-period**

Syntax	**dot1x timeout quiet-period** <*0-65535*> **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

Example	The following example shows how to configure port 802.1x quiet period. Switch#**configure terminal** Switch(config)# **interface** GigabitEthernet 2 Switch(config-if)# **dot1x timeout quiet-period** 300 Switch# **show authentication interface** GigabitEthernet 2 

```
Switch(config)# interface GigabitEthernet 2
Switch(config-if)# dot1x timeout quiet-period 300
Switch(config-if)# exit
Switch(config)# exit
Switch#  show authentication interface GigabitEthernet 2
Interface Configurations

Interface GigabitEthernet2
  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              : 256
  VLAN Assign Mode       : static
  Common Timers
    Reauthenticate Period: 3600
    Inactive Timeout     : 60
    Quiet Period         : 300
  802.1x Parameters
    EAP Max Request      : 2
    EAP TX Period        : 10
```

4.28 DOT1X TIMEOUT SERVER-TIMEOUT

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.

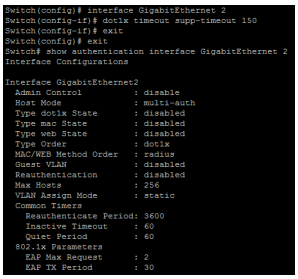
Switch#**configure terminal**

Switch(config)# **interface** {interface-id}

Switch(config-if)# **dot1x timeout server-timeout** <*1-65535*>

Switch(config-if)# **no dot1x timeout server-timeout**

Syntax	**dot1x timeout server-timeout** <*1-65535*> **no dot1x timeout server-timeout**
Parameter	<*1-65535*> Number of seconds that lapse before the device resends a request to the authentication server.
Default	Default server timeout is 30 seconds.
Mode	Interface Configuration

Example	The following example shows how to configure port 802.1x server timeout. Switch#**configure terminal** Switch(config)# **interface** GigabitEthernet 2 Switch(config-if)# **dot1x timeout supp-timeout** 150 Switch# **show authentication interface** GigabitEthernet 2  Switch(config)# interface GigabitEthernet 2 Switch(config-if)# dot1x timeout supp-timeout 150 Switch(config-if)# exit Switch(config)# exit Switch# show authentication interface GigabitEthernet 2 Interface Configurations Interface GigabitEthernet2 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 : 256 VLAN Assign Mode : static Common Timers Reauthenticate Period: 3600 Inactive Timeout : 60 Quiet Period : 60 802.1x Parameters EAP Max Request : 2 EAP TX Period : 30

4.29 DOT1X TIMEOUT SUPP-TIMEOUT

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.

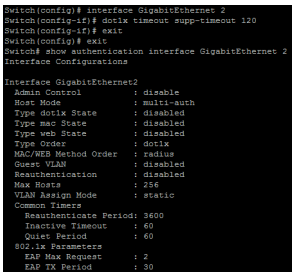
Switch#**configure terminal**

Switch(config)# **interface** {interface-id}

Switch(config-if)# **dot1x timeout supp-timeout** <*1-65535*>

Switch(config-if)# **no dot1x timeout supp-timeout**

Syntax	**dot1x timeout supp-timeout** <*1-65535*> **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

Example	The following example shows how to configure port 802.1x supplicant timeout. Switch#**configure terminal** Switch(config)# **interface** GigabitEthernet 2 Switch(config-if)# **dot1x timeout supp-timeout** 120 Switch# **show authentication interface** GigabitEthernet 2 

```
Switch(config)# interface GigabitEthernet 2
Switch(config-if)# dot1x timeout supp-timeout 120
Switch(config-if)# exit
Switch(config)# exit
Switch# show authentication interface GigabitEthernet 2
Interface Configurations

Interface GigabitEthernet2
  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              : 256
  VLAN Assign Mode       : static
  Common Timers
    Reauthenticate Period: 3600
    Inactive Timeout     : 60
    Quiet Period         : 60
  802.1x Parameters
    EAP Max Request      : 2
    EAP TX Period        : 30
```

4.30 DOT1X TIMEOUT TX-PERIOD

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. Use **“no”** form of this command to restore default value.

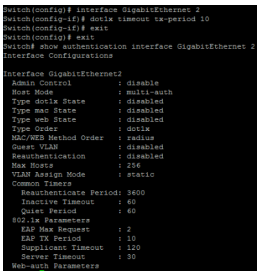
Switch#**configure terminal**

Switch(config)# **interface** {interface-id}

Switch(config-if)# **dot1x timeout tx-period** <*1-65535*>

Switch(config-if)# **no dot1x timeout tx-period**

Syntax	**dot1x timeout tx-period** <*1-65535*> **no dot1x timeout tx-period**
Parameter	<*1-65535*> 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.
Default	Default EAP TX period is 30 seconds.
Mode	Interface Configuration

Example	The following example shows how to configure port 802.1x EAP TX period. Switch#**configure terminal** Switch(config)# **interface** GigabitEthernet 2 Switch(config-if)# **dot1x timeout tx-period** 10 Switch# **show authentication interface** GigabitEthernet 2 

```
Switch(config)# interface GigabitEthernet 2
Switch(config-if)# dot1x timeout tx-period 10
Switch(config-if)# exit
Switch(config)# exit
Switch# show authentication interface GigabitEthernet 2
Interface Configurations

Interface GigabitEthernet2
  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              : 256
  VLAN Assign Mode       : static
  Common Timers
    Reauthenticate Period: 3600
    Inactive Timeout     : 60
    Quiet Period         : 60
  802.1x Parameters
    EAP Max Request      : 2
    EAP TX Period        : 10
    Supplicant Timeout   : 120
    Server Timeout       : 30
  Web-auth Parameters
```

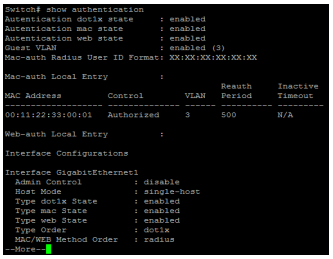
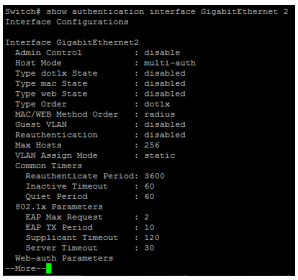
4.31 SHOW AUTHENTICATION

Use "**show authentication"** command to show all authentication manager configurations. Use **"show authentication interface"** command to show authentication manager configuration of specific port.

Switch# **show authentication**

Switch# **show authentication interfaces** *{IF_PORTS}*

Syntax	**show authentication** **show authentication interfaces** *{IF_PORTS}*
Parameter	**Interfaces** *IF_PORTS* Specify port list to show port configurations
Mode	Privileged EXEC

Example	This example shows how to show the mac authentication configurations of port GigabitEthernet 1. Switch# **show authentication**  Switch# **show authentication interface GigabitEthernet 2** 

4.32 SHOW AUTHENTICATION SESSIONS

Use **“show authentication sessions”** command to show authentication detail session information.

Switch# **show authentication sessions [detail]**

Switch# **show authentication sessions interface** *{IF_PORTS}*

Switch# **show authentication sessions session-id** *{WORD}*

Switch# **show authentication session type (dot1x|mac|web)**

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** *IF_PORTS* Show session detail information of specific port **session-id** *WORD* Show session detail information of specific session id **Type (dot1x|mac|web)** Show session detail information of specific authentication type
Mode	Privileged EXEC

Example	This example shows how to show current authentication session brief and detail information. Switch# **show authentication sessions** Switch# **show authentication sessions detail**

DIAGNOSTIC

IE2000 Series Switches Diagnostics offer proactive diagnostics and real-time alerts and provides higher network availability and increased operational efficiency. Log files of a switch are classified into: user log files and diagnostic log files. A diagnostic log file records the service processing flow and fault information.These logs sent to the log buffer, console, or terminal monitors. You can set up a switch to automatically transfer diagnostic information to a remote server. If a fault occurs, you can provide troubleshooting and support.

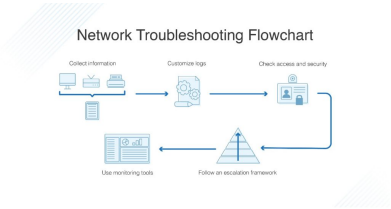
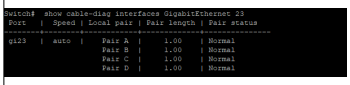


Fig 5.1.1 Network Troubleshooting Flowchart

5.1 SHOW CABLE-DIAG

To show the estimated copper cable length attached to a specific interface, use the command show cable-diag in the Privileged EXEC mode. For the proper information of the cable length, the interface must be active and linked up.

Switch#**show cable-diag interfaces** *{IF_NMLPORTS}*

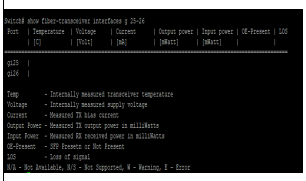
Syntax	**show cable-diag interfaces** *{IF_NMLPORTS}*
Parameter	Interfaces *{IF_NMLPORTS}* Display the cable diagnostic information of the copper media for an interface ID or a list of interfaces IDs.
Mode	Privileged EXEC
Example	The following example shows the result of cable diagnostic for the interface GigabitEthernet 23 Switch# **show cable-diag interfaces GigabitEthernet 23** 

```
Switch#  show cable-diag interfaces GigabitEthernet 23
 Port    |  Speed | Local pair | Pair length | Pair status
---------+--------+------------+-------------+----------------
 gi23    |  Auto  |    Pair A  |     1.00    | Normal
                   |    Pair B  |     1.00    | Normal
                   |    Pair C  |     1.00    | Normal
                   |    Pair D  |     1.00    | Normal
```

5.2 SHOW FIBER-TRANSCEIVER

To show the diagnostic information of the fiber transceivers use the command. show fiber-transceiver in the Privilege EXEC mode.

Switch#**show fiber-transceiver interfaces** *{IF_NMLPORTS}*

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
Mode	Privileged EXEC
Example	The following example shows the diagnostic information for the interface g 25 and 26 , if, no SFP inserted. Switch# **show fiber-transceiver interfaces** g 25-26 

DHCP (Dynamic Host Configuration Protocol)

Syntax	**dhcp-server group** **no dhcp-server group**
Default	DHCP VLAN Interface Group setting is disabled
Mode	In Global configuration for Management VLAN. VLAN Interface Configuration for other than management VLAN.

Example

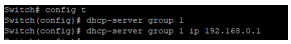
The example shows how to set DHCP VLAN Interface Group setting for Management VLAN .

You can verify settings by the following **show run** command.

Switch#**configure terminal**

Switch(config)# **dhcp-server group** 1

Switch(config)# **dhcp-server group** 1 **ip** 192.168.0.1



The example shows how to set DHCP VLAN Interface Group setting for other than management VLAN .

Switch#**configure terminal**

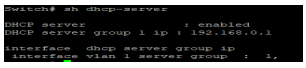
Switch(config)#**interface vlan2**

Switch(config-if)# **dhcp-server group** 1

Switch(config)# **dhcp-server group** 1 **ip** 192.168.0.1

Verifying the DHCP Server

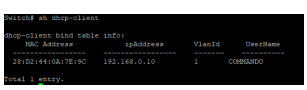
Switch# sh dhcp-server



Verifying the DHCP Client

Switch# sh dhcp-client

Note:- Only Static binded clients are shown.



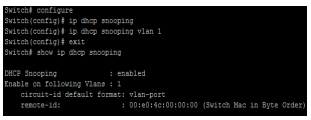
6.5 IP DHCP SNOOPING

Use the ip dhcp snooping command to enable DHCP Snooping function. Use the **“no”** form of this command to disable.

Switch#**configure terminal**

Switch(config)# **ip dhcp snooping**

Switch(config)# **no ip dhcp snooping**

Syntax	**ip dhcp snooping** **no ip dhcp snooping**
Default	DHCP snooping is disabled
Mode	Global Configuration
Example	The example shows how to enable DHCP Snooping on VLAN 1. You can verify settings by the following show ip dhcp snooping command. Switch#**configure terminal** Switch(config)# **ip dhcp snooping** Switch(config)# **ip dhcp snooping vlan 1** Switch# **show ip dhcp snooping** 

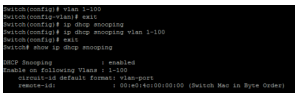
6.6 IP DHCP SNOOPING VLAN

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.

Switch#**configure terminal**

Switch(config)# **ip dhcp snooping vlan** *{VLAN-LIST}*

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

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. Example 1:- Switch#**configure terminal** Switch(config)# **vlan** 1-100 Switch(config)# **exit** Switch(config)# **ip dhcp snooping** Switch(config)# **ip dhcp snooping vlan** 1-100 Switch# **show ip dhcp snooping**  Example 2:- Switch#**configure terminal** Switch(config)# **no ip dhcp snooping vlan** 30-40 Switch(config)# **show ip dhcp snooping** 

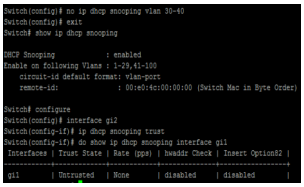
6.7 IP DHCP SNOOPING TRUST

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.

Switch#**configure terminal**

Switch(config)# **ip dhcp snooping trust**

Switch(config)# **no ip dhcp snooping trust**

Syntax	**ip dhcp snooping trust** **no ip dhcp snooping trust**
Default	DHCP snooping trust is disabled
Mode	Interface Configuration
Example	The example shows how to set interface gi1 to trust. You can verify settings by the following show ip dhcp snooping interface command. Switch#**configure terminal** Switch(config)# **interface** gi2 Switch(config-if)# **ip dhcp snooping trust** Switch(config-if)# **do show ip dhcp snooping interface** gi1 

6.8 IP DHCP SNOOPING VERIFY

Use the **ip dhcp snooping verify** command to verify MAC address function on interface.The **“mac-address”** drop DHCP packets that chaddr and ethernet-source-mac is not match.

Switch#**configure terminal**

Switch(config)#**interface** *{Interface-ID}*

Switch(config-if)# **ip dhcp snooping verify mac-address**

Switch(config-if)# **no ip dhcp snooping verify mac-address**

Syntax	**ip dhcp snooping verify mac-address** **no ip dhcp snooping verify mac-address**
Default	DHCP snooping verify mac-address is disabled
Mode	Interface Configuration

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. Switch#**configure terminal** Switch(config)# **interface** gi2 Switch(config-if)# **ip dhcp snooping verify mac-address** Switch(config-if)# **do show ip dhcp snooping interface** gi2 

6.9 IP DHCP SNOOPING RATE-LIMIT

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.

Switch#**configure terminal**

Switch(config)#**interface** *{Interface-ID}*

Switch(config-if)# **ip dhcp snooping rate-limit** <*1-300*>

Switch(config-if)# **no ip dhcp snooping rate-limit**

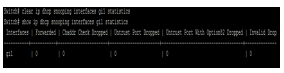
Syntax	**ip dhcp snooping rate-limit** <*1-300*> **no ip dhcp snooping rate-limit**
Parameter	<*1-300*> Set 1 to 300 PPS of DHCP packet rate limitation
Default	Default is un-limited of DHCP packet
Mode	Interface Configuration

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. Switch#configure terminal Switch(config)# **interface** gi2 Switch(config-if)# **ip dhcp snooping rate-limit** 30 Switch(config-if)# **do show ip dhcp snooping interfaces** gi2 

6.10 CLEAR IP DHCP SNOOPING STATISTICS

Use the **clear ip dhcp snooping interfaces statistics** command to clear statistics that are recorded on interface.

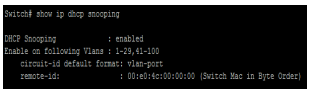
Switch# **clear ip dhcp snooping interfaces** *{IF_PORTS}* **statistics**

Syntax	**clear ip dhcp snooping interfaces** *{IF_PORTS}***statistics**
Parameter	*IF_PORTS* specifies ports to clear statistics
Mode	Privileged EXEC
Example	The example shows how to clear statistics on interface gi1. You can verify settings by the following show ip dhcp snooping interface statistics command. Switch# **clear ip dhcp snooping interfaces gi1 statistics** Switch# **show ip dhcp snooping interfaces gi1 statistics** 

6.11 SHOW IP DHCP SNOOPING

Use the show ip dhcp snooping command to show settings of DHCP Snooping.

Switch#**show ip dhcp snooping**

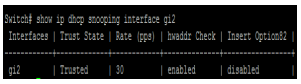
Syntax	**show ip dhcp snooping**
Mode	Privileged EXEC
Example	The example shows how to show settings of DHCP Snooping Switch# **show ip dhcp snooping** 

6.12 SHOW IP DHCP SNOOPING INTERFACE

Use the show ip dhcp snooping interfaces command to show settings or statistics of interface.

Switch# **show ip dhcp snooping interfaces** *{IF_PORTS}*

Switch# **show ip dhcp snooping interfaces** *{IF_PORTS}* **statistics**

Syntax	**show ip dhcp snooping interfaces** *{IF_PORTS}* **show ip dhcp snooping interfaces** *{IF_PORTS}* **statistics**
Parameter	*IF_PORTS* specifies ports to show statistics
Mode	Privileged EXEC
Example	The example shows how to show settings of interface gi1. Switch# **show ip dhcp snooping interface gi2** 

```
Switch# show ip dhcp snooping interface gi2
 Interfaces | Trust State | Rate (pps) | hwaddr Check | Insert Option82 |
------------+-------------+------------+--------------+-----------------+
gi2         | Trusted     | 30         | enabled      | disabled        |
```

6.13 SHOW IP DHCP SNOOPING BINDING

Use the **show ip dhcp snooping binding** command to show binding entries that learned by DHCP Snooping.

Switch# **show ip dhcp snooping binding**

Syntax	**show ip dhcp snooping binding**
Mode	Privileged EXEC
Example	The example shows how to show binding entries that learned by DHCP Snooping. Switch# **show ip dhcp snooping binding** 

6.14 IP DHCP SNOOPING OPTION

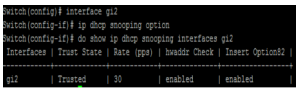
Use the **ip dhcp snooping option** command to enable that insert option82 content into packet. Use the **“no”** form of this command to disable.

Switch#**configure terminal**

Switch(config)#**interface** *{Interface-ID}*

Switch(config-if)# **ip dhcp snooping option**

Switch(config-if)# **no ip dhcp snooping option**

Syntax	**ip dhcp snooping option** **no ip dhcp snooping option**
Default	DHCP snooping option82 is disabled
Mode	Interface Configuration
Example	The example shows how to enable option82 insertion. You can verify settings by the following show ip dhcp snooping interface command. Switch#**configure terminal** Switch(config)# **interface** gi2 Switch(config-if)# **ip dhcp snooping option** Switch(config-if)# **do show ip dhcp snooping interfaces gi2** 

6.15 IP DHCP SNOOPING OPTION ACTION

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.

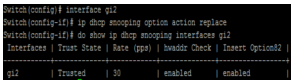
Switch#**configure terminal**

Switch(config)#**interface** *{Interface-ID}*

Switch(config-if)#**ip dhcp snooping option action (drop|keep|replace)**

Switch(config-if)#**no ip dhcp snooping option action**

Syntax	**ip dhcp snooping option action (drop|keep|replace)** **no ip dhcp snooping option action**
Parameter	**Drop** Drop packets with option82 that are received from un trusted port. **Keep** Keep original option82 content in packet. **Replace** Replace option82 content by switch setting.
Default	DHCP snooping option82 is drop
Mode	Interface Configuration

Example	The example shows how to set action to replace option82 content. You can verify settings by the following show running-config command. Switch#**configure terminal** switch(config)# **interface gi2** switch(config-if)# **ip dhcp snooping option action replace** 

6.16 IP DHCP SNOOPING OPTION CIRCUIT-ID

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.

Switch#**configure terminal**

Switch(config-if)# **ip dhcp snooping [vlan** *<1-4094>***] option circuit-id** *{STRING}*

Switch(config-if)# **no ip dhcp snooping [vlan** *<1-4094>***] option circuit-id**

Syntax	**ip dhcp snooping [vlan** *<1-4094>***] option circuit-id** *STRING* **no ip dhcp snooping [vlan** *<1-4094>***] option circuit-id**
Parameter	**Vlan***<1-4094>*VLAN ID to set user defined circuit-id string **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

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#**configure terminal** switch(config)# **interface** gi2 switch(config-if)# **ip dhcp snooping vlan** 1 **option circuit-id** test 

6.17 IP DHCP SNOOPING OPTION REMOTE-ID

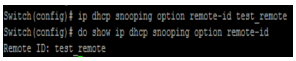
Use the **ip dhcp snooping option remote-id** command to set user-defined remote-id string. Remote-id is a global and unique string. Use the **“no”** form of this command to default setting.

Switch#**configure terminal**

Switch(config)# **ip dhcp snooping option remote-id** *{STRING}*

Switch(config)# **no ip dhcp snooping option remote-id**

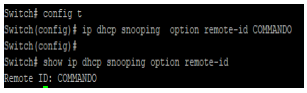
Syntax	**ip dhcp snooping option remote-id** *{STRING}* **no ip dhcp snooping option remote-id**
Parameter	*STRING* Remote-id string, 1 to 63 ASCII characters, no spaces.
Default	Default remote-id is the switch MAC address in byte order
Mode	Global Configuration

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. Switch#**configure terminal** Switch(config)# **ip dhcp snooping option remote-id test_remote** switch(config)# **do show ip dhcp snooping option remote-id** 

6.18 SHOW IP DHCP SNOOPING OPTION

Use the **show ip dhcp snooping option** remote-id command to show remote-id string.

Switch#**show ip dhcp snooping option remote-id**

Syntax	**show ip dhcp snooping option remote-id**
Mode	Privileged EXEC
Example	The example shows how to show remote-id string Switch# **show ip dhcp snooping option remote-id** 

6.19 IP DHCP SNOOPING DATABASE

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.

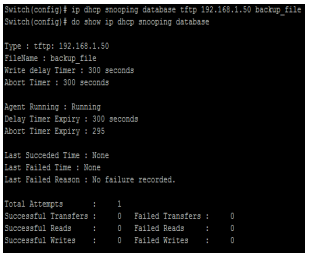
Switch#**configure terminal**

Switch(config)# **ip dhcp snooping database flash**

Switch(config)# **ip dhcp snooping database tftp (**A.B.C.D|HOSTNAME**)** *{NAME}*

Switch(config)# **no ip dhcp snooping database**

Syntax	**ip dhcp snooping database flash** **ip dhcp snooping database tftp (A.B.C.D|HOSTNAME)** *{NAME}* **no ip dhcp snooping database**
Parameter	(A.B.C.D|HOSTNAME)Specify the IP address or hostname of remote TFTP server *NAME* Input name of backup file
Default	DHCP snooping database is disabled
Mode	Global Configuration

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 show ip dhcp snooping database command. Switch#**configure terminal** Switch(config)# **ip dhcp snooping database tftp** 192.168.1.50 **backup_file** Switch(config)# **do show ip dhcp snooping database** 

6.20 IP DHCP SNOOPING DATABASE WRITE-DELAY

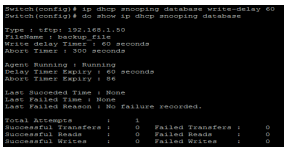
Use the **ip dhcp snooping database write-delay** command to modify the write-delay timer. Use the **"no"** form of this command to default setting.

Switch#**configure terminal**

Switch(config)# **ip dhcp snooping database write-delay***<15-86400>*

Switch(config)# **no 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

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#**configure terminal** Switch(config)# **ip dhcp snooping database write-delay** 60 Switch(config)# **do show ip dhcp snooping database** 

6.21 IP DHCP SNOOPING DATABASE TIMEOUT

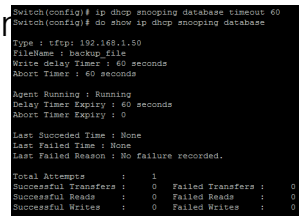
Use the **ip dhcp snooping database timeout** command to modify the timeout timer. Use the **“no”** form of this command to default setting.

Switch#**configure terminal**

Switch(config)# **ip dhcp snooping database timeout**<*0-86400*>

Switch(config)# **no ip dhcp snooping database timeout**

Syntax	**ip dhcp snooping database timeout**<*0-86400*> **no ip dhcp snooping database timeout**

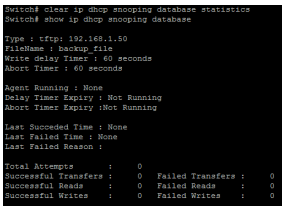
Parameter	<*15-86400*>Specifies the seconds of timeout.Specify (in seconds)how long to wait for the database transfer process to finish before stopping the process. Use 0 to define an infinite duration, which means to continue trying the transfer indefinitely
Default	DHCP snooping database timeout is 300 seconds
Mode	Global Configuration
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#**configure terminal** Switch(config)# **ip dhcp snooping database timeout 60** Switch(cor  **ip dhcp snooping**

```
Switch(config)# ip dhcp snooping database timeout 60
Switch(config)# do 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 : 0

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
```

6.22 CLEAR IP DHCP SNOOPING DATABASE STATISTICS

Use the **clear ip dhcp snooping database statistics** command to clear statistics of DHCP Snooping database.

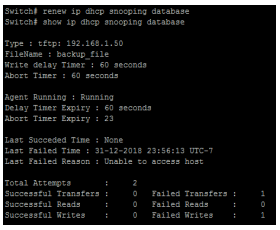
Switch# **clear ip dhcp snooping database statistics**

Syntax	**clear ip dhcp snooping database statistics**
Mode	Privileged EXEC
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. switch# **clear ip dhcp snooping database statistics** switch# **show ip dhcp snooping database** 

6.23 RENEW IP DHCP SNOOPING DATABASE

Use the **renew ip dhcp snooping database** command to renew DHCP Snooping database from backup file.

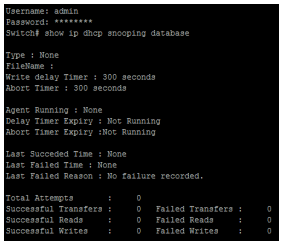
Switch# **renew ip dhcp snooping database**

Syntax	**renew ip dhcp snooping database**
Mode	Privileged EXEC
Example	The example shows how to renew DHCP Snooping database. You can verify settings by the following show ip dhcp snooping database and show ip dhcp snooping binding command. Switch# **renew ip dhcp snooping database** Switch# **show ip dhcp snooping database** 

6.24 SHOW IP DHCP SNOOPING DATABASE

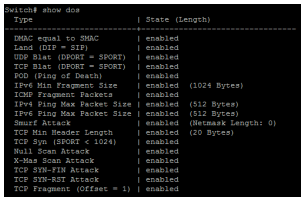
Use the **show ip dhcp snooping database** command to show settings of DHCP Snooping agent.

Switch# **show ip dhcp snooping database**

Syntax	**show ip dhcp snooping database**
Mode	Privileged EXEC
Example	The example shows how to show settings of DHCP Snooping agent. Switch # **show ip dhcp snooping database** 

```
Username: admin
Password: ********
Switch# show ip dhcp snooping database

Type : None
FileName :
Write delay Timer : 300 seconds
Abort Timer : 300 seconds

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

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

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

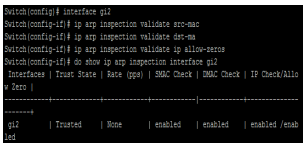
DOS Denial-of-Service (DoS)

Syntax	**show dos** **show dos interface** *{IF_PORTS}*
Parameter	**interface***{IF_PORTS}* An interface ID or the list of interface IDs
Mode	Privileged EXEC
Example	The following example shows the global DoS protection configuration. Switch# **show dos** 

```
Switch# 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
```

DYNAMIC ARP INSPECTION

Syntax	**ip arp inspection validate src-mac** **ip arp inspection validate dst-mac** **ip arp inspection validate ip [allow-zeros]** **no ip arp inspection validate src-mac** **no ip arp inspection validate dst-mac** **no ip arp inspection validate ip [allow-zeros]**
Default	Default is disabled of all validation
Mode	Interface Configuration

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. Switch#**configure terminal** Switch(config)# **interface** gi2 Switch(config-if)# **ip arp inspection validate src-mac** Switch(config-if)# **ip arp inspection validate dst-ma** Switch(config-if)# **ip arp inspection validate ip allow-zeros** Switch(config)# **do show ip arp inspection interface** gi2 

8.5 IP ARP INSPECTION RATE-LIMIT

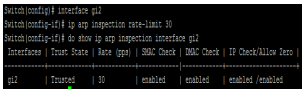
Use the **ip arp inspection rate-limit** command to set rate limitation on interface. The switch drop ARP packets after receives more than configured rate of packets per second. Use the **“no”** form of this command to return to default settings.

Switch#**configure terminal**

Switch(config)# **ip arp inspection rate-limit** *<1-50>*

Switch(config)# **no 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

Example	The example shows how to set rate limit to 30 pps on interface gi2. You can verify settings by the following show ip arp inspection interface command. Switch#**configure terminal** Switch(config)# **interface** gi2 Switch(config)# **ip arp inspection rate-limit** 30 Switch(config)# **do show ip arp inspection interface** gi2 

8.6 CLEAR IP ARP INSPECTION STATISTICS

Use the **clear ip arp inspection interfaces statistics** command to clear statistics that are recorded on interface.

Switch#**clear ip arp inspection interfaces** *{IF_PORTS}* **statistics**

Syntax	**clear ip arp inspection interfaces** *{IF_PORTS}* **statistics**
Parameter	*IF_PORTS* specifies ports to clear statistics
Mode	Privileged EXEC
Example	The example shows how to clear statistics on interface gi1. You can verify settings by the following show ip arp inspection interface statistics command. switch# **clear ip arp inspection interfaces gi2 statistics** switch# **show ip arp inspection interfaces gi2** 

```
Switch# show ip arp inspection interface gi2
Interfaces | Trust State | Rate (pps) | SMAC Check | DMAC Check | IP Check/Allow Zero |
-----------+-------------+------------+------------+------------+---------------------+
gi2        | Trusted     | None       | disabled   | disabled   | disabled/disabled
```

8.7 SHOW IP ARP INSPECTION

Use the **show ip arp inspection** command to show settings of Dynamic Arp Inspection.

Switch#**show ip arp inspection**

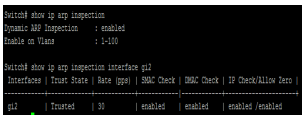
Syntax	**show ip dhcp snooping**
Mode	Privileged EXEC
Example	The example shows how to show settings of Dynamic Arp Inspection Switch# **show ip arp inspection** 

8.8 SHOW IP ARP INSPECITON INTERFACE

Use the **show ip arp inspection interfaces** command to show settings or statistics of interface.

Switch#**show ip arp inspection interfaces** *{IF_PORTS}*

Switch#**show ip arp inspection interfaces** *{IF_PORTS}* **statistics**

Syntax	**show ip arp inspection interfaces** *{IF_PORTS}* **show ip arp inspection interfaces** *{IF_PORTS}***statistics**
Parameter	*IF_PORTS* specifies ports to show statistics
Mode	Privileged EXEC
Example	switch# **show ip arp inspection** 

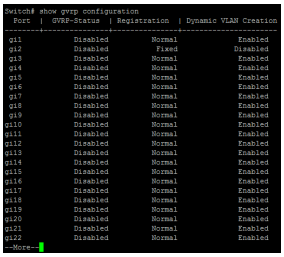
GVRP (GARP VLAN Registration Protocol)

Syntax	**show gvrp**
Mode	Privileged EXEC
Example	The following example specifies that display gvrp test. Switch# **show gvrp** 

9.8 SHOW GVRP CONFIGURATION

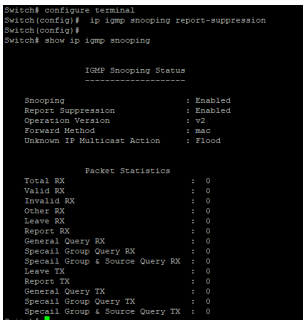
This command will display the ports configuration info.

Switch# **show gvrp configuration**

Syntax	**show gvrp configuration [interface** *{IF_PORTS}***]**
Parameter	**none [interfaces** *IF_PORTS***]** Display all ports configuration Display Specifies posts configuration
Mode	Privileged EXEC
Example	The following example specifies that display gvrp port configuration test. Switch# **show gvrp configuration** 

```
Switch# show gvrp configuration
  Port   |  GVRP-Status  | Registration  | Dynamic VLAN Creation
---------+---------------+---------------+----------------------
gi1              Disabled          Normal              Enabled
gi2              Disabled           Fixed            Disabled
gi3              Disabled          Normal              Enabled
gi4              Disabled          Normal              Enabled
gi5              Disabled          Normal              Enabled
gi6              Disabled          Normal              Enabled
gi7              Disabled          Normal              Enabled
gi8              Disabled          Normal              Enabled
gi9              Disabled          Normal              Enabled
gi10             Disabled          Normal              Enabled
gi11             Disabled          Normal              Enabled
gi12             Disabled          Normal              Enabled
gi13             Disabled          Normal              Enabled
gi14             Disabled          Normal              Enabled
gi15             Disabled          Normal              Enabled
gi16             Disabled          Normal              Enabled
gi17             Disabled          Normal              Enabled
gi18             Disabled          Normal              Enabled
gi19             Disabled          Normal              Enabled
gi20             Disabled          Normal              Enabled
gi21             Disabled          Normal              Enabled
gi22             Disabled          Normal              Enabled
--More--
```

IGMP SNOOPING

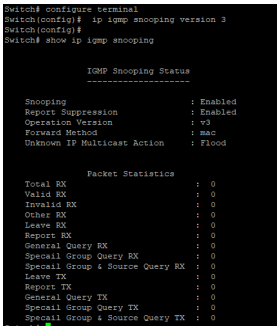
Syntax	**ip igmp snooping report-suppression** **no ip igmp snooping report-suppression**
Default	Default is enabled
Mode	Global Configuration
Example	The following example specifies that disable ip igmp snooping report-suppression test. Switch#**configure terminal** Switch(config)# **ip igmp snooping report-suppression** Switch #**show ip igmp snooping** 

10.3 IP IGMP SNOOPING VERSION

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

Switch#**configure terminal**

Switch(config)# **ip igmp snooping version (**2|3**)**

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
Example	The following example specifies that set ip igmp snooping version 3. Switch#**configure terminal** Switch(config)# **ip igmp snooping version 3** 

10.4 IP IGMP SNOOPING UNKNOWN-MULTICAST ACTION

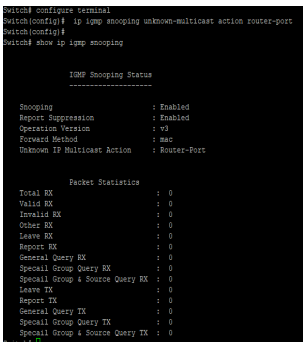
When igmp and mld snooping disabled, it can't set action router-port.When disable igmp snooping &mld snooping, it set unknown multicast action flood. When action is router-port to flood or drop, it will delete the unknown multicast group entry.Use the ip igmp snooping unknown-multicast action command to change action. Use the **"no"** form of this command to restore to default.You can verify settings by the show ip igmp snooping command.

Switch#**configure terminal**

Switch(config)# **ip igmp snooping unknown-multicast action (drop | flood |router-port)**

Switch(config)# **no ip igmp snooping unknown-multicast action**

Syntax	**ip igmp snooping unknown-multicast action (drop | flood |router-port)** **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

Example	The following example specifies that set ip igmp unknown multicast action router-port test. Switch#**configure terminal** Switch(config)# **ip igmp snooping** Switch(config)# **ip igmp snooping unknown-multicast action router-port** Switch#**show ip igmp snooping** 

```
Switch# configure terminal
Switch(config)#  ip igmp snooping unknown-multicast action router-port
Switch(config)#
Switch# 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                      :  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
```

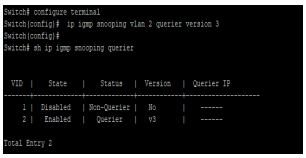
10.5 IP IGMP SNOOPING QUERIER

When enable **ip igmp vlan querier**, there will process router select, the select successful will send general and specific query. 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.

Switch#**configure terminal**

Switch(config)#**ip igmp snooping vlan** *{VLAN-LIST}***querier [version (2|3)]**

Switch(config)#**no ip igmp snooping [vlan] querier**

Syntax	**ip igmp snooping vlan** *{VLAN-LIST}* **querier [version (2|3)]** **no ip igmp snooping [vlan] querier**
Parameter	*VLAN-LIST* specifies VLAN ID list to set(2|3)Query version 2 or 3
Mode	Global Configuration
Example	The following example specifies that set ip igmp snooping querier test. Switch#**configure terminal** Switch(config)# **ip igmp snooping vlan** 2 **querier version** 3 

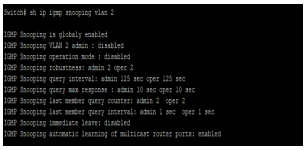
10.6 IP IGMP SNOOPING VLAN

Disable will clear all ip igmp snooping dynamic group and dynamic router port and make all static ip igmp group invalid of this vlan. It 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.

Switch#**configure terminal**

Switch(config)# **ip igmp snooping vlan** *{VLAN-LIST}*

Switch(config)# **no ip igmp snooping vlan** *{VLAN-LIST}*

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
Example	The following example specifies that set ip igmp snooping vlan test. Switch#**configure terminal** Switch(config)# **ip igmp snooping** Switch(config)# **ip igmp snooping vlan 2** 

10.7 IP IGMP SNOOPING VLAN FASTLEAVE

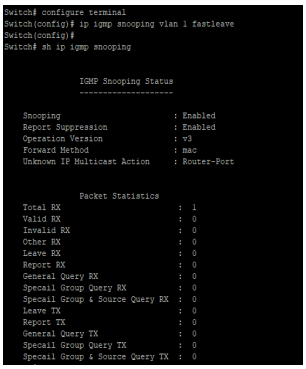
Use the **ip igmp snooping vlan fastleave** command to enable fastleave function. Group will remove port immediately when receive leave packet. Use the **“no”** form of this command to disable.You can verify settings by the show ip igmp snooping vlan command.

Switch#**configure terminal**

Switch(config)# **ip igmp snooping vlan** *{VLAN-LIST}* **fastleave**

Switch(config)# **no ip igmp snooping vlan** *{VLAN-LIST}* **fastleave**

Syntax	**ip igmp snooping vlan** *{VLAN-LIST}* **fastleave** **no ip igmp snooping vlan** *{VLAN-LIST}* **fastleave**
Parameter	*VLAN-LIST* specifies VLAN ID list to set
Mode	Global Configuration

Example	The following example specifies that set ip igmp snooping vlan fastleave test. Switch#**configure terminal** Switch(config)# **ip igmp snooping vlan 1 fastleave** Switch#**show ip igmp snooping** 

```
Switch# configure terminal
Switch(config)# ip igmp snooping vlan 1 fastleave
Switch(config)#
Switch# sh 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                         :  1
   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
```

10.8 IP IGMP SNOOPING VLAN LAST-MEMBER-QUERY-COUNT

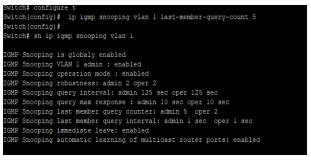
Use the **ip igmp snooping vlan last-member-query-count** command to change how many query packets will send. Use the **“no”** form of this command to restore to default.You can verify settings by the show ip igmp snooping vlan command.

Switch#**configure terminal**

Switch(config)# **ip igmp snooping vlan** *{VLAN-LIST}* **last-member-query-count** <*1-7*>

Switch(config)# **no ip igmp snooping vlan** *{VLAN-LIST}* **last-member-query-count**

Syntax	**ip igmp snooping vlan** *{VLAN-LIST}* **last-member-query-count** <*1-7*> **no ip igmp snooping vlan** *{VLAN-LIST}* **last-member-query-count**
Parameter	*VLAN-LIST* last-member-query-count <*1-7*>specifies VLAN ID list to set specifies
Default	Default is 2
Mode	Global Configuration

Example	The following example specifies that set ip igmp snooping vlan last- member-query-count test. Switch#**configure terminal** Switch(config)# **ip igmp snooping vlan 1 last-member-query-count 5** 

10.9 IP IGMP SNOOPING VLAN LAST-MEMBER-QUERY-INTERVAL

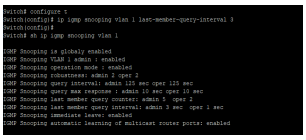
Use the **ip igmp snooping vlan last-member-query-interval** command to set interval between each query packet. Use the **“no”** form of this command to restore to default. You can verify settings by the **show ip igmp snooping vlan** command.

Switch#**configure terminal**

Switch(config)# **ip igmp snooping vlan** *{VLAN-LIST}***last-member-query-interval** *<1- 60>*

Switch(config)# **no ip igmp snooping vlan** *{VLAN-LIST}* **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* last-member-query-interval *<1-60>* specifies VLAN ID list to set specifies last member query interval to set
Default	Default is 1

Mode	Global Configuration
Example	The following example specifies that set ip igmp snooping vlan last- member-query-interval test. Switch#**configure terminal** Switch(config)# **ip igmp snooping vlan 1 last-member-query-interval 3** 

10.10 IP IGMP SNOOPING VLAN QUERY-INTERVAL

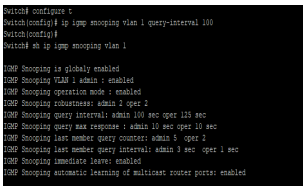
Use the **ip igmp snooping vlan query-interval** command to set interval between each query. Use the **"no"** form of this command to restore to default. You can verify settings by the **show ip igmp snooping vlan** command.

Switch#**configure terminal**

Switch(config)# **ip igmp snooping vlan** *{VLAN-LIST}* **query-interval** *<30-18000>*

Switch(config)# **no ip igmp snooping vlan** *{VLAN-LIST}***query-interval**

Syntax	**ip igmp snooping vlan** *{VLAN-LIST}* **query-interval** *<30-18000>* **no ip igmp snooping vlan** *{VLAN-LIST}* **query-interval**
Parameter	*VLAN-LIST* query-interval specifies VLAN ID list to set *<30-18000>* specifies query interval to set

Default	Default is 125
Mode	Global Configuration
Example	The following example specifies that set ip igmp snooping vlan query- interval test. Switch#**configure terminal** Switch(config)# **ip igmp snooping vlan** 1 **query-interval** 100  Switch# configure t Switch(config)# ip igmp snooping vlan 1 query-interval 100 Switch(config)# Switch# sh ip igmp snooping vlan 1 IGMP Snooping is globaly enabled IGMP Snooping VLAN 1 admin : enabled IGMP Snooping operation mode : enabled IGMP Snooping robustness: admin 2 oper 2 IGMP Snooping query interval: admin 100 sec oper 125 sec IGMP Snooping query max response : admin 10 sec oper 10 sec IGMP Snooping last member query counter: admin 5 oper 2 IGMP Snooping last member query interval: admin 3 sec oper 1 sec IGMP Snooping immediate leave: enabled IGMP Snooping automatic learning of multicast router ports: enabled

10.11 IP IGMP SNOOPING VLAN RESPONSE-TIME

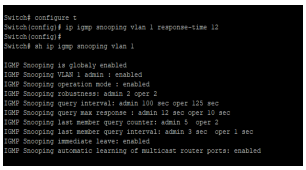
Use the **ip igmp snooping vlan response-time** command to set response time. Use the **"no"** form of this command to restore to default. You can verify settings by the **show ip igmp snooping vlan** command.

Switch#**configure terminal**

Switch(config)# **ip igmp snooping vlan** *{VLAN-LIST}***> response-time** <*5-20*>

Switch(config)# **no ip igmp snooping vlan** *{VLAN-LIST}***response-time**

Syntax	**ip igmp snooping vlan** *{VLAN-LIST}* **response-time** <*5-20*> **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

Example	The following example specifies that set ip igmp snooping vlan response- time test. Switch#**configure terminal** Switch(config)# **ip igmp snooping vlan** 1 **response-time** 12 Switch#**show ip igmp snooping vlan** 1 

10.12 IP IGMP SNOOPING VLAN ROBUSTNESS-VARIABLE

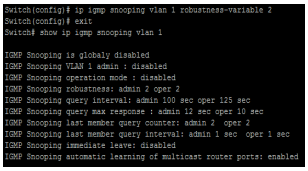
Use the **ip igmp snooping vlan robustness-variable** command to times to retry. Use the **"no"** form of this command to restore to default. You can verify settings by the **show ip igmp snooping vlan** command

Switch#**configure terminal**

Switch(config)# **ip igmp snooping vlan** *{VLAN-LIST}* **robustness-variable** <*1-7*>

Switch(config)# **no ip igmp snooping vlan** *{VLAN-LIST}* **robustness-variable**

Syntax	**ip igmp snooping vlan** *{VLAN-LIST}* **robustness-variable** <*1-7*> **no ip igmp snooping vlan** *{VLAN-LIST}* **robustness-variable**
Parameter	*VLAN-LIST*specifies VLAN ID list to set. robustness-variable <*1-7*>specifies a robustness value to set

Default	Default is 2
Mode	Global Configuration
Example	The following example specifies that set ip igmp snooping vlan parameters test. Switch#**configure terminal** Switch(config)# **ip igmp snooping vlan 1 robustness-variable 2** 

10.13 IP IGMP SNOOPING VLAN ROUTER

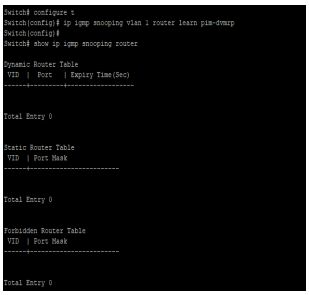
Use the **ip igmp snooping vlan router** command to enable learning router port by routing protocol packets such as PIM/PIMv2, DVMRP, MOSPF. Use the **“no”** form of this command to disable. You can verify settings by the **show ip igmp snooping vlan** command.

Switch#**configure terminal**

Switch(config)# **ip igmp snooping vlan** *{VLAN-LIST}* **router learn pim-dvmrp**

Switch(config)# **no ip igmp snooping vlan** *{VLAN-LIST}* **router learn pim-dvmrp**

Syntax	**ip igmp snooping vlan** *{VLAN-LIST}* **router learn pim-dvmrp** **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
Example	The following example specifies that set ip igmp snooping vlan router test. Switch#**configure terminal** Switch(config)# **ip igmp snooping vlan 1 router learn pim-dvmrp** Switch# **show ip igmp snooping router** 

```
Switch# configure t
Switch(config)# ip igmp snooping vlan 1 router learn pim-dvmrp
Switch(config)#
Switch# 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
------+-----------------------


Total Entry 0
```

10.14 IP IGMP SNOOPING VLAN FORBIDDEN-PORT

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.

Switch#**configure terminal**

Switch(config)# **ip igmp snooping vlan** *{VLAN-LIST}* **forbidden-port** *IF_PORTS*

Switch(config)# **no ip igmp snooping vlan** *{VLAN-LIST}***forbidden-port** *IF_PORTS*

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
Mode	Global Configuration

Example	The following example specifies that set ip igmp snooping static/forbidden port test. Switch#**configure terminal** Switch(config)# **ip igmp snooping vlan 1 forbidden-port** gi3-4 Switch# **show ip igmp snooping forward-all** 

10.15 IP IGMP SNOOPING VLAN STATIC-PORT

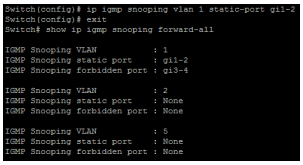
Use the **ip igmp snooping vlan static-port** command to add static forwarding port, all known vlan 1 ipv4 group will add the static ports. Use the **"no"** form of this command to delete static port. You can verify settings by the **show ip igmp snooping forward-all** command.

Switch#**configure terminal**

Switch(config)# **ip igmp snooping vlan** *{VLAN-LIST}* **static-port** *{IF_PORTS}*

Switch(config)# **no ip igmp snooping vlan** *{VLAN-LIST}* **static-port** *{IF_PORTS}*

Syntax	**ip igmp snooping vlan** *{VLAN-LIST}* **static-port** *{IF_PORTS}* **no ip igmp snooping vlan** *{VLAN-LIST}* **static-port** *{IF_PORTS}*
Parameter	*VLAN-LIST* specifies VLAN ID list to set *IF_PORTS* specifies a port list to set or remove

Mode	Global Configuration
Example	The following example specifies that set ip igmp snooping static port test. Switch#**configure terminal** Switch(config)# **ip igmp snooping vlan 1 static-port gi1-2** Switch# **show ip igmp snooping forward-all** 

10.16 IP IGMP SNOOPING VLAN FORBIDDEN-ROUTER-PORT

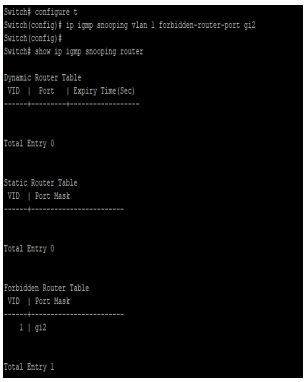
Use the **ip igmp snooping vlan forbidden-router-port** command to add static forbidden router port. This will also remove port from static router port. The forbidden router port will not forward receive query packet. Use the **“no”** form of this command to delete forbidden router port.You can verify settings by the show ip igmp snooping router command.

Switch#**configure terminal**

Switch(config)# **ip igmp snooping vlan** *{VLAN-LIST}***forbidden-router-port** *{IF_PORTS}*

Switch(config)# **no ip igmp snooping vlan** *{VLAN-LIST}***forbidden-router-port** *{IF_PORTS}*

Syntax	**ip igmp snooping vlan** *{VLAN-LIST}* **forbidden-router-port** *{IF_PORTS}* **no ip igmp snooping vlan** *{VLAN-LIST}* **forbidden-router-port** *{IF_PORTS}*

Parameter	*VLAN-LIST* specifies VLAN ID list to set *IF_PORTS* specifies a port list to set or remove
Mode	Global Configuration
Example	The following example specifies that set ip igmp snooping forbidden test. Switch#**configure terminal** Switch(config)# **ip igmp snooping vlan 1 forbidden-router-port gi2** Switch# **show ip igmp snooping router** 

```
Switch# configure t
Switch(config)# ip igmp snooping vlan 1 forbidden-router-port gi2
Switch(config)#
Switch# 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
```

10.17 IP IGMP SNOOPING VLAN STATIC-ROUTER-PORT

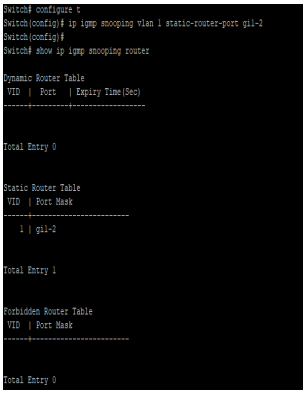
Use the **ip igmp snooping vlan static-router-port** command to add static router port. All query packets will forward to this port. Use the **"no"** form of this command to delete static router port. You can verify settings by the **show ip igmp snooping router** command.

Switch#**configure terminal**

Switch(config)# **ip igmp snooping vlan** *{VLAN-LIST}***static-router-port** *{IF_PORTS}*

Switch(config)# **no ip igmp snooping vlan** *{VLAN-LIST}***static-router-port** *{IF_PORTS}*

Syntax	**ip igmp snooping vlan** *{VLAN-LIST}* **static-router-port** *{IF_PORTS}* **no ip igmp snooping vlan** *{VLAN-LIST}* **static-router-port** *{IF_PORTS}*
Parameter	*VLAN-LIST* specifies VLAN ID list to set *IF_PORTS* specifies a port list to set or remove
Mode	Global Configuration

Example	The following example specifies that set ip igmp snooping static test. Switch#**configure terminal** Switch(config)# **ip igmp snooping vlan 1 static-router-port gi1-2**  Switch# configure t Switch(config)# ip igmp snooping vlan 1 static-router-port gi1-2 Switch(config)# Switch# show ip igmp snooping router Dynamic Router Table VID | Port | Expiry Time(Sec) ----+----+---------- Total Entry 0 Static Router Table VID | Port Mask ----+---------- 1 | gi1-2 Total Entry 1 Forbidden Router Table VID | Port Mask ----+---------- Total Entry 0

10.18 IP IGMP SNOOPING VLAN STATIC-GROUP

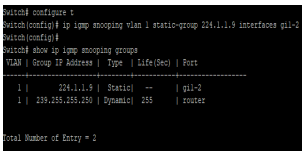
Use the **ip igmp snooping vlan static-group** command to add a static group. The static group will not learn other dynamic ports. If the dynamic group exists, then the static group will overlap the dynamic group. The static group set to valid unless igmp snooping global and vlan enable. Use the **“no”** 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.

Switch#**configure terminal**

Switch(config)# **ip igmp snooping vlan** *{VLAN-LIST}***static-group [] interfaces** *{IF_PORTS}*

Switch(config)# **no ip igmp snooping vlan** *{VLAN-LIST}***static-group [**] **interfaces** *{IF_PORTS}*

Syntax	**ip igmp snooping vlan** *{VLAN-LIST}* **static-group [] interfaces** *{IF_PORTS}* **no ip igmp snooping vlan** *{VLAN-LIST}* **static-group [**] **interfaces** *{IF_PORTS}*
Parameter	*VLAN-LIST* specifies VLAN ID list to set *ip-addr* specifies multicast group ipv4 address *IF_PORTS* specifies port list to set or remove
Mode	Global Configuration

Example	The following example specifies that set ip igmp snooping static group test. Switch#**configure terminal** Switch(config)# **ip igmp snooping vlan** 1 **static-group** 224.1.1.9 **interfaces** gi1-2 Switch# **show ip igmp snooping groups** 

10.19 IP IGMP SNOOPING VLAN GROUP

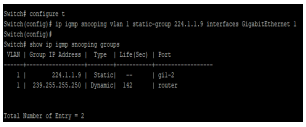
Use the **“no ip igmp snooping vlan group”** command to delete a group which could be static or dynamic.You can verify settings by the **show ip igmp snooping group** command.

Switch#**configure terminal**

Switch(config)# **ip igmp snooping vlan {VLAN-LIST}static-group interfaces GigabitEthernet** *{IF_PORTS}*

Switch(config)# **no ip igmp snooping vlan {VLAN-LIST}static-group interfaces GigabitEthernet** *{ IF_PORTS}*

Syntax	**ip igmp snooping vlan {VLAN-LIST}static-group interfaces GigabitEthernet** *{ IF_PORTS}* **no ip igmp snooping vlan {VLAN-LIST}static-group interfaces GigabitEthernet** *{ IF_PORTS}*
Parameter	VLAN-LIST specifies VLAN ID list to set ip-addr specifies multicast group ipv4 address
Mode	Global Configuration

Example	The following example specifies that set ip igmp snooping static group test. Switch#**configure terminal** Switch(config)# **ip igmp snooping vlan** 1 **static-group** 224.1.1.9 **interfaces GigabitEthernet** 1 Switch#**show ip igmp snooping groups** 

10.20 PROFILE RANGE

Use the profile command to generate IGMP profile. You can verify settings by the show ip igmp profile command

Switch#**configure terminal**

Switch(config)# **ip igmp profile** *{Profile-No}*

Switch(config-igmp-profile)#**profile range ip [ip-addr] action (permit | deny)**

Syntax	**profile range ip [ip-addr] action (permit | deny)**
Parameter	**[ip-addr](permit | deny)** Start ipv4 multicast address End ipv4 multicast address **Permit:** allow Multicast address range ip address learning **deny:** do not allow Multicast address range ip address learning
Mode	igmp profile configuration mode

Example	The following example specifies that set ip igmp profile test. Switch#**configure terminal** Switch(config)# **ip igmp profile 1** Switch(config-igmp-profile)# **profile range ip** 224.1.1.1 224.1.1.8 **action permit**  Switch# configure t Switch(config)# ip igmp profile 1 Switch(config-igmp-profile)# profile range ip 224.1.1.1 224.1.1.8 action permit Switch(config-igmp-profile)# Switch# sh ip igmp profile IP igmp profile index: 1 IP igmp profile action: permit Range low ip: 224.1.1.1 Range high ip: 224.1.1.8

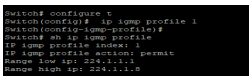
10.21 IP IGMP PROFILE

Use the **ip igmp profile** command to enter profile configuration. Use the **“no”** form of this command to delete profile.You can verify settings by the show ip igmp profile command.

Switch#**configure terminal**

Switch(config)# **ip igmp profile** <*1-128*>

Switch(config)# **no ip igmp profile** <*1-128*>

Syntax	**ip igmp profile** <*1-128*> **no ip igmp profile** <*1-128*>
Parameter	<*1-128*>specifies profile ID
Mode	Global Configuration
Example	The following example specifies that set ip igmp profile test. Switch#**configure terminal** Switch(config)# **ip igmp profile 1** 

10.22 IP IGMP FILTER

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. Use the **“no”** form of this command to delete profile. You can verify settings by the **show ip igmp filter** command.

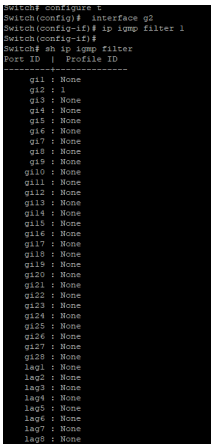
Switch#**configure terminal**

Switch(config)# **interface** *{Interface-ID}*

Switch(config-if)#**ip igmp filter** <*1-128*>

Switch(config-if)#**no ip igmp filter**

Syntax	**ip igmp filter** <*1-128*> **no ip igmp filter**
Parameter	<*1-128*>specifies profile ID
Mode	Port Configuration

Example	The following example specifies that set ip igmp filter test. Switch#**configure terminal** Switch(config)# **interface** gi2 Switch(config-if)#**ip igmp filter** 1 

```
Switch# configure t
Switch(config)# interface g2
Switch(config-if)# ip igmp filter 1
Switch(config-if)#
Switch# sh ip igmp filter
Port ID  |  Profile ID
---------+-------------
     gi1 : None
     gi2 : 1
     gi3 : None
     gi4 : None
     gi5 : None
     gi6 : None
     gi7 : None
     gi8 : None
     gi9 : None
    gi10 : None
    gi11 : None
    gi12 : None
    gi13 : None
    gi14 : None
    gi15 : None
    gi16 : None
    gi17 : None
    gi18 : None
    gi19 : None
    gi20 : None
    gi21 : None
    gi22 : None
    gi23 : None
    gi24 : None
    gi25 : None
    gi26 : None
    gi27 : None
    gi28 : None
   lag1 : None
   lag2 : None
   lag3 : None
   lag4 : None
   lag5 : None
   lag6 : None
   lag7 : None
   lag8 : None
```

10.23 IP IGMP MAX-GROUPS

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. Use the **“no”** form of this command to restore to default. You can verify settings by the show ip igmp max-groups command.

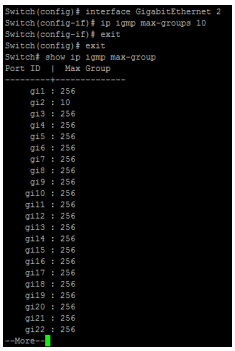
Switch#**configure terminal**

Switch(config)# **interface** *{Interface-ID}*

Switch(config-if)#**ip igmp max-groups** *<0-1024>*

Switch(config-if)#**no ip igmp max-groups**

Syntax	**ip igmp max-groups** *<0-1024>* **no ip igmp max-groups**
Parameter	*<0-1024>* The maximum number of IGMP groups that an interface can join.
Default	Default is 1024
Mode	Port Configuration

Example	The following example specifies that set ip igmp max-groups test. Switch#**configure terminal** Switch(config)# **interface** g2 Switch(config-if)#**ip igmp max-groups 10** 

10.24 IP IGMP MAX-GROUPS ACTION

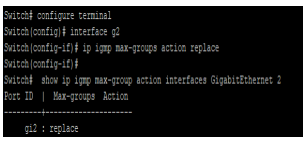
Use the ip igmp max-groups action command to set the action when the numbers of groups reach the limitation. Use the **“no”** form of this command to restore to default. You can verify settings by the show ip igmp max-groups command.

Switch#**configure terminal**

Switch(config)# **interface** *{Interface-ID}*

Switch(config-if)#**ip igmp max-groups action (deny | replace)**

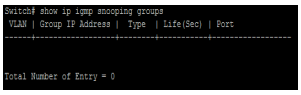
Syntax	**ip igmp max-groups action (deny | replace)**
Parameter	(**deny | replace) Deny:** current port igmp group arrived max-groups, don’t add group. **Replace:** current port igmp group arrived max-groups, remove port for rand group, and add port to new group.
Default	Default action is deny
Mode	Port Configuration

Example	The following example specifies that set action replace test. Switch#**configure terminal** Switch(config)#**interface** g2 Switch(config-if)#**ip igmp max-groups action replace** Switch# **show ip igmp max-group action interfaces** GigabitEthernet 2 

10.25 CLEAR IP IGMP SNOOPING GROUPS

This command will clear the ip igmp groups for dynamic or static or all of type. You can verify settings by the show ip igmp snooping groups command.

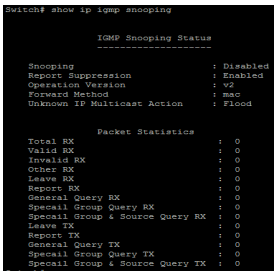
Switch# **clear ip igmp snooping groups [(dynamic | static)]**

Syntax	**clear ip igmp snooping groups [(dynamic | static)]**
Parameter	**none** Clear ip igmp groups include dynamic and static (dynamic | static) Ip igmp group type is dynamic or static
Mode	Privileged EXEC
Example	The following example specifies that clear ip igmp snooping groups test. Switch# **clear ip igmp snooping groups** Switch# **show ip igmp snooping groups** 

10.26 CLEAR IP IGMP SNOOPING STATISTICS

This command will clear the igmp statistics. You can verify settings by the show ip igmp snooping command.

Switch# **clear ip igmp snooping statistics**

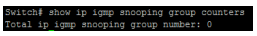
Syntax	**clear ip igmp snooping statistics**
Mode	Privileged EXEC
Example	The following example specifies that clear ip igmp snooping statistics test. Switch# **clear ip igmp snooping statistics** Switch# **show ip igmp snooping** 

```
Switch# 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
  Leave TX                          :  0
  Report TX                         :  0
  General Query TX                  :  0
  Specail Group Query TX            :  0
  Specail Group & Source Query TX   :  0
```

10.27 SHOW IP IGMP SNOOPING GROUPS COUNTERS

This command will display the **ip igmp snooping group counters** include static group.

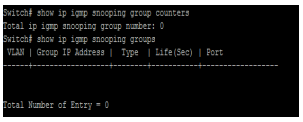
Switch# **show ip igmp snooping group counters**

Syntax	**show ip igmp snooping group counters**
Mode	Privileged EXEC
Example	The following example specifies that display ip igmp snooping group counter test. Switch# **show ip igmp snooping group counters** 

10.28 SHOW IP IGMP SNOOPING GROUPS

This command will display the ip igmp groups for dynamic or static or all of type.

Switch# **show ip igmp snooping groups [(dynamic | static)]**

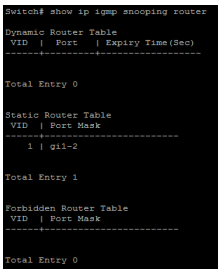
Syntax	**show ip igmp snooping groups [(dynamic | static)]**
Parameter	**none** Show ip igmp groups include dynamic and static **(dynamic | static)** Display Ip igmp group type is dynamic or static
Mode	Privileged EXEC
Example	The following example specifies that show ip igmp snooping groups. Switch# **show ip igmp snooping groups** 

```
Switch# show ip igmp snooping group counters
Total ip igmp snooping group number: 0
Switch# show ip igmp snooping groups
 VLAN | Group IP Address |  Type  | Life(Sec) | Port
------+------------------+--------+-----------+----------------


Total Number of Entry = 0
```

10.29 SHOW IP IGMP SNOOPING ROUTER

This command will display the ip igmp router info.

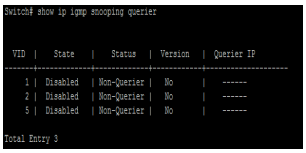
Switch# **show ip igmp snooping router [(dynamic | forbidden |static)]**

Syntax	**show ip igmp snooping router [(dynamic | forbidden |static)]**
Parameter	**none** Show ip igmp router include dynamic and static and forbidden **(dynamic | forbidden | static)** Display Ip igmp router info for different type
Mode	Privileged EXEC
Example	The following example specifies that show ip igmp snooping router. Switch# **show ip igmp snooping router** 

10.30 SHOW IP IGMP SNOOPING QUERIER

This command will display all of the static vlan ip igmp,querier info.

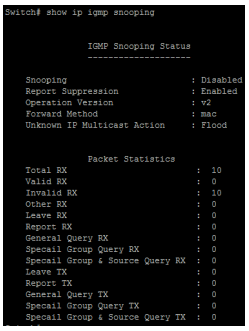
Switch# **show ip igmp snooping querier**

Syntax	**show ip igmp snooping querier**
Mode	Privileged EXEC
Example	The following example specifies that show ip igmp snooping querier test. Switch# **show ip igmp snooping querier** 

10.31 SHOW IP IGMP SNOOPING

This command will display ip igmp snooping global info.

Switch# **show ip igmp snooping**

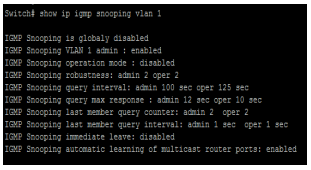
Syntax	**show ip igmp snooping**
Mode	Privileged EXEC
Example	The following example specifies that show ip igmp snooping test. Switch# **show ip igmp snooping** 

```
Switch# 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                       :  10
   Valid RX                       :  0
   Invalid RX                     :  10
   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
```

10.32 SHOW IP IGMP SNOOPING VLAN

This command will display ip igmp snooping vlan info.

Switch# **show ip igmp snooping vlan *[VLAN-LIST]***

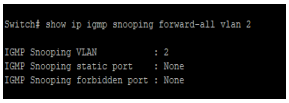
Syntax	**show ip igmp snooping vlan [***VLAN-LIST* **]**
Parameter	**none** Show all ip igmp snooping vlan info *[VLAN-LIST]* Show specifies vlan ip igmp snooping info
Mode	Privileged EXEC
Example	The following example specifies that show ip igmp snooping vlan test. Switch# **show ip igmp snooping vlan** 1 

```
Switch# show ip igmp snooping vlan 1

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

10.33 SHOW IP IGMP SNOOPING FORWARD-ALL

This command will display ip igmp snooping forward all info.

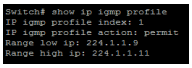
Switch#**show ip igmp snooping forward-all *[vlan** VLAN-LIST**]***

Syntax	**show ip igmp snooping forward-all [vlan** *VLAN-LIST***]**
Parameter	**none** Show all ip igmp snooping vlan forward-all info **[vlan***VLAN-LIST***]** Show specifies vlan of ip igmp forward info.
Mode	Privileged EXEC
Example	The following example specifies that show ip igmp snooping forward-all test. Switch# **show ip igmp snooping forward-all vlan 2** 

10.34 SHOW IP IGMP PROFILE

This command will display ip igmp profile info.

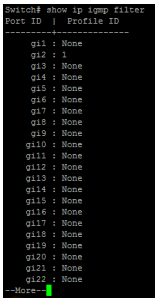
Switch# **show ip igmp profile** ***[<1-128>]***

Syntax	**show ip igmp profile [***<1-128>***]**
Parameter	**none** Show all ip igmp snooping profile info [*<1-128>*] Show specifies index profile info
Mode	Privileged EXEC
Example	The following example specifies that show ip igmp profile test. Switch# **show ip igmp profile** 

10.35 SHOW IP IGMP FILTER

This command will display ip igmp port filter info.

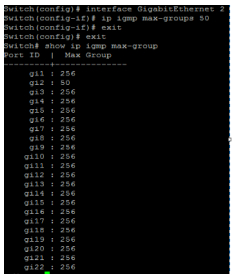
Switch# **show ip igmp filter** ***[interfaces*** *IF_PORTS**]***

Syntax	**show ip igmp filter [interfaces** *IF_PORTS***]**
Parameter	**none** Show all port filter **[interfaces***IF_PORTS***]** Show specifies ports filter
Mode	Privileged EXEC
Example	The following example specifies that show ip igmp filter test. Switch# **show ip igmp filter** 

10.36 SHOW IP IGMP MAX-GROUP

This command will display ip igmp port max-group.

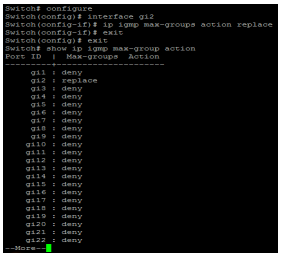
Switch# **show ip igmp max-group** ***[interfaces*** *IF_PORTS]*

Syntax	**show ip igmp max-group [interfaces** *IF_PORTS***]**
Parameter	**none** Show all port max-group ***[interfaces*** *IF_PORTS]* Show interfaces
Mode	Privileged EXEC
Example	The following example specifies that show ip igmp max-group test. Switch#**configure terminal** Switch(config)#**interface** *{Interface-ID}* Switch(config-if)#**ip igmp max-groups** 50 Switch# **show ip igmp max-group** 

10.37 SHOW IP IGMP MAX-GROUP ACTION

This command will display ip igmp port max-group action.

Switch# **show ip igmp max-group action** ***[interfaces*** *IF_PORTS**]***

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
Mode	Privileged EXEC
Example	The following example specifies that show ip igmp max-group action test. Switch#**configure terminal** Switch(config)#**interface** gi2 Switch(config-if)#**ip igmp max-groups action replace** Switch# **show ip igmp max-group action** 

IP SOURCE GUARD

IP SOURCE GUARD

IP Source Guard is a security feature that restricts IP traffic on untrusted Layer 2 ports by filtering traffic based on the DHCP snooping binding database or manually configured IP source bindings. This feature helps prevent IP spoofing attacks when a host tries to spoof and use the IP address of another host. Any IP traffic coming into the interface with a source IP address other than that assigned (via DHCP or static configuration) will be filtered out on the untrusted Layer 2 ports.

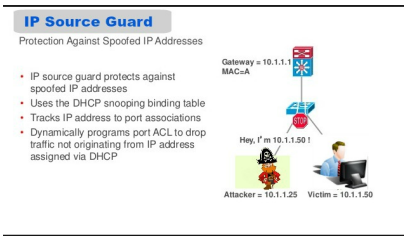


Fig 11.1 IP Source Guard Concept

The IP Source Guard feature is enabled in combination with the DHCP snooping feature on untrusted Layer 2 interfaces. It builds and maintains an IP source binding table that is learned by DHCP snooping or manually configured (static IP source bindings). An entry in the IP source binding table contains the IP address and the associated MAC and VLAN numbers. The IP Source Guard is supported on Layer 2 ports only, including access and trunk ports.

IP Source Guard prevents IP and/or MAC address spoofing attacks on untrusted layer two interfaces. When IP source guard is enabled, all traffic is blocked except for DHCP packets. Once the host gets an IP address through DHCP, only the DHCP-assigned source IP address is permitted. You can also configure a static binding instead of using DHCP.

Comparison between DAI and IP Source Guard:-

Dynamic ARP Inspection	IP Source Guard
- DHCP Snooping creates IP to MAC bindings - DAI Intercepts all ARP requests - Intercepted ARP is validated against IP to MAC binding - Does not switch ARP packets with invalid source address - Used primarily to prevent MITM attacks	- Initially all traffic blocked - Snoops DHCP Address - Creates IP to MAC binding - Installs per port VACL to deny traffic other than snooped source - Protects against IP and MAC spoofing - Will not prevent a MITM attack
Dynamic ARP Inspection	IP Source Guard

Fig 11.2 Comparison between DAI and IP Source Guard

11.1 IP SOURCE VERIFY

Uses 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. Use the no form of this command to disable. You can verify settings by the show ip source interfaces command.

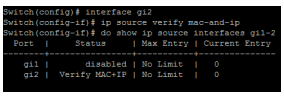
Switch#**configure terminal**

Switch(config)# **interface** *{Interface-ID}*

Switch(config-if)# **ip source verify** ***[mac-and-ip]***

Switch(config-if)# **no ip source verify**

Syntax	**ip source verify** ***[mac-and-ip]*** **no ip source verify**
Parameter	**mac-and-ip** Verify by mac and ip address bundle
Default	IP Source Guard is disabled on interface. Default is that verifying ip address only.
Mode	Port Configuration

Example	The example shows how to enable IP Source Guard with source IP address filtering on interface gi1. Switch#configure terminal Switch(config)# **interface** gi2 Switch(config-if)# **ip source verify** Switch(config-if)# **ip source verify mac-and-ip** Switch(config-if)# **do show ip source interfaces gi1-2** 

11.2 IP SOURCE BINDING

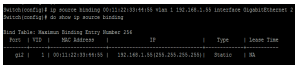
Use the ip source binding command to create a static IP source binding entry has an IP address, its associated MAC address, VLAN ID interface. Use the **"no"** form of this command to delete static entry.You can verify settings by the **"show ip source binding"** command.

Switch#**configure terminal**

Switch(config)# **ip source binding** {A:B:C:D:E:F} **vlan** *<1-4094>* *(*A.B.C.D) **interface** *{IF_PORT}*

Switch(config)# **no ip source binding** {A:B:C:D:E:F} **vlan** *<1-4094>* *(*A.B.C.D) **interface** *{IF_PORT}*

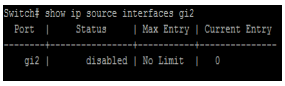
Syntax	**ip source binding** {A:B:C:D:E:F} **vlan** *<1-4094>* *(*A.B.C.D) **interface** *{IF_PORT}* **no ip source binding** {A:B:C:D:E:F} **vlan** *<1-4094>* *(*A.B.C.D) **interface** *{IF_PORT}*
Parameter	A:B:C:D:E:F Specify a MAC address of a binding entry VLAN *<1-4094>*Specify a VLAN ID of a binding entry A.B.C.D Specify IP address and MASK of a binding entry. *IF_PORT* Specify interface of a binding entry.
Mode	Global Configuration

Example	The example shows how to add a static IP source binding entry. Switch#**configure terminal** Switch(config)# **ip source binding** 00:11:22:33:44:55 **vlan** 1 192.168.1.55 **interface** GigabitEthernet 1 Switch(config)# **do show ip source binding** 

11.3 SHOW IP SOURCE INTERFACE

Use the show ip source interface command to show settings of IP Source Guard of interface.

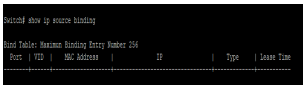
Switch# **show ip source interfaces** *{IF_PORTS}*

Syntax	**show ip source interfaces** *IF_PORTS*
Parameter	*IF_PORTS* specifies ports to show
Mode	Privileged EXEC
Example	The example shows how to show settings of IP Source Guard of interface gi1 Switch# **show ip source interfaces gi2** 

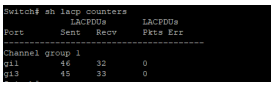
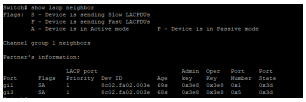
11.4 SHOW IP SOURCE BINDING

Use the show ip source binding command to show binding entries of IP Source Guard.

Switch# **show ip source binding *[(dynamic|static)]***

Syntax	**show ip source binding [(dynamic|static)]**
Parameter	dynamic Show entries that added by DHCP snooping learn static Show entries that added by user
Mode	Privileged EXEC
Example	The example shows how to show static binding entries of IP Source Guard. Switch# **show ip source binding** 

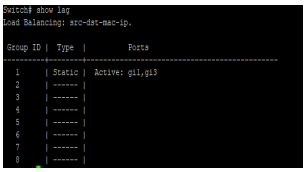
LINK AGGREGATION

Syntax	**show lacp sys-id** **show lacp [**<*1-8*>**] counters** **show lacp [**<*1-8*>**] (internal | neighbor) [detail]**
Mode	Privileged EXEC
Example	This example shows how to show LACP statistics. Switch# **show lacp counters**  Switch# **show lacp internal**  This example shows how to show LACP remote information. Switch# **show lacp neighbor** 

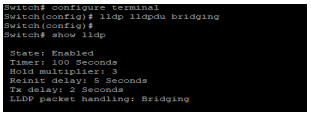
12.7 SHOW LAG

Use **“show lag”** command to show current LAG load balance algorithm and members active/inactive status.

Switch# **show lag**

Syntax	**show lag**
Mode	Privileged EXEC
Example	This example shows how to show current LAG status. Switch# **show lag** 

LLDP

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 disabled, LLDP packets are flooded (forwarded to all interfaces).
Default	Default LLDP PDU handling behavior when LLDP disabled is flooding
Mode	Global Configuration
Example	This example sets LLDP disable action to bridging. Switch# **configure terminal** Switch(config)# **lldp lldpdu bridging** Switch# **show lldp** 

13.7 LLDP MED

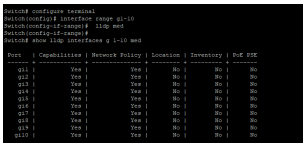
Use **“lldp med”** to configure the LLDP MED enable status. If LLDP MED is enabled, LLDP MED capability TLV and other selected MED TLV would be attached. The configuration could be shown by **“show lldp med”** command. Use the **“no”** form of this command to disable the LLDP MED status.

Switch# **configure terminal**

Switch(config)# **interface** *{Interfac-ID}*

Switch(config-if)# **lldp med**

Switch(config-if)# **no lldp med**

Syntax	**lldp med** **no lldp med**
Default	lldp med
Mode	Port Configuration
Example	This example sets port gi1 to enable LLDP MED, port gi2 to disable LLDP MED. Switch# **configure terminal** Switch(config)# **interface range** g1-10 Switch(config-if-range)# **lldp med** Switch# **show lldp interfaces** g 1-10 **med** 

13.8 LLDP MED FAST-START-REPEAT-COUNT

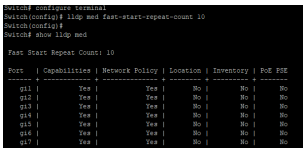
Use **“lldp med fast-start-repeat-count”** command to configure the LLDP PDU fast start TX repeat count. When port links up, it will send LLDP PDU immediately to notify link partner. The number of LLDP PDU sends when it links up depends on fast-start-repeat-count configuration. The LLDP PDU fast-start 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. Use the **“no”** form of this command to restore count to default.

Switch# **configure terminal**

Switch(config)# **lldp med fast-start-repeat-count** <*1-10*>

Switch(config)# **no lldp med fast-start-repeat-count**

Syntax	**lldp med fast-start-repeat-count** <*1-10*> **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

Example	This example sets fast start repeat count to 10. Switch# **configure terminal** Switch(config)# **lldp med fast-start-repeat-count** 10 Switch# **show lldp med** 

```
Switch# configure terminal
Switch(config)# lldp med fast-start-repeat-count 10
Switch(config)#
Switch# show lldp med

 Fast Start Repeat Count: 10

 Port    | Capabilities | Network Policy | Location | Inventory | PoE PSE
 --------+--------------+----------------+----------+-----------+--------
    gi1  |      Yes     |       Yes      |    No    |     No    |    No
    gi2  |      Yes     |       Yes      |    No    |     No    |    No
    gi3  |      Yes     |       Yes      |    No    |     No    |    No
    gi4  |      Yes     |       Yes      |    No    |     No    |    No
    gi5  |      Yes     |       Yes      |    No    |     No    |    No
    gi6  |      Yes     |       Yes      |    No    |     No    |    No
    gi7  |      Yes     |       Yes      |    No    |     No    |    No
```

13.9 LLDP MED LOCATION

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. Use the **“no”** form of this command to clear location data.

Switch# **configure terminal**

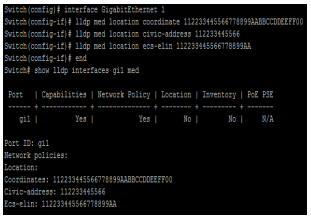
Switch(config)#**interface** *{Interface-ID}*

Switch(config-if)# **lldp med location (coordination|civic-address|ecs-elin) ADDR**

Switch(config-if)# **no lldp med location (coordination|civic-address|ecs-elin)**

Syntax	**lldp med location (coordination|civic-address|ecs-elin) ADDR** **no lldp med location (coordination|civic-address|ecs-elin)**

Parameter	Co-ordination civic-address ecs-elin ADDR Location type to be configured. “ecs-elin” is abbreviation of emergency call service – emergency location identifier number 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. For ecs-elin, the length is 10 to 25 bytes.
Default	**Default** Deafult is no location data.
Mode	Mode Port Configuration

Example	This example sets location data for interface gi1. Switch# **configure terminal** Switch(config)# **interface** gi1 Switch(config-if)# **lldp med location coordinate 1122334455667788 99AABBCCDDEEFF00** Switch(config-if)# **lldp med location civic-address 112233445566** Switch(config-if)# **lldp med location ecs-elin 11223344556677889 9AA** Switch# **show lldp interfaces gi1 med** 

13.10 LLDP MED NETWORK-POLICY

Use **“lldp med network-policy”** command to configure the LLDP MEDnetwork 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 cannot be created since it is in auto mode. The network policy table configuration could be shown by **“show lldp med”** command.

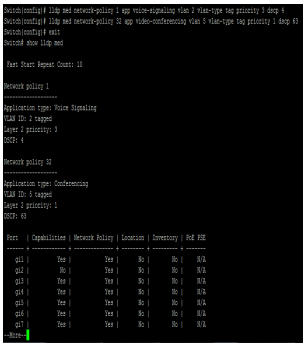
Use the **“no”** form of this command to remove network policy entry of specific index. A network policy can be removed only when it is not bind to any port.

Switch# **configure terminal**

Switch(config)# **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>*

Switch(config)# **no lldp med network-policy** *<1-32>*

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-signaling** Specify the network policy application type. *<1-4094>*Specify the VLAN IDtag untag Specify the VLAN tag status *<0-7>*Specify the L2 priority *<0-63>*Specify the DSCP value

Mode	Global Configuration
Example	This example create 2 network policies. Switch# **configure terminal** 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** 

```
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(config)# exit
Switch# 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      |    No    |     No    |   N/A
   gi2  |      No      |       Yes      |    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
--More--
```

13.11 LLDP MED NETWORK-POLICY (INTERFACE)

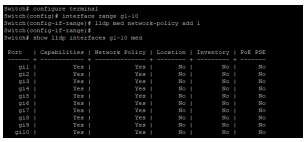
Use **“lldp med network-policy”** command to bind the network policy to port interface. The bonded network policy of one port should be with different types. If network policy TLV is selected over a port, the bonded network policies would be attached in LLDP MED PDU. The configuration of network policy binding could be shown by **“show lldp med” command.**

Switch# **configure terminal**

Switch(config)# **interface** *{Interface-ID ranges}*

Switch(config-if-range)#**lldp med network-policy (add|remove)** *<1-32>*

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
Mode	Port Configuration

Example	This example binds network policy for interface gi1 and gi2. Switch# **show lldp med** Switch# **configure terminal** Switch(config)# **interface range** g1-10 Switch(config-if-range)#**lldp med network-policy add** 1 Switch# **show lldp interfaces** g1-10 **med** 

13.12 LLDP MED TLV-SELECT

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. Use the **“no”** form of this command to remove all selected MED TLV over the dedicated ports.

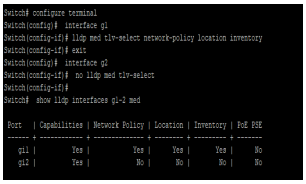
Switch# **configure terminal**

Switch(config)# **interface** *{Interface-ID}*

Switch(config-if)# **lldp med tlv-select MEDTLV [MEDTLV] [MEDTLV] [MEDTLV]**

Switch(config-if)# **no lldp med tlv-select**

Syntax	**lldp med tlv-select MEDTLV [MEDTLV] [MEDTLV] [MEDTLV]** **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
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# **configure terminal** Switch(config)# **interface** g1 Switch(config-if)# **lldp med tlv-select network-policy location inventory** Switch(config)# **interface** g2 Switch(config-if)# **no lldp med tlv-select** Switch# **show lldp interfaces** g1-2 **med** 

```
Switch# configure terminal
Switch(config)#  interface g1
Switch(config-if)# lldp med tlv-select network-policy location inventory
Switch(config-if)# exit
Switch(config)#  interface g2
Switch(config-if)#  no lldp med tlv-select
Switch(config-if)#
Switch#  show lldp interfaces g1-2 med

 Port   | Capabilities | Network Policy | Location | Inventory | PoE PSE
 -------+--------------+----------------+----------+-----------+--------
    g1  |      Yes     |       Yes      |    Yes   |     Yes   |    No
    g2  |      Yes     |        No      |    No    |     No    |    No
```

13.13 LLDP TLV-SELECT

Use **“lldptlv-select”** command to attach selected TLV in PDU. The configuration could be shown by **“show lldp”** command. Use the **“no”** form of this command to remove all selected TLV.

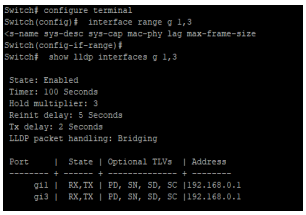
Switch# **configure terminal**

Switch(config)# **interface** *{Interface-ID ranges}*

Switch(config-if-range)# **lldp tlv-select TLV** [TLV] [TLV] [TLV] [TLV] [TLV] [TLV] [TLV]

Switch(config-if-range)# **no lldp tlv-select**

Syntax	**Lldp tlv-select TLV [TLV] [TLV] [TLV] [TLV] [TLV] [TLV] [TLV]** **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- addr (management address).
Mode	Port Configuration

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# **configure terminal** Switch(config)# **interface range** g 1,3 Switch(config-if-range)# **lldp tlv-select port-desc sys-name sys-desc sys-cap mac-phy lag max-frame-size** Switch(config-if-range)# **end** Switch# **show lldp interfaces** g 1,3 

13.14 LLDP TLV-SELECT PVID

Use **“lldptlv-select pvid”** command to configure the 802.1 PVID TLV attachenable status. The configuration could be shown by **“show lldp”** command. Use the **“no”** form of this command to restore the pvid to default value.

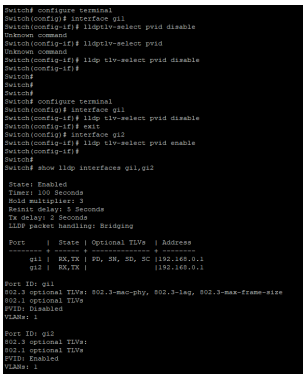
Switch# **configure terminal**

Switch(config)# **interface** *{Interface-ID}*

Switch(config-if)# **lldp tlv-select pvid (disable|enable)**

Switch(config-if)# **no lldp tlv-select pvid**

Syntax	**Lldp tlv-select pvid (disable|enable)** **no lldp tlv-select pvid**
Parameter	**Disable** Disable LLDP 802.1 PVID TLV attach state **Enable** Enable LLDP 802.1 PVID TLV attach state
Mode	Port Configuration

Example	This example sets port gi1 PVID TLV attaches status to disable and port gi2 to enable. Switch# **configure terminal** Switch(config)# **interface** gi1 Switch(config-if)# **lldp tlv-select pvid disable** Switch(config-if)# **interface** gi2 Switch(config-if)# **lldp tlv-select pvid enable** Switch# **show lldp interfaces** gi1,gi2 

13.15 LLDP TLV-SELECT VLAN-NAME

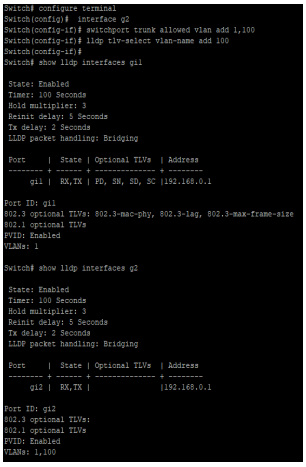
Use **“lldp tlv-select vlan-name”** command to add or remove VLAN list for 802.1 VLAN-NAME TLV. The configuration could be shown by **“show lldp”** command.

Switch# **configure terminal**

Switch(config)# **interface** *{Interface-ID}*

Switch(config-if)# **lldp tlv-select vlan-name (add|remove)** *{VLAN-LIST}*

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
Mode	Port Configuration

Example	This example add VLAN 100 to VLAN-NAME TLV for port gi10. Switch# **configure terminal** Switch(config)# **vlan** 100 Switch(config-vlan)# **exit** Switch(config)# **interface** g2 Switch(config-if)# **switchport trunk allowed vlan add 1,100** Switch(config-if)# **lldp tlv-select vlan-name add** 100 Switch(config-if)# **end** Switch# **show lldp interfaces gi1** Switch# **show lldp interfaces g2** 

13.16 LLDP TX

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.

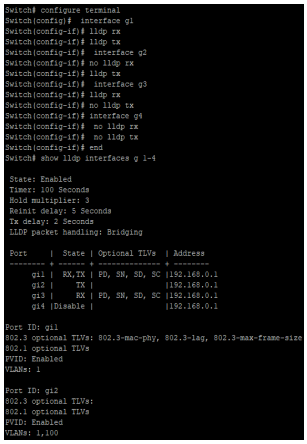
Switch# **configure terminal**

Switch(config)# **interface** *{Interface-ID}*

Switch(config-if)# **lldp tx**

Switch(config-if)# **no lldp tx**

Syntax	**lldp tx** **no lldp tx**
Mode	Port Configuration

Example	This example sets port gi1 to enable LLDP TX, port gi2 to disable RX but enable TX, port gi3 to enable RX but disable TX, port gi4 to disable RX and TX. Switch# **configure terminal** Switch(config)# **interface** g1 Switch(config-if)# **lldp rx** Switch(config-if)# **lldp tx** Switch(config-if)# **interface** g2 Switch(config-if)# **no lldp rx** Switch(config-if)# **lldp tx** Switch(config-if)# **interface** g3 Switch(config-if)# **lldp rx** Switch(config-if)# **no lldp tx** Switch(config-if)# **interface** g4 Switch(config-if)# **no lldp rx** Switch(config-if)# **no lldp tx** Switch(config-if)# **end** Switch# **show lldp interfaces** g 1-4 

13.17 LLDP TX-DELAY

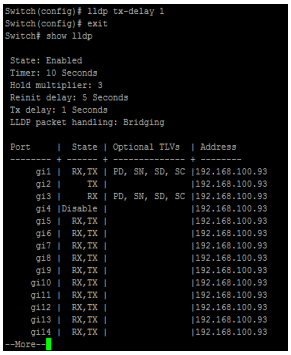
Use **“lldp tx-delay”** command to configure the delay in seconds between successive LLDP frame transmissions. The delay starts to count in any case LLDP PDU is sent such as by LLDP PDU advertise routine, LLDP PDU content change, port link up, etc. The configuration could be shown by **“show lldp”** command. Use the **“no”** form of this command to restore the delay to default value.

Switch# **configure terminal**

Switch(config)# **lldp tx-delay** <*1-8192*>

Switch(config)# **no lldp tx-delay**

Syntax	**lldp tx-delay** <*1-8192*> **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

Example	This example sets LLDP PDU TX delay to 10 seconds. Switch# **configure terminal** Switch(config)# **lldp tx-delay 1** Switch# **show lldp** 

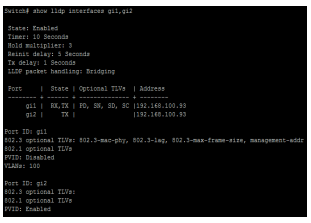
```
Switch(config)# lldp tx-delay 1
Switch(config)# exit
Switch# show lldp

 State: Enabled
 Timer: 10 Seconds
 Hold multiplier: 3
 Reinit delay: 5 Seconds
 Tx delay: 1 Seconds
 LLDP packet handling: Bridging

 Port     |  State | Optional TLVs  | Address
 -------- + ------ + -------------- + -------
      gi1 |  RX,TX | PD, SN, SD, SC |192.168.100.93
      gi2 |     TX |                |192.168.100.93
      gi3 |     RX | PD, SN, SD, SC |192.168.100.93
      gi4 |Disable |                |192.168.100.93
      gi5 |  RX,TX |                |192.168.100.93
      gi6 |  RX,TX |                |192.168.100.93
      gi7 |  RX,TX |                |192.168.100.93
      gi8 |  RX,TX |                |192.168.100.93
      gi9 |  RX,TX |                |192.168.100.93
     gi10 |  RX,TX |                |192.168.100.93
     gi11 |  RX,TX |                |192.168.100.93
     gi12 |  RX,TX |                |192.168.100.93
     gi13 |  RX,TX |                |192.168.100.93
     gi14 |  RX,TX |                |192.168.100.93
--More--
```

13.18 SHOW LLDP

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. Single 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).

Switch# **show lldp**

Switch# **show lldp interface** *{IF_NMLPORTS}*

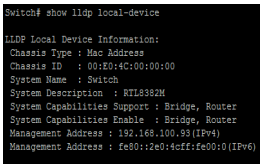
Syntax	**show lldp** **show lldp interface** *{IF_NMLPORTS}*
Parameter	*IF_NMLPORTS* Specify the ports to display information
Mode	Privileged EXEC
Example	This example displays lldp information of port gi1 and gi2 Switch# **show lldp interfaces gi1,gi2** 

13.19 SHOW LLDP LOCAL-DEVICE

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.

Switch# **show lldp local-device**

Switch# **show lldp interfaces***{IF_NMLPORTS}***local-device**

Syntax	**show lldp local-device** **show lldp interfaces***{IF_NMLPORTS}* **local-device**
Parameter	*IF_NMLPORTS* Specify the ports to display information
Mode	Privileged EXEC
Example	This example displays the local device information. Switch# **show lldp local-device** 

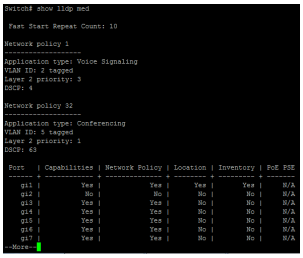
```
Switch# show lldp local-device

LLDP Local Device Information:
 Chassis Type : Mac Address
 Chassis ID   : 00:E0:4C:00:00:00
 System Name  : Switch
 System Description  : RTL8382M
 System Capabilities Support : Bridge, Router
 System Capabilities Enable  : Bridge, Router
 Management Address : 192.168.100.93(IPv4)
 Management Address : fe80::2e0:4cff:fe00:0(IPv6)
```

13.20 SHOW LLDP MED

Use **“show lldp med”** command to display the LLDP MED configuration information.

Switch# **show lldp med**

Switch# **show lldp interfaces***{IF_NMLPORTS}***med**

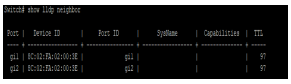
Syntax	**show lldp med** **show lldp interfaces***{IF_NMLPORTS}* **med**
Parameter	*IF_NMLPORTS* Specify the ports to display information
Mode	Privileged EXEC
Example	This example displays the LLDP MED information. Switch# **show lldp med** 

13.21 SHOW LLDP NEIGHBOR

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.

Switch# **show lldp neighbor**

Switch# **show lldp interfaces***{IF_NMLPORTS}***neighbor**

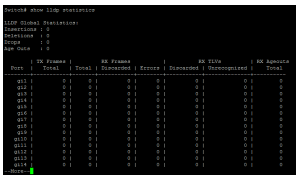
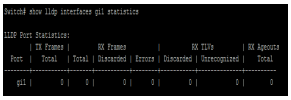
Syntax	**show lldp neighbor** **show lldp interfaces***{IF_NMLPORTS}* **neighbor**
Parameter	*IF_NMLPORTS* Specify the ports to display information
Mode	Privileged EXEC
Example	This example displays the neighbor information. Switch# **show lldp neighbor** 

13.23 SHOW LLDP STATISTICS

Use **“show lldp statistics”** command to display the LLDP RX/TX statistics.

Switch# **show lldp statistics**

Switch# **show lldp interfaces***{IF_NMLPORTS}***statistics**

Syntax	**show lldp statistics** **show lldp interfaces***{IF_NMLPORTS}* **statistics**
Parameter	*IF_NMLPORTS* Specify the ports to display information
Mode	Privileged EXEC
Example	This example display the LLDP statistics. Switch# **show lldp statistics**  Switch(config)# **show lldp interfaces gi1 statistics** 

13.24 CLEAR LLDP STATISTICS

Use **“clear lldp globle statistics”** command to clear the LLDP RX/TX statistics.

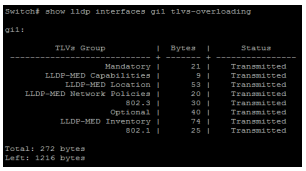
Switch# **clear lldp globle statistics**

Syntax	**clear lldp globle statistics**
Mode	Privileged EXEC
Example	This example shows how to clear LLDP statistics. Switch# **clear lldp statistics**

13.25 SHOW LLDP TLV-OVERLOADING

The LLDP PDU is composed by TLVs and selected number TLVs may compose a large PDU that the system cannot 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. Use **“show lldptlv-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.

Switch# **show lldp interfaces***{IF_NMLPORTS}***tlvs-overloading**

Syntax	**show lldp interfaces***{IF_NMLPORTS}* **tlvs-overloading**
Parameter	*IF_NMLPORTS* Specify the ports to display information
Mode	Privileged EXEC
Example	This example display the LLDP TLVs overloading status of port gi1. Switch# **show lldp interfaces gi1 tlvs-overloading** 

```
Switch# show lldp interfaces gi1 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
                      802.3 |      30 |    Transmitted
                   Optional |      40 |    Transmitted
          LLDP-MED Inventory |      74 |    Transmitted
                      802.1 |      25 |    Transmitted

Total: 272 bytes
Left: 1216 bytes
```

LOGGING

Almost all information technology systems generate a log, which serves as a record of all the activity that the system conducted in its operation. Such logs are generated by network infrastructure devices (firewalls, switches, domain name service devices, routers, load balancers), computer platforms (servers, appliances, and smartphones), operating systems (Windows, Linux, IoS) and applications (client/server, web applications, cloud-based utilities).

In an application, a network log is typically a file that contains a record of events that occurred in the application. It contains the record of user and process access calls to objects, attempts at authentication, and other activity. Generally, an event is categorized as an error, a warning, or an informational activity. The specific format and data that are in a log are typically determined by the application designer, to meet various application requirements, and then implemented by the application developer.

14.1 CLEAR LOGGING

To clear the log messages from the internal logging buffer and flash, use command **“clear logging”** in the Privileged EXEC mode.

Switch# **clear logging**

Syntax	**clear logging**
Parameter	**buffered** Clear the log messages stored in the RAM. **file** Clear the log messages stored in the Flash.
Mode	Privileged EXEC
Example	The following example clear the log messages stored in RAM and Flash. Switch# **clear logging buffered** Switch# **clear logging file**

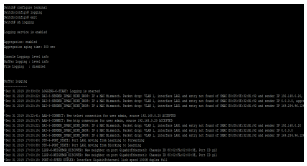
14.2 LOGGING

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. 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.

Switch#**configure terminal**

Switch(config)# **logging**

Switch(config)# **no logging**

Syntax	**logging** **no logging**
Default	Logging service is enabled
Mode	Global Configuration
Example	The following example disables and enables the logging service on the switch. Switch#**configure terminal** Switch(config)# **no logging** Switch(config)# **logging** 

14.3 LOGGING HOST

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.

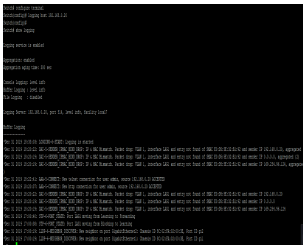
Switch# **configure terminal**

Switch(config)# **logging host (ip-addr|hostname) [facility facility] [port port] [severity sev]**

Switch(config)# **no logging host (ip-addr|hostname)**

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)
Mode	Global Configuration

Example	The following example adds the remote logging rules by IP and Hostname. Switch# **configure terminal** Switch(config)# **logging host 192.168.0.20** 

14.4 LOGGING SEVERITY

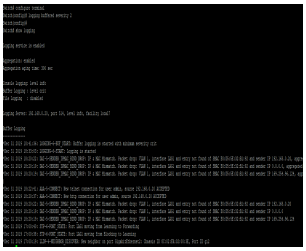
To set the minimum severity for the messages that are logged to RAM, console, or Flash, use the command logging severity in the Global Configuration mode. Use the **“no”** form of the command to remove the mechanism of logging to RAM, console, or Flash individually.

Switch# **configure terminal**

Switch(config)# **logging (buffered|console|file) [severity sev]**

Switch(config)# **no logging (buffered|console|file)**

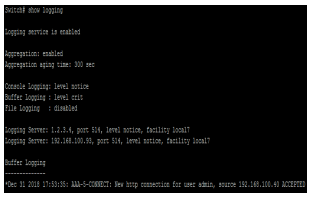
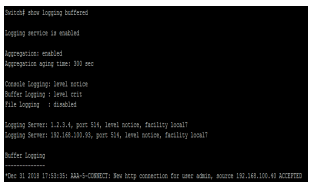
Syntax	**logging (buffered|console|file) [severity sev]** **no logging (buffered|console|file)**
Parameter	**buffered** Log messages to RAM. **console** Log messages to console buffer. **file** Log messages to Flash. **severity** sev Specify the minimum severity of the logging messages. The valid range is from 0 to 7, and the number 0 to 7 represents emergency, 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
Example	The following example sets the minimum severity level of logging to RAM and Flash as debugging. Switch# **configure terminal** Switch(config)# **logging buffered severity 2** 

14.5 SHOW LOGGING

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.

Switch# **show logging [buffered|file]**

Syntax	**show logging [buffered|file]**
Parameter	Buffered Display the log messages stored in the RAM. File Display the log messages stored in the Flash.
Mode	Privileged EXEC
Example	The following example shows the global logging configuration. Switch# **show logging**  Switch# **show logging buffered** 

MAC ADDRESS TABLE

A MAC address table, sometimes called a Content Addressable Memory (CAM) table, is used on Ethernet switches to determine where to forward traffic on a LAN. Now let's break this down a little bit to understand how the MAC address table is built and used by an Ethernet switch to help traffic move along the path to its destination.

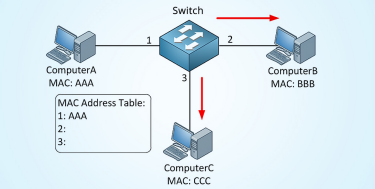


Fig 15.1 MAC Address Table

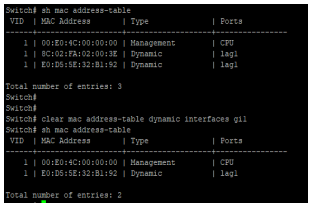
Normally your switch will automatically learn MAC addresses and fill its MAC address table (CAM table) by looking at the source MAC address of incoming frames and flooding frames if it doesn’t know where to forward the frame.

```
Switch# sh mac address-table
 VID  | MAC Address       | Type              | Ports
------+-------------------+-------------------+----------------
   1  | 00:E0:4C:00:00:00 | Management        | CPU
   1  | 8C:02:FA:02:00:3E | Dynamic           | lag1
   1  | E0:D5:5E:32:B1:92 | Dynamic           | lag1

Total number of entries: 3
```

15.1 CLEAR MAC ADDRESS-TABLE

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 Privileged EXEC mode.

Switch# **clear mac address-table dynamic [interfaces** *IF_PORTS***| vlan vlan-id]**

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
Mode	Privileged EXEC
Example	The following example clears the learned MAC addresses on the interface gi1. Switch# **clear mac address-table dynamic interfaces gi1** 

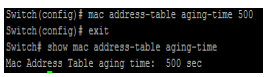
```
Switch# sh mac address-table
 VID  | MAC Address       | Type              | Ports
------+-------------------+-------------------+---------------
    1 | 00:E0:4C:00:00:00 | Management        | CPU
    1 | 8C:02:FA:02:00:3E | Dynamic           | lag1
    1 | E0:D5:5E:32:B1:92 | Dynamic           | lag1

Total number of entries: 3
Switch#
Switch#
Switch# clear mac address-table dynamic interfaces gi1
Switch# sh mac address-table
 VID  | MAC Address       | Type              | Ports
------+-------------------+-------------------+---------------
    1 | 00:E0:4C:00:00:00 | Management        | CPU
    1 | E0:D5:5E:32:B1:92 | Dynamic           | lag1

Total number of entries: 2
```

15.2 MAC ADDRESS-TABLE AGING-TIME

To set the aging time of the MAC address table, use the command macAddress-table aging-time in the Global Configuration mode.

Switch# **configure terminal**

Switch(config)# **mac accress-table aging-time** {seconds}

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
Example	The following example set the agimg time to 500 seconds. Switch# **configure terminal** Switch(config)# **mac address-table aging-time** 500 Switch# **show mac address-table aging-time** 

15.3 MAC ADDRESS-TABLE STATIC

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 unicast MAC address. To delete the static entry from the MAC address table, use the **“no”** form of the command.

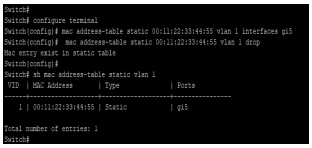
Switch# **configure terminal**

Switch(config)# **mac address-table static mac-addr vlan vlan-id interfaces** *{IF_PORTS}*

Switch(config)# **mac address-table static mac-addr vlan vlan-id drop**

Switch(config)# **no mac address-table static mac-addr vlan vlan-id**

Syntax	**mac address-table static mac-addr vlan** {vlan-id} **interfaces** *{IF_PORTS}* **mac address-table static mac-addr vlan** {vlan-id} **drop** **no mac address-table static mac-addr vlan vlan-id**
Parameter	**mac-addr** 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.
Mode	Global Configuration

Example	The following example adds a static address into MAC address table. Switch#**configure terminal** Switch(config)# **mac address-table static** 00:11:22:33:44:55 **vlan** 1 **interfaces** gi5 Switch(config)# **mac address-table static** 00:11:22:33:44:55 **vlan** 1 **drop** 

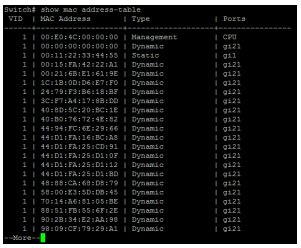
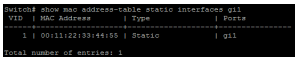
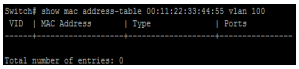
15.4 SHOW MAC ADDRESS-TABLE

To show the entry in the MAC address table, use the command show macaddress-table in the Privileged EXEC mode.

Switch# **show mac address-table [dynamic|static] [interface** *IF_PORTS***] [vlan vlan- id]**

Switch# **show mac address-table [**mac-addr**] [**vlan vlan-id**]**

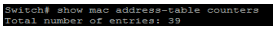
Syntax	**show mac address-table [dynamic|static] [interface** *IF_PORTS***] [vlan vlan- id]** **show mac address-table [mac-addr] [vlan vlan-id]**
Parameter	**dynamic** Display only dynamic MAC addresses **static** Display only static MAC addresses **Interface** *IF_PORTS* Display the MAC addresses entries 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
Mode	Privileged EXEC

Example	The following example displays the entire MAC address table. Switch# **show mac address-table**  Switch# **show mac address-table static interfaces gi1**  Switch# **show mac address-table 00:11:22:33:44:55 vlan 100** 

15.5 SHOW MAC ADDRESS-TABLE COUNTERS

To display the total entries in the MAC address table, use the command show mac address-table counters in the Privileged EXEC mode.

Switch# **show mac address-table counters**

Syntax	**show mac address-table counters**
Mode	Privileged EXEC
Example	The following example display numbers of addresses in the address table. Switch# **show mac address-table counters** 

15.6 SHOW MAC ADDRESS-TABLE AGING-TIME

To show MAC address aging time, use the command show mac address-table aging-time in the Privileged EXEC mode.

Switch# **show mac address-table aging-time**

Syntax	**show mac address-table aging-time**
Mode	Privileged EXEC
Example	The following example displays aging time for the MAC address table. Switch# **show mac address-table aging-time** Switch# show mac address-table aging-time Mac Address Table aging time: 500 sec

MAC VLAN

MAC VLAN :-The **MAC**-based **VLAN** feature allows incoming untagged packets to be assigned to a **VLAN** and thus classify traffic based on the source **MAC** address of the packet. You define a **MAC** to **VLAN** mapping by configuring an entry in the **MAC** to **VLAN** table

16.1 VLAN MAC-VLAN GROUP (GLOBAL)

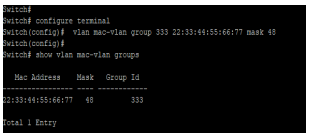
Use the vlan mac-vlan group command to create MAC address group. Use the **"no"** form of this command to delete specify group.

Switch#**configure terminal**

Switch(config)# **vlan mac-vlan group** *<1- 2147483647>* **mac-address mask** *<9-48>*

Switch(config)# **no vlan mac-vlan group mac-address mask** *<9-48>*

Syntax	**vlan mac-vlan group** *<1- 2147483647>* **mac-address mask** *<9-48>* **no vlan mac-vlan group mac-address mask** *<9-48>*
Parameter	*<1-2147483647>*Specify the group ID **mac-address**Specify the MAC address to be mapped. *<9-48>*Specify the mask length of MAC address.
Mode	Global Configuration

Example	The following example shows how to create a MAC group with group ID 3. Switch#**configure terminal** Switch(config)# **vlan mac-vlan group 333 22:33:44:55:66:77 mask 48** Switch# **show vlan mac-vlan groups** 

16.2 VLAN MAC-VLAN GROUP (INTERFACE)

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.

Switch#**configure terminal**

Switch(config)# **interface** {Interface-ID}

Switch(config-if)# **vlan mac-vlan group** *<1- 2147483647>* **vlan** *<1-4094>*

Switch(config-if)# **no vlan mac-vlan [group** *<1- 2147483647>***]**

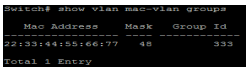
Syntax	**vlan mac-vlan group** *<1- 2147483647>* **vlan <1-4094>** **no vlan mac-vlan [group** *<1-2147483647>***]**
Parameter	*<1-2147483647>* Specify the group ID. (optional in no form) Delete all mapping group if not specify. *<1-4094>* Specify the VLAN ID to give to match packet
Mode	Interface Configuration

Example	The following example shows how to mapping group id 333 to VLAN 100 on interface GigabitEthernet 1. Switch# Switch# **configure terminal** Switch(config)# **interface GigabitEthernet** 3 Switch(config-if)# **switchport mode hybrid** Switch(config-if)# **vlan mac-vlan group** 333 **vlan** 2 Switch(config-if)# Switch# **show vlan mac-vlan groups** Image not found or type unknown Image not found or type unknown

16.3 SHOW VLAN MAC-VLAN GROUPS

Use the show vlan mac-vlan groups command to display mac groups configuration.

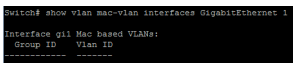
Switch# **show vlan mac-vlan groups**

Syntax	**show vlan mac-vlan groups**
Mode	Privileged EXEC
Example	This following example shows how to display mac group. Switch# **show vlan mac-vlan groups** 

16.4 SHOW VLAN MAC-VLAN INTERFACES

Use the show vlan mac-vlan interface command in EXEC mode to display the mac-vlan interfaces setting.

Switch# **show vlan mac-vlan [interfaces** *IF_PORTS***]**

Syntax	**show vlan mac-vlan [interfaces** *IF_PORTS***]**
Parameter	*IF_PORTS* (Optional) Specify interfaces mac vlan to display. Display all ports if not specif.
Mode	Privileged EXEC
Example	The following example shows how to display the MAC-Based VLAN interfaces setting Switch# **show vlan mac-vlan interfaces GigabitEthernet 1** 

MANAGEMENT ACL

An Access Control List (ACL) is a set of rules that is usually used to filter network traffic. ACLs can be configured on network devices with packet filtering compatibilities, such as routers and firewalls.

ACLs contain a list of conditions that categorize packets and help you determine when to allow or deny network traffic. They are applied on the interface basis to packets leaving or entering an interface

Access-list (ACL) is a set of rules defined for controlling the network traffic and reducing network attack. ACLs are used to filter traffic based on the set of rules defined for the incoming or outgoing of the network.

ACL features –

• The set of rules defined are matched serial wise i.e matching starts with the first line, then 2nd, then 3rd and so on.

• The packets are matched only until it matches the rule. Once a rule is matched then no further comparison takes place and that rule will be performed.

• There is an implicit deny at the end of every ACL, i.e., if no condition or rule matches then the packet will be discarded.

Once the access-list is built, then it should be applied to inbound or outbound of the interface:

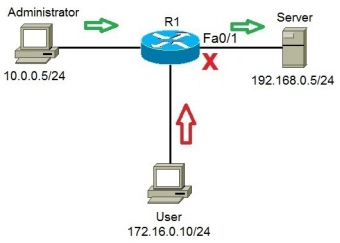


Fig 17.1 ACL Feature

Also there are two categories of access list,

• Numbered access list – These are the access list which cannot be deleted specifically once created i.e. if we want to remove any rule from an Access-list then this is not permitted in the case of numbered access list. If we try to delete a rule from access list then the whole access list will be deleted. The numbered access list can be used with

both standard and extended access list.

• Named access list – In this type of access list, a name is assigned to identify an access list. It is allowed to delete a named access list unlike numbered access list. Like numbered access list, these can be used with both standard and extended access list.

Rules for ACL –

• The standard Access-list is generally applied close to the destination (but not always).

• The extended Access-list is generally applied close to the source (but not always).

• We can assign only one ACL per interface per protocol per direction, i.e., only one inbound and outbound ACL is permitted per interface.

• We can't remove a rule from an Access-list if we are using numbered Access-list. If we try to remove a rule then whole ACL will be removed. If we are using named access lists then we can delete a specific rule.

• Every new rule which is added into the access list will be placed at the bottom of the access list therefore before implementing the access lists, analyses the whole scenario carefully.

• As there is an implicit deny at the end of every access list, we should have at least a permit statement in our Access-list otherwise all traffic will be denied.

• Standard access lists and extended access lists cannot have the same name.

Advantages of ACL –

• Improve network performance.

• Provides security as administrator can configure the access list according to the needs and deny the unwanted packets from entering the network.

• Provides control over the traffic as it can permit or deny according to the need of network.

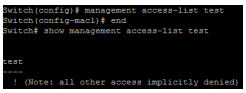
17.1 MANAGEMENT ACCESS-LIST

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.

Switch#**configure terminal**

Switch(config)# **management access-list** *[NAME]*

Switch(config)#**no management access-list** *[NAME]*

Syntax	**management access-list NAME** **no management access-list NAME**
Parameter	NAME The name of management ACL
Mode	Global Configuration
Example	The following example shows how to add a management ACL with name **“test”** Switch#**configure terminal** Switch(config)# **management access-list** test 

17.2 MANAGEMENT ACCESS-CLASS

Use the management access-class command to activate a management ACL. Use the **“no”** form of this command to delete.

Switch#**configure terminal**

Switch(config)# **management access-class** *[NAME]*

Switch(config)# **no management access-class**

Syntax	**management access-class** *[NAME]* **no management access-class**
Parameter	NAME The name of management ACL to be used
Mode	Global Configuration
Example	The following example shows how to add a management ACL with name **“test”** Switch#**configure terminal** Switch(config)# **management access-class** test 

17.3 DENY

Use the deny command to add deny rules that drop those packets hit the rule.

Switch#**configure terminal**

Switch(config)# **management access-list** *[NAME]*

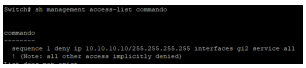
Switch(config-macl)# **sequence** *<1-65535>***] deny interfaces** *{IF_PORTS}* **service (all|http|https|snmp|ssh|telnet)**

Switch(config-macl)# **[sequence** *<1-65535>***] deny ip** A.B.C.D/A.B.C.D **interfaces** *{IF_PORTS}***service (all|http|https|snmp|ssh|telnet)**

Switch(config-macl)# **[sequence** *<1-65535>***] deny ipv6** *X:X::X:X/<0-128>* **interfaces** *{IF_PORTS}***service (all|http|https|snmp|ssh|telnet)**

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

Parameter	*<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.DSpecify 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
Mode	Management Access-List Configuration

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 gi2. Switch#**configure terminal** Switch(config)# **management access-list** commando Switch(config-macl)#**sequence 1 deny ip 10.10.10.10/255.255.255.255 interfaces gi2 service all**  Switch# sh management access-list commando 

17.4 PERMIT

Use the permit command to add permit rules that bypass those packets hit the rule.

Switch#**configure terminal**

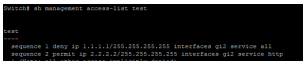
Switch(config)# **management access-list** *[NAME]*

Switch(config-macl)# **sequence** <*1-65535*>**] permit interfaces** *{IF_PORTS}* **service(all|http|https|snmp|ssh|telnet)**

Switch(config-macl)# **[sequence** <*1-65535*>**] permit ip** A.B.C.D/A.B.C.D **interfaces** *{IF_PORTS}***service (all|http|https|snmp|ssh|telnet)**

Switch(config-macl)# **[sequence** <*1-65535*>**] permit ipv6** *X:X::X:X/<0-128>* **interfaces** *{IF_PORTS}***service (all|http|https|snmp|ssh|telnet)**

Syntax	**[sequence** <*1-65535*>**] permit interfaces** *{IF_PORTS}* **service** **(all|http|https|snmp|ssh|telnet)** **[sequence** <*1-65535*>**] permit ip** A.B.C.D/A.B.C.D **interfaces** *{IF_PORTS}* **service (all|http|https|snmp|ssh|telnet)** **[sequence** <*1-65535*>**] permit ipv6** *X:X::X: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
Mode	Management Access-List Configuration
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 gi2. Switch#**configure terminal** Switch(config)# **management access-list test** Switch(config-macl)# **sequence 2 permit ip 2.2.2.2/255.255.255.255 interfaces gi2 service http**  

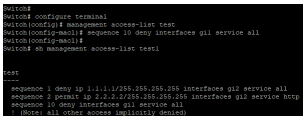
17.5 NO SEQUENCE

Use the **“no”** sequence command to delete an entry in management ACL.

Switch#**configure terminal**

Switch(config)# **management access-list** *[NAME]*

Switch(config-macl)# **no sequence** *<1-65535>*

Syntax	**no sequence** *<1-65535>*
Parameter	*<1-65535>*Specify sequence index of ACL entry to delete.
Mode	Management Access-List Configuration
Example	The following example shows how to delete an entry. Switch#**configure terminal** Switch(config)# **management access-list** test Switch(config-macl)# **sequence 10 deny interfaces gi1 service all** 

17.6 SHOW MANAGEMENT ACCESS-CLASS

Use the show management access-class command to show the active management access-list.

Switch# **show management access-class**

Syntax	**show management access-class**
Mode	Privileged EXEC
Example	The example shows how to show management access-class Switch# **show management access-class** 

17.7 SHOW MANAGEMENT ACCESS-LIST

Use the show management access-list command to show management ACL.

Switch# **show management access-list** *[NAME]*

Syntax	**show management access-list** *[NAME]*
Parameter	*NAME* Specify the name of management ACL to displayed
Mode	Privileged EXEC
Example	The example shows how to show management access-list Switch# **show management access-list 1** 

MIRROR

You can analyze network traffic passing through ports by using Switched Port Analyzer (SPAN). This sends a copy of the traffic to another port on the switch that has been connected to a SwitchProbe device, another Remote Monitoring (RMON) probe or security device. SPAN mirrors receive or transmit (or both) traffic on one or more source ports to a destination port for analysis.

Remote SPAN (RSPAN) extends SPAN by enabling RMON of multiple switches across your network. The traffic for each RSPAN session is carried over a user-specified RSPAN VLAN that is dedicated for that RSPAN session in all participating switches. The SPAN traffic from the sources is copied onto the RSPAN VLAN through a reflector port and then forwarded over trunk ports carrying the RSPAN VLAN to any RSPAN destination session monitoring the RSPAN VLAN.

SPAN and RSPAN do not affect the switching of network traffic on source ports. A copy of the packets received or sent by the source interfaces are sent to the destination interface. Except for traffic that is required for the SPAN or RSPAN session, reflector ports and destination ports do not receive or forward traffic.

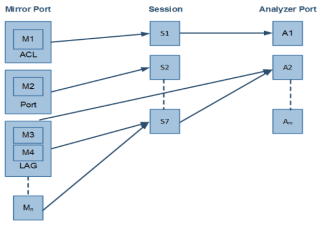


Fig 18.1 Mirror and Analyzer Port

18.1 MIRROR SESSION DESTINATION INTERFACE

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.

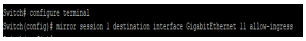
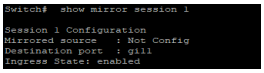
Switch#**configure terminal**

Switch(config)# **mirror session** *<1-4>* **destination interface IF_NMLPORT [allow-ingress]**

Switch(config)# **no mirror session** <*1-4*>**destination interface IF_NMLPORT**

Switch(config)# **no mirror session (**<*1-4*>**| all)**

Syntax	**mirror session** <*1-4*> **destination interface IF_NMLPORT [allow-ingress]** **no mirror session** <*1-4*>**destination interface IF_NMLPORT** **no mirror session (**<*1-4*>**| all)**
Parameter	<*1-4*> Specify the mirror session to configure **IF_NMLPORT** Specify the SPAN destination. A destination must be aphysical port allow-ingress Enable ingress traffic forwarding.
Default	No monitor sessions are configured.
Mode	Global Configuration

Example	The following example shows how to create a local session 1 to monitor both sent and received traffic on source port GigabitEthernet2. Switch#**configure terminal** Switch(config)#**mirror session** 1 **destination interface GigabitEthernet 11 allow-ingress**   To disable Mirror session Switch#**configure terminal** Switch(config)#**no mirror session** 1 **destination interface** GigabitEthernet 11 Switch(config)# **no mirror session all**

18.2 MIRROR SESSION SOURCE INTERFACE

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.

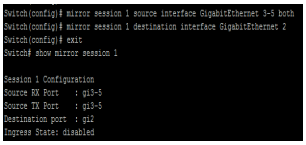
Switch#**configure terminal**

Switch(config)# **mirror session** <*1-4*> **source interfaces IF_PORTS (both | rx | tx)**

Switch(config)# **no mirror session** <*1-4*>**source interfaces IF_PORTS (both | rx | tx)**

Switch(config)# **no mirror session (**<*1-4*>**| all)**

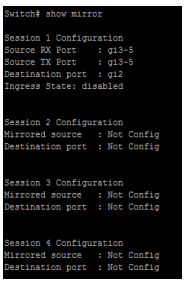
Syntax	**mirror session** <*1-4*> **source interfaces IF_PORTS (both | rx | tx)** **no mirror session** <*1-4*>**source interfaces IF_PORTS (both | rx | tx)** **no mirror session (**<*1-4*>**| all)**
Parameter	<*1-4*> Specify the mirror session to configure **IF_PORTS** Specify the source interface, Valid interfaces include physical ports and port channels. both Mirror tx and rx direction rx Mirror rx direction only tx Mirror tx direction only
Mode	Global Configuration

Example	The following example shows how to create a local SPAN session 1 to monitor both sent and received rate on source port gi3-5. Switch#**configure terminal** Switch(config)# **mirrorsession** 1 **sourceinterfaces** GigabitEthernet 3-5 **both** Switch(config)# **mirror session** 1 **destination interface** GigabitEthernet 2 Switch# **show mirror session**1 

18.3 SHOW MIRROR

Use the show mirror command to display mirror session configuration.

Switch#**show mirror [session** <*1-4*>**]**

Syntax	**show mirror [session** <*1-4*>**]**
Parameter	<*1-4*>Specify the mirror session to display
Mode	Privileged EXEC
Example	This following example shows how to display mirror session configuration Switch# **show mirror** 

```
Switch# show mirror

Session 1 Configuration
Source RX Port    : g13-5
Source TX Port    : g13-5
Destination port  : g12
Ingress State: disabled


Session 2 Configuration
Mirrored source   : Not Config
Destination port  : Not Config


Session 3 Configuration
Mirrored source   : Not Config
Destination port  : Not Config


Session 4 Configuration
Mirrored source   : Not Config
Destination port  : Not Config
```

MLD SNOOPING

In IPv4, Layer 2 switches can use IGMP snooping to limit the flooding of multicast traffic by dynamically configuring Layer 2 interfaces so that multicast traffic is forwarded to only those interfaces associated with IP multicast address. In IPv6, MLD snooping performs a similar function. With MLD snooping, IPv6 multicast data is selectively forwarded to a list of ports that want to receive the data, instead of being flooded to all ports in a VLAN. This list is constructed by snooping IPv6 multicast control packets.

MLD is a protocol used by IPv6 multicast routers to discover the presence of multicast listeners (nodes configured to receive IPv6 multicast packets) on its directly attached links and to discover which multicast packets are of interest to neighboring nodes. MLD is derived from IGMP; MLD version 1 (MLDv1) is equivalent to IGMPv2, and MLD version 2 (MLDv2) is equivalent to IGMPv3. MLD is a sub protocol of Internet Control Message Protocol version 6 (ICMPv6), and MLD messages are a subset of ICMPv6 messages, identified in IPv6 packets by a preceding Next Header value of 58.

The switch can snoop on both MLDv1 and MLDv2 protocol packets and bridge IPv6 multicast data based on destination IPv6 multicast MAC addresses. The switch can be configured to perform MLD snooping and IGMP snooping simultaneously.

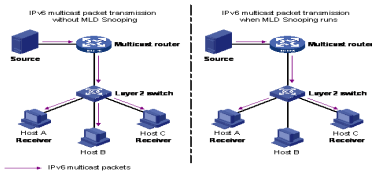


Fig 19.1 MLD snooping concept

19.1 IPV6 MLD SNOOPING

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. You can verify settings by the show ipv6 mld snooping command.

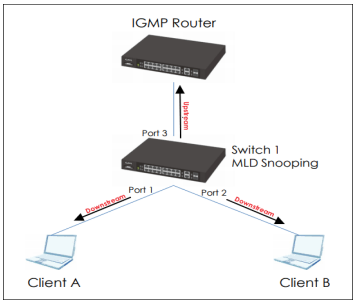


Fig 19.2 ipv6 mld snooping

Switch#**configure terminal**

Switch(config)# **ipv6 mld snooping**

Switch(config)# **no ipv6 mld snooping**

Syntax	**ipv6 mld snooping** **no ipv6 mld snooping**
Default	Default is disabled
Mode	Global Configuration
Example	The following example specifies that set ipv6 mld snooping test. Switch#**configure terminal** Switch(config)# **ipv6 mld snooping** Switch(config)#**no ipv6 mld snooping**

19.2 IPV6 MLD SNOOPING REPORT-SUPPRESSION

Use the ipv6 mld snooping report-suppression command to enable MLD snooping report-suppression function. Use the **“no”** form of this command to disable. Disable report-suppression will forward all received reports to the vlan router ports. You can verify settings by the show ipv6 mld snooping command.

Switch#**configure terminal**

Switch(config)# **ipv6 mld snooping report-suppression**

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

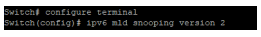
Syntax	**ipv6 mld snooping report-suppression** **no ipv6 mld snooping report-suppression**
Parameter	None
Default	Default is enabled
Mode	Global Configuration
Example	The following example specifies that disable ipv6 mld snooping report-suppression test. Switch#**configure terminal** Switch(config)# **ipv6 mld snooping report-suppression** Switch# configure terminal Switch(config)# ipv6 mld snooping report-suppression Switch(config)# **no ipv6 mld snooping report-suppression**

19.3 IPV6 MLD SNOOPING VERSION

Use the ipv6 mld snooping version command to change MLD support version. Version 2 packet won't be processed if choose version 1.You can verify settings by the show ip igmp snooping command.

Switch#**configure terminal**

Switch(config)#**ipv6 mld snooping version (1|2)**

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
Example	The following example specifies that set ipv6 mld snooping version 2. Switch#**configure terminal** Switch(config)# **ipv6 mld snooping version 2** 

19.4 IPV6 MLD SNOOPING UNKNOWN-MULTICAST ACTION

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. Use the ipv6 mld snooping unknown-multicast action command to change action. Use the **"no"** form of this command to restore to default. You can verify settings by the show ipv6 mld snooping command.

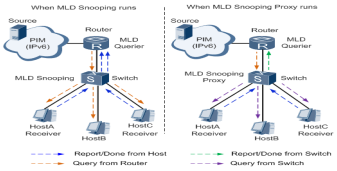


Fig 19.3 MLD SNOOPING action

Switch#**configure terminal**

Switch(config)# **ipv6 mld snooping unknown-multicast action (drop | flood |router-port)**

Switch(config)# **no ipv6 mld snooping unknown-multicast action**

Syntax	**ipv6 mld snooping unknown-multicast action (drop | flood |router-port)** **no ipv6 mld snooping unknown-multicast action**
Parameter	**(drop | flood | router- port)**Dropflood in vlan or forward to router port of unknown multicast packet
Default	Default is flood
Mode	Global Configuration

Example	The following example specifies that set ipv6 mld unknown multicast action router-port test. Switch#**configure terminal** Switch(config)# **ipv6 mld snooping unknown-multicast action router-port** Switch# configure terminal Switch(config)# ipv6 mld snooping unknown-multicast action router-port

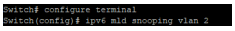
19.5 IPV6 MLD SNOOPING VLAN

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. Use the ipv6 mld snooping vlan command to enable MLD on VLAN. Use the **“no”** form of this command to disable. You can verify settings by the show ipv6 mld snooping vlan command.

Switch#**configure terminal**

Switch(config)# **ipv6 mld snooping vlan**

Switch(config)# **no ipv6 mld snooping vlan**

Syntax	**ipv6 mld snooping vlan** **no ipv6 mld snooping vlan**
Parameter	*VLAN-LIST* specifies VLAN ID list to set
Mode	Global Configuration
Example	The following example specifies that set ipv6 mld snooping vlan test. Switch#**configure terminal** Switch(config)# **ipv6 mld snooping vlan** 2 

19.6 IPV6 MLD SNOOPING VLAN PARAMETERS

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.

Switch#**configure terminal**

Switch(config)# **ipv6 mld snooping vlan last-member-query-count** <*1-7*>

Switch(config)# **no ipv6 mld snooping vlan last-member-query-count**

Switch(config)# **ipv6 mld snooping vlan last-member-query-interval** <*1- 60*>

Switch(config)# **no ipv6 mld snooping vlan last-member-query-interval[no]**

Switch(config)# **ipv6 mld snooping vlan router learn pim-dvmrp[no]**

Switch(config)# **ipv6 mld snooping vlan fastleave**

Switch(config)# **ipv6 mld snooping vlan query-interval** <*30-18000*>

Switch(config)# **no ipv6 mld snooping vlan query-interval**

Switch(config)# **ipv6 mld snooping vlan response-time** <*5-20*>

Switch(config)# **no ipv6 mld snooping vlan response-time**

Switch(config)# **ipv6 mld snooping vlan robustness-variable** <*1-7*>

Switch(config)# **no ipv6 mld snooping vlan robustness-variable**

Syntax	**ipv6 mld snooping vlan last-member-query-count** <*1-7*> **no ipv6 mld snooping vlan last-member-query-count** **ipv6 mld snooping vlan last-member-query-interval** <*1- 60*> **no ipv6 mld snooping vlan last-member-query-interval[no]** **ipv6 mld snooping vlan router learn pim-dvmrp[no]** **ipv6 mld snooping vlan fastleave** **ipv6 mld snooping vlan query-interval** <*30-18000*> **no ipv6 mld snooping vlan query-interval** **ipv6 mld snooping vlan response-time** <*5-20*> **no ipv6 mld snooping vlan response-time** **ipv6 mld snooping vlan robustness-variable** <*1-7*> **no ipv6 mld snooping vlan robustness-variable**
Parameter	*VLAN-LIST* specifies VLAN ID list to set **last-member-query-count**<*1-7*> **last-member-query-interval**<*1-60*> **query-interval**<*30-18000*> **response-time**<*5-20*> **robustness-variable** specifies a robustness value to set, default is 2 <*1-7*>

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

Example	The following example specifies that set ipv6 mld snooping vlan parameters test. Switch#**configure terminal** 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 MLD Snooping is globaly enabled MLD Snooping VLAN 1 admin : disabled MLD Snooping oper mode : disabled MLD Snooping robustness: admin 4 oper 2 MLD Snooping query interval: admin 100 sec oper 125 sec MLD Snooping query max response : admin 12 sec oper 10 sec MLD Snooping last member query counter: admin 5 oper 2 MLD Snooping last member query interval: admin 3 sec oper 1 sec MLD Snooping last immediate leave: enabled

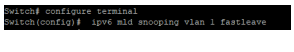
19.7 IPV6 MLD SNOOPING VLAN FASTLEAVE

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.You can verify settings by the show ipv6 mld snooping vlan command.

Switch#**configure terminal**

Switch(config)# **ipv6 mld snooping vlanfastleave**

Switch(config)# **no ipv6 mld snooping vlanfastleave**

Syntax	**ipv6 mld snooping vlanfastleave** **no ipv6 mld snooping vlanfastleave**
Parameter	*VLAN-LIST* specifies VLAN ID list to set
Default	Default is disabled
Mode	Global Configuration
Example	The following example specifies that set ipv6 mld snooping vlan fastleave test. Switch#**configure terminal** Switch(config)# **ipv6 mld snooping vlan** 1 **fastleave**  Switch(config)# **no ipv6 mld snoopingvlan** 1 **fastleave**

19.8 IPV6 MLD SNOOPING VLAN LAST-MEMBER-QUERY-COUNT

Use the ipv6 mld snooping vlan last-member-query-count command to change how many query packets will send. Use the **“no”** form of this command to restore to default. You can verify settings by the show ipv6 mld snooping vlan command

Switch#**configure terminal**

Switch(config)#**ipv6 mld snooping vlan last-member-query-count** <*1-7*>

Switch(config)#**no ipv6 mld snooping vlan last-member-query-count**

Syntax	**ipv6 mld snooping vlan last-member-query-count** <*1-7*> **no ipv6 mld snooping vlan last-member-query-count**
Parameter	VLAN-LIST last-member-query-count <*1-7*> specifies VLAN ID list to set. Specifies last member query count to set
Default	Default is 2
Mode	Global Configuration

Example	The following example specifies that set ipv6 mld snooping vlan last- member-query-count test. Switch#**configure terminal** Switch(config**)# ipv6 mld snooping vlan** 1 **last-member-query-count** 5 Switch(config)# **no ipv6 mld snooping vlan** 1 **last-member-query-count** 5

19.9 IPV6 MLD SNOOPING VLAN LAST-MEMBER-QUERY-INTERVAL

Use the ipv6 mld 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 ipv6 mld snooping vlan command.

Switch#**configure terminal**

Switch(config)#**ipv6 mld snooping vlan last-member-query-interval** <*1- 60*>

Switch(config)# **no ipv6 mld snooping vlan last-member-query-interval**

Syntax	**ipv6 mld snooping vlan last-member-query-interval** <*1- 60*> **no ipv6 mld snooping vlan last-member-query-interval**
Parameter	VLAN-LIST last-member-query-interval <*1-60*> specifies VLAN ID list to set.specifies last member query interval to set
Default	Default is 1
Mode	Global Configuration

Example	The following example specifies that set ipv6 mld snooping vlan last- member-query-interval test. Switch#**configure terminal** Switch(config)# **ipv6 mld snooping vlan** 1 **last-member-query-interval** 3  Switch(config)#**no ipv6 mld snooping vlan** 1 **last-member-query-interval** 3

19.10 IPV6 MLD SNOOPING VLAN QUERY-INTERVAL

Use the ipv6 mld snooping vlan query-interval command to set interval between each query. Use the **“no”** form of this command to restore to default. You can verify settings by the show ipv6 mld snooping vlan command.

Switch#**configure terminal**

Switch(config)#**ipv6 mld snooping vlan query-interval** *<30-18000>*

Switch(config)# **no ipv6 mld snooping vlan query-interval**

Syntax	**ipv6 mld snooping vlan query-interval** *<30-18000>* **no ipv6 mld snooping vlan query-interval**
Parameter	VLAN-LIST query-interval *<30-18000>* specifies VLAN ID list to set specifies query interval to set
Default	Default is 125
Mode	Global Configuration
Example	The following example specifies that set ipv6 mld snooping vlan query- interval test. Switch#**configure terminal** Switch(config)# **ipv6 mld snooping vlan** 1 **query-interval** 100 Switch# configure terminal Switch(config)# ipv6 mld snooping vlan 1 query-interval 100

19.11 IPV6 MLD SNOOPING VLAN RESPONSE-TIME

Use the ipv6 mld snooping vlan response-time command to set response time. Use the **“no”** form of this command to restore to default. You can verify settings by the show ipv6 mld snooping vlan command.

Switch#**configure terminal**

Switch(config)#**ipv6 mld snooping vlan response-time** <*5-20*>

Switch(config)# **no ipv6 mld snooping vlan response-time**

Syntax	**ipv6 mld snooping vlan response-time** *<5-20>* **no ipv6 mld snooping vlan response-time**
Parameter	VLAN-LIST specifies VLAN ID list to set response-time *<5-20>* specifies VLAN ID list to set
Default	Default is 10
Mode	Global Configuration
Example	The following example specifies that set ipv6 mld snooping vlan response- time test. Switch#**configure terminal** Switch(config)# **ipv6 mld snooping vlan** 1 **response-time** 12 Switch# configure terminal Switch(config)# ipv6 mld snooping vlan 1 response-time 12

19.12 IPV6 MLD SNOOPING VLAN ROBUSTNESS-VARIABLE

Use the ipv6 mld snooping vlan robustness-variable command to times to retry. Use the **“no”** form of this command to restore to default. You can verify settings by the show ipv6 mld snooping vlan command.

Switch#**configure terminal**

Switch(config)#**ipv6 mld snooping vlan robustness-variable** <*1-7*>

Switch(config)# **no ipv6 mld snooping vlan robustness-variable**

Syntax	**ipv6 mld snooping vlan robustness-variable** <*1-7*> **no ipv6 mld snooping vlan robustness-variable**
Parameter	VLAN-LIST robustness-variable<*1-7*> specifies VLAN ID list to set.specifies a robustness value to set
Default	Default is 2
Mode	Global Configuration
Example	The following example specifies that set ipv6 mld snooping vlan parameters test. Switch#**configure terminal** Switch(config)# **ip igmp snooping vlan** 1 **robustness-variable** 5  Switch(config)# **no ip igmp snooping vlan** 1 **robustness-variable**

19.13 IPV6 MLD SNOOPING VLAN ROUTER

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. You can verify settings by the show ipv6 mld snooping vlan command.

Switch#**configure terminal**

Switch(config)#**ipv6 mld snooping vlan router learn pim-dvmrp**

Switch(config)# **no ipv6 mld snooping vlan router learn pim-dvmrp**

Syntax	**ipv6 mld snooping vlan router learn pim-dvmrp** **no ipv6 mld snooping vlan router learn pim-dvmrp**
Parameter	VLAN-LIST specifies VLAN ID list to set
Mode	Global Configuration
Example	The following example specifies that set ipv6 mld snooping vlan router test. Switch#**configure terminal** Switch(config)# **ipv6 mld snooping vlan** 99 **router learn pim-dvmrp**  Switch(config)# **no ipv6 mld snooping vlan** 99 **router learn pim-dvmrp**

19.14 IPV6 MLD SNOOPING VLAN STATIC-PORT

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. You can verify settings by the show ipv6 mld snooping forward-all command.

Switch#**configure terminal**

Switch(config)#**ipv6 mld snooping vlan static-port** *{IF_PORTS}*

Switch(config)# **no ipv6 mld snooping vlan static-port** *{IF_PORTS}*

Syntax	**ipv6 mld snooping vlan static-port** *{IF_PORTS}* **no ipv6 mld snooping vlan static-port** *{IF_PORTS}*
Parameter	VLAN-LIST specifies VLAN ID list to set *{IF_PORTS}* specifies a port list to set or remove
Default	No static port by default
Mode	Global Configuration

Example	The following example specifies that set ipv6 mld snooping static port test. Switch#**configure terminal** Switch(config)# **ipv6 mld snooping vlan** 1 **static-port** gi3-5 ``` Switch# configure terminal Switch(config)# ipv6 mld snooping vlan 1 static-port gi3-5 ``` Switch(config)# **no ipv6 mld snooping vlan** 1 **static-port** gi3-5

19.15 IPV6 MLD SNOOPING VLAN FORBIDDEN-ROUTER-PORT

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 .Use the **“no”** form of this command to delete forbidden router port. You can verify settings by the show ipv6 mld snooping router command.

Switch#**configure terminal**

Switch(config)#**ipv6 mld snooping vlan forbidden-router-port** *{IF_PORTS}*

Switch(config)#**no ipv6 mld snooping vlan forbidden-router-port**

{IF_PORTS}

Syntax	**ipv6 mld snooping vlan forbidden-router-port** *{IF_PORTS}* **no ipv6 mld snooping vlan forbidden-router-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 router ports by default
Mode	Global Configuration

Example	The following example specifies that set ipv6 mld snooping forbidden test. Switch#**configure terminal** Switch(config**)# ipv6 mld snooping vlan** 1 **forbidden-router-port** gi2  Switch(config)# **no ipv6 mld snooping vlan** 1 **forbidden-router-port** gi2

19.16 IPV6 MLD SNOOPING VLAN FORBIDDEN-ROUTER-PORT

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 .Use the **"no"** form of this command to delete forbidden router port. You can verify settings by the show ipv6 mld snooping router command.

Switch#**configure terminal**

Switch(config)#**ipv6 mld snooping vlan forbidden-router-port** *{IF_PORTS}*

Switch(config)#**no ipv6 mld snooping vlan forbidden-router-port**

{IF_PORTS}

Syntax	**ipv6 mld snooping vlan forbidden-router-port** *{IF_PORTS}* **no ipv6 mld snooping vlan forbidden-router-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 router ports by default
Mode	Global Configuration
Example	The following example specifies that set ipv6 mld snooping forbidden test. Switch#**configure terminal** Switch(config)# **ipv6 mld snooping vlan** 1 **forbidden-router-port** gi2  Switch(config)# **no ipv6 mld snooping vlan** 1 **forbidden-router-port** gi2

19.17 IPV6 MLD SNOOPING VLAN STATIC ROUTER PORT

Use the ipv6 mld snooping vlan static-router-port command to add static router port. All query packets will forward to this port. Use the **"no"** form of this command to delete static router port. You can verify settings by the show ipv6 mld snooping router command.

Switch#**configure terminal**

Switch(config)#**ipv6 mld snooping vlan static-router-port** *{IF_PORTS}*

Switch(config)#**no ipv6 mld snooping vlan static-router-port** *{IF_PORTS}*

Syntax	**ipv6 mld snooping vlan static-router-port** *{IF_PORTS}* **no ipv6 mld snooping vlan static-router-port** *{IF_PORTS}*
Parameter	VLAN-LIST specifies VLAN ID list to set *{IF_PORTS}* specifies a port list to set or remove
Default	None static router ports by default
Mode	Global Configuration
Example	The following example specifies that set ipv6 mld snooping static test. Switch#**configure terminal** Switch(config)# **ipv6 mld snooping vlan** 1 **static-router-port** gi1-2  Switch(config)# **no ipv6 mld snooping vlan** 1 **static-router-port** gi1-2

19.18 IPV6 MLD SNOOPING VLAN STATIC-GROUP

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. 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 ipv6 mld snooping group command.

Switch#**configure terminal**

Switch(config)#**ipv6 mld snooping vlan static-group** [**] interfaces** *{IF_PORTS}*

Switch(config)#**no ipv6 mld snooping vlan static-group interfaces** *{IF_PORTS}*

Syntax	**ipv6 mld snooping vlan static-group** [**] **interfaces** *{IF_PORTS}* **no ipv6 mld snooping vlan static-group interfaces** *{IF_PORTS}*
Parameter	specifies VLAN ID list to set specifies multicast group ipv4 address *{IF_PORTS}* specifies port list to set or remove
Default	No static group by default
Mode	Global Configuration

Example	The following example specifies that set ipv6 mld snooping static group test. Switch#**configure terminal** Switch(config**)#ipv6 mld snooping vlan** 1 **static-group** ff13::1 **interfaces** gi1-2  Switch(config)# **no ipv6 mld snooping vlan** 1 **static-group** ff13::1 **interfaces** gi1-2

19.19 IPV6 MLD SNOOPING VLAN GROUP

Use the no ipv6 mld snooping vlan group command to delete a group which could be static or dynamic. You can verify settings by the show ipv6 mld snooping group command.

Switch#**configure terminal**

Switch(config)#**no ipv6 mld snooping vlan group**

Syntax	**no ipv6 mld snooping vlan group**
Parameter	VLAN-LIST specifies VLAN ID list to set ipv6-addr specifies multicast group ipv6 address
Mode	Global Configuration
Example	The following example specifies that set ipigmp snooping static group test. Switch#**configure terminal** Switch(config**)# no ipigmp snooping vlan** 1 **group** ff13::1

19.20 PROFILE RANGE

Use the profile command to generate MLD profile. You can verify settings by the show ipv6 mld profile command.

Switch#**configure terminal**

Switch(config)# **ipv6 mld profile** {Profile-No}

Switch(config-mld-profile)#**profile range ipv6 [ipv6-addr] action (permit | deny)**

Syntax	**profile range ipv6 [ipv6-addr] action (permit | deny)**
Parameter	Start ipv6 multicast address [ipv6-addr] End ipv6 multicast address (permit | deny) Permit: allow Multicast address range ip address learning deny: do not allow Multicast address range ip address learning
Mode	mld profile configuration mode
Example	The following example specifies that set ipv6 mld profile test. Switch#**configure terminal** Switch(config)# **ipv6 mld profile** 1 Switch(config-mld-profile)# **profile range ipv6** ff13::1 ff13::10 **action permit** Switch(config)# ipv6 mld profile 1 Switch(config-mld-profile)# profile range ipv6 ff13::1 ff13::10 action permit

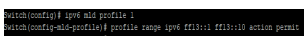
19.21 IPV6 MLD PROFILE

Use the ipv6 mld profile command to enter profile configuration Use the **“no”** form of this command to delete profile. You can verify settings by the show ipv6 mld profile command.

Switch#**configure terminal**

Switch(config)#**ipv6 mld profile**<*1-128*>

Switch(config)# **no ipv6 mld profile**<*1-128*>

Syntax	**ipv6 mld profile**<*1-128*> **no ipv6 mld profile**<*1-128*>
Parameter	<*1-128*>specifies profile ID
Mode	Global Configuration
Example	The following example specifies that set ipv6 mld profile test. Switch#**configure terminal** Switch(config)# **ipv6 mld profile** 1  Switch(config)# **no ipv6 mld profile** 1

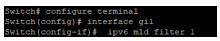
19.22 IPV6 MLD FILTER

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. Use the **“no”** form of this command to delete profile. You can verify settings by the show ipv6 mld filter command.

Switch#**configure terminal**

Switch(config)#**ipv6 mld filter** *<1-128>*

Switch(config)# **no ipv6 mld filter**

Syntax	**ipv6 mld filter** *<1-128>* **no ipv6 mld filter**
Parameter	*<1-128>* specifies profile ID [interfaces IF_PORTS] Specifies interfaces to display
Mode	Port Configuration
Example	The following example specifies that set ipv6 mld filter test. Switch#**configure terminal** Switch(config)# **interface** gi1 Switch(config-if)# **ipv6 mld filter** 1 

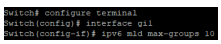
19.23 IPV6 MLD MAX-GROUPS

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. Use the **“no”** form of this command to restore to default. You can verify settings by the show ipv6 mld max-groups command.

Switch#**configure terminal**

Switch(config)#**ipv6 mld max-groups** *<0-1024>*

Switch(config)# **no ipv6 mld max-groups**

Syntax	**ipv6 mld max-groups** *<0-1024>* **no ipv6 mld max-groups**
Parameter	*<0-1024>*specifies profile ID
Default	Default is 1024
Mode	Port Configuration
Example	The following example specifies that set ipv6 mld max-groups test. Switch#**configure terminal** Switch(config)# **interface** gi1 Switch(config-if)# **ipv6 mld max-groups** 10 

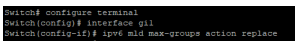
19.24 IP IGMP MAX-GROUPS ACTION

Use the ipv6 mld max-groups action command to set the action when the numbers of groups reach the limitation. Use the **“no”** form of this command to restore to default. You can verify settings by the show ipv6 mld max-groups command.

Switch#**configure terminal**

Switch(config)# **interface** {INTERFCE-ID}

Switch(config-if)#**ipv6 mld max-groups action (deny | replace)**

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
Example	The following example specifies that set action replace test. Switch#**configure terminal** Switch(config)# **interface** gi1 Switch(config-if)#**ipv6 mld max-groups action replace** 

19.25 CLEAR IPV6 MLD SNOOPING GROUPS

This command will clear the ipv6 mld groups for dynamic or static or all of type. You can verify settings by the show ipv6 mld snooping groups command.

Switch#**clear ipv6 mld snooping groups [(dynamic | static)]**

Syntax	**clear ipv6 mld snooping groups [(dynamic | static)]**
Parameter	**None** Clear ipv6 mld groups include dynamic and static (dynamic | static) ipv6 mld group type is dynamic or static
Mode	Privileged EXEC
Example	The following example specifies that clear ipv6 mld snooping groups test. Switch# **clear ipv6 mld snooping groups static**

19.26 CLEAR IPV6 MLD SNOOPING STATISTICS

This command will clear the igmp statistics. You can verify settings by the show ipv6 mld snooping command.

Switch#**clear ipv6 mld snooping statistics**

Syntax	**clear ipv6 mld snooping statistics**
Mode	Privileged EXEC
Example	The following example specifies that clear ipv6 mld snooping statistics test. Switch# **clear ipv6 mld snooping statistics**

19.27 SHOW IPV6 MLD SNOOPING GROUPS COUNTERS

This command will display the ipv6 mld group counter include static group.

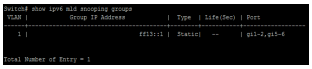
Switch#**show ipv6 mld snooping groups counters**

Syntax	**show ipv6 mld snooping groups counters**
Mode	Privileged EXEC
Example	The following example specifies that display ipv6 mld snooping group counter test. Switch# **show ipv6 mld snooping group counters** Total ipv6 mld snooping group number: 1 Switch# show ipv6 mld snooping group counters Total ipv6 mld snooping group number: 1

19.28 SHOW IPV6 MLD SNOOPING GROUPS

This command will display the ipv6 mld groups for dynamic or static or all of type.

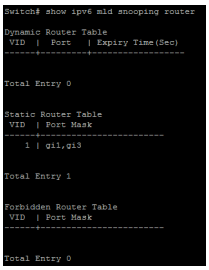
Switch#**show ipv6 mld snooping groups [(dynamic | static)]**

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

19.29 SHOW IPV6 MLD SNOOPING ROUTER

This command will display the ipv6 mld router info.

Switch#**show ipv6 mld snooping router [(dynamic | forbidden |static)]**

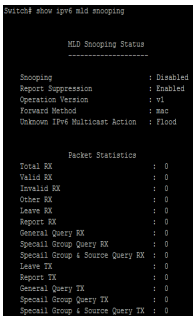
Syntax	**show ipv6 mld snooping router [(dynamic | forbidden |static)]**
Parameter	none Show ipv6 mld router include dynamic and static and forbidden (dynamic |forbidden | static)Display ipv6 mld router info for different type
Mode	Privileged EXEC
Example	The following example specifies that show ipv6 mld snooping router test. Switch# **show ipv6 mld snooping router** 

19.30 SHOW IPV6 MLD SNOOPING

This command will display ipv6 mld snooping global info.

Switch#**show ipv6 mld snooping**

Syntax	**show ipv6 mld snooping**

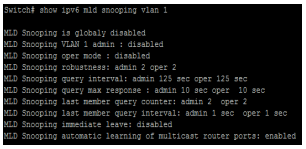
Mode	Privileged EXEC
Example	The following example specifies that show ipv6 mld snooping test. Switch# **show ipv6 mld snooping** 

```
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
```

19.31 SHOW IPV6 MLD SNOOPING VLAN

This command will display ipv6 mld snooping vlan info.

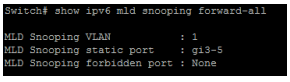
Switch#**show ipv6 mld snooping vlan**

Syntax	**show ipv6 mld snooping vlan**
Parameter	**none** Show all ipv6 mld snooping vlan info Show specifies vlan ipv6 mld snooping info
Default	Show all ipv6 mld snooping vlan info
Mode	Privileged EXEC
Example	The following example specifies that show ipv6 mld snooping vlan test. Switch# **show ipv6 mld snooping vlan** 1 

19.32 SHOW IPV6 MLD SNOOPING FORWARD-ALL

This command will display ipv6 mld snooping forward all info.

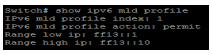
Switch#**show ipv6 mld snooping forward-all [vlan]**

Syntax	**show ipv6 mld snooping forward-all [vlan]**
Parameter	**none** Show all ipv6 mld snooping vlan forward-all info [vlan] Show specifies vlan of ipv6 mld forward info
Default	Show all vlan ipv6 mld forward all info
Mode	Privileged EXEC
Example	The following example specifies that show ipv6 mld snooping forward-all test. Switch# **show ipv6 mld snooping forward-all** 

19.33 SHOW IPV6 MLD PROFILE

This command will display ipv6 mld profile info.

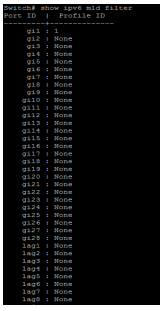
Switch#**show ipv6 mld profile[***<1-128>***]**

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
Example	The following example specifies that show ipv6 mld profile test. Switch# **show ipv6 mld profile** 

19.34 SHOW IPV6 MLD FILTER

This command will display ipv6 mld port filter info.

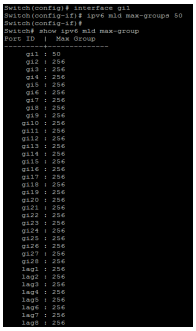
Switch#**show ipv6 mld filter [interfaces***{IF_PORTS}***]**

Syntax	**show ipv6 mld filter [interfaces** *{IF_PORTS}***]**
Parameter	**none** Show all port filter [interfaces *{IF_PORTS}*] Show specifies ports filter
Mode	Privileged EXEC
Example	The following example specifies that show ipv6 mld filter test. Switch# **show ipv6 mld filter** 

19.35 SHOW IPV6 MLD MAX-GROUP

This command will display ipv6 mld port max-group.

Switch#**show ipv6 mld max-group [interfaces***{IF_PORTS}***]**

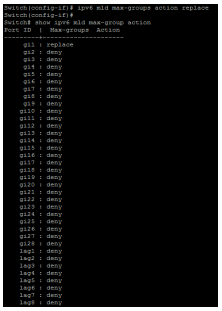
Syntax	**show ipv6 mld max-group [interfaces** *{IF_PORTS}***]**
Parameter	**none** Show all port max-group [interfaces *{IF_PORTS}*] Show specifies ports max-group
Mode	Privileged EXEC
Example	The following example specifies that show ipv6 mld max-group test. Switch# **show ipv6 mld max-group** 

19.36 SHOW IPV6 MLD PORT MAX-GROUP ACTION

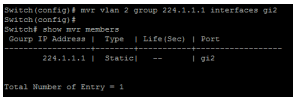
This command will display ipv6 mld port max-group action.

Switch#**show ipv6 mld max-group action [interfaces***{IF_PORT}***]**

Syntax	**show ipv6 mld max-group action [interfaces***{IF_PORT}***]**

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
Example	The following example specifies that show ipv6 mld max-group action test. Switch# **show ipv6 mld max-group action** 

Multicast VLAN Registration (MVR)

Syntax	**mvr vlangroupinterfaces***{IF_PORTS}* **no mvr vlan**< *VLAN-ID*>**groupinterfaces** *{IF_PORTS}*
Parameter	*VLAN-ID* specifies MVR VLAN ID for static group *ip-addr* Specifies multicast MVR group address *IF_PORT S* specifies port list to set or remove
Mode	Global Configuration
Example	The following example specifies that set mvr static group test. The configure must configure mvr receiver port firstly.(eg. mvr port type) Switch(config)# **mvr vlan** 2 **group** 224.1.1.1 **interfaces** gi2 Switch# **show mvr members** 

20.9 CLEAR MVR MEMBERS

This command will clear the mvr groups for selected type.

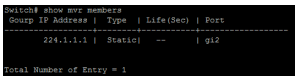
Switch#**clear mvr members [dynamic|static]**

Syntax	**clear mvr members [dynamic|static]**
Parameter	**dynamic** specifies MVR dynamic group **static** specifies MVR static group
Default	Clear all of mvr group
Mode	Privileged EXEC
Example	The following example specifies that clear all mvr groups test. Switch# **clear mvr members** Switch# clear mvr members Switch#

20.10 SHOW MVR MEMBERS

This command will display the mvr groups for all of type.

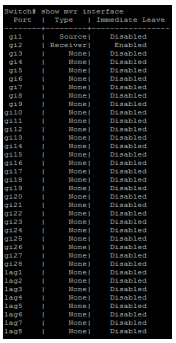
Switch#**show mvr members**

Syntax	**show mvr members**
Mode	Privileged EXEC
Example	The following example specifies that show mvr groups test. Switch# **show mvr members** 

20.11 SHOW MVR INTERFACE

This command will display mvr port type and port immediate status.

Switch#**show mvr interface** *{IF_PORTS}*

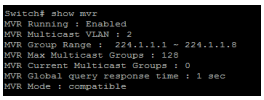
Syntax	**show mvr interface** *{IF_PORTS}*
Parameter	*IF_PORTS* Show specifies port list configuration
Mode	Privileged EXEC
Example	The following example specifies that show mvr interface test. Switch# **show mvr interface** 

```
Switch# show mvr interface
  Port   |  Type    | Immediate Leave
---------|----------|----------------
gi1      |   Source|    Disabled
gi2      | Receiver|     Enabled
gi3      |     None|    Disabled
gi4      |     None|    Disabled
gi5      |     None|    Disabled
gi6      |     None|    Disabled
gi7      |     None|    Disabled
gi8      |     None|    Disabled
gi9      |     None|    Disabled
gi10     |     None|    Disabled
gi11     |     None|    Disabled
gi12     |     None|    Disabled
gi13     |     None|    Disabled
gi14     |     None|    Disabled
gi15     |     None|    Disabled
gi16     |     None|    Disabled
gi17     |     None|    Disabled
gi18     |     None|    Disabled
gi19     |     None|    Disabled
gi20     |     None|    Disabled
gi21     |     None|    Disabled
gi22     |     None|    Disabled
gi23     |     None|    Disabled
gi24     |     None|    Disabled
gi25     |     None|    Disabled
gi26     |     None|    Disabled
gi27     |     None|    Disabled
gi28     |     None|    Disabled
lag1     |     None|    Disabled
lag2     |     None|    Disabled
lag3     |     None|    Disabled
lag4     |     None|    Disabled
lag5     |     None|    Disabled
lag6     |     None|    Disabled
lag7     |     None|    Disabled
lag8     |     None|    Disabled
```

20.12 SHOW MVR

This command will display mvr global information.

Switch#**show mvr**

Syntax	**show mvr**
Mode	Privileged EXEC
Example	The following example specifies that show mvr test. Switch# **show mvr** 

PORT

The switch comes with default port settings that should allow you to connect to the Ethernet Ports without any necessary configuration. Should there be a need to change the name of the ports, Port State, negotiation settings or flow control settings etc., you can do this in the Port settings by below commands

21.1 BACK-PRESSURE

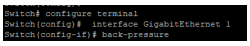
Use "**back-pressure**" command to make port to enable back pressure feature. Use **"no"** form of this command to disable back pressure feature. The only way to show this configuration is using "**show running-config**" command.

Switch#**configure terminal**

Switch(config-if)# **back-pressure**

Switch(config-if)# **no back-pressure**

Syntax	**back-pressure** **no back-pressure**
Default	Default back pressure state is enabled.
Mode	Interface Configuration

Example	This example shows how to configure port gi1 and gi2 to be protected port. Switch#**configure terminal** Switch(config)# **interface** GigabitEthernet 1 Switch(config-if)# **back-pressure**  Switch(config-if)# **no back-pressure**

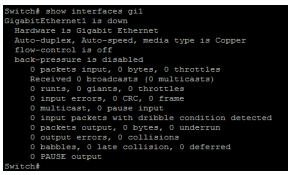
21.2 CLEAR INTERFACE

Use "**clear interface**" command to clear statistic counters on specific ports.

Switch#**configure terminal**

Switch(config)# **clear interfaces** *{IF_PORTS}* **counters**

Syntax	**clear interfaces***{IF_PORTS}***counters**
Parameter	*IF_PORTS* Specify port to clear counters
Default	No default value for this command.
Mode	Privileged EXEC

Example	This example shows how to clear counters on port gi1. Switch# **clear interfaces** gi1 **counters** This example shows how to show current counters Switch# **show interfaces** gi1 

21.3 DESCRIPTION

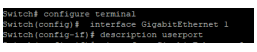
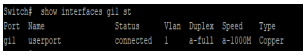
Use "**description**" command to give the port a name to identify it easily. If description includes space character, please use double quoted to wrap it. Use **"no"** form to restore description to empty string.

Switch#**configure terminal**

Switch(config)#**interface** {Interface-ID}

Switch(config-if)#**description** WORD<*1-32*>

Switch(config-if)#**no description**

Syntax	**description** WORD<*1-32*> **no description**
Parameter	WORD<*1-32*> Specify port description string.
Mode	Interface Configuration
Example	This example shows how to modify port descriptions. Switch#**configure terminal** Switch(config)# **interface** GigabitEthernet 1 Switch(config-if)# **description userport**  

21.4 DUPLEX

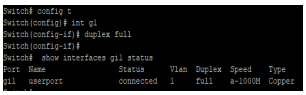
Use "**duplex**" command to change port duplex configuration.

Switch#**configure terminal**

Switch(config)#**interface** {Interface-ID}

Switch(config-if)#**duplex (auto | full | half)**

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

Example	This example shows how to modify port duplex configuration. Switch#**configure terminal** Switch(config)# **interface** GigabitEthernet 1 Switch(config-if)# **duplex full** Switch(config-if)# **exit** This example shows how to show current interface link speed Switch# **show interfaces status** 

21.5 EEE

Use "**eee**" command to make port to enable the energy efficient Ethernet Feature .Use **"no"** form of this command to disable eee. IEEE 802.3az Energy Efficient Ethernet (EEE) is a standard that allows physical layer transmitters to consume less power during periods of low data activity. The only way to show this configuration is using "**show running-config**" command.

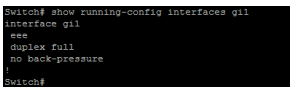
Switch#**configure terminal**

Switch(config)#**interface** {Interface-ID}

Switch(config-if)# **eee**

Switch(config-if)#**no eee**

Syntax	**eee** **no eee**
Parameter	None
Default	Default eee state is disabled
Mode	Interface Configuration

Example	This example shows how to configure port gi1 and gi2 to be protected port. Switch#**configure terminal** Switch(config)# **interface** GigabitEthernet 1 Switch(config-if)# **eee** This example shows how to show current jumbo-frmae size Switch# **show running-config** interface gi1 

21.6 FLOWCONTROL

Use "**flowcontrol**" command to change port flow control configuration. Use **"no"** form to restore flow control to default (off) configuration.

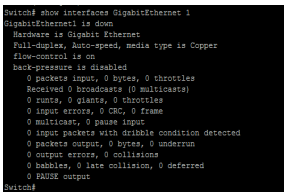
Switch#**configure terminal**

Switch(config)#**interface** {Interface-ID}

Switch(config-if)#**flowcontrol (auto | off | on)**

Switch(config-if)#**no 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

Example	This example shows how to modify port duplex configuration. Switch(config)# **interface** GigabitEthernet 1 Switch(config-if)# **flowcontrol on** This example shows how to show current flow control configuration Switch# **show interfaces**GigabitEthernet 1 

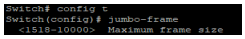
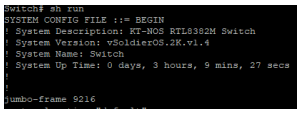
21.7 JUMBO-FRAME

A **jumbo frame** is an Ethernet **frame** with a payload greater than the standard maximum transmission unit (MTU) of 1,500 bytes. **Jumbo frames** are used on local area networks that support at least 1 Gbps and can be as large as 10,000 bytes. Use "**jumbo-frame** " command to modify maximum frame size. The only way to show this configuration is using **"show running-config"** command.

Switch#**configure terminal**

Switch(config)#**jumbo-frame***<1518-10000>*

Syntax	**jumbo-frame***<1518-10000>*
Parameter	*<1518-10000>*Specify the maximum frame size.
Default	Default maximum frame size is 1522.
Mode	Global Configuration

Example	This example shows how to modify maximum frame size on gi1 to 10000 bytes. Switch#**configure terminal** Switch(config)# **jumbo-frame** 9216  This example shows how to show current jumbo-frame size Switch# **show running-config jumbo-frame** 9216 

21.8 MEDIA-TYPE

Use "**media-type**" command to change combo port media type. Use **"no"** form of this command to restore media type to default.

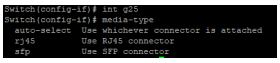
Switch#**configure terminal**

Switch(config)#**interface** {Interface-ID}

Switch(config-if)#**media-type (auto-select | rj45 | sfp)**

Switch(config-if)#**no media-type**

Syntax	**media-type (auto-select | rj45 | sfp)** **no media-type**

Parameter	**auto-select** Select media automatically. **rj45** Select copper media. **sfp** Select fiber media.
Default	Default media type is auto.
Mode	Interface Configuration
Example	This example shows how to modify combo port media type to copper. Switch#**configure terminal** Switch(config)# interface gi25 Switch(config-if)# **media-type rj45** 

21.9 PROTECTED

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. Use **"no"** form to make port unprotected.

Switch#**configure terminal**

Switch(config)#**interface** {Interface-ID}

Switch(config-if)# **protected**

Switch(config-if)#**no protected**

Syntax	**protected** **no protected**
Default	Default protected state is no protected.
Mode	Interface Configuration

Example	This example shows how to configure port gi1 and gi2 to be protected port. Switch#**configure terminal** Switch(config)# **interface range** gi11-12 Switch(config-if-range)# **protected** This example shows how to show current protected port state. Switch# **show interfaces** GigabitEthernet 11-12 **protected** 

21.10 SHOW INTERFACE

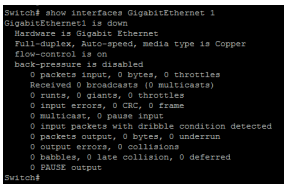
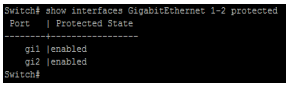
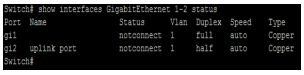
Use "**show interface**" command to show detail port counters, parameters and status. Use "**show interface status**" command to show brief port status. Use "**show interface protected**" command to show protected status.

Switch# **show interfaces** *{IF_PORTS}*

Switch# **show interfaces** *{IF_PORTS}* **status**

Switch# **show interfaces** *{IF_PORTS}* **protected**

Syntax	**show interfaces***{IF_PORTS}* **show interfaces***{IF_PORTS}* **status** **show interfaces***{IF_PORTS}* **protected**
Parameter	*{IF_PORTS}*Specify port to show.

Mode	Privileged EXEC
Example	This example shows how to show current counters Switch# **show interfaces** GigabitEthernet 1  This example shows how to show current protected port state. Switch# **show interfaces** GigabitEthernet 1-2 **protected**  This example shows how to show current port status Switch# **show interfaces** GigabitEthernet 1-2 **status** 

21.11 SPEED

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.

Switch#**configure terminal**

Switch(config)#**interface** {Interface-ID}

Switch(config-if)# **speed (10 | 100 | 1000)**

Switch(config-if)# **speed auto [(10 | 100 | 1000 | 10/100)]**

Switch(config-if)#**speed nonegtiate**

Switch(config-if)#**no speed nonegtiate**

Syntax	**speed (10 | 100 | 1000)** **speed auto [(10 | 100 | 1000 | 10/100)]** **speed nonegtiate** **no speed nonegtiate**

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
Example	This example shows how to modify port speed configuration. Switch#**configure terminal** Switch(config)# **interface** GigabitEthernet 1 Switch(config-if)# **speed 100** Switch# **show running-config interfaces** GigabitEthernet 1 

21.12 SHUTDOWN

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.

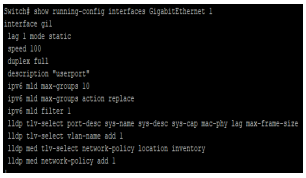
Switch#**configure terminal**

Switch(config)#**interface** {Interface-ID}

Switch(config-if)# **shutdown**

Switch(config-if)#**no shutdown**

Syntax	**shutdown** **no shutdown**
Default	Default port admin state is no shutdown.
Mode	Interface Configuration

Example	This example shows how to modify port duplex configuration. Switch#**configure terminal** Switch(config)# **interface** gi1 Switch(config-if)# **shutdown** This example shows how to show current admin state configuration Switch# **show running-config interfaces** gi1  Switch# show running-config interfaces GigabitEthernet 1 interface gi1 lag 1 mode static speed 100 duplex full description "userport" ipv6 mld max-groups 10 ipv6 mld max-groups action replace ipv6 mld filter 1 lldp tlv-select port-desc sys-name sys-desc sys-cap mac-phy lag max-frame-size lldp tlv-select vlan-name add 1 lldp med tlv-select network-policy location inventory lldp med network-policy add 1

PORT ERROR DISABLE

When a **port** is in **error-disabled** state, it is effectively shut down and no traffic is sent or received on that **port**. The ErrDisable feature is implemented to handle critical situations where the switch detected excessive or late collisions on a port, port duplex misconfiguration, Ether Channel misconfiguration, Bridge Protocol Data Unit (BPDU) port-guard violation, UniDirectional Link Detection (UDLD), and other causes.

The error-disable function let the switch to shut down a port when it encounters physical, driver or configuration problems. A port being error-disabled is not by itself a cause for alarm, but for a reason of a problem that must be resolved.

When a port is in error-disabled state, it will shut down and no traffic is sent or received on that port.

22.1 ERRDISABLE RECOVERY CAUSE

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.

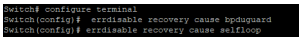
Switch#**configure terminal**

Switch(config)#**errdisable recovery cause(all|acl|arp-inspection |bpduguard| broadcast-flood|dhcp-rate-limit|psecure-violation|selfloop|unicast-flood|unknown-multicastflood)**

Switch(config)#**no errdisable recovery cause(all| acl| arpinspection |bpduguard|broadcast-flood|dhcp-rate-limit|psecure-violation| selfloop| unicast-flood|unknown- multicastflood)**

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 flooding 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
Example	The following example enables the port error disable recovery for the STP BPDU Guard and self-loog cause. Switch#**configure terminal** Switch(config)# **errdisable recovery cause bpduguard** Switch(config)# **errdisable recovery cause selfloop**  The following example To remove the port error disable recovery from the specific cause. Switch#**configure terminal** Switch(config)# **no errdisable recovery cause bpduguard** Switch(config)# **no errdisable recovery cause selfloop**

22.2 ERRDISABLE RECOVERY INTERVAL

To set the recovery time of the error disabled ports, use the command errdisable recovery interval in the Global Configuration mode.

Switch#**configure terminal**

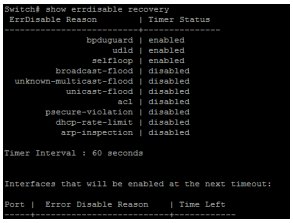
Switch(config)# **errdisable recovery interval** (seconds)

Syntax	**errdisable recovery interval** seconds
Parameter	**seconds** The time in seconds to recover from a specific error- disable state. The valid range is 0 to 86400 seconds, and the default value is 300 seconds.
Default	The default recovery time is 300 seconds
Mode	Global Configuration
Example	The following example set the agimg time to 500 seconds. Switch#**configure terminal** Switch(config)# **errdisable recovery interval** 60

22.3 SHOW ERRDISABLE RECOVERY

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.

Switch# **show errdisable recovery**

Syntax	**show errdisable recovery**
Mode	Privileged EXEC
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 | enabled
                        udld | enabled
                    selfloop | enabled
           broadcast-flood   | disabled
  unknown-multicast-flood    | disabled
             unicast-flood   | disabled
                       acl   | disabled
          psecure-violation  | disabled
            dhcp-rate-limit  | disabled
             arp-inspection  | disabled

Timer Interval : 60 seconds


Interfaces that will be enabled at the next timeout:

Port |  Error Disable Reason    | Time Left
-----+--------------------------+-----------
```

PORT SECURITY

Port Security helps secure the network by preventing unknown devices from forwarding packets. When a link goes down, all dynamically locked addresses are freed. The port security feature offers the following benefits:

You can limit the number of MAC addresses on a given port. Packets that have a matching MAC address (secure packets) are forwarded; all other packets (unsecure packets) are restricted.

You can enable port security on a per port basis. Port security implements two traffic filtering methods, dynamic locking and static locking. These methods can be used concurrently.

Dynamic locking

you can specify the maximum number of MAC addresses that can be learned on a port. The maximum number of MAC addresses is platform dependent and is given in the software Release Notes. After the limit is reached, additional MAC addresses are not learned. Only frames with an allowable source MAC addresses are forwarded.

Dynamically locked addresses can be converted to statically locked addresses. Dynamically locked MAC addresses are aged out if another packet with that address is not seen within the age-out time. You can set the time out value. Dynamically locked MAC addresses are eligible to be learned by another port. Static MAC addresses are not eligible for aging.

Static locking

you can manually specify a list of static MAC addresses for a port. Dynamically locked addresses can be converted to statically locked addresses.

By using port security, a network administrator can associate specific MAC addresses with the interface, which can prevent an attacker to connect his device. This way you can restrict access to an interface so that only the authorized devices can use it. If an unauthorized device is connected, you can decide what action the switch will take, for example discarding the traffic and shutting down the port.

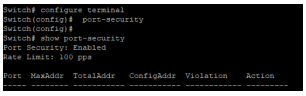
23.1 PORT-SECURITY (GLOBAL)

The "**port-security**" command enables the port security functionality globally. Use the **"no"** form of this command to disable. You can verify settings by the show port-security command.

Switch#**configure terminal**

Switch(config)# **port-security**

Switch(config)# **no port-security**

Syntax	**port-security** **no port-security**
Default	Default is disabled
Mode	Global Configuration
Example	The following example shows how to enable port security Switch#**configure terminal** Switch(config)# **port-security** Switch# **show port-security** 

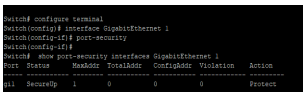
23.2 PORT-SECURITY (INTERFACE)

The "**port-security**" command enables the port security functionality on this port. Use the **"no"** form of this command to disable. You can verify settings by the show port-security interface command.

Switch#**configure terminal**

Switch(config)# **port-security**

Switch(config)# **no port-security**

Syntax	**port-security** **no port-security**
Mode	Port Configuration
Example	The following example shows how to enable port security on interface GigabitEthernet 1 Switch#**configure terminal** Switch(config)# **interface** GigabitEthernet 1 Switch(config-if)# **port-security** Switch# **show port-security interfaces** GigabitEthernet 1 

23.3 PORT-SECURITY ADDRESS-LIMIT

Use the "**port-security address-limit**" command to set the learning-limit number and the violation action. Use the **"no"** form of this command to restore the default settings. You can verify settings by the show port-security interface command.

Switch#**configure terminal**

Switch(config)#**port-security address-limit** *<1-256>* **action (forward |discard |shutdown)**

Switch(config)#**no port-security address-limit**

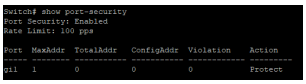
Syntax	**port-security address-limit***<1-256>* **action (forward| discard| shutdown)** **no port-security address-limit**
Parameter	*<1-256>*The learning-limit number. It specifies how many MAC addresses this port can learn. **forward** Forward this packet whose SMAC is new to system and exceed the learning-limit number. **discard** Discard this packet whose SMAC is new to system and exceed the learning-limit number. **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
Example	The following example shows how to enable port security on port 1 and set the learning limit number to 10. Switch#**configure terminal** Switch(config)# **interface** GigabitEthernet 1 Switch(config-if)# **port-security address-limit** 1 Switch(config-if)# **port-security violation protect** Switch# **show port-security interfaces** GigabitEthernet 1 

23.4 SHOW PORT-SECURITY

Use "**show port-security**" command to show port-security global information.

Switch# **show port-security**

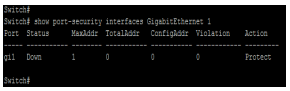
Syntax	**show port-security**
Mode	Privileged EXEC
Example	This example shows how to show port-security configurations. Switch# **show port-security** 

```
Switch# show port-security
Port Security: Enabled
Rate Limit: 100 pps

Port  MaxAddr  TotalAddr   ConfigAddr  Violation    Action
----- -------- ----------- ----------- ---------- --------
gi1   1        0           0           0          Protect
```

23.5 SHOW PORT-SECURITY INTERFACE

Use "**show port-security interfaces**" command to show port-security information of the specified port.

Switch# **show port-security interface** *{IF_PORTS}*

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
Example	This example shows how to show port-security configurations on interface GigabitEthernet 1. Switch# **show port-security interfaces** GigabitEthernet 1 

```
Switch#
Switch# show port-security interfaces GigabitEthernet 1
Port  Status      MaxAddr  TotalAddr  ConfigAddr  Violation    Action
----- ----------- -------- ---------- ----------- ---------- ---------
gi1   Down        1        0          0           0          Protect

Switch#
```

24. PROTOCOL VLAN

Protocol-based VLAN processes traffic based on protocol. You can use a protocol-based VLAN to define filtering criteria for untagged packets. If you do not change the port configuration or configure a protocol-based VLAN, switch assigns untagged packets to VLAN 1. You can override this default behavior by defining port-based VLANs, protocol-based VLANs, or both. Switch always processes tagged packets according to the 802.1q standard and does not forward them to protocol-based VLANs.

If you assign a port to a protocol-based VLAN for a specific protocol, switch assigns the protocol-based VLAN ID to untagged frames that it receives on the port for that protocol. For other protocols, switch assigns the port VLAN ID to untagged frames that it receives on the port, either the default PVID1 or a PVID that you assigned to the port.

You define a protocol based VLAN by creating a group. Each group has a one-to-one relationship with a VLAN ID, can include one to three protocol definitions, and can include multiple ports. When you create a group, you must specify a name. The smart switch assigns a group ID automatically.

24.1 VLAN PROTOCOL-VLAN GROUP (GLOBAL)

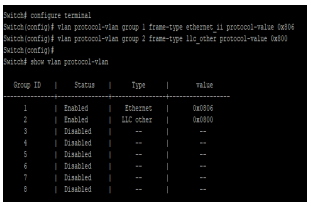
Use the vlan protocol-vlan group Global Configuration mode command to add protocol vlan group with specific proto type and value. Use the **“no”** form of this command to remove protocol vlan group setting. You can verify your setting by entering the show vlan proto-vlan Privileged EXEC command.

Switch# **configure terminal**

Switch(config)# **vlan protocol-vlan group**<*1-8*> **frame-type (ethernet_ii |llc_other|snap_1042) protocol-value** VALUE

Switch(config)# **no vlan protocol-vlan group**<*1-8*>

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
Mode	Global Configuration
Example	The following example show how to configure protocol vlan group: Switch# **configure terminal** 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 terminal
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(config)#
Switch# show vlan protocol-vlan

  Group ID    |    Status    |     Type     |       value
--------------+--------------+--------------+--------------
      1       |   Enabled    |   Ethernet   |     0x0806
      2       |   Enabled    |  LLC other   |     0x0800
      3       |   Disabled   |      --      |      --
      4       |   Disabled   |      --      |      --
      5       |   Disabled   |      --      |      --
      6       |   Disabled   |      --      |      --
      7       |   Disabled   |      --      |      --
      8       |   Disabled   |      --      |      --
```

24.2 VLAN PROTOCOL-VLAN GROUP (INTERFACE)

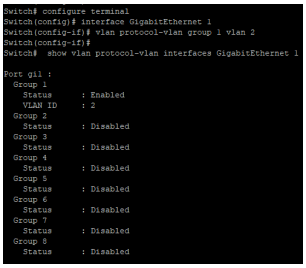
Use the vlan protocol-vlan binding Interface Configuration mode command to binding protocol VLAN Group on specified interfaces. Use the **“no”** form of this command to cancel protocol VLAN Group Binding. You can verify your setting by entering the show vlan protocol-vlan interfaces IF_PORTS Privileged EXEC command

Switch# **configure terminal**

Switch(config-if)# **vlan protocol-vlan group** *<1-8>* **vlan** *<1-4094>*

Switch(config-if)# **no vlan protocol-vlan group** *<1-8>*

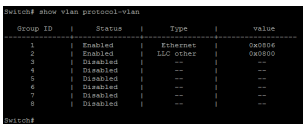
Syntax	**vlan protocol-vlan group** *<1-8>***vlan** *<1-4094>* **no vlan protocol-vlan group** *<1-8>*
Parameter	*<1-8>* Specify protocol vlan group to binding *<1-4094>* Specifies the Proto VLAN ID to configure.
Mode	Interface configuration

Example	The following example how to configure Protocol VLAN function on specified interfaces. Switch# **configure terminal** Switch(config)# **interface** GigabitEthernet 1 Switch(config-if)# **vlan protocol-vlan group** 1 **vlan** 2 Switch# **show vlan protocol-vlan interfaces** GigabitEthernet 1 

24.3 SHOW VLAN PROTOCOL-VLAN

Use the show vlan proto-vlan command in EXEC mode to display Proto VLAN group configuration.

Switch# **show vlan protocol-vlan[group**<*1-8*>**]**

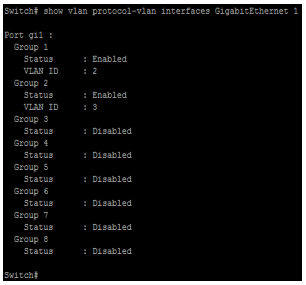
Syntax	**show vlan protocol-vlan[group**<*1-8*>**]**
Parameter	<*1-8*>Specify protocol vlan group to display
Mode	Privileged EXEC
Example	The following example how to display Proto VLAN group configuration Switch# **show vlan protocol-vlan** 

```
Switch# show vlan protocol-vlan
  Group ID    |    Status    |     Type     |     value
--------------+--------------+--------------+--------------
      1       |   Enabled    |   Ethernet   |    0x0806
      2       |   Enabled    |  LLC other   |    0x0600
      3       |   Disabled   |      --      |      --
      4       |   Disabled   |      --      |      --
      5       |   Disabled   |      --      |      --
      6       |   Disabled   |      --      |      --
      7       |   Disabled   |      --      |      --
      8       |   Disabled   |      --      |      --
Switch#
```

24.4 SHOW VLAN PROTOCOL-VLAN INTERFACES

Use the show vlan protocol-vlan interface command in EXEC mode to display the Protocol VLAN interfaces setting.

Switch# **show vlan protocol-vlan interfaces***{IF_PORTS}*

Syntax	**show vlan protocol-vlan interfaces** *{IF_PORTS}*
Parameter	*{IF_PORTS}* Specify interfaces protocol vlan to display
Mode	Privileged EXEC
Example	The following example shows how to display the Protocol VLAN interfaces setting Switch# **show vlan protocol-vlan interfaces** GigabitEthernet 1 

```
Switch# show vlan protocol-vlan interfaces GigabitEthernet 1

Port gi1 :
  Group 1
    Status      : Enabled
    VLAN ID     : 2
  Group 2
    Status      : Enabled
    VLAN ID     : 3
  Group 3
    Status      : Disabled
  Group 4
    Status      : Disabled
  Group 5
    Status      : Disabled
  Group 6
    Status      : Disabled
  Group 7
    Status      : Disabled
  Group 8
    Status      : Disabled

Switch#
```

PROTOCOL VLAN

Protocol-based VLAN processes traffic based on protocol. You can use a protocol-based VLAN to define filtering criteria for untagged packets. If you do not change the port configuration or configure a protocol-based VLAN, switch assigns untagged packets to VLAN 1. You can override this default behavior by defining port-based VLANs, protocol-based VLANs, or both. Switch always processes tagged packets according to the 802.1q standard and does not forward them to protocol-based VLANs.

If you assign a port to a protocol-based VLAN for a specific protocol, switch assigns the protocol-based VLAN ID to untagged frames that it receives on the port for that protocol. For other protocols, switch assigns the port VLAN ID to untagged frames that it receives on the port, either the default PVID1 or a PVID that you assigned to the port.

You define a protocol based VLAN by creating a group. Each group has a one-to-one relationship with a VLAN ID, can include one to three protocol definitions, and can include multiple ports. When you create a group, you must specify a name. The smart switch assigns a group ID automatically.

24.1 VLAN PROTOCOL-VLAN GROUP (GLOBAL)

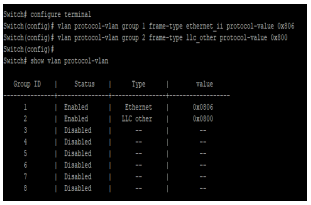
Use the vlan protocol-vlan group Global Configuration mode command to add protocol vlan group with specific proto type and value. Use the **“no”** form of this command to remove protocol vlan group setting. You can verify your setting by entering the show vlan proto-vlan Privileged EXEC command.

Switch# **configure terminal**

Switch(config)# **vlan protocol-vlan group**<*1-8*> **frame-type (ethernet_ii |llc_other|snap_1042) protocol-value** VALUE

Switch(config)# **no vlan protocol-vlan group**<*1-8*>

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
Mode	Global Configuration

Example	The following example show how to configure protocol vlan group: Switch# **configure terminal** 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 terminal
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(config)#
Switch# show vlan protocol-vlan

 Group ID   |    Status    |     Type      |       value
------------+--------------+---------------+-------------------
     1      |  Enabled     |   Ethernet    |      0x0806
     2      |  Enabled     |  LLC other    |      0x0800
     3      |  Disabled    |      --       |       --
     4      |  Disabled    |      --       |       --
     5      |  Disabled    |      --       |       --
     6      |  Disabled    |      --       |       --
     7      |  Disabled    |      --       |       --
     8      |  Disabled    |      --       |       --
```

24.2 VLAN PROTOCOL-VLAN GROUP (INTERFACE)

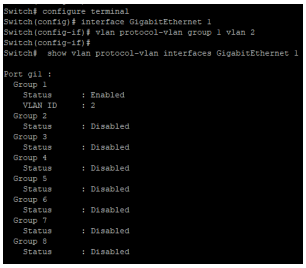
Use the vlan protocol-vlan binding Interface Configuration mode command to binding protocol VLAN Group on specified interfaces. Use the **“no”** form of this command to cancel protocol VLAN Group Binding. You can verify your setting by entering the show vlan protocol-vlan interfaces IF_PORTS Privileged EXEC command

Switch# **configure terminal**

Switch(config-if)# **vlan protocol-vlan group** *<1-8>* **vlan** *<1-4094>*

Switch(config-if)# **no vlan protocol-vlan group** *<1-8>*

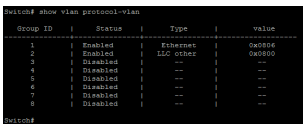
Syntax	**vlan protocol-vlan group** *<1-8>***vlan** *<1-4094>* **no vlan protocol-vlan group** *<1-8>*
Parameter	*<1-8>* Specify protocol vlan group to binding *<1-4094>* Specifies the Proto VLAN ID to configure.
Mode	Interface configuration

Example	The following example how to configure Protocol VLAN function on specified interfaces. Switch# **configure terminal** Switch(config)# **interface** GigabitEthernet 1 Switch(config-if)# **vlan protocol-vlan group** 1 **vlan** 2 Switch# **show vlan protocol-vlan interfaces** GigabitEthernet 1 

24.3 SHOW VLAN PROTOCOL-VLAN

Use the show vlan proto-vlan command in EXEC mode to display Proto VLAN group configuration.

Switch# **show vlan protocol-vlan[group**<*1-8*>**]**

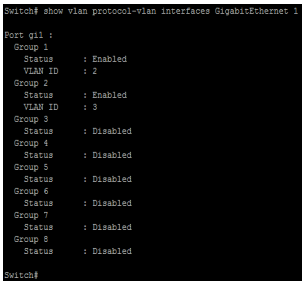
Syntax	**show vlan protocol-vlan[group**<*1-8*>**]**
Parameter	<*1-8*>Specify protocol vlan group to display
Mode	Privileged EXEC
Example	The following example how to display Proto VLAN group configuration Switch# **show vlan protocol-vlan** 

```
Switch# show vlan protocol-vlan
  Group ID    |    Status    |     Type     |     value
--------------+--------------+--------------+--------------
      1       |   Enabled    |   Ethernet   |    0x0806
      2       |   Enabled    |  LLC other   |    0x0600
      3       |   Disabled   |      --      |      --
      4       |   Disabled   |      --      |      --
      5       |   Disabled   |      --      |      --
      6       |   Disabled   |      --      |      --
      7       |   Disabled   |      --      |      --
      8       |   Disabled   |      --      |      --
Switch#
```

24.4 SHOW VLAN PROTOCOL-VLAN INTERFACES

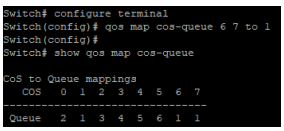
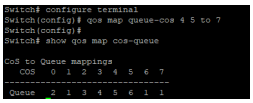
Use the show vlan protocol-vlan interface command in EXEC mode to display the Protocol VLAN interfaces setting.

Switch# **show vlan protocol-vlan interfaces***{IF_PORTS}*

Syntax	**show vlan protocol-vlan interfaces** *{IF_PORTS}*
Parameter	*{IF_PORTS}* Specify interfaces protocol vlan to display
Mode	Privileged EXEC
Example	The following example shows how to display the Protocol VLAN interfaces setting Switch# **show vlan protocol-vlan interfaces** GigabitEthernet 1 

```
Switch# show vlan protocol-vlan interfaces GigabitEthernet 1

Port gi1 :
  Group 1
    Status      : Enabled
    VLAN ID     : 2
  Group 2
    Status      : Enabled
    VLAN ID     : 3
  Group 3
    Status      : Disabled
  Group 4
    Status      : Disabled
  Group 5
    Status      : Disabled
  Group 6
    Status      : Disabled
  Group 7
    Status      : Disabled
  Group 8
    Status      : Disabled

Switch#
```

QOS

Mode	Global Configuration
Example	This example shows how to map cos 6 and 7 to queue 1. Switch#**configure terminal** 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#**configure terminal** Switch(config)# **qos map queue-cos** 4 5 **to** 7 Switch# **show qos map queue-cos** 

25.4 QOS QUEUE

The device support total 8 queues for QoS queuing. 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.

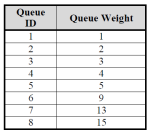
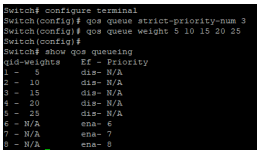
Switch#**configure terminal**

Switch(config)#**qos queue strict-priority-num**

Switch(config)#**qos queue weight SEQUENCE**

Switch#**show qos queueing**

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. 
Mode	Global Configuration
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#**configure terminal** Switch(config)# **qos queue strict-priority-num** 3 Switch(config)# **qos queue weight** 5 10 15 20 25 Switch# **show qos queueing** 

Queue ID	Queue Weight
1	1
2	2
3	3
4	4
5	5
6	9
7	13
8	15

25.5 QOS REMARK

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.

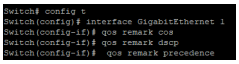
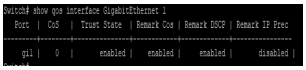
Use **“qos remark”** command to enable remarking feature on specific type. And use **“no qow remark”** command to disable it.

Switch#**configure terminal**

Switch(config)#**qos remark (cos | dscp | precedence)**

Switch(config)# **no qos remark (cos | dscp | precedence)**

Syntax	**qos remark (cos | dscp | precedence)** **no qos remark (cos | dscp | precedence)**
Parameter	cos Enable/Disable cos remarking. dscp Enable/Disable dscp remarking. precedence Enable/Disable precedence remarking
Default	Default CoS remarking is disabled. Default DSCP remarking is disabled. Default IP Precedence remarking is disabled.
Mode	Interface Configuration

Example	This example shows how to enable remarking features on interface gi1. Switch#**configure terminal** Switch(config)# **interface** GigabitEthernet 1 Switch(config-if)# **qos remark cos** Switch(config-if)# **qos remark dscp** Switch(config-if)# **qos remark precedence**  Switch# **show qos interface** GigabitEthernet 1 

25.6 QOS TRUST

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.

CoS

IEEE 802.1p defined 3bits priority value in vlan tag. Trust this value in packets and assign queue according to cos-queue map.

DSCP

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.

IP Precedence

The highest 3bits priority value in IP packet ToS field. Trust this value in packets and assign queue according to precedence-queue map.

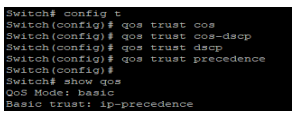
CoS-DSCP

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.

Switch#**configure terminal**

Switch(config)#**qos trust (cos | cos-dscp | dscp | precedence)**

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
Example	This example shows how to change qos basic mode trust types. Switch#**configure terminal** Switch(config)# **qos trust cos** Switch(config)# **qos trust cos-dscp** Switch(config)# **qos trust dscp** Switch(config)# **qos trust precedence** This example shows how to check current qos trust type. Switch# **show qos**  Switch# config t Switch(config)# qos trust cos Switch(config)# qos trust cos-dscp Switch(config)# qos trust dscp Switch(config)# qos trust precedence Switch(config)# Switch# show qos QoS Mode: basic Basic trust: ip-precedence

25.7 QOS TRUST (INTERFACE)

Interface Configuration 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.

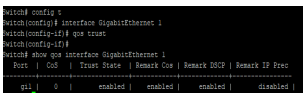
Use **“qos trust”** to enable trust state on interface and use **“no qos trust”** to disable trust state on interface.

Switch#**configure terminal**

Switch(config)#**qos trust**

Switch(config)# **no qos trust**

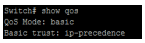
Syntax	**qos trust** **no qos trust**
Default	Default interface qos trust state is enabled.
Mode	Interface Configuration

Example	This example shows how to disable qos trust state on interface gi1. Switch#**configure terminal** Switch(config)# **interface** GigabitEthernet 1 Switch(config-if)#**qos trust** Switch# **show qos interface** GigabitEthernet 1 

25.8 SHOW QOS

Use **“show qos”** command to show qos state and trust type.

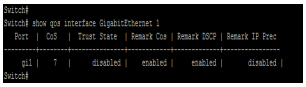
Switch#**show qos**

Syntax	**show qos**
Mode	Privileged EXEC
Example	This example shows how to check current qos mode. Switch# **show qos** 

25.9 SHOW QOS INTERFACE

Use **“show qos interfaces”** command to show port default cos, remarking state and remarking type state information.

Switch#**show qos interface** *{IF_PORTS}*

Syntax	**show qos interface***{IF_PORTS}*
Parameter	*{IF_PORTS}*Select port to show qos configurations
Mode	Privileged EXEC
Example	This example shows how to show qos configurations on interface gi1. Switch# **show qos interface** GigabitEthernet 1 

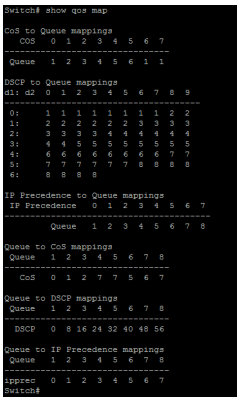
```
Switch#
Switch# show qos interface GigabitEthernet 1
  Port  |  CoS  | Trust State | Remark Cos | Remark DSCP | Remark IP Prec
--------+-------+-------------+------------+-------------+---------------
   gi1  |   7   |   disabled  |   enabled  |   enabled   |   disabled
Switch#
```

25.10 SHOW QOS MAP

Use **“show qos map”** command to show all kinds of mapping for qos remapping and remarking features.

Switch#**show qos map [(cos-queue | dscp-queue | precedence-queue | queue-cos | queue-dscp | queue-precedence)]**

Syntax	**show qos map [(cos-queue | dscp-queue | precedence-queue | queue-cos |queue-dscp | queue-precedence)]**
Parameter	cos-queue Show CoS to queue map. dscp-queue Show DSCP to queue map. precedence-queue Show IP Precedence to queue map. queue-cos Show queue to CoS map. queue-dscp Show queue to DSCP map. queue-precedence Show queue to IP Precedence map.
Mode	Privileged EXEC

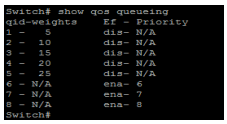
Example	This example shows how to show all qos maps. Switch# **show qos map** 

```
Switch# show qos map

CoS to Queue mappings
   COS   0  1  2  3  4  5  6  7
 ---------------------------------
 Queue   1  2  3  4  5  6  1  1

DSCP to Queue mappings
d1: d2  0  1  2  3  4  5  6  7  8  9
 ---------------------------------------
 0:     1  1  1  1  1  1  1  1  2  2
 1:     2  2  2  2  2  2  2  3  3  3
 2:     3  3  3  3  4  4  4  4  4  4
 3:     4  4  5  5  5  5  5  5  5  5
 4:     6  6  6  6  6  6  6  6  7  7
 5:     7  7  7  7  7  7  8  8  8  8
 6:     8  8  8  8

IP Precedence to Queue mappings
 IP Precedence   0  1  2  3  4  5  6  7
 ---------------------------------------
         Queue   1  2  3  4  5  6  7  8

Queue to CoS mappings
 Queue   1  2  3  4  5  6  7  8
 ---------------------------------
    CoS   0  1  2  7  7  5  6  7

Queue to DSCP mappings
 Queue   1  2  3  4  5  6  7  8
 ---------------------------------
  DSCP   0  8 16 24 32 40 48 56

Queue to IP Precedence mappings
 Queue   1  2  3  4  5  6  7  8
 ---------------------------------
ipprec   0  1  2  3  4  5  6  7
Switch#
```

25.11 SHOW QOS QUEUEING

Use "**show qos queueing"** command to show qos queueing information.

Switch#**show qos queueing**

Syntax	**show qos queueing**
Mode	Privileged EXEC
Example	This example shows how to check current qos queueing information. Switch# **show qos queueing** 

```
Switch# show qos queueing
qid-weight#    Ef - Priority
1 -   5         dis- N/A
2 -  10         dis- N/A
3 -  15         dis- N/A
4 -  20         dis- N/A
5 -  25         dis- N/A
6 - N/A         ena- 6
7 - N/A         ena- 7
8 - N/A         ena- 8
Switch#
```

RATE LIMIT

Rate-limiting for all traffic operates on a per-port basis to allow only the specified bandwidth to be used for inbound or outbound traffic. When traffic exceeds the configured limit, it is dropped. This effectively sets a usage level on a given port and is a tool for enforcing maximum service level commitments granted to network users. This feature operates on a per-port level and is not configurable on port trunks. Rate-limiting is designed to be applied at the network edge to limit traffic from non-critical users or to enforce service agreements such as those offered by Internet Service Providers (ISPs) to provide only the bandwidth for which a customer has paid.

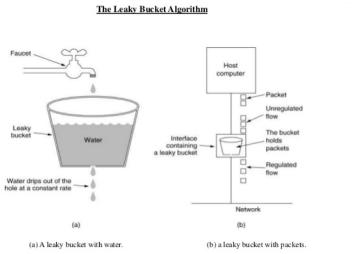


Fig 26.1 Leaky bucket Model

All traffic rate-limiting, Rate-limiting for all traffic operates on a per-port basis to allow only the specified bandwidth to be used for inbound or outbound traffic. When traffic exceeds the configured limit, it is dropped. This effectively sets a usage level on a given port and is a tool for enforcing maximum service level commitments granted to network users. This feature operates on a per-port level and is not configurable on port trunks. Rate-limiting is designed to be applied at the network edge to limit traffic from non-critical users or to enforce service agreements such as those offered by Internet Service Providers (ISPs) to provide only the bandwidth for which a customer has paid.

Uses:-

• Rate-limiting can be applied by a RADIUS server during an authentication client session. Applying rate-limiting to desirable traffic is not recommended.

• The switches also support ICMP rate-limiting to mitigate the effects of certain ICMP-based attacks. ICMP traffic is necessary for network routing functions. For this reason, blocking all ICMP traffic is not recommended.

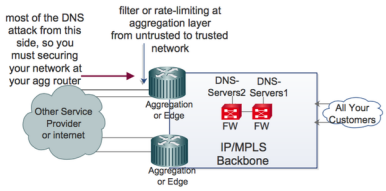


Fig 26.2 Rate limiting on Aggregation Layer

26.1 RATE LIMIT EGRESS

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.

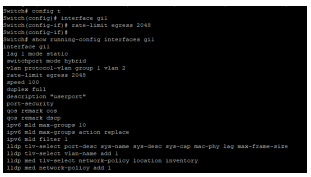
Switch# **configure terminal**

Switch(config)# **interface** { Interface-ID}

Switch(config-if)#**rate-limit egress <16-1000000>**

Switch(config-if)#**no rate-limit egress**

Syntax	**rate-limit egress <16-1000000>** **no rate-limit egress**
Parameter	<16-1000000> Specify the committed information rate.
Default	Default rate limit is disabled.
Mode	Interface configuration

Example	The following example shows how to configure ingress port rate limit and egress port shaper. Switch# **configure terminal** Switch(config)# **interface** gi1 Switch(config-if)# **rate-limit egress** 2048 Switch# **show running-config interfaces** gi1 

```
Switch# config t
Switch(config)# interface gi1
Switch(config-if)# rate-limit egress 2048
Switch(config-if)#
Switch# show running-config interfaces gi1
interface gi1
 lag 1 mode static
 switchport mode hybrid
 vlan protocol-vlan group 1 vlan 2
 rate-limit egress 2048
 speed 100
 duplex full
 description "userport"
 port-security
 qos remark cos
 qos remark dscp
 ipv6 mld max-groups 10
 ipv6 mld max-groups action replace
 ipv6 mld filter 1
 lldp tlv-select port-desc sys-name sys-desc sys-cap mac-phy lag max-frame-size
 lldp tlv-select vlan-name add 1
 lldp med tlv-select network-policy location inventory
 lldp med network-policy add 1
```

26.2 RATE LIMIT EGRESS QUEUE

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 show running-config interface command.

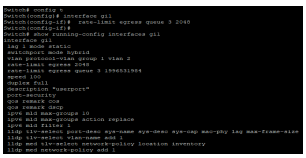
Switch# **configure terminal**

Switch(config)# **interface** { Interface-ID}

Switch(config-if)#**rate-limit egress queue**<1-8><16-1000000>

Switch(config-if)#**no rate-limit egress queue**<1-8>

Syntax	**rate-limit egress queue**<1-8><16-1000000> **no rate-limit egress queue**<1-8>

Parameter	<1-8>Specify the egress shaper queue number <16-1000000>Specify the queue rate
Default	Default queue rate limit is disabled.
Mode	Interface configuration
Example	The following example show how to configure ingress port rate limit and egress port shaper. Switch# **configure terminal** Switch(config)# **interface** gi1 Switch(config-if)# **rate-limit egress queue** 3 2048 Switch# **show running-config interfaces** gi1 

26.3 RATE LIMIT INGRESS

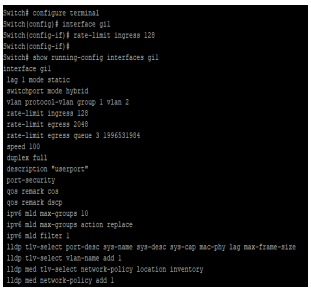
Use the "**rate-limit ingress**" command to limit the incoming traffic rate on a port. Use the **"no"** form of this command to disable the rate limit. You can verify your setting by entering the show running-config interfaces command.

Switch# **configure terminal**

Switch(config)# **interface** { Interface-ID}

Switch(config-if)#**rate-limit ingress**<16-1000000>

Switch(config-if)#**no rate-limit ingress**

Syntax	**rate-limit ingress**<16-1000000> **no rate-limit ingress**
Parameter	<16-1000000>Specify the ingress limit rate <1-8>Specify the egress shaper queue number
Default	Rate limiting is disabled.
Mode	Interface configuration
Example	The following example shows how to configure ingress port rate limit. Switch# **configure terminal** Switch(config)# **interface** gi1 Switch(config-if)# **rate-limit ingress** 128 Switch# **show running-config interfaces** gi1 

```
Switch# configure terminal
Switch(config)# interface gi1
Switch(config-if)# rate-limit ingress 128
Switch(config-if)#
Switch# show running-config interfaces gi1
interface gi1
 lag 1 mode static
 switchport mode hybrid
 vlan protocol-vlan group 1 vlan 2
 rate-limit ingress 128
 rate-limit egress 2048
 rate-limit egress queue 3 1996831904
 speed 100
 duplex full
 description "userport"
 port-security
 qos remark cos
 qos remark dscp
 ipv6 mld max-groups 10
 ipv6 mld max-groups action replace
 ipv6 mld filter 1
 lldp tlv-select port-desc sys-name sys-desc sys-cap mac-phy lag max-frame-size
 lldp tlv-select vlan-name add 1
 lldp med tlv-select network-policy location inventory
 lldp med network-policy add 1
```

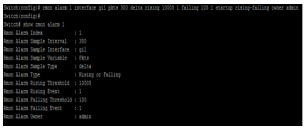
RMON

Syntax	**show rmon event** <*1-65535*> **log**
Parameter	<*1-65535*>specifies event index to show event log
Default	No entry and log is exist
Mode	Privileged EXEC
Example	The example shows how to show rmon event log. Switch# **show rmon event** 1 **log** 

27.8 SHOW RMON ALARM

Use the show rmon alarm command to show existed RMON alarm entry.

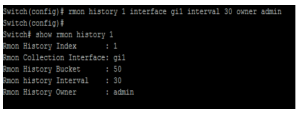
Switch #**show rmon alarm** (*<1-65535>*| **all**)

Syntax	**show rmon alarm** (*<1-65535>*| all)
Parameter	*<1-65535>*specifies alarm index to show all Show all existed alarm
Mode	Privileged EXEC
Example	The example shows how to show rmon alarm entry. Switch#configure terminal Switch(config**)# rmon alarm** 1 **interface** gi1pkts300 **delta rising** 100001 **falling** 1001 **startup rising-falling owner** admin Switch#**show rmon alarm** 1 

27.9 SHOW RMON HISTORY

Use the show rmon history command to show existed RMON history entry.

Switch #**show rmon history** (*<1-65535>*| **all**)

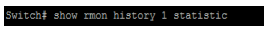
Syntax	**show rmon history** (*<1-65535>*| **all**)
Parameter	*<1-65535>*specifies history index to show all Show all existed history
Mode	Privileged EXEC
Example	The example shows how to show RMON history entry. switch(config)# rmon history 1 interface gi1 interval 30 owner admin switch# **show rmon history** 1 

```
Switch(config)# rmon history 1 interface gi1 interval 30 owner admin
Switch(config)#
Switch# show rmon history 1
Rmon History Index       : 1
Rmon Collection Interface: gi1
Rmon History Bucket      : 50
Rmon history Interval    : 30
Rmon History Owner       : admin
```

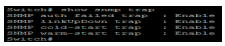
27.10 SHOW RMON HISTORY STATISTIC

Use the show rmon history statistic command to show statistics that are recorded by RMON history.

Switch #**show rmon history** <*1-65535*>**statistic**

Syntax	show rmon history <*1-65535*>statistic
Parameter	<*1-65535*>specifies history index to show history statistic
Mode	Privileged EXEC
Example	The example shows how to show RMON history statistics switch# **show rmon history** 1 **statistics** 

SNMP

Syntax	**show snmp trap**
Mode	Privileged EXEC
Example	The following example shows the status of SNMP traps. Switch# **show snmp trap** 

28.7 SHOW SNMP VIEW

To show the SNMP view defined on the switch, use the command show snmp view in the Privileged EXEC mode.

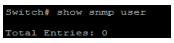
Switch# **show snmp view**

Syntax	**show snmp view**
Mode	Privileged EXEC
Example	The following example shows the configuration of SNMP view. Switch# **show snmp view** 

28.8 SHOW SNMP USER

To show the SNMP users defined on the switch, use the command show snmp user in the Privileged EXEC mode.

Switch# **show snmp user**

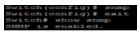
Syntax	**show snmp user**
Mode	Privileged EXEC
Example	The following example shows the configuration of SNMP user. Switch# **show snmp user** 

28.9 SNMP

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.

Switch# **configure terminal**

Switch(config)# **snmp**

Syntax	snmp
Default	SNMP is disabled by default
Mode	Global Configuration
Example	The following example enables the SNMP. Switch# **configure terminal** Switch(config)# **snmp** 

28.10 SNMP COMMUNITY

To define the SNMP community that permit access for SNMP v1 and v2, use the command snmp community in the Global Configuration mode.

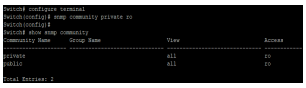
Switch# **configure terminal**

Switch(config)#**snmp community community-name [view view-name] (ro|rw)**

Switch(config)#**snmp community community-name group group-name**

Switch(config)#**no snmp community community-name**

Syntax	**snmp community community-name [view view-name] (ro|rw)** **snmp community community-name group group-name** **no snmp community community-name**
Parameter	**community-name** The SNMP community name. Its maximum length is 20 characters. **view** view-name Specify the SNMP view configured by the command snmp view to define the object available to the community. **ro** Read only access (default) **rw** Writable access **group** group-name Specify the SNMP group configured by the command **snmp** group to define the object available to the community.

Mode	Global Configuration
Example	The following example defines the SNMP community named private with the default view all, and the access right is read-only. Switch# **configure terminal** Switch(config)# **snmp community private ro** 

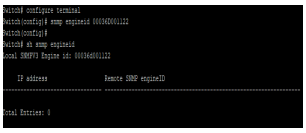
28.11 SNMP ENGINEID

To define the SNMP engine on the switch, use the command snmp engineid in the Global Configuration mode.

Switch# **configure terminal**

Switch(config)# **snmp engineid 00036D001122**

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
Example	The following example configure the switch SNMP engine ID Switch# **configure terminal** Switch(config)# **snmp engineid 00036D001122** 

28.12 SNMP ENGINEID RMOTE

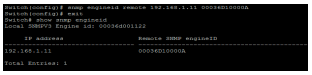
To define the remote host for SNMP engine, use the command snmp engineid remote in the Global Configuration mode and use the **“no”** form of the command to delete the remote host from the SNMP engine.

Switch# **configure terminal**

Switch(config)# **snmp engineid remote (ip-addr|ipv6-addr)** *[ENGINEID]*

Switch(config)# **no snmp engineid remote (ip-addr|ipv6-addr)**

Syntax	**snmp engineid remote (ip-addr|ipv6-addr)** ENGINEID **no snmpengineid 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
Mode	Global Configuration

Example	The following example adds the remote 192.168.1.11 into SNMP engine Switch# **configure terminal** Switch(config)# **snmp engineid remote** 192.168.1.1 100036D10000A 

28.13 SNMP GROUP

To define the SNMP group, use the command snmp group in the Global 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 mapped to the SNMP views defined in this command. The security level for SNMP v1 or v2 is always noauth.

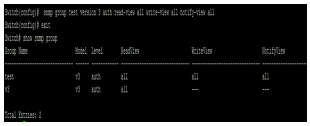
Switch# **configure terminal**

Switch(config)# **snmp group group-name (1|2c|3) (noauth|auth|priv) read-view read-view write-view write-view [notify-view notify-view]**

Switch(config)# **no snmp group group-name security-mode version (1|2c|3)**

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.
Mode	Global Configuration

Example	The following example adds SNMPv3 group Switch# **configure terminal** Switch(config)# **snmp group v3 version 3 auth read-view all** **write-view all notify-view all** 

28.14 SNMP HOST

To configure the hosts to receive SNMP notifications, use the command snmp host in the Global Configuration mode and use the **“no”** form of the command to delete the configuration.

Switch# **configure terminal**

Switch(config)# **snmp host (ip-addr|ipv6-addr|hostmane) [traps|informs] [version (1|2c)] community-name [udp-port udp-port] [timeout timeout] [retries retries]**

Switch(config)# **snmp host (ip-addr|ipv6-addr|hostmane) [traps|informs] version 3**

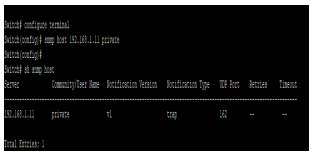
[(auth|noauth|priv)] community-name [udp-port udp-port] [timeout

timeout] [retries retries]

Switch(config)# **no snmp host (ip-addr|ipv6-addr|hostmane) [traps|informs] [version (1|2c|3)]**

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	The default SNMP version for the command is SNMPv1.
Mode	Global Configuration
Example	The following example adds the receipt 192.168.1.11 for the SNMP traps notification. Switch# **configure terminal** Switch(config)# **snmp host 192.168.1.11 private** 

```
Switch# configure terminal
Switch(config)# snmp host 192.168.1.11 private
Switch(config)#
Switch# sh snmp host
Server          Community/User Name  Notification Version  Notification Type  UDP Port  Retries  Timeout
--------------------------------------------------------------------------------------------------------
192.168.1.11    private              v1                    trap               162       --       --

Total Entries: 1
```

28.15 SNMP TRAP

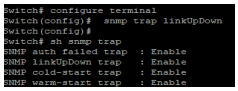
To send the SNMP traps, use the command snmp trap in the Global Configuration mode and use the **“no”** form of the command to disable the SNMP traps.

Switch# **configure terminal**

Switch(config)# **snmp trap (auth|cold-start|linkUpDown|port-security|warm-start)**

Switch(config)# **no snmp trap (auth|cold-start|linkUpDown|port-security |warm-start)**

Syntax	**snmp trap (auth|cold-start|linkUpDown|port-security|warm-start)** **no snmp trap (auth|cold-start|linkUpDown|port-security |warm-start)**
Parameter	**auth** Enable the SNMP authentication failure trap. **cold-start** Enable the SNMP cold start-up failure trap. **linkUpDown** Enable the SNMP link up and down failure trap. **port-security** Enable the SNMP port security trap. **warm-start** Enable the SNMP warm start-up failure trap.
Default	All the SNMP traps are enabled
Mode	Global Configuration

Example	The following example disables and enables the SNMP link up and down traps individually. Switch# **configure terminal** Switch(config)# **snmp trap linkUpDown** 

28.16 SNMP USER

To define a SNMP user, use the command snmp user in the GlobalConfiguration mode and use the **“no”** form to delete the SNMP user.

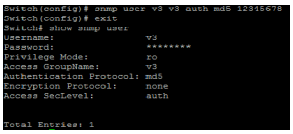
Switch# **configure terminal**

Switch(config)# **snmp user username group-name [auth (md5|sha) AUTHPASSWD] snmp user username group-name auth (md5|sha) AUTHPASSWD priv PRIVPASSWD**

Switch(config)# **no snmp user username**

Syntax	**snmp user username group-name [auth (md5|sha) AUTHPASSWD] snmp user username group-name auth (md5|sha) AUTHPASSWD priv PRIVPASSWD** **no snmp user username**

Parameter	**username** 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. **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. **auth (md5|)** Specify the HMAC-MD5-96 authentication protocol as the user authentication. **auth (sha|)** Specify the HMAC-SHA-96 authentication protocol as the user authentication. AUTHPASSWD The password for authentication and the range of length is from 8 to 32 characters. **Priv** PRIVPASSWD The private password for the privacy key, and the range of length is from 8 to 64 characters
Mode	Global Configuration

Example	The following example adds SNMP user v3 into the group v3 by the MD5 authentication. Switch# **configure terminal** Switch(config)# **snmp user v3 v3 auth md5 12345678** 

28.17 SNMP VIEW

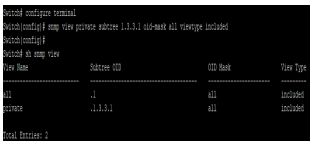
To configure the SNMP view, use the command snmp view in the Global Configuration mode and use the **“no”** form of the command to delete the SNMP view.The default SNMP view cannot be deleted and modified by users. By default, the maximum numbers of SNMP view is limited to 16.

Switch# **configure terminal**

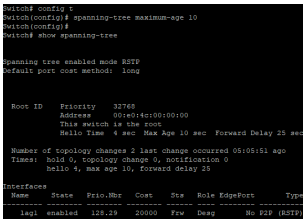
Switch(config)# **snmp view view-name subtreeoid-tree oid-mask (all|oid-mask) viewtype(included|excluded)**

Switch(config)# **no snmp view view-name subtree (all|oid-tree)**

Syntax	**snmp view view-name subtreeoid-tree oid-mask (all|oid-mask) viewtype(included|excluded)** **no snmp view view-name subtree (all|oid-tree)**
Parameter	**view-name** The SNMP view name. Its maximum length is 30 characters. **subtreeoid-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 11111010.10000000. The length of the OID mask must be less than the length of subtreeOID.Viewtype **(included|excluded)**Include or exclude the selected MIBs in the view.
Mode	Global Configuration

Example	The following example defines the SNMP view. Switch# **configure terminal** Switch(config)# **snmp view private subtree** 1.3.3.1 **oid-mask all viewtype included** 

SPANNING TREE

Syntax	**spanning-tree maximum-age** *{seconds}* **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
Example	The following example configures STP maximum age to 10. Switch#**configure terminal** Switch(config)# **spanning-tree maximum-age 10** 

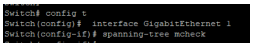
29.20 SPANNING-TREE MCHECK

To restart the Spanning Tree Protocol (STP) migration process (re-negotiate forcibly with its neighborhood) on the specific interface, use the command spanning-tree mcheck in the Interface Configuration mode.

Switch#**configure terminal**

Switch(config)# **interface** {Interface-ID}

Switch(config-if)# **spanning-tree mcheck**

Syntax	**spanning-tree mechek**
Mode	Interface Configuration
Example	The following example restarts the STP negotiation on the interface gi1. Switch#**configure terminal** Switch(config)# **interface GigabitEthernet 1** Switch(config-if)# **spanning-tree mcheck** 

29.21 SPANNING-TREE MODE

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.

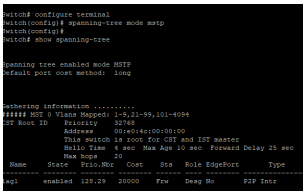
When the switch is configured as MSTP mode, it can use STP and RSTP for the backward compatibility with switches working in STP and RSTP mode individually. For the RSTP configuration, the switch can also use STP for the switches working in the STP operation.

Switch#**configure terminal**

Switch(config)# **spanning-tree mode (mstp|rstp|stp)**

Switch(config)# **no spanning-tree force-version**

Syntax	**spanning-tree mode (mstp|rstp|stp)** **no spanning-tree force-version**
Parameter	**mstp** Enable the Multiple Spanning Tree (MSTP) operation. **rstp** Enable the Rapid Spanning Tree (RSTP) operation. **stp** Enable the Spanning Tree (STP) operation.
Default	The default mode is rstp.
Mode	Global Configuration

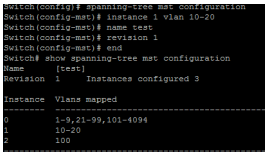
Example	The following example sets the STP operation to MSTP. Switch#**configure terminal** Switch(config)# **spanning-tree mode mstp** 

29.22 SPANNING-TREE MST CONFIGURATION

To enter the MST configuration mode for the MSTP configuration modification, use the command spanning-tree mst configuration in the Global Configuration mode.

Switch#**configure terminal**

Switch(config)# **spanning-tree mst configuration**

Syntax	**spanning-tree mst configuration**
Mode	Global Configuration
Example	The following example modifies the MSTP configuration in the MST Configuration mode. Switch#configure terminal Switch(config)# **spanning-tree mst configuration** Switch(config-mst)# **instance 1 vlan 10-20** Switch(config-mst)# **name test** Switch(config-mst)# **revision 1** 

```
Switch(config)# spanning-tree mst configuration
Switch(config-mst)# instance 1 vlan 10-20
Switch(config-mst)# name test
Switch(config-mst)# revision 1
Switch(config-mst)# end
Switch# show spanning-tree mst configuration
Name      [test]
Revision  1     Instances configured 3

Instance  Vlans mapped
--------  ---------------------------------------------------------------
0         1-9,21-99,101-4094
1         10-20
2         100
-------------------------------------------------------------------------
```

29.23 SPANNING-TREE MST COST

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. When configuring the path cost on the CIST (instance 0), it is equal to the command spanning-tree cost in the Interface Configuration mode.

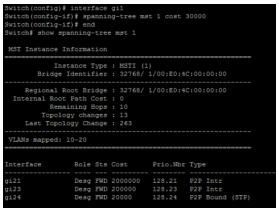
Switch#**configure terminal**

Switch(config)# **interface** {Interface-ID}

Switch(config-if)# **spanning-tree mst instance-id cost** *{cost}*

Switch(config-if)# **no spanning-tree mst instance-id cost** *{cost}*

Syntax	**spanning-tree mst instance-id cost** *{cost}* **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
Example	The following example configures the path cost of interface fa1 on the instance 1 to 30000 Switch#**configure terminal** Switch(config)# **interface** gi1 Switch(config-if)# **spanning-tree mst 1 cost 30000** 

29.24 SPANNING-TREE MST PORT-PRIORITY

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.

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.

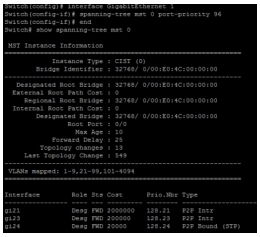
Switch#**configure terminal**

Switch(config)# **interface** {Interface-ID}

Switch(config-if)# **spanning-tree mst instance-id port-priority** *{priority}*

Switch(config-if)# **no spanning-tree mst instance-id** *{port-priority}*

Syntax	**spanning-tree mst instance-id port-priority** *{priority}* **no spanning-tree mst instance-id** *{port-priority}*
Parameter	**instance-id** Specify the instance ID. The valid range is from 0 to 15. *priority* Specify the interface priority on the specific instance.
Default	The default port priority on each instance is 128
Mode	Interface Configuration

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 Switch#**configure terminal** Switch(config)# **interface gi1** Switch(config-if)# **spanning-tree mst 0 port-priority 96** 

29.25 SPANNING-TREE MST PRIORITY

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.

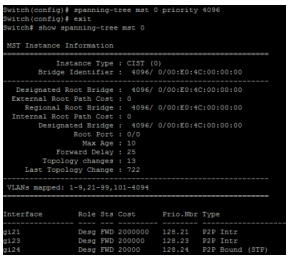
The value of bridge priority must be the multiple of 4096. A switch with the lowest priority is the root of the STP topology. For the configuration of bridge priority on the CIST (instance 0), it is equal to the command spanning-tree priority in the Global Configuration mode.

Switch#**configure terminal**

Switch(config)# **spanning-tree mst instance instance-id priority** *{priority}*

Switch(config)# **no spanning-tree mst instance instance-id** *{priority}*

Syntax	**spanning-tree mst instance instance-id priority** *{priority}* **no spanning-tree mst instance instance-id** *{priority}*
Parameter	**instance-id** Specify the instance ID. The valid range is from 0 to 15. *priority* Specify the bridge priority on the specific instance. The valid range is from 0 to 61440. It ensures the probability 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
Example	The following example modifies the bridge priority to 4096 on instance 0 and instance 1 individually. Switch#**configure terminal** Switch(config)# **spanning-tree mst 0 priority 4096** 

```
Switch(config)# spanning-tree mst 0 priority 4096
Switch(config)# exit
Switch# show spanning-tree mst 0

MST Instance Information
==========================================================================
            Instance Type : CIST (0)
        Bridge Identifier :  4096/ 0/00:E0:4C:00:00:00
--------------------------------------------------------------------------
  Designated Root Bridge :  4096/ 0/00:E0:4C:00:00:00
 External Root Path Cost : 0
    Regional Root Bridge :  4096/ 0/00:E0:4C:00:00:00
 Internal Root Path Cost : 0
       Designated Bridge :  4096/ 0/00:E0:4C:00:00:00
                 Root Port : 0/0
                   Max Age : 10
           Forward Delay : 25
       Topology changes : 13
   Last Topology Change : 722
--------------------------------------------------------------------------
VLANs mapped: 1-9,21-99,101-4094
==========================================================================

Interface        Role Sta Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
gi21             Desg FWD 2000000   128.21   P2P Intr
gi23             Desg FWD 200000    128.23   P2P Intr
gi24             Desg FWD 20000     128.24   P2P Bound (STP)
```

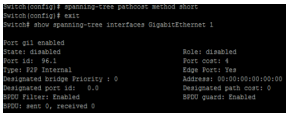
29.26 SPANNING-TREE PATHCOST METHOD

To set the spanning tree path cost method, use the command spanning-tree pathcost method in the Global Configuration mode.

If the short method is specified, the switch calculates the path cost in the range 1 through65535; otherwise, it calculates the path cost in the range 1 to 200000000.

Switch#**configure terminal**

Switch(config)# **spanning-tree pathcost method (long|short**)

Syntax	**spanning-tree pathcost method (long|short**)
Parameter	**long** The range for the path cost is from 1 to 200000000. **short** The range for the path cost is from 1 to 65535
Default	The default path cost method is long.
Mode	Global Configuration
Example	The following example modifies path cost method to short. Switch#**configure terminal** Switch(config)# **spanning-tree pathcost method short** 

29.27 SPANNING-TREE PORT-PRIORITY

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. The priority value must be the multiple of 16.

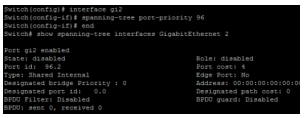
Switch#**configure terminal**

Switch(config)# **interface** {Interface-ID}

Switch(config-if)# **spanning-tree port-priority** *{priority}*

Switch(config-if)# **no spanning-tree port-priority** *{priority}*

Syntax	**spanning-tree port-priority** *{priority}* **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

Example	The following example modifies the port priority to 96 for the interface gi2 . Switch#**configure terminal** Switch(config)# **interface** gi2 Switch(config-if)# **spanning-tree port-priority 96** 

29.28 SPANNING-TREE PRIORITY

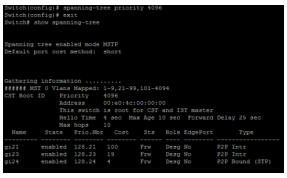
To configure the bridge priority, use the command spanning-tree mst priority in the Global Configuration mode. To restore the default configuration, use the no form of the command. The value of bridge priority must be the multiple of 4096. A switch with the lowest priority is the root of the STP topology. When switches with the same priority configuration in the environment, the switch with lowest MAC address would be selected as the root bridge.

Switch#**configure terminal**

Switch(config)# **spanning-tree priority** *{priority}*

Switch(config)# **no spanning-tree** *{priority}*

Syntax	**spanning-tree priority** *{priority}* **no spanning-tree** *{priority}*

Parameter	**instance-**id Specify the instance ID. The valid range is from 0 to 15. *priority* Specify the bridge STP priority. The valid range is from 0 to 61440. It ensures the probability 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 the STP topology.
Default	The default priority for the switch 32768.
Mode	Global Configuration
Example	The following example modifies the bridge priority to 4096. Switch#**configure terminal** Switch(config)# **spanning-tree priority 4096** 

29.29 SPANNING-TREE TX-HOLD-COUNT

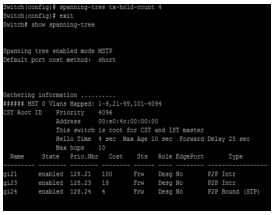
To limit the maximum numbers of packets transmission per second, use the command spanning-tree tx-hold-count in the Global Configuration mode. For the default configuration, use the **“no”** form of the command.

Switch#**configure terminal**

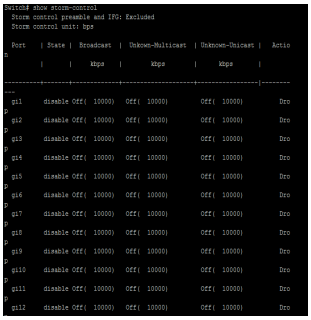
Switch(config)# **spanning-tree tx-hold-count** *{count}*

Switch(config)# **no spanning-tree tx-hold-count***{count}*

Syntax	**spanning-tree tx-hold-count** *{count}* **no spanning-tree tx-hold-count***{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

Example	The following example sets the tx-hold-count to 4. Switch#**configure terminal** Switch(config)# **spanning-tree tx-hold-count 4**  Switch(config)# spanning-tree tx-hold-count 4 Switch(config)# exit Switch# show spanning-tree Spanning tree enabled mode MSTP Default port cost method: short Gathering information ..... ###### MST 0 Vlans Mapped: 1-9,21-99,101-4094 CST Root ID Priority 4096 Address 00:e0:4c:00:00:00 This switch is root for CST and IST master Hello Time 4 sec Max Age 10 sec Forward Delay 25 sec Max hops 10 Name State Prio.Nbr Cost Sts Role EdgePort Type gi21 enabled 128.21 100 Frw Desg No P2P Intr gi23 enabled 128.23 19 Frw Desg No P2P Intr gi24 enabled 128.24 4 Frw Desg No P2P Bound (STP)

STORM CONTROL

Syntax	**show storm-control** **show storm-control interface** *{IF_PORTS}*
Parameter	*IF_PORTS* Specify port to show.
Mode	Privileged EXEC
Example	This example shows how to show storm control global configuration. Switch# **show storm-control** 

```
Switch# show storm-control
 Storm control preamble and IFG: Excluded
 Storm control unit: bps

 Port    | State |  Broadcast  |  Unknown-Multicast  | Unknown-Unicast |   Actio
n       |       |     Kbps    |        Kbps         |      Kbps       |
---------+-------+-------------+---------------------+-----------------+-------
---
 gi1     disable Off(  10000)   Off(  10000)         Off(  10000)         Dro
p
 gi2     disable Off(  10000)   Off(  10000)         Off(  10000)         Dro
p
 gi3     disable Off(  10000)   Off(  10000)         Off(  10000)         Dro
p
 gi4     disable Off(  10000)   Off(  10000)         Off(  10000)         Dro
p
 gi5     disable Off(  10000)   Off(  10000)         Off(  10000)         Dro
p
 gi6     disable Off(  10000)   Off(  10000)         Off(  10000)         Dro
p
 gi7     disable Off(  10000)   Off(  10000)         Off(  10000)         Dro
p
 gi8     disable Off(  10000)   Off(  10000)         Off(  10000)         Dro
p
 gi9     disable Off(  10000)   Off(  10000)         Off(  10000)         Dro
p
 gi10    disable Off(  10000)   Off(  10000)         Off(  10000)         Dro
p
 gi11    disable Off(  10000)   Off(  10000)         Off(  10000)         Dro
p
 gi12    disable Off(  10000)   Off(  10000)         Off(  10000)         Dro
```

30.2 STORM-CONTROL

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 disablestorm 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.

Switch#**configure terminal**

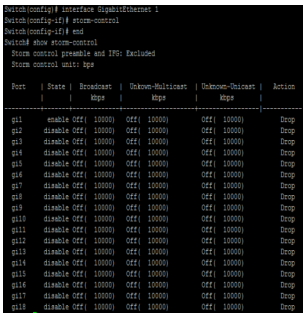
Switch(config)# **interface** {Interface-ID}

Switch(config-if)# **storm-control**

Switch(config-if)# **no storm-control**

Switch(config-if)# **storm-control (broadcast | unknown-unicast | unknown-multicast)**
no storm-control (broadcast | unknown-unicast | unknown-multicast)

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

Mode	Interface Configuration
Example	This example shows how to enable storm control on interface gi1. Switch#**configure terminal** 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#**configure terminal** 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** 

30.3 STORM-CONTROL ACTION

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.

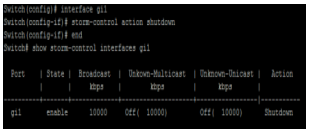
Switch#**configure terminal**

Switch(config)# **interface** {Interface-ID}

Switch(config-if)# **storm-control action (drop | shutdown)**

Switch(config-if)# **no storm-control action**

Syntax	**storm-control action (drop | shutdown)** **no storm-control action**
Parameter	drop shutdown Storm control rate calculates by octet-based
Default	Default storm control action is drop.
Mode	Interface Configuration

Example	This example shows how to configure storm control action to shutdown port on interface gi1. Switch#**configure terminal** Switch(config)# **interface gi1** Switch(config-if)# **storm-control action shutdown** This example shows how to show storm control action on interface gi1. Switch# **show storm-control interfaces gi1** 

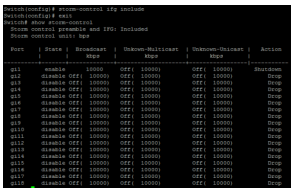
30.4 STORM-CONTROL IFG

Storm control mechanism will try to calculate ingress packets is exceed configured rate or not and do corresponding action. Use storm-control ifg command to include/exclude the preamble and inter frame gap into the calculating.

Switch#**configure terminal**

Switch(config)# **storm-control ifg (include | exclude)**

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

Example	This example shows how to configure storm inter frame gap to include. Switch#**configure terminal** Switch(config)# **storm-control ifg include** This example shows how to show storm control global configuration. Switch# **show storm-control** 

30.5 STORM-CONTROL LEVEL

Each control type is allowed to have different storm control rate. Use **“storm-control (broadcast|unknown-unicast|unknown-multicast)level”** command to configure it. Use **“no”** form to restore to default rate.

Switch#**configure terminal**

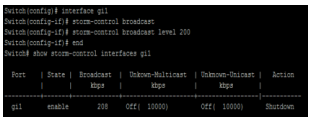
Switch(config)# **interface** {Interface-ID}

Switch(config-if)# **storm-control (broadcast | unknown-unicast | unknown-multicast) level** <*1-1000000*>

Switch(config-if)# **no storm-control (broadcast | unknown-unicast | unknown-multicast) level**

Syntax	**storm-control (broadcast | unknown-unicast | unknown-multicast) level**<*1-1000000*> **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. For bps, range is 16-1000000 For pps, range is 1-262143
Default	Default broadcast storm control rate is 10000. Default unknown multicast storm control rate is 10000. Default unknown unicast storm control rate is 10000.
Mode	Interface Configuration

Example	This example shows how to enable broadcast storm control and configure broadcast storm control rate to 200. Switch#**configure terminal** 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** 

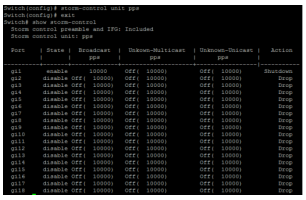
30.6 STORM-CONTROL UNIT

Storm control mechanism will try to calculate ingress packets is exceed configured rate or not and do corresponding action. Use storm-control unit command to change the unit of calculating method.

Switch#**configure terminal**

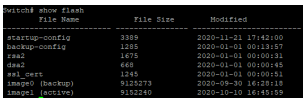
Switch(config)# **storm-control unit (bps | pps)**

Syntax	**storm-control unit (bps | pps)**
Parameter	bps Storm control rate calculates by octet-based pps Storm control rate calculates by packet-based
Default	Default storm control unit is bps
Mode	Global Configuration

Example	This example shows how to configure storm control rate unit as pps. Switch#**configure terminal** Switch(config)# **storm-control unit pps** This example shows how to show storm control global configuration. Switch# **show storm-control** 

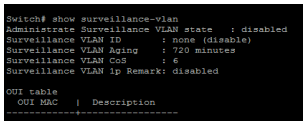
```
Switch(config)# storm-control unit pps
Switch(config)# exit
Switch# show storm-control
 Storm control preamble and IFG: Included
 Storm control unit: pps

 Port    | State |  Broadcast  |  Unknown-Multicast  | Unknown-Unicast |   Action
         |       |     pps     |         pps         |       pps       |
---------+-------+-------------+---------------------+-----------------+----------
 gi1       enable     10000    Off( 10000)          Off( 10000)        Shutdown
 gi2       disable Off( 10000)  Off( 10000)          Off( 10000)        Drop
 gi3       disable Off( 10000)  Off( 10000)          Off( 10000)        Drop
 gi4       disable Off( 10000)  Off( 10000)          Off( 10000)        Drop
 gi5       disable Off( 10000)  Off( 10000)          Off( 10000)        Drop
 gi6       disable Off( 10000)  Off( 10000)          Off( 10000)        Drop
 gi7       disable Off( 10000)  Off( 10000)          Off( 10000)        Drop
 gi8       disable Off( 10000)  Off( 10000)          Off( 10000)        Drop
 gi9       disable Off( 10000)  Off( 10000)          Off( 10000)        Drop
 gi10      disable Off( 10000)  Off( 10000)          Off( 10000)        Drop
 gi11      disable Off( 10000)  Off( 10000)          Off( 10000)        Drop
 gi12      disable Off( 10000)  Off( 10000)          Off( 10000)        Drop
 gi13      disable Off( 10000)  Off( 10000)          Off( 10000)        Drop
 gi14      disable Off( 10000)  Off( 10000)          Off( 10000)        Drop
 gi15      disable Off( 10000)  Off( 10000)          Off( 10000)        Drop
 gi16      disable Off( 10000)  Off( 10000)          Off( 10000)        Drop
 gi17      disable Off( 10000)  Off( 10000)          Off( 10000)        Drop
 gi18      disable Off( 10000)  Off( 10000)          Off( 10000)        Drop
```

SYSTEM FILE

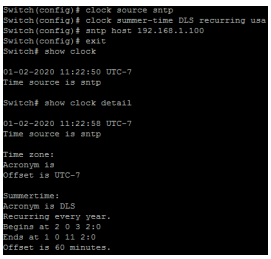
Example	This example shows how to show all files status stored in flash. Switch# **show flash** 

```
Switch# show flash
        File Name              File Size       Modified
------------------------ --------------- -------------------
startup-config           3389            2020-11-21 17:42:00
backup-config            1285            2020-01-01 00:13:57
rsa2                     1675            2020-01-01 00:00:31
dsa2                     668             2020-01-01 00:00:45
ssl_cert                 1245            2020-01-01 00:00:51
image0 (backup)          9125273         2020-09-30 16:28:18
image1 (active)          9152240         2020-10-10 16:45:59
```

SURVEILLANCE VLAN

Syntax	**show surveillance-vlan** **show surveillance-vlan interfaces [IF_PORTS]**
Parameter	*IF_PORTS* Specifies interfaces to display surveillance VLAN settings in OUI mode
Mode	Privileged EXEC
Example	The following example show how to display surveillance vlan OUI mode settings Switch# **show surveillance-vlan** 

TIME

Syntax	**show clock [detail]**
Parameter	detail Show more detail information of clock
Mode	Privileged EXEC
Example	The example shows how to show clock of switch and detail information. Switch#**configure terminal** Switch(config)# **clock source sntp** Switch(config)# **clock summer-time DLS recurring usa** Switch(config)# **sntp host 192.168.1.100** Switch# **show clock** Switch# **show clock detail**  Switch(config)# clock source sntp Switch(config)# clock summer-time DLS recurring usa Switch(config)# sntp host 192.168.1.100 Switch(config)# exit Switch# show clock 01-02-2020 11:22:50 UTC-7 Time source is sntp Switch# show clock detail 01-02-2020 11:22:58 UTC-7 Time source is sntp Time zone: Acronym is Offset is UTC-7 Summertime: Acronym is DLS Recurring every year. Begins at 2 0 3 2:0 Ends at 1 0 11 2:0 Offset is 60 minutes.

33.6 SNTP

Use the sntp command to set remote SNTP server. Use the no form of this command to default setting.You can verify your setting by entering the show sntp Privileged EXEC command.

Switch#**configure terminal**

Switch(config)# **sntp host HOSTNAME [***port <1-65535>***]**

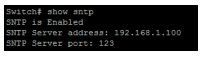
Switch(config)# **no sntp**

Syntax	**sntp host HOSTNAME [***port <1-65535>***]** **no sntp**
Parameter	HOSTNAME Specify ip address or hostname of sntp server sntp Specify server port of sntp server
Default	No default SNTP server defined. Default server port is 123 when server created.
Mode	Global Configuration
Example	The example shows how to set remote SNTP server of switch. Switch#**configure terminal** Switch(config)# **clock source sntp** Switch(config)# **sntp host 192.168.1.100** Switch(config)# **show sntp** 

33.7 SHOW SNTP

Use the show sntp command to remote SNTP server information.

Switch# **show sntp**

Syntax	**show sntp**
Mode	Privileged EXEC
Example	The example shows how to show remote SNTP server. Switch# **show sntp** 

UDLD

Unidirectional Link Detection (**UDLD**) is a data link layer protocol from Cisco Systems to monitor the physical configuration of the cables and detect unidirectional links. **UDLD** complements the Spanning Tree Protocol which is used to eliminate switching loops.

UDLD allow two switches to verify if they can both send and receive data on a point-to-point connection. UDLD works with the Layer 1 (L1) mechanisms to determine the physical status of a link. UDLD can be run on both fiber optic and twisted-pair copper links.

All connected devices must support UDLD for the protocol to successfully identify and disable unidirectional links. When UDLD detects a unidirectional link, it administratively shuts down the affected port and alerts administrator. Unidirectional links can cause a variety of problems, including spanning-tree topology loop

If two devices, A and B, are connected via a pair of optical fibers, one used for sending from A to B and other for sending from B to A, the link is bidirectional (two-way). If one of this fiber is broken, the link has become one-way or unidirectional. The goal of the UDLD protocol is to detect a broken bidirectional link.

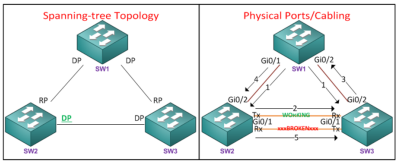


Fig 34.1 Spanning Tree Topology

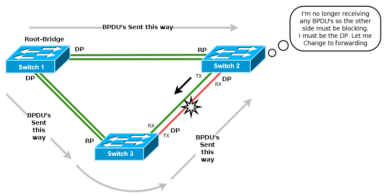


Fig 34.2 BPDU Route

UDLD supports two modes of operation: normal (the default) and aggressive. In normal mode, UDLD can detect unidirectional links due to misconnected ports on fiber-optic connections.

Modes of Operation

UDLD supports two modes of operation: normal (the default) and aggressive.

In normal mode, UDLD can detect unidirectional links due to misconnected interfaces on fiber-optic connections.

In aggressive mode, UDLD can also detect unidirectional links due to one-way traffic on fiber-optic and twisted-pair links and to misconnected interfaces on fiber-optic links. In UDLD aggressive mode, when a port on a bidirectional link that has a UDLD neighbor relationship established stops receiving UDLD packets, UDLD tries to reestablish the connection with the neighbor. After eight failed retries, the port is disabled.

34.1 ERRDISABLE RECOVERY CAUSE UDLD

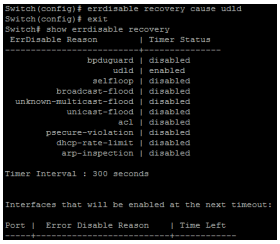
Use the errdisable recovery cause udld to enable auto recovery of UniDirectional Link Detection (UDLD). Use the **“no”** to disable it.

Switch#c**onfigure terminal**

Switch(config)# **errdisable recovery cause udld**

Switch(config)# **no errdisable recovery cause udld**

Syntax	**errdisable recovery cause udld** **no errdisable recovery cause udld**
Default	Error disable auto recovery is disabled by default.
Mode	Global EXEC

Example	The example shows how to enable auto recovery of UniDirectional Link Detection (UDLD). Switch#**configure terminal** Switch(config)# **errdisable recovery cause udld** Switch# **show errdisable recovery** 

```
Switch(config)# errdisable recovery cause udld
Switch(config)# exit
Switch# show errdisable recovery
 ErrDisable Reason        | Timer Status
--------------------------+--------------
              bpduguard | disabled
                   udld | enabled
               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
-----+--------------------------+-----------
```

34.2 UDLD

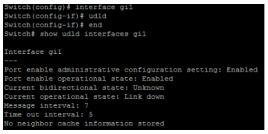
Use the udld command to enable UniDirectional Link Detection (UDLD) normal mode of interface. Use the **“no”** form of this command to restore to default setting. You can verify your setting by entering the show udld interface Privileged EXEC command.

Switch#**configure terminal**

Switch(config)#**interface** {Interface-ID}

Switch(config-if)# **udld**

Switch(config-if)# **no udld**

Syntax	**udld** **no udld**
Mode	Interface Configuration
Example	The example shows how to enable UniDirectional Link Detection (UDLD) normal mode in interface gi1. Switch#**configure terminal** Switch(config)# **interface** gi1 Switch(config-if)# **udld** Switch# **show udld interfaces** gi1 

34.3 UDLD AGGRESSIVE

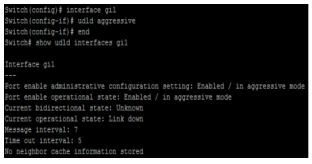
Use the udld aggressive command to enable UniDirectional Link Detection (UDLD) aggressive mode of interface. Use the **“no”** form of this command to restore to default setting. You can verify your setting by entering the show udld interface Privileged EXEC command.

Switch#**configure terminal**

Switch(config)#**interface** {Interface-ID}

Switch(config-if)# **udld aggressive**

Switch(config-if)# **no udld aggressive**

Syntax	**udld aggressive** **no udld aggressive**
Mode	Interface Configuration
Example	The example shows how to enable udld aggressive mode in interface gi1. Switch#**configure terminal** Switch(config)# **interface** gi1 Switch(config-if)# **udld aggressive** Switch# **show udld interfaces** gi1 

34.4 UDLD MESSAGE TIME

Use the udld message time to set interval of UniDirectional Link Detection (UDLD) sent message.

Switch#**configure terminal**

Switch(config)# **udld message time message-time-interval**

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
Example	The example shows how to set interval of UniDirectional Link Detection (UDLD) message. Switch#**configure terminal** Switch(config)# **udld message time 30**

34.5 UDLD RESET

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. 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.

Switch# **udld reset**

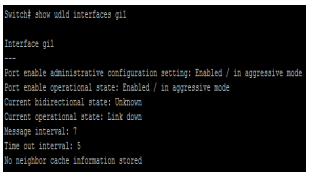
Syntax	**udld reset**
Mode	Privileged EXEC
Example	The example shows how to reset all interfaces disabled by UDLD Switch# **udld reset**

34.6 SHOW UDLD

Use the show udld command to display UniDirectional Link Detection (UDLD) administrative and operational status for all ports or the specified port.

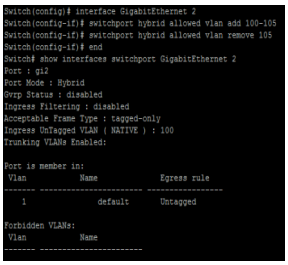
Switch# **show udld**

Switch# **show udld interfaces** {*IF_NMLPORTS}*

Syntax	**show udld** **show udld interfaces** {*IF_NMLPORTS}*
Parameter	*{IF_NMLPORTS}* Specify the normal interfaces to display udld information
Mode	Privileged EXEC
Example	The example shows how to show UniDirectional Link Detection (UDLD) settings and operational status of interface gi1. Switch# **show udld interfaces gi1**  Switch# show udld interfaces gi1 Interface gi1 --- Port enable administrative configuration setting: Enabled / in aggressive mode Port enable operational state: Enabled / in aggressive mode Current bidirectional state: Unknown Current operational state: Link down Message interval: 7 Time out interval: 5 No neighbor cache information stored

VLAN

Syntax	**switchport hybrid allowed vlan add** *{VLAN-LIST}* **switchport hybrid allowed vlan remove** *{ VLAN-LIST}* **[(tagged|untagged)]**
Parameter	*VLAN-LIST* Specifies the VLAN list to be added or remove. **(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

Example	This example sets port GigabitEthernet 2 VLAN to join the VLAN 100 as tagged member. Switch#**configure terminal** Switch(config)# **interface** GigabitEthernet 2 Switch(config-if)# **switchport hybrid allowed vlan add 100-105** Switch(config-if)# **switchport hybrid allowed vlan remove 105** Switch# **show interfaces switchport GigabitEthernet 2** 

35.8 SWITCHPORT ACCESS VLAN

Use the switchport access vlan port configuration command to set native vlan on interface. The vlan will be pvid on interface as well. Use the **“no”** form of this command to restore to default vlan. You can verify your setting by entering the show interfaces switchport Privileged EXEC command.

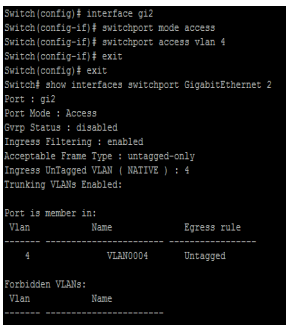
Switch#**configure terminal**

Switch (config)#**interface** {Interface-ID}

Switch(config-if)# **switchport access vlan** *<1-4094>*

Switch(config-if)# **no 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

Example	This example sets Access port gi10 native VLAN ID to 100. Switch#**configure terminal** Switch(config)# **interface** gi2 Switch(config-if)# **switchport mode access** Switch(config-if)# **switchport access vlan** 4 Switch# **show interfaces switchport** GigabitEthernet 2  Switch(config)# interface gi2 Switch(config-if)# switchport mode access Switch(config-if)# switchport access vlan 4 Switch(config-if)# exit Switch(config)# exit Switch# show interfaces switchport GigabitEthernet 2 Port : gi2 Port Mode : Access Gvrp Status : disabled Ingress Filtering : enabled Acceptable Frame Type : untagged-only Ingress UnTagged VLAN (NATIVE) : 4 Trunking VLANs Enabled: Port is member in: Vlan Name Egress rule ------- ------------------------ ----------------- 4 VLAN0004 Untagged Forbidden VLANs: Vlan Name ------- ----------------------

35.9 SWITCHPORT TUNNEL VLAN

Use the switchport tunnel vlan port configuration command to set dot1q tunnel vlan on interface. The vlan will be pvid on interface as well. Use the **“no”** form of this command to remove vlan on interface. The tunnel vlan id will set to reserve vlan 4095. You can verify your setting by entering the show interfaces switchport Privileged EXEC command.

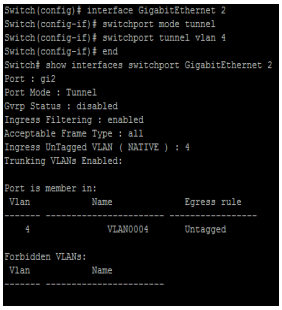
Switch#**configure terminal**

Switch (config)#**interface** {Interface-ID}

Switch(config-if)# **switchport tunnel vlan** <*1-4094*>

Switch(config-if)# **no switchport tunnel vlan**

Syntax	**switchport tunnel vlan** <*1-4094*> **no switchport tunnel vlan**
Parameter	<*1-4094*>Specifies the tunnel VLAN ID.
Default	Default is vlan 1
Mode	Port Configuration

Example	This example sets Tunnel port GigabitEthernet 2 native VLAN to 4. Switch#**configure terminal** Switch(config)# **interface** GigabitEthernet 2 Switch(config-if)# **switchport mode tunnel** Switch(config-if)# **switchport tunnel vlan** 4 Switch# **show interfaces switchport** GigabitEthernet 2  Switch(config)# interface GigabitEthernet 2 Switch(config-if)# switchport mode tunnel Switch(config-if)# switchport tunnel vlan 4 Switch(config-if)# end Switch# show interfaces switchport GigabitEthernet 2 Port : gi2 Port Mode : Tunnel Gvrp Status : disabled Ingress Filtering : enabled Acceptable Frame Type : all Ingress UnTagged VLAN (NATIVE) : 4 Trunking VLANs Enabled: Port is member in: Vlan Name Egress rule ------- ------------------------ ----------------- 4 VLAN0004 Untagged Forbidden VLANs: Vlan Name ------- ------------------------

35.10 SWITCHPORT TRUNK NATIVE VLAN

Use the switchport trunk native vlan port configuration command to set native vlan on interface. Use the **“no”** form of this command to restore to default vlan. You can verify your setting by entering the show interfaces switchport Privileged EXEC command.

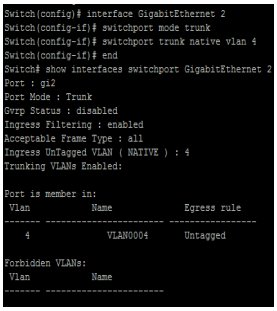
Switch#**configure terminal**

Switch (config)#**interface** {Interface-ID}

Switch(config-if)# **switchport trunk native vlan** *<1-4094>*

Switch(config-if)# **no switchport trunk native vlan**

Syntax	**switchport trunk native vlan** *<1-4094>* **no switchport trunk native vlan**
Parameter	*<1-4094>*Specifies the native VLAN ID.
Default	Default is vlan 1
Mode	Default is vlan 1

Example	This example sets Trunk port GigabitEthernet 2 native VLAN to 4. Switch#**configure terminal** Switch(config)# **interface** GigabitEthernet 2 Switch(config-if)# **switchport mode trunk** Switch(config-if)# **switchport trunk native vlan** 4 Switch# **show interfaces switchport** GigabitEthernet 2 

```
Switch(config)# interface GigabitEthernet 2
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport trunk native vlan 4
Switch(config-if)# end
Switch# show interfaces switchport GigabitEthernet 2
Port : gi2
Port Mode : Trunk
Gvrp Status : disabled
Ingress Filtering : enabled
Acceptable Frame Type : all
Ingress UnTagged VLAN ( NATIVE ) : 4
Trunking VLANs Enabled:

Port is member in:
 Vlan            Name             Egress rule
------- ---------------------- ----------------
    4              VLAN0004       Untagged

Forbidden VLANs:
 Vlan            Name
------- ----------------------
```

35.11 SWITCHPORT TRUNK ALLOWED VLAN

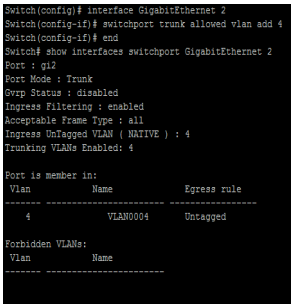
Use the switchport trunk allow vlan add port configuration command to allow vlan on interface. Use the switchport trunk allows vlan remove port configuration command to remove vlan on interface. You can verify your setting by entering the show interfaces switchport Privileged EXEC command.

Switch#**configure terminal**

Switch (config)#**interface** {Interface-ID}

Switch(config-if)# **switchport trunk allowed vlan (add | remove) (VLAN-LIST | all)**

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.
Mode	Port Configuration

Example	This example sets Trunk port GigabitEthernet 2 to add the allowed VLAN 4. Switch# **configure** Switch(config)# **interface** GigabitEthernet 2 Switch(config-if)# **switchport trunk allowed vlan add** 4 Switch# **show interfaces switchport** GigabitEthernet 2  Switch(config)# interface GigabitEthernet 2 Switch(config-if)# switchport trunk allowed vlan add 4 Switch(config-if)# end Switch# show interfaces switchport GigabitEthernet 2 Port : gi2 Port Mode : Trunk Gvrp Status : disabled Ingress Filtering : enabled Acceptable Frame Type : all Ingress UnTagged VLAN (NATIVE) : 4 Trunking VLANs Enabled: 4 Port is member in: Vlan Name Egress rule ------- ---------- ---------- 4 VLAN0004 Untagged Forbidden VLANs: Vlan Name ------- ----------

35.12 SWITCHPORT DEFAULT-VLAN TAGGED

Use the switchport default vlan tagged port configuration command to become default vlan tagged member. Use the **“no”** switchport default vlan tagged port configuration command to restore to default. You can verify your setting by entering the show interfaces switchport Privileged EXEC command.

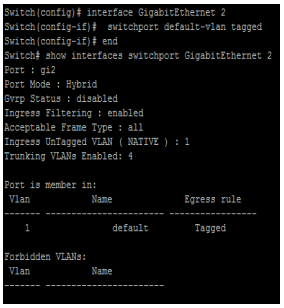
Switch#**configure terminal**

Switch (config)#**interface** {Interface-ID}

Switch(config-if)# **switchport default-vlan tagged**

Switch(config-if)# **no switchport default-vlan tagged**

Syntax	**switchport default-vlan tagged** **no switchport default-vlan tagged**
Default	Default is untagged
Mode	Port Configuration

Example	This example sets Trunk port GigabitEthernet 2 membership with the default VLAN to tag. Switch#**configure terminal** Switch(config)# **interface** GigabitEthernet 2 Switch(config-if)# **switchport default-vlan tagged** Switch# **show interfaces switchport** GigabitEthernet 2  Switch(config)# interface GigabitEthernet 2 Switch(config-if)# switchport default-vlan tagged Switch(config-if)# end Switch# show interfaces switchport GigabitEthernet 2 Port : gi2 Port Mode : Hybrid Gvrp Status : disabled Ingress Filtering : enabled Acceptable Frame Type : all Ingress UnTagged VLAN (NATIVE) : 1 Trunking VLANs Enabled: 4 Port is member in: Vlan Name Egress rule ------- ---------- ---------- 1 default Tagged Forbidden VLANs: Vlan Name ------- ----------

35.13 SWITCHPORT FORBIDDEN DEFAULT-VLAN

Use the switchport forbidden default-vlan port configuration command to forbid default-vlan on interface. Use the **“no”** switchport forbidden default-vlan port configuration command to restore to default. You can verify your setting by entering the show interfaces switchport Privileged EXEC command.

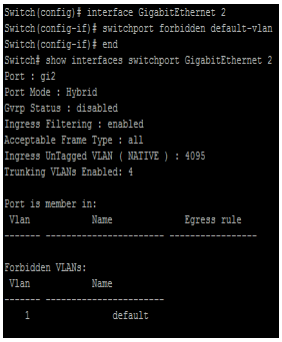
Switch#**configure terminal**

Switch (config)#**interface** {Interface-ID}

Switch(config-if)# **switchport forbidden default-vlan**

Switch(config-if)# **no switchport forbidden default-vlan**

Syntax	**switchport forbidden default-vlan** **no switchport forbidden default-vlan**
Default	Default is allowed
Mode	Port Configuration

Example	This example sets the membership of the default VLAN with port GigabitEthernet 2 to Forbidden. Switch#**configure terminal** Switch(config)# **interface** GigabitEthernet 2 Switch(config-if)# **switchport forbidden default-vlan** Switch# **show interfaces switchport** GigabitEthernet 2  Switch(config)# interface GigabitEthernet 2 Switch(config-if)# switchport forbidden default-vlan Switch(config-if)# end Switch# show interfaces switchport GigabitEthernet 2 Port : gi2 Port Mode : Hybrid Gvrp Status : disabled Ingress Filtering : enabled Acceptable Frame Type : all Ingress UnTagged VLAN (NATIVE) : 4095 Trunking VLANs Enabled: 4 Port is member in: Vlan Name Egress rule ------- ---------- ---------- Forbidden VLANs: Vlan Name ------- ---------- 1 default

35.14 SWITCHPORT FORBIDDEN VLAN

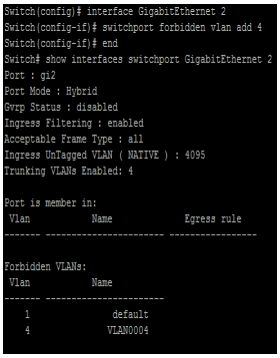
Uses the switchport forbidden vlan add port configuration command to forbid vlan on interface. Use the switchport forbidden vlan remove port configuration command to accept vlan on interface. You can verify your setting by entering the show interfaces switchport Privileged EXEC command.

Switch#**configure terminal**

Switch (config)#**interface** {Interface-ID}

Switch(config-if)# **switchport forbidden vlan (add | remove)** *VLAN-LIST*

Syntax	**switchport forbidden vlan (add | remove)** *VLAN-LIST*
Parameter	(add | remove) Add or remove forbidden membership. *VLAN-LIST* Specify the VLAN list.
Mode	Port Configuration

Example	This example sets the membership of the VLAN 4 with port GigabitEthernet 2 to Forbidden. Switch#**configure terminal** Switch(config)# **interface** GigabitEthernet 2 Switch(config-if)# **switchport forbidden vlan add** 4 Switch# **show interfaces switchport** GigabitEthernet 2  Switch(config)# interface GigabitEthernet 2 Switch(config-if)# switchport forbidden vlan add 4 Switch(config-if)# end Switch# show interfaces switchport GigabitEthernet 2 Port : gi2 Port Mode : Hybrid Gvrp Status : disabled Ingress Filtering : enabled Acceptable Frame Type : all Ingress UnTagged VLAN (NATIVE) : 4095 Trunking VLANs Enabled: 4 Port is member in: Vlan Name Egress rule ------- ---------- ---------- Forbidden VLANs: Vlan Name ------- ---------- 1 default 4 VLAN0004

35.15 SWITCHPORT VLAN TPID

Use the switchport vlan tpid port configuration command to set TPID on interface. You can verify your setting by entering the show running-config Privileged EXEC command.

Switch#**configure terminal**

Switch (config)#**interface** {Interface-ID}

Switch(config-if)# **switchport vlan tpid (0x8100|0x88a8|0x9100|0x9200)**

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
Example	This example sets the TPID to 0x9100 on interface GigabitEthernet 2. Switch#**configure terminal** Switch(config)# **interface** GigabitEthernet 2 Switch(config-if)# **switchport vlan tpid 0x9100** 

35.16 MANAGEMENT-VLAN

Use the management vlan Global Configuration mode command to set management vlan id. Vlan id must be created first. Use the **“no”** form of this command to restore to default setting. You can verify your setting by entering the show management-vlan Privileged EXEC command.

Switch#**configure terminal**

Switch(config)# **management-vlan vlan** *<1-4094>*

Switch(config)# **no management-vlan**

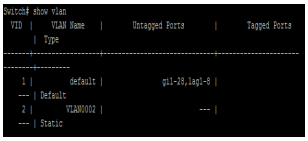
Syntax	**management-vlan vlan** *<1-4094>* **no management-vlan**
Parameter	*<1-4094>* Specify the VLAN ID of management-vlan.
Default	Default management vlan is 1.
Mode	Global Configuration

Example	The following example specifies that management vlan 2 is created Switch#**configure terminal** Switch(config)# **vlan** 2 Switch(config)# **management-vlan vlan** 2 The following example specifies that management-vlan is restored to be default VLAN. Switch(config)# **no management-vlan**

35.17 SHOW VLAN

Display information about vlan entry.

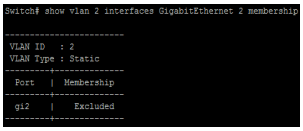
Switch# **show vlan [(VLAN-LIST|dynamic|static)]**

Syntax	**show vlan [(VLAN-LIST|dynamic|static)]**
Parameter	(VLANLIST|dynamic|static)Specify vlan id to show information or show all static or dynamic vlan entries.
Mode	Privileged EXEC
Example	The following example specifies that show vlan Switch# **show vlan** 

35.18 SHOW VLAN INTERFACE MEMBERSHIP

Display information about vlan membership on interfaces.

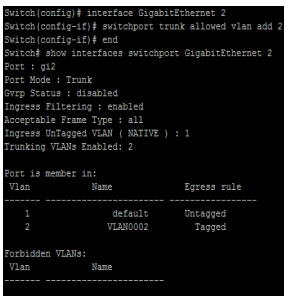
Switch# **show vlan VLAN-LIST interfaces** *{IF_PORTS}* **membership**

Syntax	**show vlan VLAN-LIST interfaces** *{IF_PORTS}* **membership**
Parameter	Specify vlan to show *IF_PORTS* Specify interface is to show
Mode	Privileged EXEC
Example	The following example specifies that show vlan interface membership Switch# **show vlan 2 interfaces** GigabitEthernet 2 **membership** 

35.19 SHOW INTERFACE SWITCHPORT

Display information about default vlan.

Switch# **show interface switchport interfaces** {*IF*_PORTS}

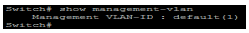
Syntax	**show interface switchport interfaces** {*IF*_PORTS}
Default	*IF_PORTS* Specify interfaces protocol vlan to display
Mode	Privileged EXEC
Example	The following example specifies that show interfacce switchport. Switch#**configure terminal** Switch(config)# **interface** GigabitEthernet 2 Switch(config-if)# **switchport trunk allowed vlan add** 2 Switch# **show interfaces switchport** GigabitEthernet 2 

```
Switch(config)# interface GigabitEthernet 2
Switch(config-if)# switchport trunk allowed vlan add 2
Switch(config-if)# end
Switch# show interfaces switchport GigabitEthernet 2
Port : gi2
Port Mode : Trunk
Gvrp Status : disabled
Ingress Filtering : enabled
Acceptable Frame Type : all
Ingress UnTagged VLAN ( NATIVE ) : 1
Trunking VLANs Enabled: 2

Port is member in:
 Vlan            Name                Egress rule
------- ----------------------- ----------------
    1               default       Untagged
    2              VLAN0002         Tagged

Forbidden VLANs:
 Vlan            Name
------- -----------------------
```

35.20 SHOW MANAGEMENT-VLAN

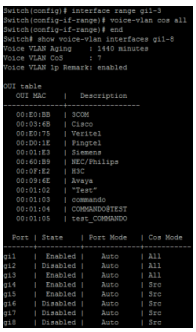
Display information about management vlan.

Switch# **show management-vlan**

Syntax	**show management-vlan**
Mode	Privileged EXEC
Example	The following example specifies that show management vlan Switch# **show management-vlan** 

VOICE VLAN

Syntax	**voice-vlan cos (src | all)** **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

Example	The following example how to configure voice packet QoS attributes on an interface, Switch#**configure terminal** Switch(config)#**interface range** gi1-3 Switch(config-if)#**voice-vlan cos all** Switch# **show voice-vlan interfaces gi1-8** 

```
Switch(config)# interface range gi1-3
Switch(config-if-range)# voice-vlan cos all
Switch(config-if-range)# end
Switch# show voice-vlan interfaces gi1-8
Voice VLAN Aging     : 1440 minutes
Voice VLAN CoS       : 7
Voice VLAN ip Remark: enabled

OUI table
   OUI MAC      |   Description
----------------+----------------
   00:E0:BB   | 3COM
   00:03:6B   | Cisco
   00:E0:75   | Veritel
   00:D0:1E   | Pingtel
   00:01:E3   | Siemens
   00:60:B9   | NEC/Philips
   00:0F:E2   | H3C
   00:09:6E   | Avaya
   00:01:02   | "Test"
   00:01:03   | commando
   00:01:04   | COMMANDO@TEST
   00:01:05   | test_COMMANDO

 Port | State    | Port Mode   | Cos Mode
------+----------+-------------+----------
gi1    | Enabled |    Auto     | All
gi2    | Disabled |   Auto     | All
gi3    |  Enabled |   Auto     | All
gi4    |  Enabled |   Auto     | Src
gi5    |  Enabled |   Auto     | Src
gi6    | Disabled |   Auto     | Src
gi7    | Disabled |   Auto     | Src
gi8    | Disabled |   Auto     | Src
```

36.7 VOICE-VLAN MODE

Use the voice-vlan mode global configuration command to configure the voice VLAN mode for interface. Use the **“no”** form to restore to default mode. You can verify your setting by entering the show voice-vlan interfaces Privileged EXEC command.

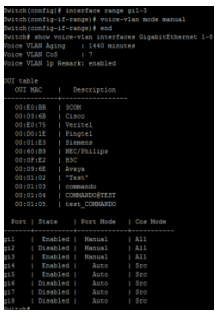
Switch#**configure terminal**

Switch(config)#**interface** {Interface-ID}

Switch(config-if)#**voice-vlan mode (auto|manual)**

Switch(config-if)#**no voice-vlan mode**

Syntax	**voice-vlan mode (auto|manual)** **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

Example	The following example how to configure voice mode to manual Switch#**configure terminal** Switch(config)#**interface range** gi1-3 Switch(config-if)#**voice-vlan mode manual** Switch# **show voice-vlan interfaces** GigabitEthernet 1-8 

```
Switch(config)# interface range gi1-3
Switch(config-if-range)# voice-vlan mode manual
Switch(config-if-range)# end
Switch# show voice-vlan interfaces GigabitEthernet 1-8
Voice VLAN Aging    : 1440 minutes
Voice VLAN CoS      : 7
Voice VLAN lp Remark: enabled

OUI table
   OUI MAC     |   Description
-------------------------------
   00:E0:BB    | 3COM
   00:03:6B    | Cisco
   00:E0:75    | Veritel
   00:D0:1E    | Pingtel
   00:01:E3    | Siemens
   00:60:B9    | NEC/Philips
   00:0F:E2    | H3C
   00:09:6E    | Avaya
   00:01:02    | "Test"
   00:01:03    | commando
   00:01:04    | COMMANDO@TEST
   00:01:05    | test_COMMANDO

 Port | State     | Port Mode   | Cos Mode
------+-----------+-------------+----------
gi1    |  Enabled  |  Manual     | All
gi2    |  Disabled |  Manual     | All
gi3    |  Enabled  |  Manual     | All
gi4    |  Enabled  |  Auto       | Src
gi5    |  Enabled  |  Auto       | Src
gi6    |  Disabled |  Auto       | Src
gi7    |  Disabled |  Auto       | Src
gi8    |  Disabled |  Auto       | Src
```

36.8 VOICE-VLAN AGING-TIME

Use the voice vlan aging-time global configuration command to configure the voice VLAN aging timeout. Use the **“no”** form to restore to default time. You can verify your setting by entering the show voice vlan Privileged EXEC command.

Switch#**configure terminal**

Switch(config)# **voice-vlan aing-time** <*30-65536*>

Switch(config)# **no voice-vlan aing-time**

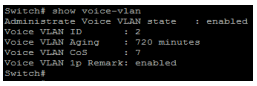
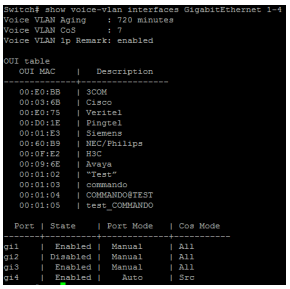
Syntax	**voice-vlan aing-time** *<30-65536>* **no voice-vlan aing-time**
Parameter	*<30-65536>* Specify the voice VLAN aging timeout interval in minutes
Default	The default aging-timeout value is 1440 minutes
Mode	Global Configuration
Example	The following example shows how to set aging time. Switch#**configure terminal** Switch(config)# **voice-vlan aging-time** 720 Switch# **show voice-vlan** Switch(config)# voice-vlan aging-time 720 Switch(config)# end Switch# show voice-vlan Administrate Voice VLAN state : enabled Voice VLAN ID : 2 Voice VLAN Aging : 720 minutes Voice VLAN CoS : 7 Voice VLAN ip Remark: enabled

36.9 SHOW VOICE-VLAN

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.

Switch# **show voice-vlan**

Switch# **show voice-vlan interfaces***{IF_PORTS}*

Syntax	**show voice-vlan** **show voice-vlan interfaces***{IF_PORTS}*
Parameter	*IF_PORTS* Specifies interfaces to display voice VLAN settings in oui mode
Mode	Privileged EXEC
Example	The following example show how to display voice vlan oui mode settings Switch# **show voice-vlan**  Switch# **show voice-vlan interfaces GigabitEthernet 1-4** 

STATIC ROUTING

What does Static Routing mean?

Static routing is a type of network routing technique. Static routing is not a routing protocol; instead, it is the manual configuration and selection of a network route, usually managed by the network administrator.

Static Routing

Routing is one of the most essential procedures in data communication. It ensures that data travels from one network to another with optimal speed and minimal delay, and that its integrity is maintained in the process.Static routing is considered the simplest form of routing.

Broadly, routing is performed in two different ways:

• Dynamic routing continuously updates its routing table with paths and their cost/metric, while making optimal routing decisions based on changing network operating environments.

• Static routing performs routing decisions with preconfigured routes in the routing table, which can be changed manually only by administrators. Static routes are normally implemented in those situations where the choices in route selection are limited, or there is only a single default route available. Also, static routing can be used if you have only few devices for route configuration and there is no need for route change in the future.

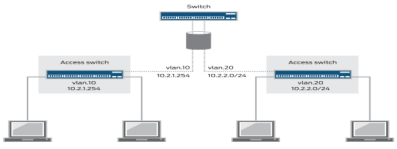


Fig 37.1 Static route for inter LAN routing

37.1 INTERFACE

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.

Switch#**configure terminal**

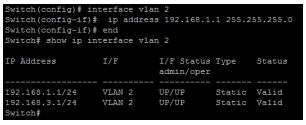
Switch(config)# **interface vlan**{VLAN-ID}

Switch(config-if)# **ip address** {ip-addr} {mask}

Switch(config)# **no interface vlan** {VLAN-ID}

Switch(config-if)# **no ip address**

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

Example	The following example shows how to config ip interface. Switch#**configure terminal** Switch(config)# **interface vlan** 2 Switch(config-if)# **ip address** 192.168.3.1 255.255.255.0 Switch# **show ip interface vlan** 2 

37.2 IPV4 ROUTES

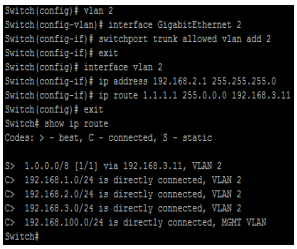
Use the ip route command in global mode to configure a static route rule. Use the **“no”** ip route command to delete a static routing rule.You can verify your setting by entering the show ip route Privileged EXEC command.

Switch#**configure terminal**

Switch(config)# **ip route** {dest-ipaddr} **mask** {router-ipaddr}

Switch(config)# **no ip route** {dest-ipaddr} **mask** {router-ipaddr}

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 mode.

Example	The following example shows how to configure a static route. Switch#**configure terminal** Switch(config)# **vlan** 2 Switch(config)# **interface** GigabitEthernet 2 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**  Switch(config)# vlan 2 Switch(config-vlan)# interface GigabitEthernet 2 Switch(config-if)# switchport trunk allowed vlan add 2 Switch(config-if)# exit Switch(config)# interface vlan 2 Switch(config-if)# ip address 192.168.2.1 255.255.255.0 Switch(config-if)# ip route 1.1.1.1 255.0.0.0 192.168.3.11 Switch(config)# exit Switch# show ip route Codes: > - best, C - connected, S - static S> 1.0.0.0/8 [1/1] via 192.168.3.11, VLAN 2 C> 192.168.1.0/24 is directly connected, VLAN 2 C> 192.168.2.0/24 is directly connected, VLAN 2 C> 192.168.3.0/24 is directly connected, VLAN 2 C> 192.168.100.0/24 is directly connected, MGMT VLAN Switch#

37.3 IPV4 ARP

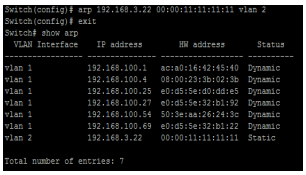
Use the arp command to add a static arp entry. Use the **“no”** arp command to delete a static arp entry. You can verify your setting by entering the show arp Privileged EXEC command.

Switch#**configure terminal**

Switch(config)# **arp** {ip-addr mac-addr} **vlan** {VLAN-ID}

Switch(config)# **no arp** {ip-addr mac-addr} **vlan** {VLAN-ID}

Syntax	**arp**{ip-addr mac-addr} **vlan** {VLAN-ID} **no arp**{ip-addr mac-addr} **vlan** {VLAN-ID}
Parameter	**ip-addr** IP address of ARP entry **mac-addr** MAC address of ARP entry **vlanid** Vlan ID of this arp entry
Default	The device contains ARP entries of the vlan interface.
Mode	Global Configuration mode

Example	The following example shows how to configure and view a static arp entry. Switch#**configure terminal** Switch(config)# **arp** 192.168.3.22 00:00:11:11:11:11 **vlan** 2 Switch# **show arp** 

```
Switch(config)# arp 192.168.3.22 00:00:11:11:11:11 vlan 2
Switch(config)# exit
Switch# show arp
  VLAN Interface    IP address        HW address       Status
---------------- --------------- ----------------- ---------
vlan 1            192.168.100.1    ac:a0:16:42:45:40  Dynamic
vlan 1            192.168.100.4    08:00:23:5b:52:3b  Dynamic
vlan 1            192.168.100.25   e0:d5:5e:d0:dd:e5  Dynamic
vlan 1            192.168.100.27   e0:d5:5e:32:b1:92  Dynamic
vlan 1            192.168.100.54   50:3e:aa:26:24:3c  Dynamic
vlan 1            192.168.100.69   e0:d5:5e:32:b1:22  Dynamic
vlan 2            192.168.3.22     00:00:11:11:11:11  Static

Total number of entries: 7
```

37.4 IPV6 INTERFACE

Use the interface vlan global configuration command to config ip interface on the device.Use the ipv6 enable command in vlan interface mode to enable ipv6 function. Use the **“no”** ipv6 enables command to disable ipv6 function. Use the **“no”** interface vlan command to delete ip interface on the device.You can verify your setting by entering the show ipv6 interface vlanPrivileged EXEC command.

Switch#**configure terminal**

Switch(config)# **interface vlan** {VLAN-ID}

Switch(config-if)# **ipv6 enable**

Switch(config)# **no interface vlan** {VLAN-ID}

Switch(config-if)# **no ipv6 enable**

Syntax	**interface vlan** {VLAN-ID} **ipv6 enable** **no interface vlan** {VLAN-ID} **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

Example	The following example shows how to config ip interface. Switch#**configure terminal** Switch(config)# **interface vlan 2** Switch(config-if)# **ipv6 enable** Switch# **show ipv6 interface vlan 2** 

37.5 IPV6 ADDRESS

Use the ipv6 address command in vlan interface mode to config a manual ipv6 address. Use the **“no”** ipv6 address command in vlan interface mode to delete all manual ipv6 addresses on this vlan interface.You can verify your setting by entering the show ipv6 interface vlan Privileged EXEC command.

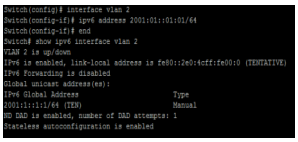
Switch#**configure terminal**

Switch(config)# **interface** {Interface-ID}

Switch(config-if)# **ipv6 address ipv6-addr**

Switch(config-if)# **no ipv6 address**

Syntax	**ipv6 address ipv6-addr** **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
Example	The following example shows how to config ip interface. Switch#**configure terminal** Switch(config)# **interface vlan** 2 Switch(config-if)# **ipv6 address** 2001:01::01:01/64 Switch# **show ipv6 interface vlan** 2 

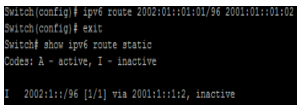
37.6 IPV6 ROUTES

Use the ipv6 route command to configure a static ipv6 routing entry. Use the **“no”** ipv6 address command to delete a static ipv6 routing entry.You can verify your setting by entering the show ipv6 route staticPrivileged EXEC command.

Switch#**configure terminal**

Switch(config)# **ipv6 route ipv6-addr/length route-ipv6-addr**

Switch(config)# **no ipv6 address ipv6-addr/length**

Syntax	**ipv6 route ipv6-addr/length route-ipv6-addr** **no ipv6 address ipv6-addr/length**
Parameter	**ipv6-addr/length** Destination ipv6 prefix and length **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.
Example	The following example shows how to configure an ipv6 routing entry. Switch#**configure terminal** Switch(config)# **ipv6 route 2002:01::01:01/96 2001:01::01:02** Switch# **show ipv6 route static** 

37.7 IPV6 NEIGHBORS

Use the ipv6 neighbor command to configure a static ipv6 neighbor entry. Use the **“no”** ipv6 neighbor command to delete ipv6 neighbor entry.You can verify your setting by entering the show ipv6 neighbors Privileged EXEC command.

Switch#**configure terminal**

Switch(config)# **ipv6 neighbor ipv6-addr vlan vlan-id macaddr**

Switch(config)# **no ipv6 neighbor**

Syntax	**ipv6 neighbor ipv6-addr vlan vlan-id macaddr** **no ipv6 neighbor**
Parameter	**ipv6-addr** Neighbor ipv6 address **vlanid** Vlan interface number **macaddr** MAC address of ipv6 neighbor entry
Mode	Global configuration

Example	The following example shows how to configure an ipv6 neighbor entry. Switch#**configure terminal** Switch(config)# **ipv6 neighbor** 2001:01::01:11 **vlan** 2 00:00:00:11:11:12 Switch# **show ipv6 neighbors** 

POE

Power over Ethernet (PoE) is technology that passes electric power over twisted-pair Ethernet cable to powered devices (PD), such as wireless access points, IP cameras, and VoIP phones in addition to the data that cable usually carries. It enables one RJ45 cable to provide both data connection and electric power to PDs instead of having a separate cable for each.

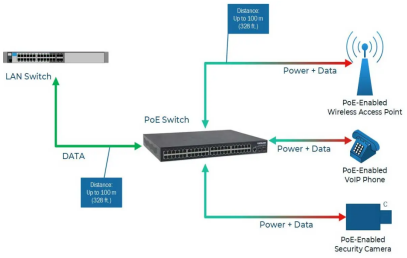


Fig 38.1 PoE Concept

PoE Standard	PoE Common Name	Power Output	Year	Comment
IEEE 802.3af	PoE	15.40 W	2003	12.95 W
IEEE 802.3at	PoE+	30 W	2009	25.50 W
IEEE 802.3bt Type 3	4PPoE, Ultra PoE, UPoE	60 W	2018	51 W
IEEE 802.3bt Type 4	Ultra PoE, UPoE, PoE++	Up to 100 W	2018	71 W for connected device (PD)

PoE, PoE+ and PoE++ Comparison Chart

As PoE/PoE+/PoE++ technology has developed the amount of power that can be sent over Ethernet cable has increased. IEEE-compliant PoE/PoE+/PoE++ switches and injectors can output anywhere from 12 watts to 100 watts of power per port.

38.1 POE PORT SETTING

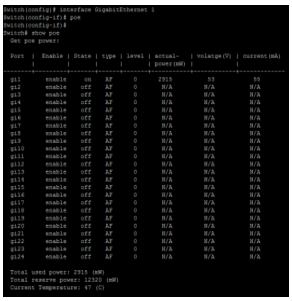
Use the poe command in interface mode to enable port poe power supply. Use the **“no”** poe command in interface mode to disable port poe power supply. You can check the port poe working status by using the show poe Privileged EXEC command.

Switch#**configure terminal**

Switch(config-if)# **poe**

Switch(config-if)# **no poe**

Syntax	**poe** **no poe**
Default	All ports are enabled for poe power supply by default. (Poe-enabled device)
Mode	interface configuration.

Example	The following example shows how to config poe. Switch#**configure terminal** Switch(config)# **interface** GigabitEthernet 1 Switch(config-if)# **poe** Switch# **show poe** 

38.2 POE PORT SCHEDULE SETTING

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.

Switch#**configure terminal**

Switch(config-if)#**poe schedule week days hour** {hours}

Switch(config-if)#**no poe schedule week days hour** {hours}

Syntax	**poe schedule week days hour** hours **no poe schedule week days hour** hours
Parameter	days Port poe power supply days hours Port poe power supply hours
Default	All ports open POE function all day by default. (Poe-enabled device)
Mode	interface configuration.

Example	The following example shows how to config poe schedule. Switch#**configure terminal** 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.