COMMANDO Solider E2000 Series Managed Switches
COMMAND Line Interface (CLI)

Software Version 1.4 onwards

INTRODUCTION

COMMANDO Soldier E2000 Series Switches are fully managed, PoE+ Gigabit Ethernet L2+ 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. 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 Soldier E2000 Series Switches Series are fixed-configuration, with flexible uplinks Gigabit Ethernet switches that provide enterprise-class access for campus and branch applications. Designed for the digital workplace, these are optimized for today's mobile and IoT needs. 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. COMMANDO Soldier E2000 Series provide easy device Desktop as well as Rack/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 802.3af-compliant PoE (Power over Ethernet) and 802.3at-compliant PoE+ (Power over Ethernet plus). Each switchport is capable to deliver 15.4 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 Soldier E2000 Series 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 Soldier E2000 Series 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.

ADMINISTRATION

General commands used in E2000 Series Switches are described in the Administration. The switch administration is to perform some basic switch administration tasks.

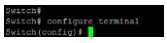
1.1 CONFIGURE

Use **"configure terminal"** command to enter global configuration mode. In global configuration mode, the prompt will show as **"Switch(config)#"**.

Switch#**configure terminal**

Switch(config)#

Syntax	**configure**
Mode	Privileged EXEC
Example	This example shows how to enter global configuration mode. Switch#configure terminal **terminal** Switch(config)#



1.2 CLEAR ARP

Use **“clear arp-cache”** command to clear all or specific one arp entry. Switch#clear arp-cache

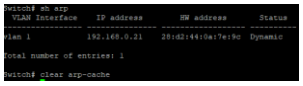
Syntax clear arp-cache

Mode User EXEC Privileged EXEC

This example shows how to clear all arp entries.

Switch#clear arp-cache

Example



Used to clear the non aged out unavailable ARP entries

1.3 CLEAR SERVICE

Use **"clear service"** command to kill all existing sessions for the select service.

Switch# clear (authentication|gvrp|interfaces|ip|ipv6 |lacp|line|lldp|logging|mac|mvr|port- security|rmon|spanning-tree)

Syntax clear (authentication|gvrp|interfaces|ip|ipv6 |lacp|line|lldp|logging|mac|mvr|port- security|rmon|spanning-tree)

Mode Privileged EXEC

This example shows how to clear interfaces,

Switch# clear interfaces GigabitEthernet 1 counters

Example

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>*]

x

Synta

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.

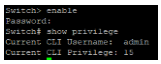
Default privilege level is 1 if no privilege level is specified on disable command.

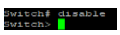
Mode User EXEC

Example

This example shows how to enter privileged EXEC mode and show current privilege level.

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

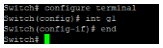
This example shows how to enter Interface Configuration mode and use end command to go back to privileged EXEC mode

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

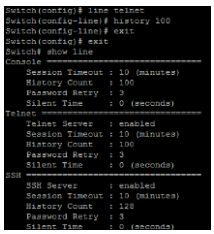
Switch(config)# line ssh

Switch(config-line)# history

200 Switch(config-line)# exit

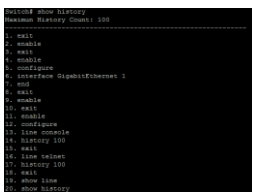
This example shows how show line information.

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

This example shows how to modify contact information

Switch#**configure terminal**

Example

Switch(config)# **hostname commando**

commando(config)#

```
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)#"**

This example shows how to enter Interface Configuration

mode Switch#**configure terminal**

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

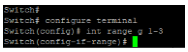
Switch(config-if)#

Example

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 E2000 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]**

address A.B.C.D Specify IPv4 address for

Parameter switch mask A.B.C.D Specify net mask

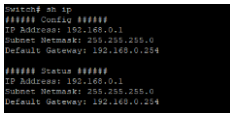
address for switch

Default Default IP address is 192.168.0.1 and default net mask is

255.255.255.0. Mode Global Configuration

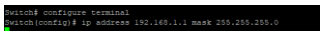
This example shows how to modify the ipv4 address of the switch.

Default setting of E2000 series Switches



Switch#**configure terminal**

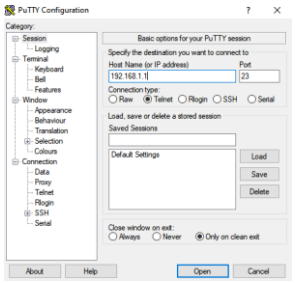
Switch(config)# **ip address 192.168.1.1 mask 255.255.255.0**



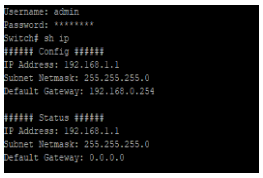
After this configuration you can access Switch with 192.168.1.1 IP address.

Example

Accessing New IP address with Telnet.



This way to access with newly set IP address.



1.11 DEFAULT-GATEWAY

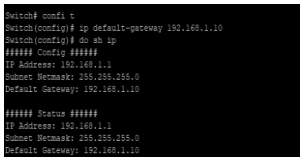
Use **“ip default-gateway”** command to modify default gateway address. And use **“no ip default-gateway”**
to restore default gateway address to factory

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.



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**

Synta x

ipv6 autoconfig

no ipv6

autoconfig

Default Default IPv6 auto config is

enabled. Mode Global Configuration

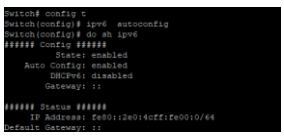
This example shows how to enable IPv6 auto config.

Switch#**configure terminal**

Switch(config)# **ipv6 autoconfig**

Example This example shows how to show current IPv6 auto config state.

Switch# **show ipv6**



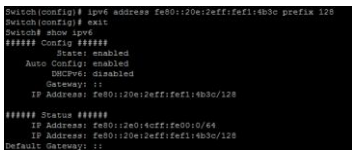
1.14 IPV6 ADDRESS

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**



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**

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

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

This example shows how to enable telnet service and show current telnet service status.

Switch#configure terminal

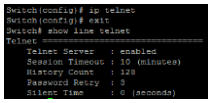
Switch(config)# ip telnet

Telnet daemon enabled.

Switch(config)# exit

Switch# show line telnet

Example



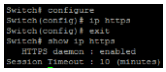
This example shows how to enable https service and show current https service status.

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	http Specify session timeout for http service. https Specify session timeout for https service. *<0-86400>* Specify session timeout minutes. 0 means never timeout.
Default	Default session timeout for http and https is 10 minutes.
Mode	Global Configuration

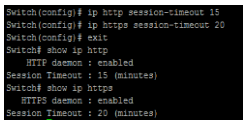
1.19 IP SSH

Example

This example shows how to change http session timeout to 15min and https session timeout to 20min

Switch#co nfigure 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

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

1.20 LINE

Example

This example show

s how to delete and re-generate ssh version 2 key files.

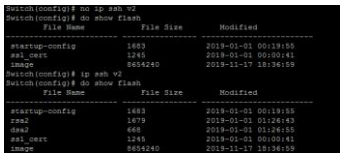
Switch#configure terminal

Switch(config)# no ip ssh v2

Switch(config)# do show flash

Switch(config)# ip ssh v2

Switch(config)# do show flash



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)**

console Select console line to

configure. Parameter Telnet Select

telnet line to configure.

Ssh Select ssh line to configure.

Mode Global Configuration

This example shows how to enter Interface Configuration mode

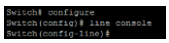
Switch# **configure**

Exampl Switch(config)# **line**

e

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

reboo

t

Mode Privileged EXEC

This example shows how to restart the system

Exampl e

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)**

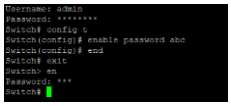
Switch(config)# **no enable [privilege** *<0-15>***]**

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

This example shows how to edit enable password for privilege level 15

Switch#configure terminal

Switch(config)# **enable password** abc



Exampl
e

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

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

Example

Switch(config)# line ssh

Switch(config-line)# password-thresh 6

Switch(config-line)# exit

This example shows how show line information.

Switch# show line

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.

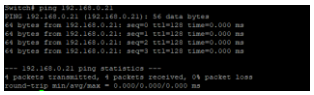
Mode

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

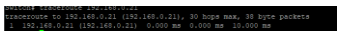
User EXEC

Privileged EXEC

Example

This example shows how to trace route host 192.168.0.21.

Switch# **traceroute 192.168.0.21**

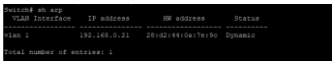


1.27 SHOW ARP

Use “show arp” command to show all arp

entries. Switch# show arp

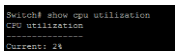
Syntax	show arp
Mode	User EXEC Privileged EXEC
Example	This example shows how to show arp entries. Switch# show arp



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**

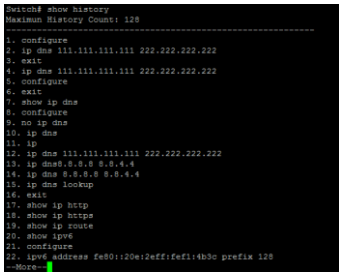
Syntax **show history**

Mode
- User EXEC
- Privileged EXEC
- Global Configuration

Example

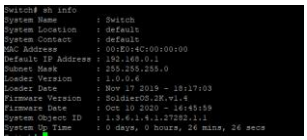
This example shows how show history commands.

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** 

1.31 SHOW IP

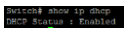
Use “show ip” command to show system IPv4 address, net mask and default gateway. Switch#show ip

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.

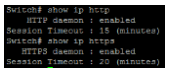
Switch#**show ip dhcp**

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** 

1.33 SHOW IP HTTP

Use “show ip http” command to show HTTP/HTTPS information. Switch#show ip (http|https)

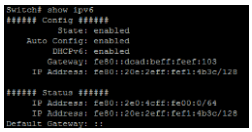
Syntax	show ip (http|https)
Mode	Privileged EXEC
Example	This example shows how to show current ipv4 address of the switch. Switch# show ip http Switch# show ip https



1.34 SHOW IPV6

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

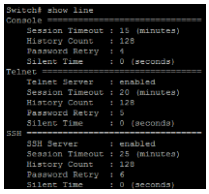
Syntax	show ipv6
Mode	User EXEC Privileged EXEC
Example	This example shows how to show current ipv6 address of the switch. Switch# show ipv6



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.

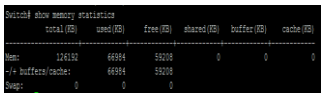
Switch#show line [(console | telnet | ssh)]

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 

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
	This example shows how to show current system memory statistics.
Example	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

This example shows how to show arp entries.

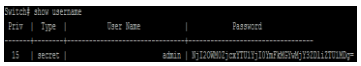
ExampleSwitch# **show privilege**

```
Switch# show privilege
Current CLI Username:  admin
Current CLI Privilege: 15
```

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**

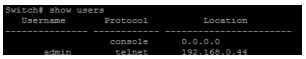


1.39 SHOW USERS

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**

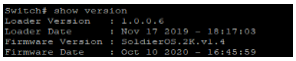


1.40 SHOW VERSION

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

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

Example

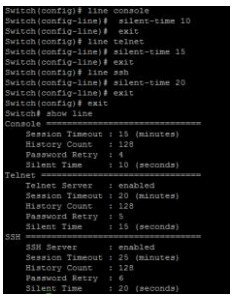
Switch(config)# line ssh

Switch(config-line)# silent-time

20 Switch(config-line)# exit

This example shows how show line information.

Switch# show line



1.42 SSL

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

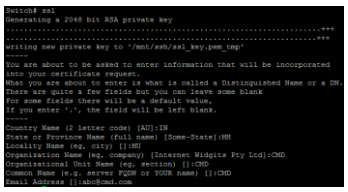
Syntax **ssl**

Mode Global Configuration

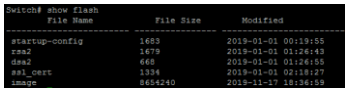
Example

This example shows how to generate certificate files.

Switch# **ssl**



Switch# **show flash**



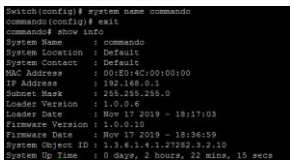
1.43 SYSTEM NAME

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**



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”**.

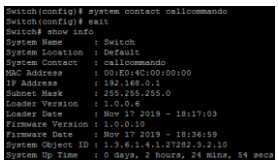
Mode Global Configuration

This example shows how to modify contact information

Switch#**configure terminal**

Switch(config)# **system contact callcommando**

Example Switch# **show info**



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

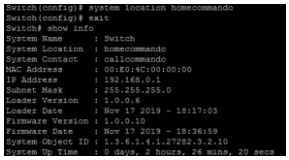
Example

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**

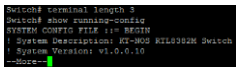


1.46 TERMINAL LENGTH

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

This example shows how to add a new user

account. Switch#configure terminal

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

Exampl e

This example shows how to show existing user accounts.

Switch# **show username**

AAA (Authentication, Authorization, Accounting)

The AAA feature allows you to verify the identity of, grant access to, and track the actions of users managing E2000 Series switches. The E2000 Series switches support Remote Access Dial-In User Service (RADIUS) or Terminal Access Controller Access Control device Plus (TACACS+) protocols.

Based on the user ID and password combination that you provide, the E2000 Series switches perform local authentication or authorization using the local database or remote authentication or authorization using one or more AAA servers. A preshared secret key provides security for communication between the E2000 series switches and AAA servers. You can configure a common secret key for all AAA servers or for only a specific AAA server.

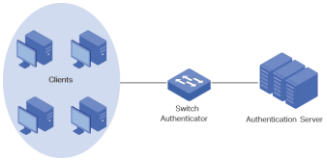


Fig 2.1.1 AAA E2000 Series Switches

AAA AUTHENTICATION

AAA security provides the following services:

1) Authentication - Identifies users, including login and password dialog, challenge and response, messaging support, and, encryption depending on the security protocol that you select. Authentication is the process of verifying the identity of the person or device accessing the E2000 Series switches. This process is based on the user ID and password combination provided by the entity trying to access the E2000 switch. The E2000 Series switches allow you to perform local authentication (using the local lookup database) or remote authentication (using one or more RADIUS or TACACS+ servers).

2) Authorization - Authorization Provides access controls.

AAA authorization is the process of assembling a set of attributes that describe what the user is authorized to perform. Authorization in E2000 Series switches is provided by attributes that are downloaded from AAA servers. Remote security servers, such as RADIUS and TACACS+, authorize users for specific rights by associating attribute-value (AV) pairs, which define those rights with the appropriate user.

3) Accounting - Provides the method for collecting information, logging the information locally, and sending the information to the AAA server for billing, auditing, and reporting.

The accounting feature tracks and maintains a log of every management session used to access the E2000 Series switches. You can use this information to generate reports for troubleshooting and auditing purposes. You can store accounting logs locally or send them to remote AAA servers.

Login authentication is used when user try to login into the switch. Such as CLI login dialog and WEBUI login web page. Enable authentication is used only on CLI for user trying to switch from User EXEC mode to Privileged EXEC mode.Both of them support following authenticate methods. TACACS+ provides more control over the authorization of commands while in RADIUS, no external authorization of commands is supported. All the AAA packets are encrypted in TACACS+ while only the passwords are encrypted in RADIUS is more secure.

Each list allows you to combine these methods with different orders. For example, we want to authenticate login user with remote TACACS+ server, but server may be crashed. Therefore, we need a backup plan, such as another Radius server. So we can configure the list with TACACS+ server as first authentication method and Radius server as second one.

Switch#**configure terminal**

Switch(config)# **aaa authentication (login | enable) (default |** *listname* **)** *[methodlist][methodlist]*

[methodlist] [methodlist]

Switch(config)# **no aaa authentication (login | enable)** {listname}

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

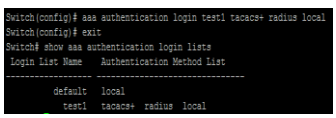
Example

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**

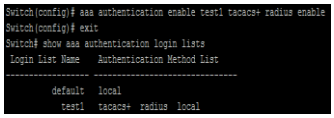


Switch(config)# **aaa authentication enable test1 tacacs+ radius**

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

Parameterlistname 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.

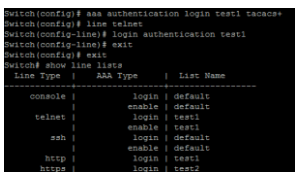
Switch(config)# **aaa authentication login test1 (tacacs+| radius | local | none |enable)**

Switch(config)# **line telnet**

Switch(config-line)# **login authentication test1**

This example shows how to show line binding

lists. Switch# **show line lists**



2.2 IP HTTP LOGIN AUTHENTICATION

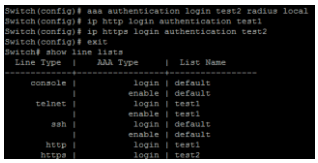
Different access methods are allowed to bind different login authentication lists. Use **"ip (http | https) login authentication"** command to bind the list to WEBUI access from http or https.

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

Parameterlistname Specify the enable authentication list name

to use. Default Default enable authentication list for each line

is **"default"**. Mode Line Configuration

Example

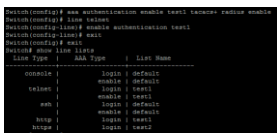
This example shows how to create a new enable authentication list and bind to telnet line.

Switch#**configure terminal**

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

Switch(config)# **line telnet**

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



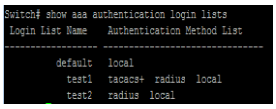
2.4 SHOW AAA AUTHENTICATION

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**

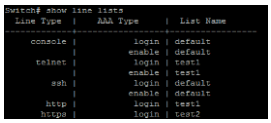
Syntax **show line lists**

Mode Privileged EXEC

This example shows how to show line binding lists.

Switch# **show line lists**

Example



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**

```
Switch(config)# tacacs default-config timeout 20
Switch(config)# tacacs default-config key tackey
Switch(config)# exit
Switch# show tacacs default-config
 Timeout|   Key
--------+--------
   20   | tackey
```

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>]*

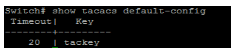
Switch(config)#**no tacacs** [**host** *{HOSTNAME}*]

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.

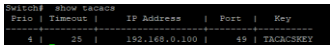
Switch#**show tacacs**

Syntax **show tacacs**

Mode Privileged EXEC

This example shows how to show existing tacacs+ server.

ExampleSwitch# **show tacacs**



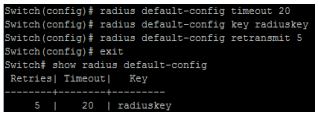
2.10 SHOW Default-config

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
e	

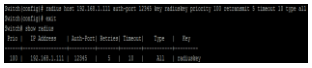
Exampl

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

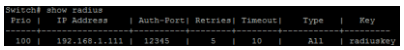
Syntax	show radius default-config
Mode	Privileged EXEC
Example	This example shows how to show default radius configurations. Switch# show radius default-config

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)

An ACL is a sequential collection of permit and deny conditions that apply to packets. Packet filtering can help limit network traffic and restrict network use by certain users or devices. ACLs filter traffic as it passes through a switch and permit or deny packets crossing specified interfaces. When a packet is received on an interface, the switch compares the fields in the packet against any applied ACLs to verify that the packet has the required permissions to be forwarded, based on the criteria specified in the access lists. One by one, it tests packets against the conditions in an access list. The first match decides whether the switch accepts or rejects the packets. Because the switch stops testing after the first match, the order of conditions in the list is critical. If no conditions match, the switch rejects the packet. If there are no restrictions, the switch forwards the packet; otherwise, the switch drops the packet. The switch can use ACLs on all packets it forwards.

You configure access lists on a switch to provide basic security for your network. If you do not configure ACLs, all packets passing through the switch could be allowed onto all parts of the network. You can use ACLs to control which hosts can access different parts of a network or to decide which types of traffic are forwarded or blocked. For example, you can allow e-mail traffic to be forwarded but not Telnet traffic.

An ACL contains an ordered list of access control entries (ACEs). Each ACE specifies permit or deny and a set of conditions the packet must satisfy in order to match the ACE. The meaning of permit or deny depends on the context in which the ACL is used.

The switch supports IP ACLs and Ethernet (MAC) ACLs:

1) IP ACLs filter IPv4 traffic, including TCP, User Datagram Protocol (UDP), Internet Group Management Protocol (IGMP), and Internet Control Message Protocol (ICMP).

2) Ethernet ACLs filter non-IP traffic.

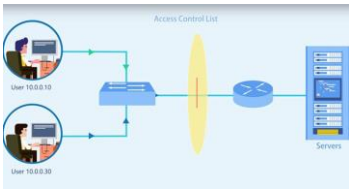


Fig 3.1.1 IP ACL E2000 series Switches

3.1 MAC ACL

MAC ACLs are ACLs that filter traffic using information in the Layer 2 header of each packet. You can use ACLs to control which hosts can access different parts of a network or to decide which types of traffic are forwarded or blocked at the router interfaces.

Use the mac acl command to create a MAC access list and to enter mac-acl configuration mode. The name of ACL must be unique that cannot have same name with other ACL or QoS policy. Once an ACL is created, an implicit **"deny any"** ACE created at the end of the ACL. That is, if there are no matches, the packets are denied. Use the no form of this command to delete.

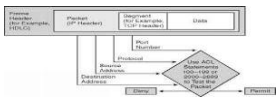


Fig 3.2.1 MAC ACL E2000 series

Switches Switch#**configure terminal**

Switch(config)# **mac acl** *{NAME}*

Switch(config)#**no mac acl** *{NAME}*

Syntax	**mac acl** *{NAME}* **no mac acl** *{NAME}*
Parameter	*NAME* Specify the name of MAC
ACL Mode	Global Configuration
Example	The example shows how to create a mac acl. You can verify settings by the following show acl command Switch#**configure terminal** Switch(config)# **mac acl** test Switch(mac-acl)# **show acl**

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

MAC access list commando
```

3.2 PERMIT (MAC)

Use the permit command to add permit conditions for a mac ACE that bypass those packets hit the ACE.

The **“sequence”** also represents hit priority when ACL bind to an interface. An ACE not specifies **“sequence”** index would assign a sequence index which is the largest existed index plus 20. If packet content can match more than one ACE, the lowest sequence ACE is hit. An ACE cannot be added if has the same conditions as existed ACE.

Switch#**configure terminal**

Switch(config)# **mac acl** *{NAME}*

Switch(config-mac-acl)#[**sequence** *<1-2147483647>*] **permit (A:B:C:D:E:F /A:B:C:D:E:F|any) (A:B:C:D:E:F/A:B:C:D:E:F|any) [vlan** *<1-4094>*] **[cos** *<0-7><0-7>*][**ethtype** *<0x0600-0xFFFF>*]

Switch(config-mac-acl)#**no sequence** *<1-2147483647>*

Syntax	[sequence *<1-2147483647>*] permit (A:B:C:D:E:F/A:B:C:D:E:F|any) (A:B:C:D:E:F/A:B:C:D:E:F|any) [vlan *<1-4094>*] [cos *<0-7><0-7>*][ethtype <0x0600-0xFFFF>] no sequence *<1-2147483647>*
Parameter	*<1-2147483647>* b (Optional) Specify sequence index of ACE, the sequence index represent the priority of an ACE in ACL. (A:B:C:D:E:F/A:B:C:D:E:F|any)Specify the source MAC address and mask of packet or any MAC address. (A:B:C:D:E:F/A:B:C:D:E:F|any)Specify the destination MAC address and mask of packet or any MAC address. [vlan*<1-4094>*] (Optional) Specify the vlan ID of packet. [cos*<0-7><0-7>*](Optional) Specify the Class of Service value and mask of packet. [ethtype*<0x0600-0xFFFF>*] (Optional) Specify Ethernet protocol number of packet.
Mode	MAC ACL Configuration

Example

The example shows how to add an ACE that permit packets with source MAC address 22:33:44:55:66:77. VLAN 3 and Ethernet type 1999. You can verify settings by the following show acl command,

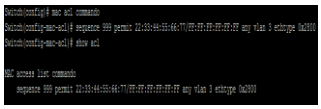
Switch#**configure terminal**

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

Switch(mac-acl)# **sequence** 999 **permit** 22:33:44:55:66:77/ FF:FF:FF:FF:FF:FF **any vlan** 3
ethtype 0x2800

Switch(mac-al)# **show**

acl



3.3 DENY (MAC) ACL

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

Switch#**configure terminal**

Switch(config)# **mac acl** *{NAME}*

Switch(config-mac-acl)#**[sequence** *<1-2147483647>*] **deny (A:B:C:D:E:F/ A:B:C:D:E:F|any) (A:B:C:D:E:F/A:B:C:D:E:F|any) [vlan** *<1-4094>*] **[cos** *<0-7><0-7>*] **[ethtype** *<0x0600-0xFFFF>*] **[shutdown]**

Switch(config-mac-acl)# **no sequence** *<1-2147483647>*

Syntax	[sequence *<1-2147483647>*] deny (A:B:C:D:E:F/A:B:C:D:E:F|any) (A:B:C:D:E:F/A:B:C:D:E:F|any) [vlan *<1-4094>*] [cos *<0-7><0-7>*] [ethtype *<0x0600-0xFFFF>*] [shutdown] no sequence *<1-2147483647>*
Parameter	*<1-2147483647>* (Optional) Specify sequence index of ACE, the sequence index represent the priority of an ACE in ACL. (A:B:C:D:E:F/A:B:C:D:E:F|any)Specify the source MAC address and mask of packet or any MAC address. (A:B:C:D:E:F/A:B:C:D:E:F|any)Specify the destination MAC address and mask of packet or any MAC address. [vlan *<1-4094>*] (Optional) Specify the vlan ID of packet. [cos *<0-7><0-7>*](Optional) Specify the Class of Service value and mask of packet. [ethtype *<0x0600-0xFFFF>*](Optional) Specify Ethernetprotocol number of packet [shutdown](Optional) Shutdown interfaces while ACE hit.
Mode	MAC ACL Configuration

The example shows how to add an ACE that denies packets with destination MAC address aa:bb:cc:xx:xx:xx and VLAN 9. You can verify settings by the following show acl command

Example

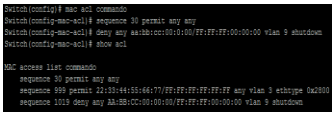
Switch#**configure terminal**

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

Switch(mac-acl)# **sequence** 30 **permit any any**

Switch(mac-acl)# **deny any** aa:bb:cc:00:0:00/FF:FF:FF:00:00:00 **vlan** 9 **shutdown**

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



3.4 IP ACL

Use the ip acl command to create an IPv4 access list and to enter ip-acl configuration mode. The name of ACL must be unique that cannot have same name with other ACL or QoS policy. Once an ACL is created, an implicit **"deny any"** ACE created at the end of the ACL. That is, if there are no matches, the packets are denied. Use the no form of this command to delete.

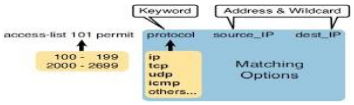


Fig 3.4.1 IP ACL with permit and

deny. Switch#**configure terminal**

Switch(config)# **ip acl** *{NAME}*

Switch(config)# **no ip acl** *{NAME}*

Syntax	**ip acl** *{NAME}* **no ip acl** *{NAME}*
Parameter	*NAME* Specify the name of IPv4
ACL Mode	Global Configuration

Example	The example shows how to create an IP ACL. You can verify settings by the following show acl command
	Switch#**configure terminal**
	Switch(config)#**ip acl iptest**
	Switch(config-ip-acl)#**do show acl**
	`Switch(config)# ip acl iptest`
	`Switch(config-ip-acl)# show acl`
	`IP access list iptest`

,

3.5 PERMIT (IP)

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

Switch#**configure terminal**

Switch(config)# ip acl *{NAME}*

Switch(config-ip-acl)#permit ip 192.168.1.0/255.255.255.0 any permit icmp any any echo-request any

Syntax

[sequence *<1-2147483647>*] permit (*<0- 255>* |ipinip|egp|igp |hmp|rdp|ipv6| ipv6:rout|ipv6:frag|rsvp|ipv6:icmp|ospf|pim|l2tp|ip) (A.B.C.D/A.B.C.D|any) (A.B.C.D/A.B.C.D|any)[(dscp|precedence) VALUE]]

[sequence*<1-2147483647>*]permit icmp(A.B.C.D/A.B.C.D|any) (A.B.C.D/A.B.C.D|any) (*<0-255>*|echo-reply|destination-unreachable|source-quench|echo-request|router-advertisement|router-solicitation|time- exceeded|timestamp|timestamp-reply|traceroute|any) (*<0- 255>*|any) [(dscp|precedence) VALUE]

[sequence*<1-2147483647>*]permit tcp (A.B.C.D/A.B.C.D|any) (*<0-65535>* |echo|discard|daytime|ftp-data|ftp|telnet|smtp|time|hostname|whois|tacacs-ds|domain|www|pop2|pop3|syslog|talk|klogin|kshell|sunrpc|drip|PORT_RANGE|any) (A.B.C.D/A.B.C.D|any) (*<0-65535>*|echo|discard|daytime|ftp-data|ftp|telnet|smtp|time|hostname|whois| tacacs-ds|domain|www|pop2|pop3|syslog|talk|klogin|kshell|sunrpc|drip|PORT_RANGE|any)[match- all TCP_FLAG][(dscp|precedence) VALUE]

[sequence*<1-2147483647>*]permitudp (A.B.C.D/A.B.C.D|any) (*<0-65535>* |echo|discard| time|nameserver|tacacs-ds|domain|bootps|bootpc|tftp|sunrpc|ntp|netbios- ns|snmp| snmptrap|who|syslog|talk|rip|PORT_RANGE|any) (A.B.C.D/A.B.C.D|any)

<0-65535>|echo |discard|time|nameserver|tacacsds|domain|bootps|bootpc|tftp|sunrpc|ntp|netbios-ns| snmp|snmptrap|who|syslog|PORT_RANGE|any) [(dscp|precedence) VALUE]

no sequence*<1-2147483647>*

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

(A.B.C.D/A.B.C.D|any) Specify the source IPv4 address and mask of packet or any IPv4 address.

(A.B.C.D/A.B.C.D|any) Specify the destination IPv4 address and mask of packet or any IPv4 address.

[dscp VALUE](Optional) Specify the DSCP of packet.

[precedence VLAUE](Optional) Specify the IP precedence of packet.

Parameter icmp-type Specify ICMP message type for filtering ICMP packet. Enter a type name of list or a number of ICMP message type.

icmp-code Specify ICMP message code for filtering ICMP packet.

l4-source-port Specify TCP/UDP source port of for filtering TCP/UDP packet. Enter a port name of list or a number of TCP/UDP port.

l4-destination-port Specify TCP/UDP destination port of for filtering TCP/UDP packet. Enter a port name of list or a number of TCP/UDP port.

match-all Specify tcp flag for TCP packet. If a flag should be set it is prefixed by

"+".If a flag should be unset it is prefixed by "-". Available options are +urg, +ack, +psh, +rst,
+syn, +fin,-urg, -ack, -psh, -rst, -syn and -fin.To define more than 1 flag - enter additional flags one after another without a space (example +syn-ack).

Mode IP ACL Configuration

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

This command shows how to permit a source IP address subnet.

Switch#**configure terminal**

Switch(config)# **ip acl** *{commando}*

Switch(config-ip-acl)#**permit ip** 192.168.1.0/255.255.255.0 **any**

This command shows how to permit ICMP echo-request packet with any IP

address. Switch(config-ip-acl)#**permit icmp any any** echo-request **any**

Example

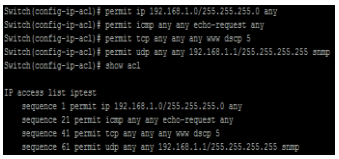
This command shows how to permit any IP address HTTP packets with DSCP 5.

Switch(config-ip-acl)#**permit tcp any any any** www **dscp** 5

This command shows how to permit any source IP address SNMP packet connect to destination IP address 192.168.1.1.

Switch(config-ip-acl)#**permit udp any any** 192.168.1.1/255.255.255.255 **snmp**

Switch(config-ip-acl)#**show acl**



3.6 DENY (IP)

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

Switch#**configure terminal**

Switch(config)# **ip acl** {iptest}

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

Syntax

[sequence *<1-2147483647>*] deny(*<0-255>*|ipinip|egp|igp|hmp|rdp|ipv6|ipv6:rout|ipv6:frag|rsvp|ipv6:icmp|ospf|pim|l2tp|ip) (A.B.C.D/A.B.C.D|any)(A.B.C.D/A.B.C.D|any)[(dscp|precedence) VALUE]] [shutdown]

[sequence *<1-2147483647>*] deny icmp (A.B.C.D/A.B.C.D|any)(A.B.C.D/A.B.C.D|any)(*<0- 255>*|echo-reply|destination-unreachable|

source-quench|echo-request|router-advertisement|router- solicitation|

time-exceeded|timestamp|timestamp-reply|traceroute|any)(<0-255>|any) [(dscp|precedence) VALUE] [shutdown]

[sequence *<1-2147483647>*]deny tcp (A.B.C.D/A.B.C.D|any) (*<0-65535>*|echo|

discard|daytime|ftp-data|ftp|telnet|smtp|time|hostname|whois|tacacs-ds|domain|www|pop2|pop3|syslog|talk|klogin|kshell|sunrpc|drip|PORT_RANGE|any)(<0-65535>|echo|discard|daytime|ftp-

data|ftp|telnet|smtp|time|hostname|whois| (A.B.C.D/A.B.C.D|any) (*<0-65535>* |echo|discard|daytime|ftp-data|ftp|telnet|smtp|time|hostname|whois|tacacsds|domain|www|pop2|pop3|syslog|talk|klogin|kshell|sunrpc|drip|PORT_RANGE|any)

[match-all TCP_FLAG] [(dscp|precedence) VALUE] [shutdown]

[sequence *<1-2147483647>*]deny udp (A.B.C.D/A.B.C.D|any)(*<0-65535>*

|echo|discard|time|nameserver|tacacs-ds|domain|bootps|bootpc|tftp|sunrpc|ntp|netbiosns|snmp|snmptrap|who|syslog|

talk|rip|PORT_RANGE|any)(A.B.C.D/A.B.C.D|any)(*<0-65535>*

|echo|discard|time|nameserver|tacacs-ds|domain|bootps|bootpc|tftp|sunrpc|ntp|netbiosns|snmp|snmptrap|who|syslog|PORT_RANGE|any) [(dscp|precedence) VALUE] [shutdown]

no sequence*<1-2147483647>*

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

(A.B.C.D/A.B.C.D|any)Specify the source IPv4 address and mask of packet or any IPv4 address.

(A.B.C.D/A.B.C.D|any)Specify the destination IPv4 address and mask of packet or any IPv4 address.

[dscp VALUE](Optional) Specify the DSCP ofpacket.

[precedence VLAUE](Optional) Specify the IP precedence of packet.

icmp-typeSpecify ICMP message type for filtering ICMP packet. Enter a type name of list or a number of ICMP message type.

Parameter

icmp-code Specify ICMP message code for filtering ICMP packet.

l4-source-portSpecify TCP/UDP source port of for filtering TCP/UDP packet. Enter a port name of list or a number of TCP/UDP port.

l4-destination-portSpecify TCP/UDP destination port of for filtering TCP/UDP packet. Enter a port name of list or a number of TCP/UDP port.

match-allSpecify tcp flag for TCP packet. If a flag should be set it is prefixed by "+".If a flag should be unset it is prefixed by "-". Available options are +urg, +ack, +psh, +rst, +syn, +fin,- urg, -ack, -psh, -rst, -syn and -fin.To define more than 1 flag - enter additional flags one after another without a space (example +syn-ack).

[shutdown](Optional) Shutdown interface while ACE hit.

Mode IP ACL Configuration

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

Switch#configure terminal

Switch(config)# ip acl iptest

Example

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

Switch(config-ip-acl)#show acl

3.7 IPV6 ACL

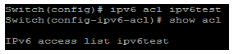
Use the ipv6 acl command to create an IPv6 access list and to enter ipv6-acl configuration mode. The name of ACL must be unique that cannot have same name with other ACL or QoS policy. Once an ACL is created, an implicit **"deny any"** ACE created at the end of the ACL. That is, if there are no matches, the packets are denied. Use the no form of this command to delete.

Switch#**configure terminal**

Switch(config)# **ipv6 acl** *{NAME}*

Switch(config)# **no ipv6 acl** *{NAME}*

Syntax	**ipv6 acl** *{NAME}* **no ipv6 acl** *{NAME}*
Parameter	*NAME* Specify the name of IPv6
ACL Mode	Global Configuration
Example	The example shows how to create an IPv6 ACL. You can verify settings by the following show acl command Switch#**configure terminal** Switch(config)#**ipv6 acl** ipv6test Switch(config-ipv6- acl)# **show acl**



3.8 PERMIT (IPV6)

Use the permit command to add permit conditions for an IPv6 ACE that bypasses those packets hit the ACE. The **"sequence"** also represents hit priority when ACL bind to an interface. An ACE not specifies **"sequence"** index would assign a sequence index which is the largest existed index plus 20. If packet content can match more than one ACE, the lowest sequence ACE is hit. An ACE cannot be added if has the same conditions as existed ACE.

Switch#**configure terminal**

Switch(config)# **ipv6 acl** {ipv6test}

Switch(config-ipv6-acl)#**permit ipv6** fe80:1122:3344:5566::1/64 **any**

Syntax

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

[sequence <1-2147483647>] permit icmp (X:X::X:X/*<0- 128>*|any)

(X:X::X:X/*<0-128>*|any) (*<0-255*>|destination- unreachable|packet-too-

big|

time-exceeded|parameter-problem|echo-request|echo-reply|mld-query|mld-report|mldv2- report|mld-done| router- solicitation|router-advertisement|nd-ns|nd-na|any) (*<0- 255>*
|any)[(dscp|precedence) VALUE]

[sequence *<1-2147483647>*] permit tcp (X:X::X:X/*<0-128>*|any)

(*<0-65535>*|echo|discard|daytime|ftp-data|ftp|telnet|smtp|
time|hostname|whois|tacacs- ds|domain|www|pop2|pop3|syslog|

talk|klogin|kshell|sunrpc|drip|PORT_RANGE|any) (X:X::X:X/*<0-128>*|any)

(*<0-65535>*|echo|discard|daytime|ftp- data|ftp|

telnet|smtp|time|hostname|whois|tacacs-ds|domain|www|pop2|
pop3|syslog|talk|klogin|kshell|sunrpc|drip|PORT_RANGE|any)[match-allTCP_FLAG]
[(dscp|precedence) VALUE]

[sequence *<1-2147483647>*] permit udp (X:X::X:X/*<0-128>*|any)

(*<0-65535>*|echo|discard|time|nameserver|tacacs-ds|domain|
bootps|bootpc|tftp|sunrpc|ntp|netbios-

n
s
|
s
n
m
p
|
s
n
m
p
t
r
a
p
|
w
h
o
|
s
y
s
l
o
g
|

talk|ri
p|POR
T_RAN
GE|an
y)
(X:X::X
:X/*<0-
128>*|
any)

(*<0-
655
35>*|
ech
o|dis

card|time|nameserver|tacacs-ds|domain| bootps|bootpc|tftp|sunrpc|ntp|netbios-ns|
snmp|snmptrap|who|syslog|PORT_RANGE|any)
[(dscp|precedence) VALUE]

no sequence *<1-2147483647>*

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

(X:X::X:X/<0-128>|any) Specify the source IPv6 address and prefix of packet or any IPv6 address.

(X:X::X:X/<0-128>|any) Specify the destination IPv6 address and prefix of packet or any IPv6 address.

[dscp VALUE](Optional) Specify the DSCP of packet.

[precedence VLAUE](Optional) Specify the IP precedence of packet.

Parameter

icmp-type Specify ICMP message type for filtering ICMP packet. Enter a type name of list or a number of ICMP message type.

icmp-code Specify ICMP message code for filtering ICMP packet.

l4-source-port Specify TCP/UDP source port of for filtering TCP/UDP packet. Enter a port name of list or a number of TCP/UDP port.

l4-destination-port Specify TCP/UDP destination port of for filtering TCP/UDP packet. Enter a port name of list or a number of TCP/UDP port.

match-all Specify tcp flag for TCP packet. If a flag should be set it is prefixed by "+".If a flag should be unset it is prefixed by "-". Available options are +urg, +ack, +psh, +rst, +syn, +fin, - urg, -ack, -psh, -rst, -syn and -fin.To define more than 1 flag - enter additional flags one after another without a space (example +syn-ack).

Mode IPv6 ACL Configuration

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

This command shows how to permit a source IP address subnet.

Switch#configure terminal

Example

Switch(config)# ipv6 acl {commando}

Switch(ipv6-acl)# permit ipv6 fe80:1122:3344:5566::1/64 any

Switch(ipv6-acl)# **show acl**

```
Switch(config-ipv6-acl)# permit ipv6 fe80:1122:3344:5566::1/64 any
Switch(config-ipv6-acl)# show acl

IPv6 access list ipv6test
    sequence 1 permit ipv6 fe80:1122:3344:5566::1/64 any
```

3.9 DENY (IPV6)

Use the deny command to add deny conditions for an IPv6 ACE that drop those packets hit the ACE. The **"sequence"** also represents hit priority when ACL bind to an interface. An ACE not specifies **"sequence"** index would assign a sequence index which is the largest existed index plus 20. If packet content can match more than one ACE, the lowest sequence ACE is hit. An ACE cannot be added if has the same conditions as existed ACE. Use **"shutdown"** to shutdown interface while ACE hit.

Switch#**configure terminal**

Switch(config)# **ipv6 acl** {ipv6test}

Switch(config-ipv6-acl)# **permit ipv6** fe80:1122:3344:5566::1/64 **any**

Syntax

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

[sequence <1-2147483647>] deny icmp (X:X::X:X/*<0-128>*|any) (X:X::X:X/*<0-128>*|any) (*<0-255>*|destination- unreachable|packet-too-big|

time-exceeded|parameter-problem|echo-request|echo-reply| mld-query|mld-report|mldv2- report|mld-done| router- solicitation|router-advertisement|nd-ns|nd-na|any) (*<0- 255>*
|any)[(dscp|precedence) VALUE] [shutdown]

[sequence *<1-2147483647>*] deny tcp (X:X::X:X/*<0-128>*|any) (*<0-65535>*|echo|discard|daytime|ftp-data|ftp|telnet|smtp|
time|hostname|whois|tacacs-ds|domain|www|pop2|pop3|syslog|talk|klogin|kshell|sunrpc|drip|PORT_RANGE|any) (X:X::X:X/*<0-128>*|any) (*<0-65535>*|echo|discard|daytime|ftp- data|ftp|

telnet|smtp|time|hostname|whois|tacacs-ds|domain|www|pop2| pop3|syslog|talk|klogin|kshell|sunrpc|drip|PORT_RANGE|any)[match-all TCP_FLAG] [(dscp|precedence) VALUE] [shutdown]

[sequence *<1-2147483647>*] deny udp (X:X::X:X/*<0-128>*|any) (*<0-65535>*|echo|discard|time|nameserver|tacacs-ds|domain|
bootps|bootpc|tftp|sunrpc|ntp|netbios- ns|snmp|snmptrap|who|syslog|

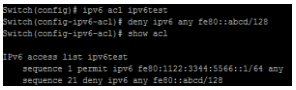
talk|rip|PORT_RANGE|any) (X:X::X:X/*<0-128>*|any) (*<0-65535>*
|echo|discard|time|nameserver|tacacs-ds|domain|
bootps|bootpc|tftp|sunrpc|ntp|netbios-

ns|
snm
p|sn
mptr
ap|
who
|sysl
og|P
ORT
_RA
NGE
|any
)
[(ds
cp|p
rece
den
ce)
VAL
UE]
[shu
tdo
wn]

no
seque
nce
<1-
21474
83647
>

Parameter	*<1-2147483647>*(Optional) Specify sequence index of ACE, the sequence index represent the priority of an ACE in ACL. (A.B.C.D/A.B.C.D|any) Specify the source IPv4 address and mask of packet or any IPv4 address. (A.B.C.D/A.B.C.D|any) Specify the destination IPv4 address and mask of packet or any IPv4 address. [dscp VALUE](Optional) Specify the DSCP of packet. [precedence VLAUE](Optional) Specify the IP precedence of packet. icmp-type Specify ICMP message type for filtering ICMP packet. Enter a type name of list or a number of ICMP message type. icmp-code Specify ICMP message code for filtering ICMP packet. l4-source-port Specify TCP/UDP source port of for filtering TCP/UDP packet. Enter a port name of list or a number of TCP/UDP port. l4-destination-port Specify TCP/UDP destination port of for filtering TCP/UDP packet. Enter a port name of list or a number of TCP/UDP port. match-all Specify tcp flag for TCP packet. If a flag should be set it is prefixed by "+".If a flag should be unset it is prefixed by "-". Available options are +urg, +ack, +psh, +rst, +syn, +fin, - urg, -ack, -psh, -rst, -syn and -fin.To define more than 1 flag - enter additional flags one after another without a space (example +syn-ack). [shutdown](Optional) Shutdown interface while ACE hit.
Mode	IP ACL Configuration
Example	The example shows how to add an ACE that denies packets with destination IP address fe80::abcd. You can verify settings by the following show acl command Switch#configure terminal Switch(config)# ipv6 acl {ipv6test} Switch(config-ip-acl)#deny ipv6 any fe80::abcd/128

Switch(config-ip-acl)#show acl



3.10 BIND ACL

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

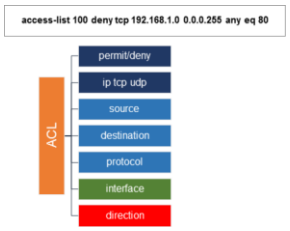


Fig 3.10.1 E2000 Series Switches bind an ACL to interface

Switch#**configure terminal**

Switch(config)# **(mac|ip|ipv6) acl** *{NAME }*

Switch(config)# **[no] (mac|ip|ipv6) acl** *{NAME}*

Syntax	**(mac|ip|ipv6) acl** *{NAME }* **[no] (mac|ip|ipv6) acl** *{NAME}*
Parameter	*(mac|ip|ipv6)* Specify a type of ACL to binding to interface **NAME** Specify the name of ACL
Mode	Interface Configuration
Example	The example shows how to bind an existed ACL to interface. Switch#**configure terminal** Switch(config)# **interface** GigabitEthernet 1 Switch(config-if)# **ip acl** iptest Switch(config-if)# **do show running-config interfaces GigabitEthernet 1**

3.11 SHOW ACL

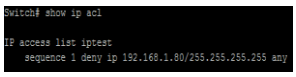
Use the show acl command to show created ACLs. You can specify macip or ipv6 to show specific type ACL or specify unique name string to show ACL with the name.

Switch#**show acl**

Switch#**show (mac|ip|ipv6) acl**

Switch#**show (mac|ip|ipv6) acl** (NAME)

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.

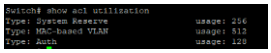
Switch#**show acl utilization**

Syntax **show acl utilization**

Mode Global

Configuration

The example shows how to show utilization Example Switch# **show acl utilization**



AUTHENTICATION MANAGER

You can control access to your network through Switch by using authentication methods such as 802.1X, MAC Based and Web Based. Authentication manager implementation that delegates responsibility for authentication to one or more authentication providers.The authentication manager port setting page control all the authentication methods, such as 802.1x, MAC authentication. It also handles network authentication requests and enforces authentication per port basis. The Auth Manager maintains operational data for all port based network connection. Use MAC-based authentication to authenticate devices based on their physical media access control (MAC) address. WEB-Based authentication enables you to authenticate users on switches by redirecting Web browser requests to a login page that requires users to input a valid username and password before they can access the network. WEB-Based Local Account can be defined as the process of verifying someone's identity by using pre-required details (Commonly username and password).

802.1X: 802.1X is an IEEE standard for port-based network access control (PNAC). It provides an authentication mechanism for devices seeking to access a LAN.

During the authentication process, the switch completes multiple message exchanges between the end device and the authentication server While 802.1X authentications is in process, only 802.1X traffic and control traffic can transit the network.

The 802.1X authentication method only works if the end device is 802.1X-enabled, but many single-purpose network devices such as printers and IP phones do not support the 802.1X protocol. You can configure MAC RADIUS authentication on interfaces that are connected to network devices that do not support 802.1X and for which you want to allow to access the LAN. When an end device that is not 802.1X-enabled is detected on the interface, the switch transmits the MAC address of the device to the authentication server. The server then tries to match the MAC address with a list of MAC addresses in its database. If the MAC address matches an address in the list, the end device is authenticated.

4.1 AUTHENTICATION

Use **“authentication”** command to enable the global setting of 802.1x/MAC/WEB authentication network access control. Use the **“no”** form of this command to disable 802.1x/MAC/WEB authentication.

Switch#**configure terminal**

Switch(config)#**authentication (dot1x|mac|web)**

Switch(config)#**no authentication**

(dot1x|mac|web)

Syntax	**authentication (dot1x|mac|web)** **no authentication (dot1x|mac|web)**
Example	The following example shows how to enable 802.1x/MAC/WEB authentication. Switch#**configure terminal** Switch(config)# **authentication dot1x** Switch(config)# **authentication mac** Switch(config)# **authentication web** Switch# **show authentication**

4.2 AUTHENTICATION (INTERFACE)

Use **“authentication”** interface command to enable the port setting of 802.1x/MAC/WEB authentication network access control. Use the **“no”** form of this command to disable 802.1x/MAC/WEB authentication.

Switch#configure terminal

Switch(config)#authentication (dot1x|mac|web)

Switch(config)#no authentication

(dot1x|mac|web)

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

Default Default is disabled for all type

Mode Interface Configuration

The following example shows how to enable 802.1x/MAC/WEB authentication.

Switch#configure terminal

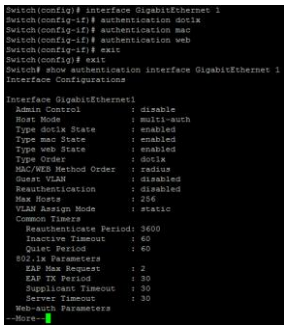
Switch(config)# interface GigabitEthernet

1 Switch(config-if)# authentication dot1x

Switch(config-if)# authentication mac

Example Switch(config-if)# authentication web

Switch# show authentication interface GigabitEthernet 1



4.3 AUTHENTICATION MAC RADIUS

Use **"authentication mac radius"** command to configure the radius user id format used by MAC authentication Radius method.

Switch#**configure terminal**

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

Syntax	**authentication mac radius [mac-case (lower|upper)] [mac delimiter(colon|dot|hyphen|none) [gap (2|4|6)]]**
Parameter	**mac-case (lower|upper)** Select radius user id to be upper case or lower case.mac- delimiter(colon|dot|hyphen|none) Select radius user id delimiter colon: XX:XX:XX:XX:XX:XX dot: XX.XX.XX.XX.XX.XX hyphen: XX-XX-XX-XX-XX-XX none: XXXXXXXXXXXX gap (2|4|6) Select delimiter gap 2: XX-XX-XX-XX-XX-XX 4: XXXX-XXXX-XXXX 6: XXXXXX-XXXXXX
Default	Default radius id format is upper case with none
delimiter. Mode	Global Configuration

The following example shows how to configure MAC authentication radius id format to be upper case with colon delimiter every 2 chars

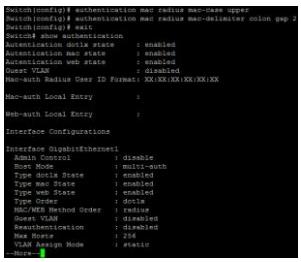
Switch#**configure terminal**

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

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

Exampl
e

Switch# **show authentication**



4.5 AUTHENTICATION MAC LOCAL

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

Switch#**configure terminal**

Switch(config)#**authentication mac local mac-addr control auth** [**vlan** *<1-4094>*] [**reauth-period** *<300-4294967294>*] [**inactive-timeout** *<60-65535>*]

Switch(config)#**authentication mac local mac-addr control**

unauth Switch(config)#**no authentication mac local mac-addr**

Syntax	**authentication mac local mac-addr control auth** [**vlan** *<1-4094>*] [**reauth-period** *<300-4294967294>*] [**inactive-timeout** *<60-65535>*] **authentication mac local mac-addr control unauth** Switch(config)#**no authentication mac local mac-addr**
Parameter	**mac-addr** MAC Authentication local MAC address. **control auth** Host with this MAC address will be authorized. **control unauth** Host with this MAC address will be force-unauthorized **vlan** *<1-4094>*MAC Authentication host assigned VLAN. **reauth-period** *<300-4294967294>*MAC Authentication host reauthentication period inactive-timeout. *<60-65535>*MAC authentication host inactive timeout.
Default	Default is no local MAC Authentication
entry. Mode	Global Configuration

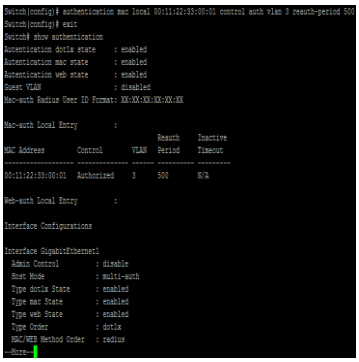
The following example shows how to add a new local mac authentication host.

Switch#configure terminal

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

Switch# show authentication

Example



4.6 AUTHENTICATION GUEST-VLAN

Use **“authentication 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.

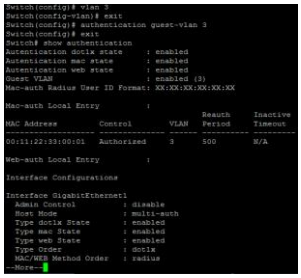
Switch#**configure terminal**

Switch(config)#**authentication guest-vlan** *<1-*

4094> Switch(config)#**no authentication guest-**

vlan

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**



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**

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

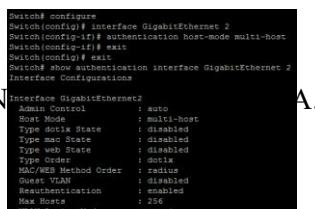
Switch(config)# **interface** {interface-name}

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



4.9 AUTHENTICATION MAX-HOSTS

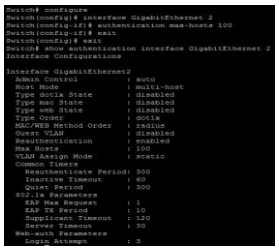
Use **"authentication max-hosts"** command to configure the port max hosts number for multi-auth mode. The host exceed the max host number is not allowed to create authentication session and do authenticating. Use **"no"** form of this command to restore default value.

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**



4.10 AUTHENTICATION METHOD

Use **"authentication method"** command to configure the port authentication method order.

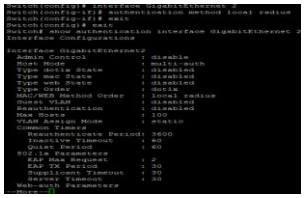
Switch#**configure terminal**

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 method.	Default is RADIUS method in first place and no other
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

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

Example

Switch# show authentication interface GigabitEthernet 2

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

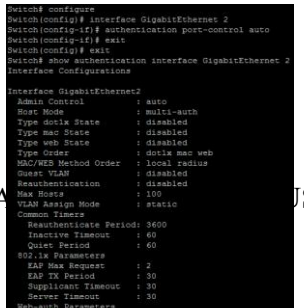
Switch#**configure terminal**

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**



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.

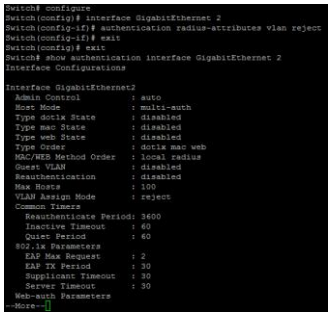
Switch#**configure terminal**

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



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

The following example shows how to enable port reauthentication.

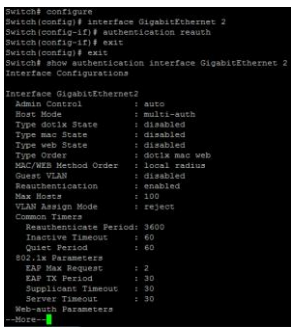
Switch#**configure terminal**

Switch(config)# **interface**

GigabitEthernet 2 Switch(config-if)#

authentication reauth

Example Switch# **show authentication interface** GigabitEthernet 2



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.

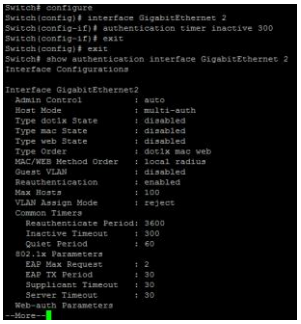
Switch#**configure terminal**

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.

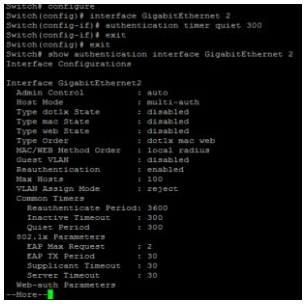
Switch#**configure terminal**

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



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.

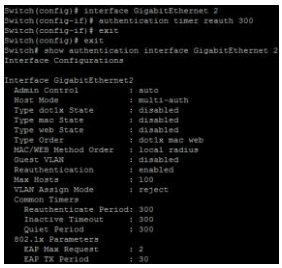
Switch#**configure terminal**

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 (encrypted CRYPT-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

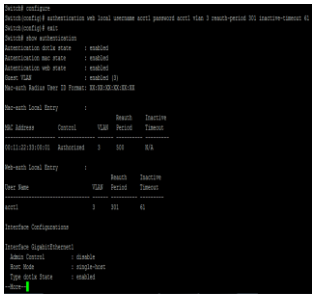
The following example shows how to add/delete a new local account.

Switch#configure terminal

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

Switch# show authentication

Exampl
e



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.

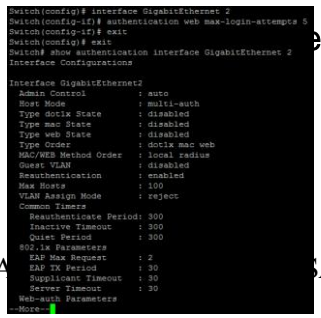
Switch#**configure terminal**

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 **ntication interface** GigabitEthernet 2



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

l authentication sessions.

The following example shows how to clear all

Switch# clear authentication sessions

Switch# show authentication sessions

4.21 DOT1X

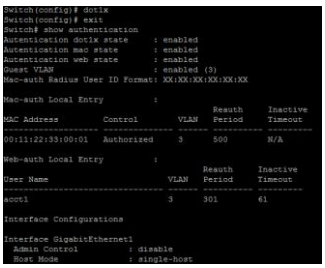
Use “dot1x” command to enable the global setting of 802.1x. The “authentication dot1x” command has the same effect as this one. This command is a backward compatible command. Use the “no” form of this command to disable 802.1 x authentications.

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



4.22 DOT1X GUEST-VLAN

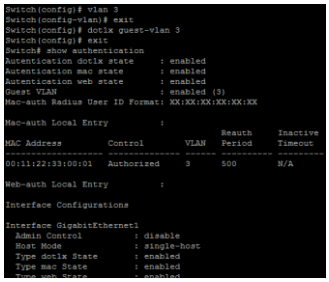
Use **“dot1x guest-vlan”** command to enable the global setting of guest VLAN and specify guest VLAN ID. Use the **“no”** form of this command to disable guest VLAN.

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**

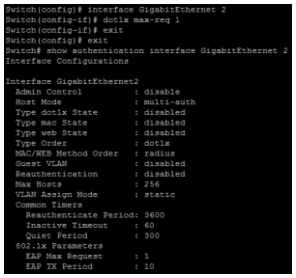
Switch(config)# **interface** {interface-

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



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.

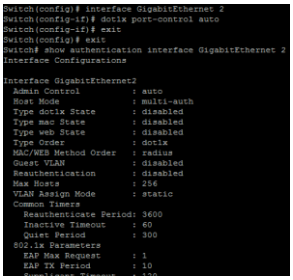
Switch#**configure terminal**

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



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

```
Switch(config)# interface GigabitEthernet 2
Switch(config-if)# dot1x 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 Method Order   : radius
  Guest VLAN             : disabled
  Reauthentication       : enabled
  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
```

4.26 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>*

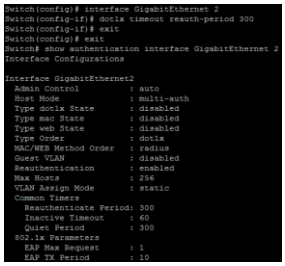
Switch(config-if)# **no dot1x timeout reauth-period**

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
	e

Exampl

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
```



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.

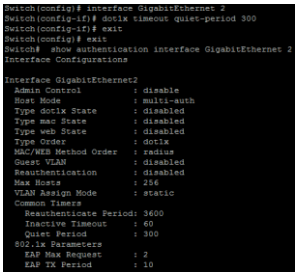
Switch#**configure terminal**

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



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.

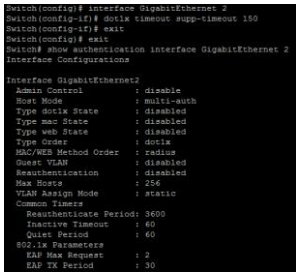
Switch#**configure terminal**

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



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.

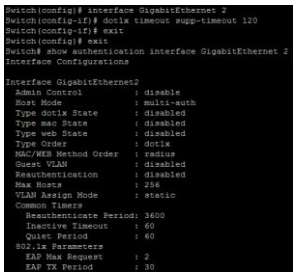
Switch#**configure terminal**

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.

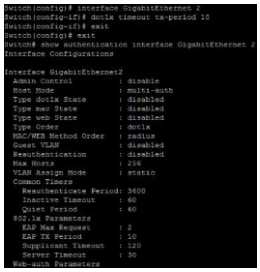
Switch#**configure terminal**

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



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

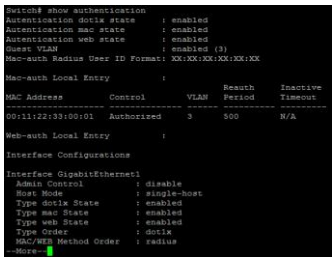
show authentication interfaces *{IF_PORTS}*

Parameter **Interfaces** *IF_PORTS* Specify port list to show port

configurations Mode Privileged EXEC

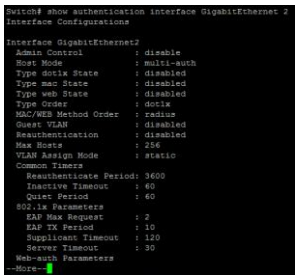
This example shows how to show the mac authentication configurations of port GigabitEthernet 1.

Switch# **show authentication**



Example

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

E2000 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.

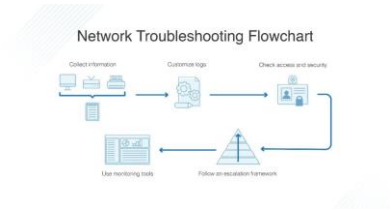


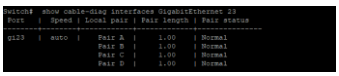
Fig 5.1.1 Network Troubleshooting Flowchart

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**

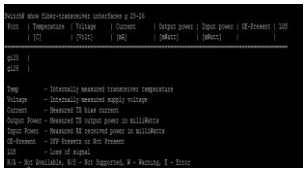


5.2 SHOW FIBER-TRANSCEIVER

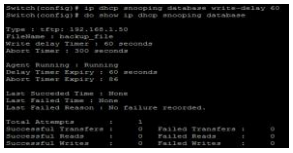
To show the diagnostic information of the fiber transceivers use the command. show fiber-transceiver in the Privilege EXEC mode.

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



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

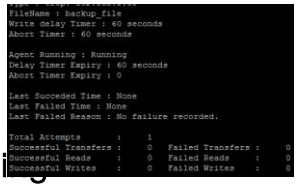
Example

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(config)#do show ip dhcp snooping



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**

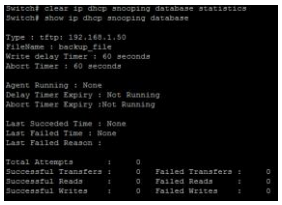
statistics Mode Privileged EXEC

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**

Example



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**

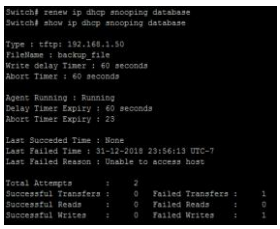
Syntax **renew ip dhcp snooping database**

Mode Privileged EXEC

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**

Example 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**

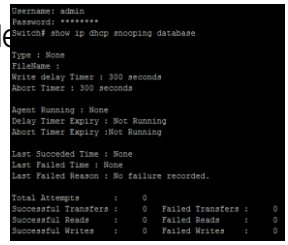
Syntax **show ip dhcp snooping database**

Mode Privileged EXEC

The example shows how to show settings of DHCP Snooping agent.

Switch # **show ip dhcp snooping database**

Example



DOS Denial-of-Service (DoS)

7.1 DOS

A **Denial-of-Service (DoS) attack** is an attack meant to shut down a machine or network, making it inaccessible to its intended users. DoS attacks accomplish this by flooding the target with traffic, or sending it information that triggers a crash. In both instances, the DoS attack deprives legitimate users (i.e. employees, members, or account holders) of the service or resource they expected.

Victims of DoS attacks often target web servers of high-profile organizations such as banking, commerce, and media companies, or government and trade organizations. Though DoS attacks do not typically result in the theft or loss of significant information or other assets, they can cost the victim a great deal of time and money to handle.

There are two general methods of DoS attacks: flooding services or crashing services. Flood attacks occur when the system receives too much traffic for the server to buffer, causing them to slow down and eventually stop. Popular flood attacks include:

• Buffer overflow attacks – the most common DoS attack. The concept is to send more traffic to a network address than the programmers have built the system to handle. It includes the attacks listed below, in addition to others that are designed to exploit bugs specific to certain applications or networks.
• ICMP flood – leverages misconfigured network devices by sending spoofed packets that ping every computer on the targeted network, instead of just one specific machine. The network is then triggered to amplify the traffic. This attack is also known as the smurf attack or ping of death.
• SYN flood – sends a request to connect to a server, but never complete. Continues until all open ports are saturated with requests and none are available for legitimate users to connect to.

Other DoS attacks simply exploit vulnerabilities that cause the target networks or service to crash. In these attacks, input is sent that takes advantage of bugs in the target that subsequently crash or severely destabilize the network, so that it can't be accessed or used.

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

Switch#**configure terminal**

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

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

Syntax

dos (daeqsa-deny|icmp-frag-pkts-deny|icmpv4-ping-max- check|icmpv6-ping-max-check|ipv6-min-frag-size-check|land-deny|nullscan-deny|pod-deny|smurf-deny|syn- sportl1024-

deny|synfin-deny|synrst-deny|tcp-frag-off-min-check|tcpblat-deny|tcphdr-min- check|udpblat-deny|xmas-deny)

dos icmp-ping-max-length MAX_LEN

dos ipv6-min-frag-size-length MIN_LEN

dos smurf-netmask MASK

dos tcphdr-min-length HDR_MIN_LEN

no dos (tcp-frag-off-min-check|synrst-deny|synfin-deny|xma- deny|nullscan-deny|syn-sportl1024-deny|tcphdr-min-check|smurf- deny|icmpv6-ping-max-check|icmpv4-ping- max-check|icmp-frag- pkts-deny|ipv6-min-frag-size-check|pod-deny|tcpblat-deny|udpblat- deny|land-deny|daeqsa-deny)

daeqsa-deny Drops the packets if the destination MAC address is equal to the source MAC address.

icmp-frag-pkts-deny Drops the fragmented ICMP packets.

icmpv4-ping-max- check Checks the maximum size of ICMP ping packets, and drops the packets larger than the maximum packet size defined by the command dos icmp-ping-max- length MAX_LEN

icmpv6-ping-max- check Checks the maximum size of ICMPv6 ping packets, and drops the packets larger than the maximum packet size defined by the command dos icmp-ping-max- length MAX_LEN.

ipv6-min-frag- size-check Checks the minimum size of IPv6 fragments, and drops the packets smaller than the minimum size defined by the command dos ipv6-min-frag-size-length MIN_LEN.

land-deny Drops the packets if the source IP address is equal to the destination IP address.

nullscan-deny Drops the packets with NULL scan.

pod-deny Avoids ping of death attack.

smurf-deny Avoids smurf attack.

syn-sportl1024-deny Drops SYN packets with sport less than 1024.

Paramet er

synfin-deny Drops the packets with SYN and FIN bits set.

synrst-deny Drops the packets with SYN and RST bits set.

tcp-frag-off-min- check Drops the TCP fragment packets with offset equals to one.

tcpblat-deny Drops the packages if the TCP source port is equal to the TCP destination port.

tcphdr-min-check Checks the minimum TCP header and drops the TCP packets with the header smaller than the minimum size defined by the command dos tcphdr-min-length HDR_MIN_LEN.

udpblat-deny Drops the packets if the UDP source port equals to the UDP destination port.

value is 512 bytes.

xmas-deny Drops the packets if the sequence number is zero, and the FIN, URG and PSH bits are set.

ipv6-min-frag- size-length MIN_LEN Specify the minimum size of IPv6 fragments. The valid range is from 0 to 65535 bytes, and default value is 1240 bytes.

smurf-netmask MASK Specify the netmask of smurf attack. The length range is from 0 to 323 bytes, and default length is 0 bytes.

tcphdr-min-length HDR_MIN_LEN Specify the minimum TCP header length. The length range is from 0 to 31 bytes, and default length is 20 bytes.

icmp-ping-max-length MAX_LEN Specify the maximum size of the ICMPv4/ICMPv6 ping packets. The valid range is from 0 to 65535 bytes, and the default

Default

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

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

Mode

Global Configuration

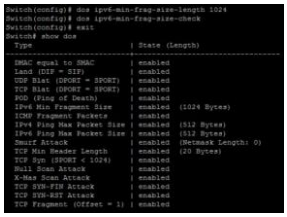
Example

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

Switch#**configure terminal**

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

Switch(config)# **dos ipv6-min-frag-size-check**



7.2 DOS (INTERFACE)

To enable the DoS on the specific interface, use the command **dos** in the Interface Configuration mode. Otherwise, use the **"no"** form of the command to disable the DoS on the interface.

Switch#**configure terminal**

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

ID} Switch(config-if)# **dos**

Switch(config-if)# **no dos**

dos

Syntax **no dos**

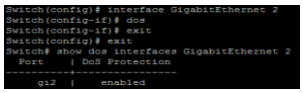
Default DoS protection is disabled on each

interface. Mode Interface Configuration

The following example enables the DoS on the interface GigabitEthernet 2.

Switch#**configure terminal**

ExampleSwitch(config)# **interface**



GigabitEthernet 2 Switch(config-if)# **dos**

7.3 SHOW DOS

To show the DoS protection configuration, use the command **show dos** in the Privileged EXEC mode. For the status of DoS protection on each interface, use the command show dos interface in the Privileged EXEC mode.

Switch# **show dos**

Switch# **show dos interface** *{IF_PORTS}*

Syntax

show dos

show dos interface *{IF_PORTS}*

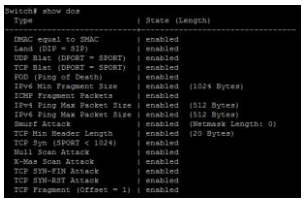
Parameter **interface** *{IF_PORTS}* An interface ID or the list of interface

IDs Mode Privileged EXEC

The following example shows the global DoS protection configuration.

Switch# **show dos**

Example



DYNAMIC ARP INSPECTION

A switch can use DAI (Dynamic ARP Inspection) to prevent certain types of attacks that leverage the use of IP ARP messages. DAI is a security feature that validates ARP packets in a network. DAI intercepts, logs, and discards ARP packets with invalid IP-to-MAC address bindings. This capability protects the network from some man-in-the-middle attacks.

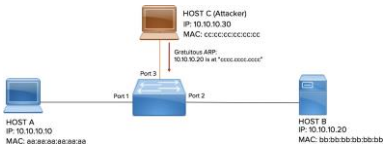


Fig 8.1 Dynamic ARP Inspection Setup

DAI ensures that only valid ARP requests and responses are

relayed. The switch performs these activities:

• Intercepts all ARP requests and responses on untrusted ports

• Verifies that each of these intercepted packets has a valid IP-to-MAC address binding before updating the local ARP cache or before forwarding the packet to the appropriate destination

• Drops invalid ARP packets

DAI determines the validity of an ARP packet based on valid IP-to-MAC address bindings stored in a trusted database, the DHCP snooping binding database. This database is built by DHCP snooping if DHCP snooping is enabled on the VLANs and on the switch. If the ARP packet is received on a trusted interface, the switch forwards the packet without any checks. On untrusted interfaces, the switch forwards the packet only if it is valid.

DAI can validate ARP packets against user-configured ARP access control lists (ACLs) for hosts with statically configured IP addresses.

8.1 IP ARP INSPECTION

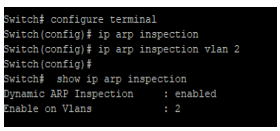
Use the **ip arp inspection** command to enable Dynamic Arp Inspection function. Use the **"no"** form of this command to disable.

Switch#**configure terminal**

Switch(config)#**ip arp inspection**

Switch(config)#**no ip arp inspection**

Syntax	**ip arp inspection** **no ip arp inspection**
Default	Dynamic Arp inspection is disabled
Mode	Global Configuration
Example	The example shows how to enable Dynamic Arp Inspection on VLAN 2. You can verify settings by the following show ip arp inspection command. Switch#**configure terminal** Switch(config)# **ip arp inspection** Switch(config)# **ip arp inspection vlan** 2 switch# **show ip arp inspection**



8.2 IP ARP INSPECTION VLAN

Use the **ip arp inspection vlan** command to enable VLANs on Dynamic Arp Inspection function. Use the
"no" form of this command to disable VLANs on Dynamic Arp Inspection function.

Switch#**configure terminal**

Switch(config)# **ip arp inspection vlan** *{VLAN-LIST}*

Switch(config)# **no ip arp inspection vlan** *{VLAN-LIST}*

Syntax	**ip arp inspection vlan** *{VLAN-LIST}* **no ip arp inspection vlan** *{VLAN-LIST}*
Parameter	*VLAN-LIST*Specify VLAN ID or a range of VLANs to enable or disable dynamic Arp inspection
Default	Default is disabled on all
VLANs Mode	Global Configuration

Example

The example shows how to enable VLAN 1-100 on Dynamic Arp Inspection, and then disable VLAN 30-40 on Dynamic Arp Inspection. You can verify settings by the following show ip arp inspection command.

Switch#**configure terminal**

Switch(config)# **vlan** 1-100

Switch(config)# **ip arp inspection**

Switch(config)# **ip arp inspection vlan** 1-100

Switch# **show ip arp inspection**

8.3 IP ARP INSPECTION TRUST

Use the **ip arp inspection trust** command to set trusted interface. The switch does not check ARP packets that are received on the trusted interface; it simply forwards it. Use the **"no"** form of this command to set untrusted interface.

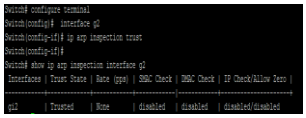
Switch#**configure terminal**

Switch(config)# **Ip arp inspection trust**

Switch(config)# **no ip arp inspection**

trust

Syntax	**ip arp inspection trust** **no ip arp inspection trust**
Default	Dynamic Arp inspection 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 arp inspection interface command. Switch#**configure terminal** Switch(config)# **interface gi2** Switch(config)# **ip arp inspection trust** Switch#**show ip arp inspection interface** gi2



8.4 IP ARP INSPECTION VALIDATE

Use the **ip arp inspection validate** command to enable validate function on interface. The **"src-mac"** drop ARP requests and reply packets that arp-sender-mac and ethernet- source-mac is not match. The **"dst- mac"** drops ARP reply packets that arp-target-mac and ethernet-dst-mac is not match. The **"ip"** drop ARP request and reply packets that sender-ip is invalid such as broadcast multicast all zero IP address and drop ARP reply packets that target-ip is invalid. The **"allow-zeros"** means won't drop all zero IP address. Use the **"no"** form of this command to disable validation.

Switch#**configure terminal**

Switch(config)# **ip arp inspection validate src-mac**

Switch(config)# **ip arp inspection validate dst-mac**

Switch(config)# **ip arp inspection validate ip [allow-zeros]**

Switch(config)# **no ip arp inspection validate src-mac**

Switch(config)# **no ip arp inspection validate dst-mac**

Switch(config)# **no ip arp inspection validate ip [allow-zeros]**

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

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.

Example

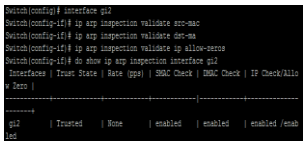
Switch#**configure terminal**

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

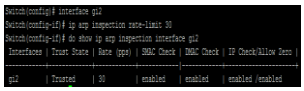
Use the **ip arp inspection rate-limit** command to set rate limitation on interface. The switch drop ARP packets after receives more than configured rate of packets per second. Use the **"no"** form of this command to return to default settings.

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

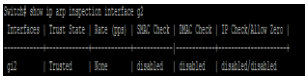
Mode Privileged EXEC

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**

Exampl e

switch# **show ip arp inspection interfaces gi2**



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

The example shows how to show settings of Dynamic Arp Inspection

Example 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

switch# **show ip arp inspection**

Example

```
Switch# show ip arp inspection
Dynamic ARP Inspection     : enabled
Enable on Vlans            : 1-100

Switch# show ip arp inspection interface gi2
 Interfaces | Trust State | Rate (pps) | SMAC Check | DMAC Check | IP Check/Allow Zero |
------------+-------------+------------+-----------+------------+---------------------+
 gi2        | Trusted     | 30         | enabled   | enabled    | enabled /enabled    |
```

GVRP (GARP VLAN Registration Protocol)

9.1 GVRP (GLOBAL)

GARP VLAN Registration Protocol (GVRP) is a Generic Attribute Registration Protocol (GARP) application that provides 802.1Q-compliant VLAN pruning and dynamic VLAN creation on 802.1Q trunk ports.

Fig 9.1 GVRP Participant List

With GVRP, the switch can exchange VLAN configuration information with other GVRP switches, prune unnecessary broadcast and unknown unicast traffic, and dynamically create and manage VLANs on switches connected through 802.1Q trunk ports. You must enable GVRP globally before any GVRP processing occurs on the switch. Enabling GVRP globally enables GVRP to perform VLAN pruning on IEEE 802.1Q trunk links. Pruning occurs only on GVRP-enabled trunks.

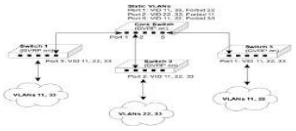


Fig 9.2 GVRP VLAN sharing

Disable **gvrp** will clear all learned dynamic vlan entry and do not learn dynamic vlan anymore. Use **'show gvrp'** to show configuration.

Switch#**configure terminal**

Switch(config)# **gvrp**

Switch(config)# **no gvrp**

Syntax	**gvrp** **no gvrp**

Default GVRP is disabled

Mode Global

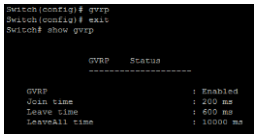
Configuration

The following example specifies that set global gvrp test.

Switch#**configure terminal**

Switch(config)# **gvrp**

Example Switch# **show gvrp**



9.2 GVRP (INTERFACE)

'no gvrp' will remove dynamic port from vlan. **'gvrp'** must work at port mode is trunk.

Switch#**configure terminal**

Switch(config)# **gvrp**

Switch(config)# **no gvrp**

Switch# **show gvrp configuration interfaces** gi2

Syntax	**gvrp** **no gvrp**
Default	GVRP is disabled on
interface Mode	Interface mode
Example	The following example specifies that set port gvrp test. The port gvrp enable must set port mode is trunk firstly. Switch#**configure terminal** Switch(config)#**interface** gi2 Switch(config-if)# **switchport mode** **trunk** Switch(config)#**gvrp** Switch# **show gvrp configuration interfaces** gi2

9.3 GVRP REGISTRATION-MODE

When set registration-mode is fixed or forbidden, will remove the port from vlan which is dynamic port and not learning vlan.

Switch#**configure terminal**

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

Switch(config-if)# **gvrp registration-mode (normal | fixed | forbidden)**

Syntax	**gvrp registration-mode (normal | fixed | forbidden)**
Parameter	**(normal | fixed | forbidden)** normal: register dynamic vlan, and transmit all vlan attribute. fixed: do not register dynamic vlan, and only transmit static vlan attribute. forbidden: do not register dynamic vlan, and only transmit default vlan attribute.
Mode	Interface mode
Example	The following example specifies that set gvrp registration mode test. Switch#**configure terminal** Switch(config)# **interface** gi2 Switch(config-if)# **gvrp registration-mode fixed**

Switch# **show gvrp configuration interfaces** gi2

9.4 GVRP VLAN-CREATE-FORBID

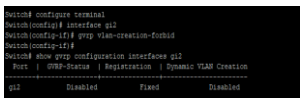
'gvrp vlan-creation-forbid' will not remove dynamic port from vlan immediate. Switch#configure terminal

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

Switch(config-if)# gvrp vlan-creation-forbid

Switch(config-if)# no gvrp vlan-creation-forbid

Syntax	gvrp vlan-creation-forbid no gvrp vlan-creation-forbid
Mode	Interface mode
Example	The following example specifies that set port gvrp vlan-creation-forbid test. Switch#configure terminal Switch(config)#interface gi2 Switch(config-if)# gvrp vlan-creation-forbid Switch(config-if)#exit Switch# show gvrp configuration interfaces gi2

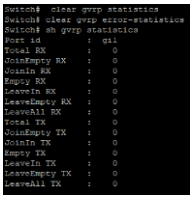


9.5 CLEAR GVRP STATISTICS

This command will clear the ports error statistics or statistics info.

Switch# clear gvrp (error-statistics | statistics) [interfaces *{IF_PORTS}*]

Syntax	clear gvrp (error-statistics | statistics) [interfaces *{IF_PORTS}*]
Parameter	(error-statistics | statistics) [interfaces IF_PORTS] Error-statistics: error gvrp packet statistics Statistics: gvrp event message statistics Specifies posts to clear statistics
Mode	Privileged EXEC
Example	The following example specifies that clear gvrp error statistics and statistics test. Switch# clear gvrp statistics Switch# clear gvrp error-statistics



9.6 SHOW GVRP STATISTICS

This command will display the ports error statistics or statistics info.

Switch# **show gvrp (statistics | error-statistics) [interfaces**

{IF_PORTS}]

Syntax **show gvrp (statistics | error-statistics) [interfaces** ***{IF_PORTS}***]

Parameter none Display all ports (statistics| error- statistics) [interfaces *IF_PORTS*]

statistics – GVRP statistics error-statistics GVRP error statistics Specifies posts

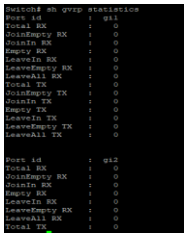
Default Display all ports statistics

info Mode Privileged EXEC

The following example specifies that display gvrp error statistics and statistics test.

Switch# **show gvrp statistics**

Example



9.7 SHOW GVRP

This command will display the gvrp global

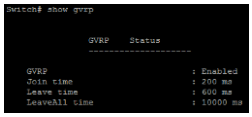
info. Switch# **show gvrp**

Syntax **show gvrp**

Mode Privileged EXEC

The following example specifies that display gvrp test.

Example 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}*]

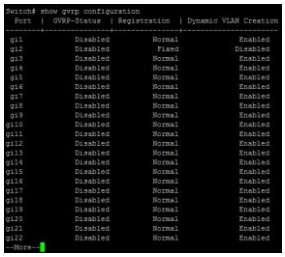
Parameter **none [interfaces** *IF_PORTS*] Display all ports configuration Display Specifies posts configuration

Mode Privileged EXEC

The following example specifies that display gvrp port configuration

test. Switch# **show gvrp configuration**

Example



IGMP SNOOPING

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

Parameter **none** Show ip igmp router include dynamic and static and forbidden

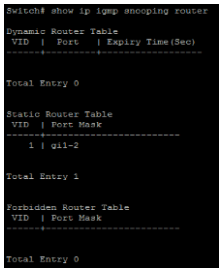
(dynamic | forbidden | static) Display Ip igmp router info for different type

Mode Privileged EXEC

The following example specifies that show ip igmp snooping

router. Switch# **show ip igmp snooping router**

Example



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**

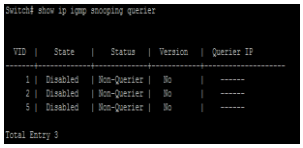
Syntax **show ip igmp snooping querier**

Mode Privileged EXEC

The following example specifies that show ip igmp snooping querier test.

Switch# **show ip igmp snooping querier**

Example



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

The following example specifies that show ip igmp snooping test.

Switch# **show ip igmp snooping**

Example

```
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

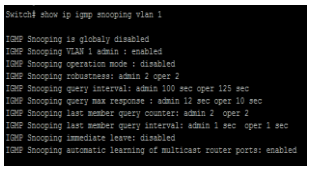
[VLAN-LIST] Show specifies vlan ip igmp snooping info

Mode Privileged EXEC

The following example specifies that show ip igmp snooping vlan test.

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

Example

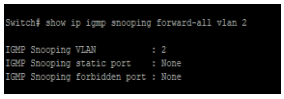


10.33 SHOW IP IGMP SNOOPING FORWARD-ALL

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

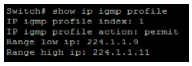
info [*<1-128>*] Show specifies index

profile info

Mode Privileged EXEC

The following example specifies that show ip igmp profile test.

Example 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

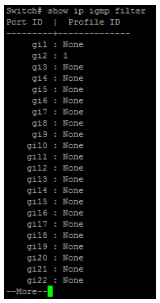
none Show all port filter

[interfaces *IF_PORTS*] Show specifies ports filter

Mode Privileged EXEC

The following example specifies that show ip igmp filter test. Switch# **show ip igmp filter**

Example



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

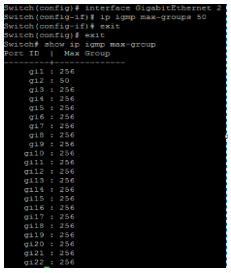
The following example specifies that show ip igmp max-group test.

Switch#**configure terminal**

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

Switch(config-if)#**ip igmp max-groups**

Example 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

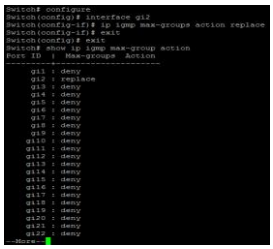
The following example specifies that show ip igmp max-group action test.

Switch#**configure terminal**

Switch(config)#**interface** gi2

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

Example 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.

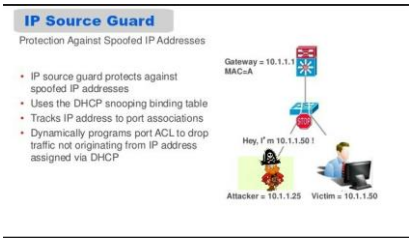


Fig 11.1 IP Source Guard Concept

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 bi[illegible] DHCP.

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

Comparison between DAI and 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.

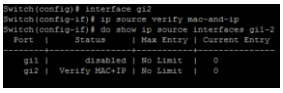
Switch#**configure terminal**

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

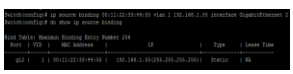
Use the ip source binding command to create a static IP source binding entry has an IP address, its associated MAC address, VLAN ID interface. Use the **"no"** form of this command to delete static entry.You can verify settings by the **"show ip source binding"** command.

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

The example shows how to show settings of IP Source Guard of interface gi1

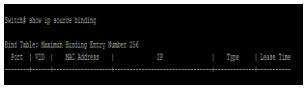
Exampl e Switch# **show ip source interfaces gi2**

```
Switch# show ip source interfaces gi2
 Port  |    Status     | Max Entry | Current Entry
-------+---------------+-----------+---------------
  gi2  |    disabled   | No Limit  |   0
```

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

LACP, a sub component of IEEE 802.3ad, provides additional functionality for link aggregation groups (LAGs). Use the link aggregation feature to aggregate one or more Ethernet interfaces to form a logical point-to-point link, known as a LAG, virtual link, or bundle. The MAC client can treat this virtual link like a single link.

Link aggregation increases bandwidth, provides graceful degradation as failure occurs, and increases availability. It provides network redundancy by load-balancing traffic across all available links. If one of the links fails, the system automatically load-balances traffic across all remaining links.

When LACP is not enabled, a local LAG might attempt to transmit packets to a remote single interface, which causes the communication to fail. When LACP is enabled, a local LAG cannot transmit packets unless a LAG with LACP is also configured on the remote end of the link.

A typical LAG deployment includes aggregate trunk links between an access switch and a distribution switch or customer edge (CE) device.

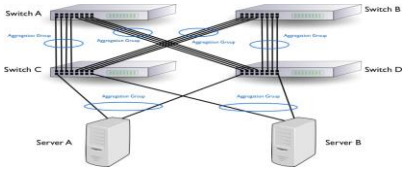


Fig 12.1 Link aggregation Concept

12.1 LAG

Link aggregation group function allows you to aggregate multiple physical ports into one logic port to increase bandwidth. This command makes normal port join into the specific LAG logic port with static or dynamic mode. Use **"no lag"** to leave the LAG logic port.

Switch#**configure terminal**

Switch(config)# **lag load-balance (src-dst-mac | src-dst-mac-ip)**

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

Switch(config-if)# **lag** *<1-8>* **mode (static | active | passive)**

Switch(config-if)# **no lag**

Note:-Use static mode to enable LAG on Ports.

Syntax	**lag** *<1-8>* **mode (static | active | passive) no lag**
Parameter	*<1-8>* Specify the LAG id for the interface **static** Specify the LAG to be static mode and join the interface into this LAG. **active** Specify the LAG to be dynamic mode and join the interface into this LAG with LACP active port. **passive** Specify the LAG to be dynamic mode and join the interface into this LAG with LACP passive port
Mode	Interface Configuration

Example

This example shows how to create a dynamic LAG and join fa1-fa3 to this LAG.

Switch#**configure terminal**

Switch(config)# **lag load-balance src-dst-mac-ip**

Switch(config)# **interface**

GigabitEthernet 1 Switch(config-if)# **lag**

1 mode static

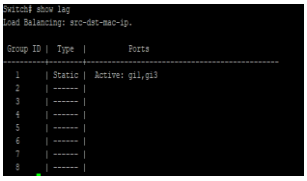
Switch(config)# **interface**

GigabitEthernet 3 Switch(config-if)# **lag**

1 mode static

To show current LAG status. Use command **show lag**

Switch# **show lag**



12.2 LAG LOAD-BALANCE

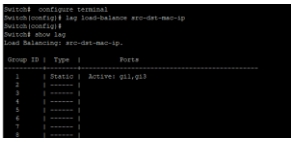
Link aggregation group port should transmit packets spread to all ports to balance traffic loading. There are two algorithms supported and this command allows you to select the algorithm.

Switch#configure terminal

Switch(config)# lag load-balance (src-dst-mac | src-dst-mac-ip)

Switch(config)# no lag load-balance

Syntax	lag load-balance (src-dst-mac | src-dst-mac-ip) no lag load-balance
Parameter	src-dst-mac Specify algorithm to balance traffic by using source and destination MAC address for all packets. src-dst-mac-ip Specify algorithm to balance traffic by using source and destination IP address for IP packets and using source and destination MAC address for non-IP packets.
Default	Default load balance algorithm is src-dst-mac
Mode	Global Configuration
Example	This example shows how to change load balance algorithm to src-dst-mac-ip. Switch#configure terminal Switch(config)# lag load-balance src-dst-mac-ip To show current load balance algorithm use show lag. Switch# show lag



12.3 LACP

Link Aggregation Control Protocol (LACP) is part of the IEEE specification

(802.3az) that enables you to bundle several physical ports together to form

a single logical

channel (LAG). The Link Aggregation Control Protocol (LACP) provides a method to control the bundling of several physical ports together to form a single logical channel. LAGs multiply the bandwidth, increase port flexibility, and provide

link redundancy between two

devices. Two types of LAGs are

supported:

Static LAG : A LAG is static if the LACP is disabled on it. The group of

ports assigned to a static LAG are always active members.

Dynamic LAG : In Dynamic LAG LACP is enabled on it. The group of ports

assigned to dynamic LAG determines which ports are active member ports. The non-active ports are standby ports ready to replace any failing active member ports.

Load Balancing Traffic forwarded to a LAG is load-balanced across the active member ports, thus achieving an effective bandwidth close to the aggregate bandwidth of all the active member ports of the LAG. Traffic load balancing over the active member ports of a LAG is managed by a hash-based distribution function that distributes Unicast and Multicast traffic based on Layer 2 or Layer 3 packet header information.

The device supports two modes of load balancing:

MAC Addresses :Based on the Destination and Source MAC addresses of all packets.

IP and MAC Addresses: Based on the Destination and Source IP addresses for IP packets, and Destination and Source MAC addresses for non-IP packets.

Timeout: The Timeout controls the period between BPDU transmissions. Long will transmit LACP packets each second, while Short will wait for 30 seconds before sending a LACP packet.

Port Priority: It controls the priority of the ports. If the LACP partner wants to form a larger group than is supported by this device then this parameter will control which ports will be active & which ports will in backup role. Lower the number means greater the priority. By default system priority for LACP is 32768.

LAG is treated by the system as a single logical port. In particular, the LAG has port attributes similar to a regular port, such as state and speed.

The device supports 8 LAGs with up to 8 ports in a LAG group. Link Aggregation Control Protocol (LACP) provides a standardized means for exchanging information between Switches connected by multiple links that require high-speed redundant links.

Switch#configure terminal

Switch(config)# lag load-balance (src-dst-mac | src-dst-mac-ip)

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

Switch(config-if)# lag *<1-8>* mode (static | active | passive)

Switch(config-if)# no lag

Note:-Use active and passive mode to enable LACP on Ports.

Syntax	lag *<1-8>* mode (static | active | passive) no lag
Parameter	*<1-8>* Specify the LAG id for the interface **static** Specify the LAG to be static mode and join the interface into this LAG. **active** Specify the LAG to be dynamic mode and join the interface into this LAG with LACP active port. **passive** Specify the LAG to be dynamic mode and join the interface into this LAG with LACP passive port
Mode	Interface Configuration

This example shows how to create a dynamic LAG and join fa1-fa3 to this LAG.

Switch#configure terminal

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

Switch(config)# interface

GigabitEthernet 1 Switch(config-if)# lag

1 mode active Switch(config)# interface

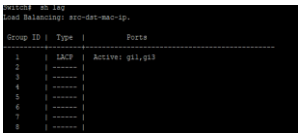
GigabitEthernet 3

Switch(config-if)# lag 1 mode active

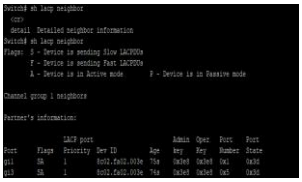
Exampl
e

This example shows how to show current LAG status.

Switch# show lag



Switch# show lacp neighbor



12.3 LACP PORT-PRIORITY

LACP port priority is used for two connected DUT to select aggregation ports. Lower port priority value has higher priority. And the port with higher priority will be selected into LAG first.

Switch#**configure terminal**

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

Switch(config-if)# **lacp port-priority** *<1-*

65535> Switch(config-if)# **no lacp port-**

priority

Syntax

lacp port-priority *<1-65535>*

no lacp port-priority

Parameter *<1-65535>* Specify port priority

value Default Default port priority is 1.

Mode Interface Configuration

Example

This example shows how to configure interface GigabitEthernet 3 with lacp port priority to 1.

Switch#**configure terminal**

Switch(config)# **interface**

GigabitEthernet 3 Switch(config-if)#

lacp port-priority 1 Switch# **show lacp**

neighbor detail

12.4 LACP SYSTEM-PRIORITY

LACP system priority is used for two connected DUT to select master switch. Lower system priority value has higher priority. And the DUT with higher priority can decide which ports are able to join the LAG. Use **"no lacp system-priority"** to restore to the default priority value.

Switch#**configure terminal**

Switch(config)# **lacp system-priority** *<1-65535>*

Switch(config)# **no lacp system-priority**

Syntax

lacp system-priority *<1-65535>*

no lacp system-priority

Parameter*<1-65535>*Specify system priority

value Default Default system priority is

32768.

Mode Global Configuration

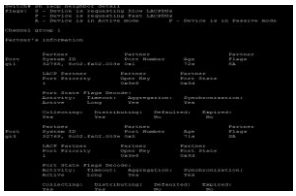
Example

This example shows how to configure lacp system priority to 32768.

Switch#**configure terminal**

Switch(config)# **lacp system-priority** 32768

Switch# **show lacp neighbor detail**



12.5 LACP TIMEOUT

LACP need to send LACP packet to partner switch to check the link status. This command configure the interval of sending LACP packets.

Switch#configure terminal

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

Switch(config-if)# lacp timeout (long |

short) Switch(config-if)# no lacp timeout

Syntax

lacp timeout (long | short)

no lacp timeout

Parameter

long Send LACP packet every 30 seconds.

short Send LACP packet every 1 second

Default

Default LACP timeout is

long. ModeInterface Configuration

Example

This example shows how to configure interface GigabitEthernet 3 lacp timeout to long.

Switch#configure terminal

Switch(config)# interface

GigabitEthernet 3 Switch(config-if)#

lacp timeout long Switch# show lacp

internal detail

12.6 SHOW LACP

Use **"show lacp sys-id"** command to displays the system identifier that is being used by LACP. The system identifier is made up of the LAPC system priority and the switch MAC address.

Use **"show lacp counter"** command to display LACP statistic information. Use **"show lacp internal"**
command to display local information.

Use **"show lacp neighbor"** command to display remote Information State of the specific port. These are the allowed values:

bndl Port is attached to an aggregator and bundled with

other ports. **Susp** Port is in a suspended state; it is not

attached to any aggregator. **hot-sby** Port is in a hot-standby

state.

1indiv Port is incapable of bundling with any other port.

1indep Port is in an independent state (not bundled but able to switch data traffic. In this case, LACP is not running on the partner port).

Down-Port is down.

State variables for the port, encoded as individual bits within a single octet with these meanings:

- bit0 LACP_Activity
- bit1 LACP_Timeout
- bit2 Aggregation
- bit3 Synchronization
- bit4 Collecting
- bit5 Distributing
- bit6 Defaulted
- bit7 Expired

Switch# **show lacp sys-id**

Switch# **show lacp** [*<1-8>*] **counters**

Switch# **show lacp** [*<1-8>*] **(internal | neighbor) [detail]**

show lacp sys-id

Syntax

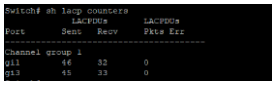
show lacp [*<1-8>*] counters

show lacp [*<1-8>*] (internal | neighbor) [detail]

Mode Privileged EXEC

This example shows how to show LACP statistics.

Switch# show lacp counters

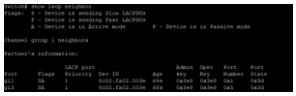


Switch# show lacp internal

Example

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**

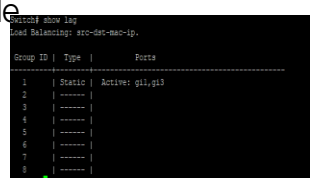
Syntax **show lag**

Mode Privileged EXEC

This example shows how to show current LAG status.

Switch# **show lag**

Example



LLDP

LLDP (Link Layer Discovery Protocol) is an IEEE (Institute of Electrical and Electronics Engineers) standard protocol (IEEE 802.1AB) that defines messages, encapsulated in Ethernet frames for the purpose of giving devices a means of announcing basic device information to other devices on the LAN (Local Area Network) through periodic retransmissions out each port every 30 seconds by default.

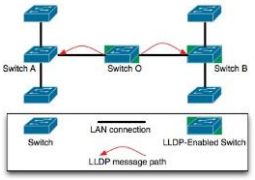


Fig 13.1 Link Layer Discovery Protocol

Concept What is the need for LLDP?

With all kinds of devices connecting to the network these days, installing, tracking and managing each of them can be quite difficult in large networks.

There are many applications for LLDP. Some of them are,

- To automate the deployment of access devices like IP Phones, Wireless Access Points, etc.
- To help troubleshoot network attached devices.
- To automate firmware management
- To discover the type and location (switch port) of a network device, connected anywhere on the network.
- To build a complete network topology (which is also automatically updated after adds/moves/changes).
- To identify and place a device (like IP phone) on the correct VLAN meant for it, automatically.
- To identify how a device can be powered up (from the main line, from an external source, etc) and how much power it needs.
- To get information like hardware revision, firmware version, serial no, manufacturer/model name, etc from LLDP supported devices connected to the network.

13.1 LLDP

Use “lldp” command to enable LLDP RX/TX ability. The LLDP enable status is displayed by “show lldp” command. Use the “no” form of this command to disable the LLDP. When LLDP is disabled, the behavior of receiving LLDP PDU would be decided by “lldp” command.

Switch# configure terminal

Switch (config)#lldp

Switch (config)#no lldp

Syntax	lldp no lldp
Mode	Global Configuration

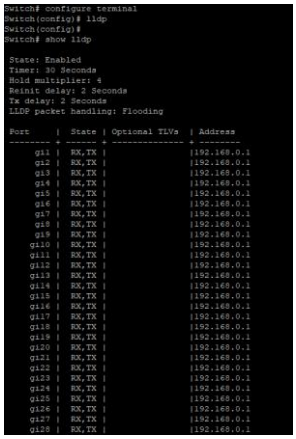
The following example sets LLDP enable/disable.

Switch# configure terminal

Switch (config)# lldp

Switch# show lldp

Example



13.2 LLDP RX

Use **“lldprx”** command to enable the LLDP PDU RX ability. The configuration could be shown by **“show lldp”** command. Use the **“no”** form of this command to disable the RX ability.

Switch# **configure terminal**

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

ID} Switch(config-if)# **lldprx**

Switch(config-if)# **no lldprx**

Syntax	**lldprx** **no lldprx**
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 range g1-** **10** Switch(config-if-range)# **lldp rx** Switch(config-if-range)# **lldp tx** Switch# **show lldp interfaces g1-** **10**

```
Switch# configure terminal
Switch(config)# interface range gi1-10
Switch(config-if-range)# lldp rx
Switch(config-if-range)# lldp tx
Switch(config-if-range)#
Switch# show lldp interfaces  gi1-10

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

 Port     |  State | Optional TLVs  | Address
 -------- + ------ + -------------- + -------
     gi1 |  RX,TX |                |192.168.0.1
     gi2 |  RX,TX |                |192.168.0.1
     gi3 |  RX,TX |                |192.168.0.1
     gi4 |  RX,TX |                |192.168.0.1
     gi5 |  RX,TX |                |192.168.0.1
     gi6 |  RX,TX |                |192.168.0.1
     gi7 |  RX,TX |                |192.168.0.1
     gi8 |  RX,TX |                |192.168.0.1
     gi9 |  RX,TX |                |192.168.0.1
    gi10 |  RX,TX |                |192.168.0.1

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

13.3 LLDP TX-INTERVAL

Use **"lldptx-interval"** command to configure the LLDP TX interval. It should be noticed that both **"lldptx- interval"** and **"lldptx-delay"** affects the LLDP PDU TX time. The larger value of the two configurations decides the TX interval. The configuration could be shown by **"show lldp"** command. Use the **"no"** form of this command to restore the interval to default value.

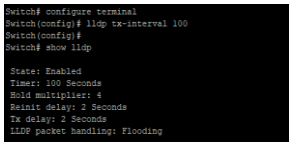
Switch# **configure terminal**

Switch(config)# **lldp tx-interval** *<5-*

32768> Switch(config)# **no lldp tx-**

interval

Syntax	**lldptx-interval** *<5-32768>* **no lldptx-interval**
Parameter	*<5-32768>* Specify the LLDP PDU TX interval in unit of second
Default	Default TX interval is 30
seconds Mode	Global Configuration
Example	This example sets LLDP TX interval to 100 seconds. Switch# **configure terminal** Switch(config)# **lldp tx-interval 100** Switch# **show lldp**



13.4 LLDP REINIT-DELAY

Use **"lldpreinit-delay"** to configure the LLDP re-initials delay. This delay avoids LLDP generate too many PDU if the port is up and down frequently. The delay starts to count when the port links down. The port would not generate LLDP PDU until the delay counts to zero. The configuration could be shown by **"show lldp"** command. Use the **"no"** form of this command to restore the delay to default value.

Switch# **configure terminal**

Switch(config)# **lldp reinit-delay** *<1-10>*

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

Syntax

Lldp reinit-delay *<1-10>*

no lldp reinit-delay

Parameter

<1-10>
Specify the LLDP re-initial delay time in unit of second.

Default

Default reinital delay is 2 seconds

Mode

Global Configuration

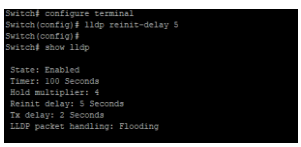
Example

This example sets LLDP re-initial delay to 5 seconds.

Switch# **configure terminal**

Switch(config)# **lldp reinit-delay** 5

Switch# **show lldp**



13.5 LLDP HOLDTIME-MULTIPLIER

Use **“lldp holdtime-multiplier”** command to configure the LLDP PDU hold multiplier that decides time-to- live (TTL) value sent in LLDP advertisements: TTL = (tx-interval * holdtime-multiplier). The configuration could be shown by **“show lldp”** command. Use the **“no”** form of this command to restore the multiplier to default value.

Switch# **configure terminal**

Switch(config)# **lldp holdtime-multiplier** *<2-10>*

Switch(config)# **no holdtime-multiplier**

Syntax

lldp holdtime-multiplier *<2-10>*

no holdtime-multiplier

Parameter *<2-10>* Specify the LLDP hold time

multiplier Default lldpholdtime-multiplier 4

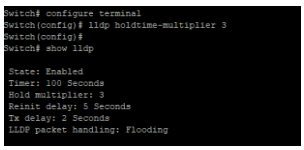
Mode Global Configuration

Example

This example sets LLDP hold time multiplier to 3. Switch# **configure terminal**

Switch(config)# **lldp holdtime-multiplier 3**

Switch# **show lldp**



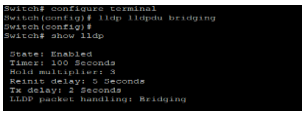
13.6 LLDP LLDPDU

Use **"lldp lldpdu"** command to configure the LLDP PDU handling behavior when LLDP is globally disabled. It should be noticed that if LLDP is globally enabled and per port LLDP RX status is configured to disabled, the received LLDP PDU would be dropped instead of taking the global disable behavior. The configuration could be shown by **"show lldp"** command. Use the **"no"** form of this command to restore the behavior to default.

Switch# **configure terminal**

Switch(config)# **lldp lldpdu (filtering|flooding|bridging)**

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.

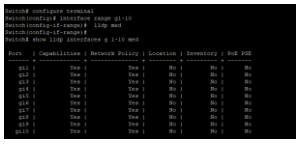
Switch# **configure terminal**

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

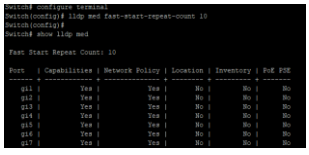
Example

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**



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.

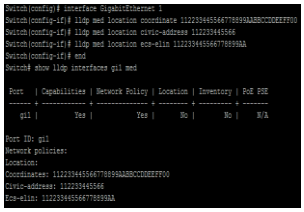
Switch# **configure terminal**

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 11223344556677889AABBCCDDEEFF00 Switch(config-if)# lldp med location civic-address 112233445566 Switch(config-if)# lldp med location ecs-elin 11223344556677889AA 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

This example create 2 network

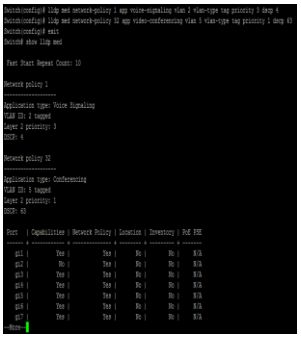
policies. Switch# **configure terminal**

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

Exampl e

Switch# **show lldp med**



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>*

add Add network policy binding for ports.

Parameter **remove** Remove network policy binding for ports.

<1-32> Specify the network policy

index Mode Port Configuration

This example binds network policy for interface gi1 and gi2.

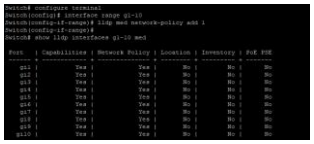
Switch# **show lldp med**

Switch# **configure terminal**

Switch(config)# **interface range** g1-10

Example 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.

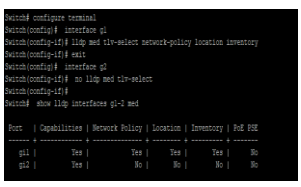
Switch# **configure terminal**

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**



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.

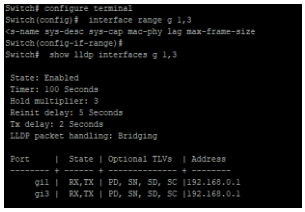
Switch# **configure terminal**

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}*

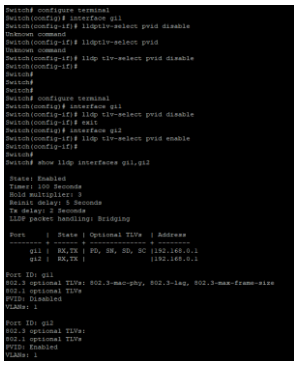
Switch(config-if)# **lldp tlv-select pvid**

(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**

g i1,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

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**

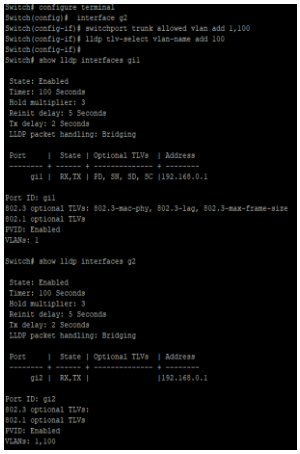
Switch(config-if)# **lldp tlv-select vlan-name add** 100

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

Exampl
e

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**

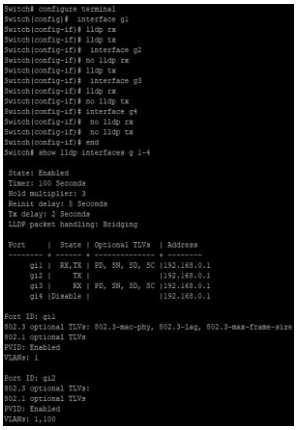
Switch(config-if)# **no lldp tx**

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

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.

Example

```
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

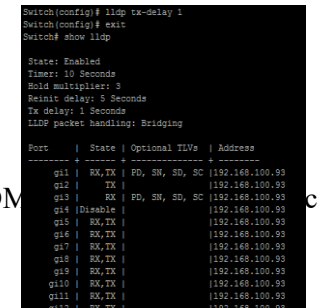
Use **"lldp tx-delay"** command to configure the delay in seconds between successive LLDP frame transmissions. The delay starts to count in any case LLDP PDU is sent such as by LLDP PDU advertise routine, LLDP PDU content change, port link up, etc. The configuration could be shown by **"show lldp"** 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	
	This example sets LLDP PDU TX delay to 10
	seconds. Switch# **configure terminal**
	Switch(config)# **lldp tx-delay 1**
	Switch# **show lldp**
Example	

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

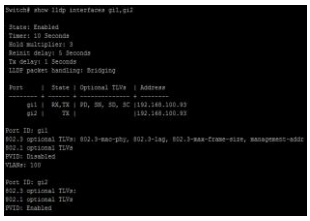
show lldp interface *{IF_NMLPORTS}*

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

This example displays the local device information.

Switch# **show lldp local-device**

Example

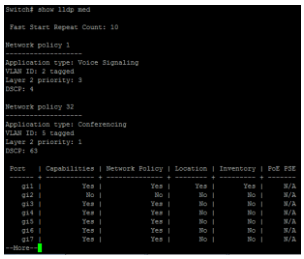
```
Switch# show lldp local-device

LLDP Local Device Information:
 Chassis Type : Mac Address
 Chassis ID   : 90: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**	



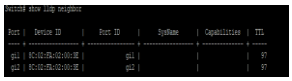
13.21 SHOW LLDP NEIGHBOR

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.

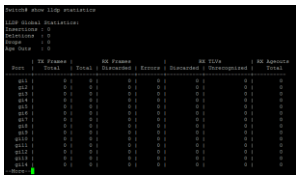
Switch# **show lldp statistics**

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

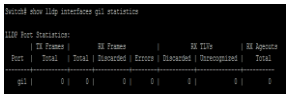
Syntax	**show lldp statistics**	
	show lldp interfaces *{IF_NMLPORTS}* **statistics**	
Parameter	*IF_NMLPORTS*	Specify the ports to display information
Mode	Privileged EXEC	

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**

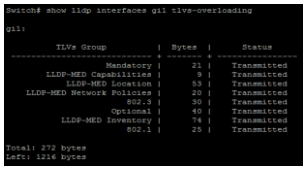
Parameter *IF_NMLPORTS* Specify the ports to display

information Mode Privileged EXEC

This example display the LLDP TLVs overloading status of port gi1.

Switch# **show lldp interfaces gi1 tlvs-overloading**

Example



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

The following example disables and enables the logging service on the switch.

Switch#**configure terminal**

Switch(config)# **no logging**

Example

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)

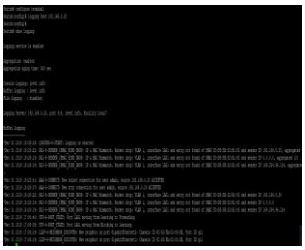
Syntax	logging host (ip-addr|hostname) [facility facility] [port port] [severity sev] no logging host (ip-addr|hostname)
Parameter	**ipv4-addr** IPv4 address of the remote logging server. **hostname** Hostname of the remote logging server. **facility** facility Specify the facility of the logging messages. 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

Exampl e

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]

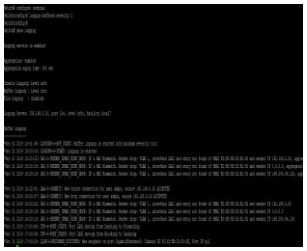
Switch(config)# no logging (buffered|console|file)

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]**

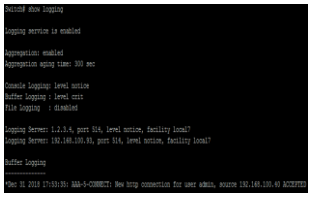
Syntax **show logging [buffered|file]**

Parameter
Buffered Display the log messages stored in the RAM. File Display the log messages stored in the Flash.

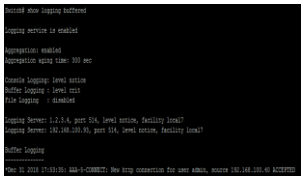
Mode Privileged EXEC

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.

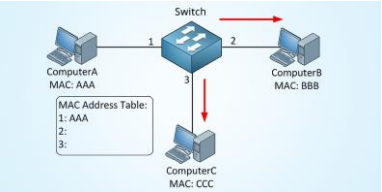


Fig 15.1 MAC Address Table

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]**

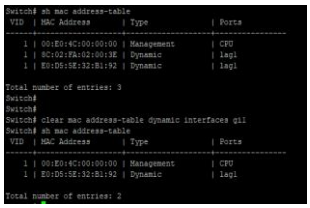
Parameter **Interfaces** IF_PORTS Delete all dynamic addresses learned on the specific interface.

vlan vlan-id Delete all source addresses learned on the specific

VLAN Mode Privileged EXEC

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

Example



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

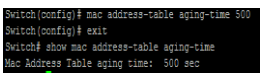
Exampl e

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

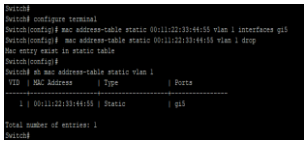
Example

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]

dynamic Display only dynamic MAC addresses

static Display only static MAC addresses

Parameter**Interface** *IF_PORTS* Display the MAC addresses entries for a specifc interface.

vlan vlan-id Display the MAC address entries for a specific VLAN.

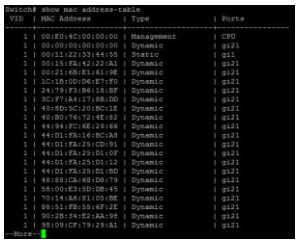
mac-addr Display entries for a specific MAC

address Mode Privileged EXEC

The following example displays the entire MAC address

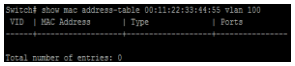
table. Switch# **show mac address-table**

Example



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**

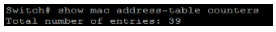
Syntax **show mac address-table counters**

Mode Privileged EXEC

The following example display numbers of addresses in the address table.

Example

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

The following example displays aging time for the MAC address table.

Example 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

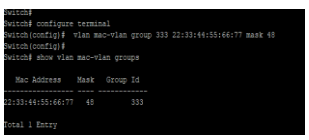
Example

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

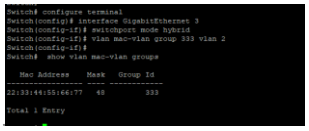


Image not found or type unknown

Image not found or type unknown

16.3 SHOW VLAN MAC-VLAN GROUPS

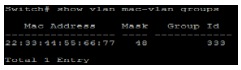
Use the show vlan mac-vlan groups command to display mac groups configuration. Switch# **show vlan mac-vlan groups**

Syntax **show vlan mac-vlan groups**

Mode Privileged EXEC

This following example shows how to display mac group.

Example Switch# **show vlan mac-vlan groups**



16.4 SHOW VLAN MAC-VLAN INTERFACES

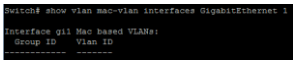
Use the show vlan mac-vlan interface command in EXEC mode to display the mac-vlan interfaces setting. Switch# **show vlan mac-vlan [interfaces** *IF_PORTS*]

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:

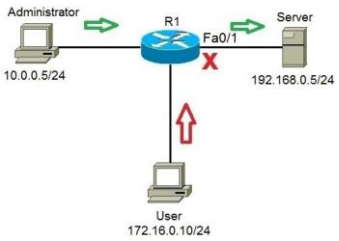


Fig 17.1 ACL Feature

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]*

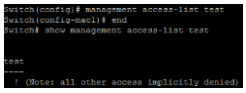
Switch(config)#**no management access-list** *[NAME]*

Syntax	**management access-list NAME** **no management access-list NAME**

ParameterNAME 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

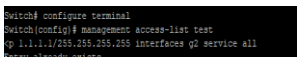
Mode Global Configuration

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

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.

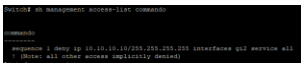
Switch#**configure terminal**

Switch(config)# **management access-list** commando

Exampl e

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

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.

Example

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
Switch(config-macl)#
Switch# sh management access-list test1

test
---
 sequence 1 deny ip 1.1.1.1/255.255.255.255 interfaces gi2 service all
 sequence 2 permit ip 2.2.2.2/255.255.255.255 interfaces gi2 service http
 sequence 10 deny interfaces gi1 service all
 ! (Note: all other access implicitly denied)
```

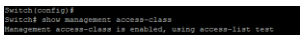
17.6 SHOW MANAGEMENT ACCESS-CLASS

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

The example shows how to show management access-class ExampleSwitch# **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

The example shows how to show management

access-list Switch# **show management access-list 1**

Example

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.

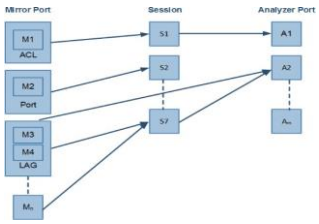


Fig 18.1 Mirror and Analyzer Port

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)**

mirror session *<1-4>* destination interface IF_NMLPORT [allow-ingress]

Syntax

no mirror session *<1-4>*destination interface IF_NMLPORT

no mirror session (*<1-4>*| all)

<1-4> Specify the mirror session to configure

Parameter

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

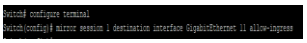
Global Configuration

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

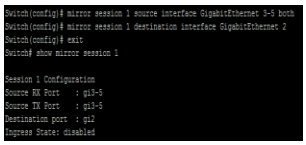
The following example shows how to create a local SPAN session 1 to monitor both sent and received rate on source port gi3-5.

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

This following example shows how to display mirror session configuration

Switch# **show mirror**

Example

```
Switch# show mirror

Session 1 Configuration
Source RX Port    : gi3-5
Source TX Port    : gi3-5
Destination port  : gi2
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
```

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

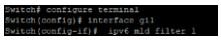
The following example specifies that set ipv6 mld filter test.

Switch#**configure terminal**

Switch(config)# **interface** gi1

Switch(config-if)# **ipv6 mld filter**

1



19.23 IPV6 MLD MAX-GROUPS

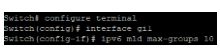
Use the ipv6 mld max-groups command to limit port learning max group number. When the port has reach limitation, new group will not add this port. Static group is excluded. Use the **"no"** form of this command to restore to default. You can verify settings by the show ipv6 mld max-groups command.

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

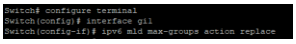
Use the ipv6 mld max-groups action command to set the action when the numbers of groups reach the limitation. Use the **"no"** form of this command to restore to default. You can verify settings by the show ipv6 mld max-groups command.

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 Syntaxclear ipv6 mld

snooping statistics Mode

Privileged EXEC

The following example specifies that clear ipv6 mld snooping statistics Exampletest.

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**

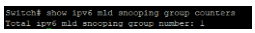
Syntax **show ipv6 mld snooping groups counters**

Mode Privileged EXEC

The following example specifies that display ipv6 mld snooping group counter test.

Example 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)]

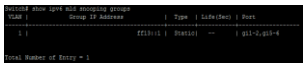
Syntax show ipv6 mld snooping groups [(dynamic | static)]

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

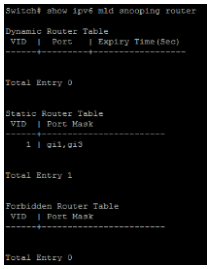
(dynamic |forbidden | static)Display ipv6 mld router info for different type

Mode Privileged EXEC

The following example specifies that show ipv6 mld snooping router

test. Switch# show ipv6 mld snooping router

Example



19.30 SHOW IPV6 MLD SNOOPING

This command will display ipv6 mld snooping global info.

Switch#show ipv6 mld snooping

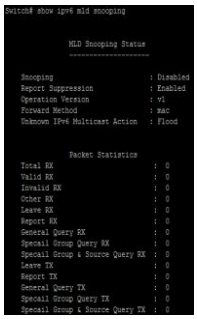
Syntax show ipv6 mld snooping

Mode Privileged EXEC

The following example specifies that show ipv6 mld snooping test.

Switch# show ipv6 mld snooping

Example



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

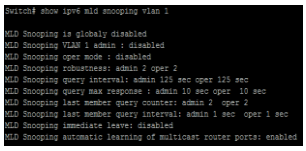
Parameter
none Show all ipv6 mld snooping vlan
info Show specifies vlan ipv6 mld snooping info

Default Show all ipv6 mld snooping vlan

info Mode Privileged EXEC

The following example specifies that show ipv6 mld snooping vlan test. Switch# show ipv6 mld snooping vlan 1

Example

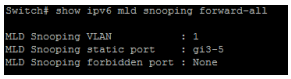


19.32 SHOW IPV6 MLD SNOOPING FORWARD-ALL

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

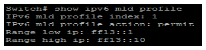
info [<1-128>] Show specifies index

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

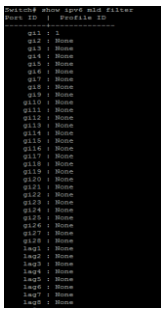
none Show all port filter

[interfaces *{IF_PORTS}*] Show specifies ports filter

Mode Privileged EXEC

The following example specifies that show ipv6 mld filter test. Switch# **show ipv6 mld filter**

Example



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

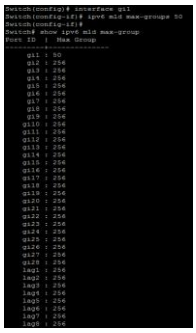
[interfaces *{IF_PORTS}*] Show specifies ports max-group

Mode Privileged EXEC

The following example specifies that show ipv6 mld max-group

test. Switch# **show ipv6 mld max-group**

Example



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	group action
Show all port max-	[interfaces *{IF_PORTS}*]Show specifies ports max-group action

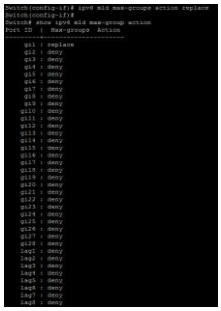
Default Show all ports ipv6 mld max-group

action Mode Privileged EXEC

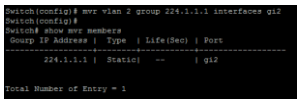
The following example specifies that show ipv6 mld max-group action test.

Switch# **show ipv6 mld max-group action**

Example



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	dynamic group specifies MVR
static	static group specifies MVR

Default Clear all of mvr

group Mode Privileged

EXEC

The following example specifies that clear all mvr groups test.

Example

Switch# clear mvr members

20.10 SHOW MVR MEMBERS

This command will display the mvr groups for all of type.

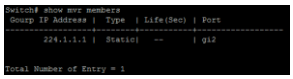
Switch#**show mvr members**

Syntax **show mvr members**

Mode Privileged EXEC

The following example specifies that show mvr groups test.

ExampleSwitch# **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}*

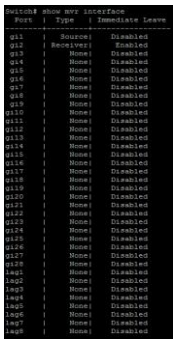
Parameter*IF_PORTS* Show specifies port list

configuration Mode Privileged EXEC

The following example specifies that show mvr interface test.

Switch# **show mvr interface**

Exampl e



20.12 SHOW MVR

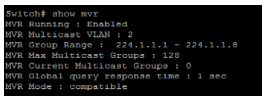
This command will display mvr global

information. Switch#**show mvr**

Syntax **show mvr**

Mode Privileged EXEC

The following example specifies that show mvr test.



Example Switch# **show mvr**

21. 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

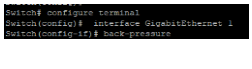
This example shows how to configure port gi1 and gi2 to be

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.

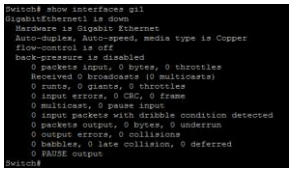
Mode Privileged EXEC

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

Example



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

ParameterWORD*<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

```
Switch# configure terminal
Switch(config)# interface GigabitEthernet 1
Switch(config-if)# description userport
```

```
Switch# show interfaces gi1 st
Port  Name              Status     Vlan  Duplex  Speed    Type
gi1   userport          connected  1     a-full  a-1000M  Copper
```

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)**

auto Specify port duplex to auto

negotiation. Parameter**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

This example shows how to modify port duplex configuration.

Switch#**configure terminal**

Switch(config)# **interface**

GigabitEthernet 1 Switch(config-if)#

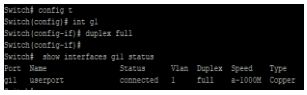
Example **duplex full** Switch(config-if)# **exit**

This example shows how to show current interface link

s ed Switch# show interfaces status

p

e



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

This example shows how to modify maximum frame size on gi1 to 10000 bytes.

Switch#**configure terminal**

Switch(config)# **jumbo-frame** 9216

Exampl e

```
Switch# config t
Switch(config)# jumbo-frame
  <1518-10000>  Maximum frame size
```

This example shows how to show current jumbo-frame size

Switch# **show running-config jumbo-frame** 9216

```
Switch# sh run
SYSTEM CONFIG FILE ::= BEGIN
! System Description: RT-NOS RTL8382M Switch
! System Version: vSoldierOS.2K.v1.4
! System Name: Switch
! System Up Time: 0 days, 3 hours, 9 mins, 27 secs
!
!
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. ModeInterface

Configuration

Example

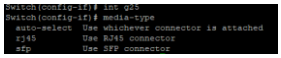
This example shows how to modify combo port media type to copper.

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

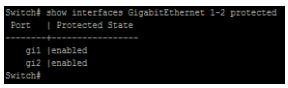
Parameter *{IF_PORTS}* Specify port to show.

Mode Privileged EXEC

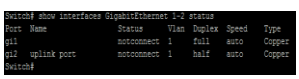
Example

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

This example shows how to modify port speed configuration.

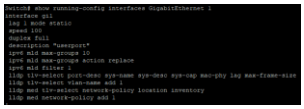
Example

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

This example shows how to modify port duplex configuration.

Switch#**configure terminal**

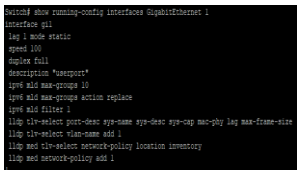
Switch(config)# **interface**

gi1 Switch(config-if)#

shutdown

Example This example shows how to show current admin state configuration

Switch# **show running-config interfaces** gi1



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

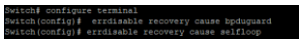
The following example enables the port error disable recovery for the STP BPDU Guard and self-loog cause.

Switch#configure terminal

Switch(config)# errdisable recovery cause bpduguard

Switch(config)# errdisable recovery cause selfloop

Example



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

Exampl e	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**

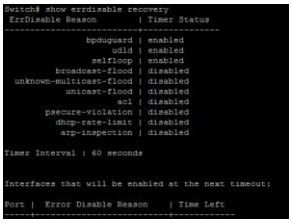
Syntax **show errdisable**

recovery Mode Privileged EXEC

The following example shows the error disable configuration, and the interfaces in the error disabled state.

Switch# **show errdisable recovery**

Example



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

The following example shows how to enable port security

Switch#configure terminal

ExampleSwitch(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

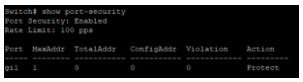
Use “**show port-security**” command to show port-security global information. Switch# **show port-security**

Syntax **show port-security**

Mode Privileged EXEC

This example shows how to show port-security configurations.

Example Switch# **show port-security**



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}*

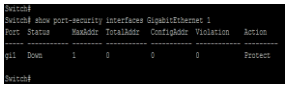
Syntax **show port-security interface** *{IF_PORTS}*

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



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

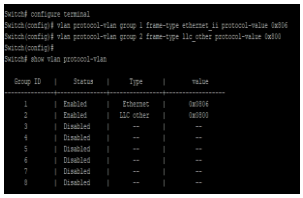
The following example show how to configure protocol vlan

group: Switch# configure terminal

Switch(config)# vlan protocol-vlan group 1 frame-type ethernet_ii protocol-value 0x806

Example

Switch(config)# vlan protocol-vlan group 2 frame-type llc_other protocol-value 0x800 Switch# show vlan protocol-vlan



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

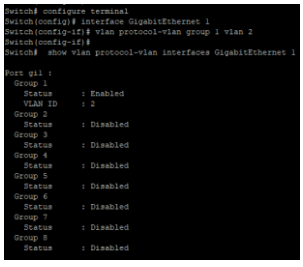
The following example how to configure Protocol VLAN function on specified interfaces.

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>*]

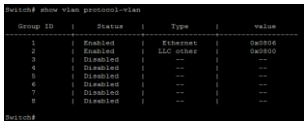
Parameter *<1-8>* Specify protocol vlan group to

display Mode Privileged EXEC

The following example how to display Proto VLAN group configuration

Switch# **show vlan protocol-vlan**

Example



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}*

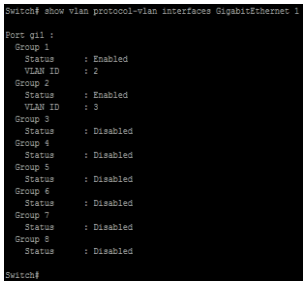
Parameter *{IF_PORTS}* Specify interfaces protocol vlan to

display Mode Privileged EXEC

The following example shows how to display the Protocol VLAN interfaces setting

Switch# **show vlan protocol-vlan interfaces** GigabitEthernet 1

Example

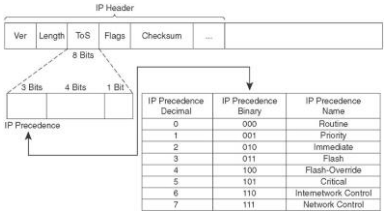


QOS

A communications network forms the backbone of any successful organization. These networks transport a multitude of applications and data, including high-quality video and delay-sensitive data such as real-time voice. The bandwidth-intensive applications stretch network capabilities and resources, but also complement, add value, and enhance every business process. Networks must provide secure, predictable, measurable, and sometimes guaranteed services. Achieving the required Quality of Service (QoS) by managing the delay, delay variation (jitter), bandwidth, and packet loss parameters on a network becomes the secret to a successful end-to-end business solution. Thus, QoS is the set of techniques to manage network resources.

IP Precedence and DSCP Compared

The IP header is defined in RFC 791, including a 1-byte field called the Type of Service (ToS) byte. The ToS byte was intended to be used as a field to mark a packet for treatment with QoS tools. The ToS byte itself was further subdivided, with the high-order 3 bits defined as the *IP Precedence* (*IPP)* field. The complete list of values from the ToS byte's original IPP 3-bit field, and the corresponding names, is provided in Figure.



IP Precedence Decimal	IP Precedence Binary	IP Precedence Name
0	000	Routine
1	001	Priority
2	010	Immediate
3	011	Flash
4	100	Flash-Override
5	101	Critical
6	110	Internetwork Control
7	111	Network Control

Fig 25.1 QoS in IP header with IP Precedence

Ethernet LAN Class of Service

Ethernet supports a 3-bit QoS marking field, but the field only exists when the Ethernet header includes either an 802.1Q or ISL trunking header. IEEE 802.1Q defines its QoS field as the 3 most significant bits of the 2-byte *Tag Control* field, calling the field the *user-priority bits*. ISL defines the 3 least-significant bits from the 1-byte *User* field, calling this field the *Class of Service (CoS)*.

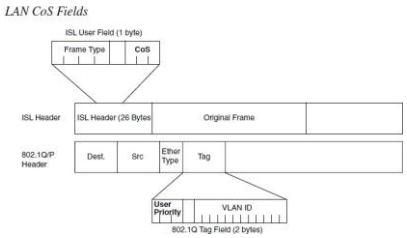


Fig 25.2 QoS in IP header with LAN CoS Feilds

25.1 QOS

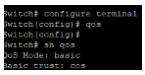
Use **“qos”** command to enable quality of service which according to basic trust type to assign queue for packets, and packets with higher priority are able to send first. Use **“no”** form of this command to disable quality of service.

Switch#**configure terminal**

Switch(config)#**qos**

Switch(config)# **no qos**

Syntax	**qos** **no qos**
Mode	Global Configuration
Example	This example shows how to change qos to basic mode. Switch#**configure terminal** Switch(config)# **qos** This example shows how to check current qos mode. Switch# **show qos**



25.2 QOS COS

Sometimes, there is no qos information in the packets, such as CoS, DSCP, IP Precedence. But we still can give the priority for packets by configuring the interface default cos value. If there is no qos information in the packets, the device will use this default cos value and find the cos-queue map to get the final destination queue. Use **"qos cos"** command to assign port default cos value.

Switch#**configure terminal**

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

ID} Switch(config-if)#**qos cos** *<0-7>*

Syntax **Qos cos** *<0-7>*

Parametercos *<0-7>*Specify the CoS value for the

interface. Default Default CoS value for interface is 0.

Mode Interface Configuration

Example

This example shows how to configure default cos value 7 on interface gi1.

Switch#**configure terminal**

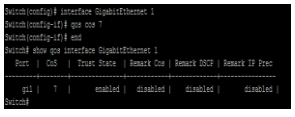
Switch(config)# **interface**

GigabitEthernet 1 Switch(config-if)# **qos**

cos 7

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

Switch# **show qos interface** GigabitEthernet 1



25.3 QOS MAP

According to different trust type, packets will be assigned to different queue based on the specific qos map. For example, if the trust type is trust cos, the device will get the cos value in packet and reference the cos- queue mapping to assign the correct queue.

The queue to cos, dscp or precedence maps are used by remarking function. If the port remarking feature is enabled, the remarking function will reference these 3 tables to remark packets.

Switch#**configure terminal**

Switch(config)#**qos map (cos-queue | dscp-queue | precedence-queue) SEQUENCE to** *<1-8>* Switch(config)#**qos map (queue-cos | queue-precedence) SEQUENCE to** *<0-7>*

Switch(config)#**qos map queue-dscp SEQUENCE to** *<0-63>*

Syntax

qos map (cos-queue | dscp-queue | precedence-queue) SEQUENCE to *<1-8>*

qos map (queue-cos | queue-precedence) SEQUENCE to *<0-7>*

qos map queue-dscp SEQUENCE to *<0-63>*

Parameter

cos-queue Configure or show CoS to queue

map dscp-queue Configure or show DSCP to

queue map

precedence-queue Configure or show IP Precedence to

queue map. queue-cos Configure or show queue to CoS

map

queue-dscp Configure or show queue to DSCP map

queue-precedence Configure or show queue to IP Precedence map

SEQUENCE Specify the cos, dscp, precedence or queue with one or multiple values.

*<1-8>*Specify th queue id

*<0-7>*Specify the cos or precedence values

*<0-63>*Specify the dscp values

The default values of cos-queue are showing in the following table.

CoS	Queue ID
0	2
1	1
2	3
3	4
4	5
5	6
6	7
7	8

The default values of dscp-queue are showing in the following table.

DSCP	Queue ID
0-7	1
8-15	2
16-23	3
24-31	4
32-39	5
40-47	6
48-55	7
56-63	8

The default values of ip precedence are showing in the following table

IP Precedence	Queue ID
0	1
1	2
2	3
3	4
4	5
5	6
6	7
7	8

Defaul t

The default values of queue-cos are showing in the following table.

Queue ID	CoS
1	1
2	0
3	2
4	3
5	4
6	5

The default values of queue-dscp are showing in the following table.

Queue ID	DSCP
1	0
2	8
3	16
4	24
5	32
6	40
7	48
8	56

The default values of queue-precedence are showing in the following table.

Queue ID	IP Precedence
1	0
2	1
3	2
4	3
5	4
6	5
7	6
8	7

Mode Global Configuration

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**

```
Switch# configure terminal
Switch(config)# qos map cos-queue 6 7 to 1
Switch(config)#
Switch# show qos map cos-queue

CoS to Queue mappings
   COS   0  1  2  3  4  5  6  7
--------------------------------
 Queue   2  1  3  4  5  6  1  1
```

Exampl
e

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**

```
Switch# configure terminal
Switch(config)# qos map queue-cos 4 5 to 7
Switch(config)#
Switch# show qos map cos-queue

CoS to Queue mappings
   COS   0  1  2  3  4  5  6  7
--------------------------------
 Queue   2  1  3  4  5  6  1  1
```

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.

5	5
6	9
7	13
8	15

Mode Global Configuration

This example shows how to setup device with 3 strict priority queues and give other weighted queues with weight 5, 10, 15, 20, 25.

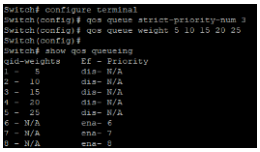
Example

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**



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

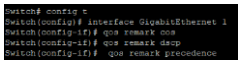
This example shows how to enable remarking features on interface gi1. Switch#configure terminal

Switch(config)# interface GigabitEthernet 1

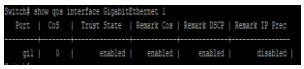
Switch(config-if)# qos remark cos

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)

cos Specify the device to trust CoS

cos-dscp Specify the device to trust DSCP for IP packets, and

Parametertrust 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

This example shows how to change qos basic mode trust types.

Switch#configure terminal

Switch(config)# qos trust cos

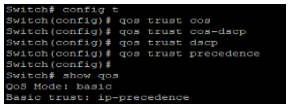
Switch(config)# qos trust cos-dscp

Example Switch(config)# qos trust dscp

Switch(config)# qos trust precedence

This example shows how to check current qos trust

type. Switch# show qos



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

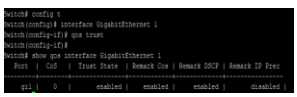
Example

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.

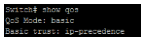
Switch#**show qos**

Syntax **show qos**

Mode Privileged EXEC

This example shows how to check current qos mode.

ExampleSwitch# **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

This example shows how to show qos configurations on interface gi1.

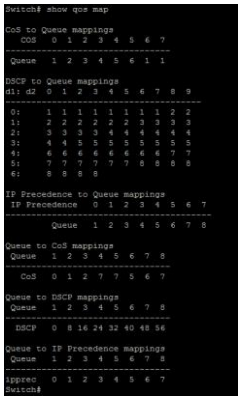
Example Switch# **show qos interface** GigabitEthernet 1

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**



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

This example shows how to check current qos queueing information.

Example Switch# **show qos queueing**

```
Switch# show qos queueing
qid-weights    Ef - Priority
1 -   5        dis- N/A
2 -  10        dis- N/A
3 -  15        dis- N/A
4 -  20        dis- N/A
5 -  25        dis- N/A
6 - N/A        ena- 6
7 - N/A        ena- 7
8 - N/A        ena- 8
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.

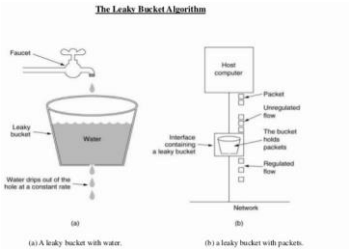


Fig 26.1 Leaky bucket Model

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:-

1. Rate-limiting can be applied by a RADIUS server during an authentication client session. Applying rate- limiting to desirable traffic is not recommended.
2. 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.

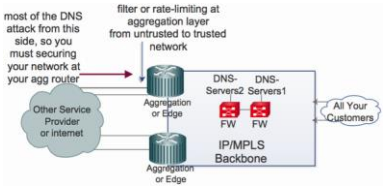


Fig 26.2 Rate limiting on Aggregation Layer

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

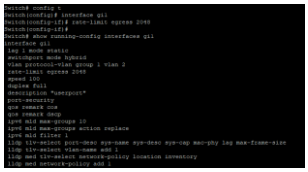
egress

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



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**

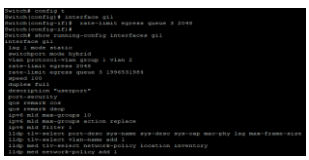
Switch(config)# **interface** { Interface-ID}

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**

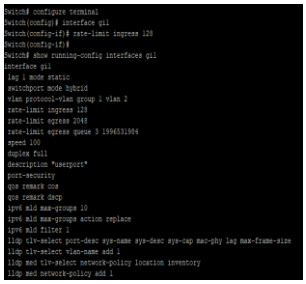
Switch(config)# **interface** { Interface-ID}

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(config-if)# **rate-limit ingress** Switch# **show running-config interfaces** gi1



Syntax **show rmon history** (*<1-65535>*| **all**)

Parameter

*<1-65535>*specifies history index to

show all Show all existed history

Mode Privileged EXEC

The example shows how to show RMON history entry.

switch(config)# rmon history 1 interface gi1 interval 30 owner admin

Example switch# **show rmon history** 1

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**

```
Switch# show rmon history 1 statistic
```

SNMP

Simple Network Management Protocol (*SNMP*) is an Internet Standard protocol for collecting and organizing information about managed devices on IP networks and for modifying that information to change device behavior.

SNMP has been defined with four major functional areas to support the core function of allowing managers to manage agents:

Data Definition—The syntax conventions for how to define the data to an agent or manager. These specifications are called the Structure of Management Information (SMI).

MIBs—Over 100 Internet standards define different MIBs, each for a different technology area, with countless vendor-proprietary MIBs as well. The MIB definitions conform to the appropriate SMI version.

Protocols—The messages used by agents and managers to exchange management data.

Security and Administration—Definitions for how to secure the exchange of data between agents and managers.

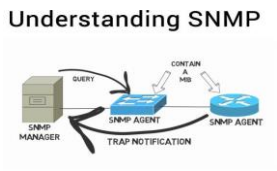


Fig 28.1 SNMP concept

SNMP Version

v1, -simple authentication with communities, but used MIB-I originally.

v2 Uses SMIv2, removed requirement for communities, added Get Bulk and Inform messages, but began with MIB-II originally. 2c Pseudo-release (RFC 1905) that allowed SNMPv1-style communities with SNMPv2; otherwise, equivalent to SNMPv2.

v3 Mostly identical to SNMPv2, but adds significantly better security, although it supports communities for backward compatibility. Uses MIB-II.

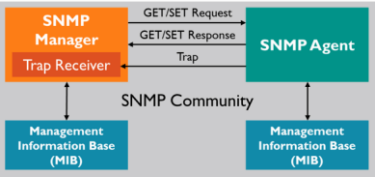


Fig 28.2 SNMP Community concept

28.1 SHOW SNMP

To show the status of Simple Network Management Protocol (SNMP), use the command show snmp in the Privileged EXEC mode.

Switch# **show snmp**

Syntax **show snmp**

Mode Privileged EXEC

The following example shows the SNMP status.

Example Switch# **show snmp**

```
Switch# show snmp
SNMP is enabled.
```

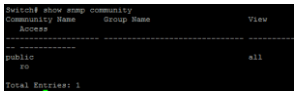
28.2 SHOW SNMP COMMUNITY

To show the configuration of snmp communities, use the command show snmp community in the Privileged EXEC mode.

Switch# **show snmp community** Syntax **show snmp community** Mode Privileged EXEC

The following example shows the SNMP communities configuration.

Example Switch# **show snmp community**



28.3 SHOW SNMP ENGINEID

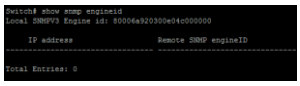
To show the SNMPv3 engine IDs defined on the switch, use the command show snmp engine id in the Privileged EXEC mode.

Syntax **show snmp engine id**

Mode Privileged EXEC

The following example shows the SNMP engine id information.

Example Switch# **show snmp engineid**



28.4 SHOW SNMP GROUP

To show the SNMP group configuration on the switch, use the command show snmp group in the Privileged EXEC mode.

Switch# **show snmp**

group Syntax **show**

snmp group Mode

Privileged EXEC

The following example shows the SNMP group configuration.

Example Switch# **show snmp group**

28.5 SHOW SNMP HOST

To show the SNMP trap notification recipients defined on the switch, use the command show snmp host in the Privileged EXEC mode.

Switch# **show snmp**

host Syntax **show**

snmp host Mode

Privileged EXEC

The following example shows the configuration of SNMP notification recipients on the switch.

Example Switch# **show snmp host**

28.6 SHOW SNMP TRAP

To show the status of SNMP traps on the switch, use the command show snmp trap in the Privileged EXEC mode.

Switch#show snmp

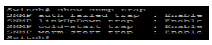
trap Syntax **show**

snmp trap Mode

Privileged EXEC

The following example shows the status of SNMP traps.

Example 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

The following example shows the configuration of SNMP view.

Example 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**

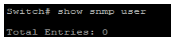
user Syntax **show**

snmp user Mode

Privileged EXEC

The following example shows the configuration of SNMP user.

Example 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

The following example enables the SNMP.

Switch# **configure terminal**

Example

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.

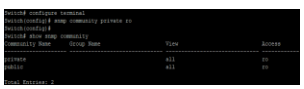
Switch# configure terminal

Switch(config)#snmp communitycommunity-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



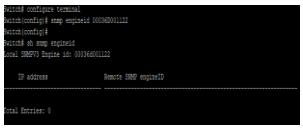
28.11 SNMP ENGINEID

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.

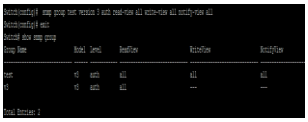
notify-view notify- view Sets the view name that sends only traps with contents that is included in SNMP view selected for notification.

The maximum length is 30 characters.

Mode Global Configuration

Exampl
e

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)]

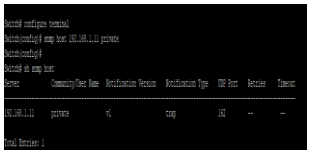
Parameter	**ip-addr** The IP adderss of recipet. **ipv6-addr** The IPv6 adderss of recipet. **hostname** The host name of recipet. **traps** Send SNMP traps to the host. It is the default action. **informs** Send SNMP informs to the host. **version (1|2c|3)** Specify the SNMP version. **noauth** Specify 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

The following example adds the receipt 192.168.1.11 for the SNMP traps notification.

Example

Switch# configure terminal

Switch(config)# snmp host 192.168.1.11 private



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

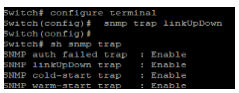
Configuration

The following example disables and enables the SNMP link up and down traps individually.

Switch# **configure terminal**

Example

Switch(config)# **snmp trap linkUpDown**



28.16 SNMP USER

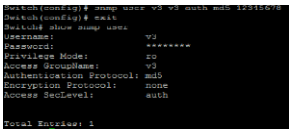
To define a SNMP user, use the command snmp user in the GlobalConfiguration mode and use the "no"
form to delete the SNMP user.

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

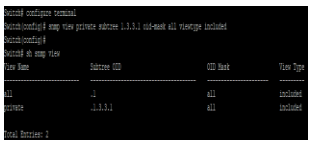
To configure the SNMP view, use the command snmp view in the Global Configuration mode and use the **"no"** form of the command to delete the SNMP view.The default SNMP view cannot be deleted and modified by users. By default, the maximum numbers of SNMP view is limited to 16.

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**



Syntax
revision rev

no revision

Parameter rev The MSTP revision number. Its valid rage is from 0 to 65535

Default The default revision number is 0.

Mode MST Configuration

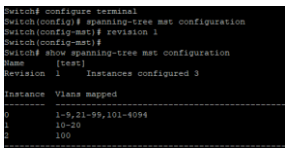
Example
The following example defines the revision MSTP configuration to 1.

Switch#configure terminal

Switch(config)# spanning-tree mst configuration

Switch(config-mst)# revision 1

Switch# show spanning-tree mst configuration



29.4 SHOW SPANNING-TREE

To display the spanning tree configuration, use the command spanning-tree in the Privileged EXEC mode. Switch# show spanning-tree

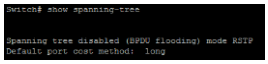
Syntax show spanning-tree

Mode Privileged EXEC

The following example shows the spanning tree configuration.

Example

```
Switch# show spanning-tree
```



29.5 SHOW SPANNING-TREE INTERFACE

To show the STP configuration and statistics for an interface, use the command show spanning-tree interface in the Privileged EXEC mode.

Switch# **show spanning-tree interfaces gi1**

Syntax **show spanning-tree interface** *{IF_PORTS}* [statistic]

Parameter

interface *IF_PORTS* An interface ID or the list of interface IDs.

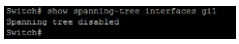
statistic Display the STP statistic for an interface.

Mode Privileged EXEC

Example

The following example shows the STP configuration for the interface gi23.

Switch# **show spanning-tree interfaces gi1**



29.6 SHOW SPANNING-TREE MST

To show the information for a specific MSTP instance, use the command show spanning-tree mst in the Privileged EXEC mode.

Switch# **show spanning-tree mst 0**

Syntax **show spanning-tree mst instance-id**

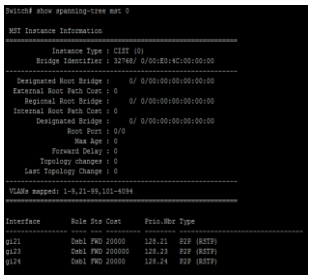
Parameterinstance-id The MSTP instance ID. Its valid range is from 0

to 15. Mode Privileged EXEC

The following example displays the information for the MSTP instance 0 and 1

individually. Switch# **show spanning-tree mst 0**

Example



29.7 SHOW SPANNING-TREE MST CONFIGURATION

To show the global MST configuration, use the command show spanning- tree mst configuration in the Privileged EXEC mode.

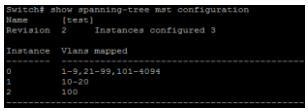
Switch# **show spanning-tree mst configuration**

Syntax **show spanning-tree mst configuration**

Mode Privileged EXEC

The following example shows the global MST configuration.

Example Switch# **show spanning-tree mst configuration**



29.8 SHOW SPANNING-TREE MST INTERFACE

To show the MSTP instance information on the specific interface, use the command show spanning-tree mst interface in the Privileged EXEC mode.

Switch# **show spanning-tree mst instance-id interface** *{IF_PORTS}*

Syntax **show spanning-tree mst instance-id interface** *{IF_PORTS}*

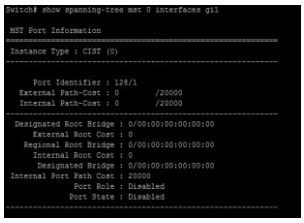
Parameter
instance-id The MSTP instance ID. Its valid range is from 0 to 15.
Interface *IF_PORTS* An interface ID or the list of interface IDs.

Mode Privileged EXEC

The following example shows the MSTP 0 and 1 information individually on the interface gi1.

Switch# **show spanning-tree mst 0 interfaces gi1**

Example



29.9 SPANNING-TREE

To enable the spanning tree, use the command spanning-tree in the Global Configuration mode and use the
"no" form of the command to disable the spanning tree on the

switch. Switch#configure terminal

Switch(config)# spanning-tree

Switch(config)# no spanning-tree

Syntax
spanning-tree

no spanning-tree

Default Spanning-Tree is enabled by

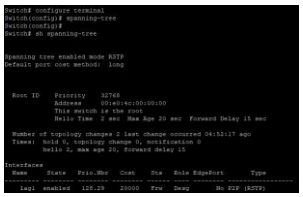
default. Mode Global Configuration

The following example disables and enables the spanning tree individually.

Switch#configure terminal

Switch(config)# spanning-tree

Example Switch# sh spanning-tree



29.10 SPANNING-TREE BPDU

BPDUs are data messages that are exchanged across the switches within an extended LAN that uses a spanning tree protocol topology. BPDU packets contain information on ports, addresses, priorities and costs and ensure that the data ends up where it was intended to go. BPDU messages are exchanged across bridges to detect loops in an network topology. The

loops are then removed by shutting down selected bridge interfaces and placing redundant switch ports in a backup, or blocked, state.

To configure the action of Bridge Protocol Data Unit (BPDU) handling when STP is disabled, use the command spanning-tree bpdu in the Global Configuration mode. To restore the configuration to the default action, use the no form of the command.

Switch#configure terminal

Switch(config)# spanning-tree bpdu (filtering|flooding)

Switch(config)# no spanning-tree bpdu

Syntax

spanning-tree bpdu (filtering|flooding)

no spanning-tree bpdu

Parameter

filtering Filter the BPDU when STP is diabled.

flooding Flood the BPDU when the STP is disabled.

Default

The default configuration is flooding.

Mode

Global Configuration

Example

The following example configures the action of BPDU handling to fliter when the STP is disabled.

Switch#configure terminal

Switch(config)# spanning-tree bpdu filtering

```
Switch# configure terminal
Switch(config)# spanning-tree bpdu filtering
```

29.11 SPANNING-TREE BPDU-FILTER

To enable the BPDU filter, use the command spanning-tree bpdu-filter in the Interface Configuration mode; and use "no" form of the command to disable the BPDU filter.

Switch#configure terminal

Switch(config)# interface {Interfac-ID}

Switch(config-if)# spanning-tree bpdu-filter

Switch(config-if)# no spanning-tree bpdu-filter

Syntax

spanning-tree bpdu-filter

no spanning-tree bpdu-filter

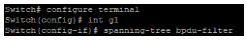
Default BPDU filter is disabled.

Mode Interface Configuration

Example

The following example enables the BPDU filter for interface GigabitEthernet 1.

Switch#configure terminal
Switch(config)# interface GigabitEthernet 1
Switch(config-if)# spanning-tree bpdu-filter



29.12 SPANNING-TREE BPDU-GUARD

To enable the BPDU filter, use the command spanning-tree bpdu-guard in the Interface Configuration mode and use no form of the command to disable the BPDU filter.

Switch#**configure terminal**

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

Switch(config-if)# **spanning-tree bpdu-guard**

Switch(config-if)# **no spanning-tree bpdu-guard**

spanning-tree bpdu-guard

Syntax **no spanning-tree bpdu-guard**

Default BPDU guard is disabled

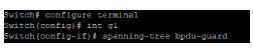
Mode Interface Configuration

The following example enables the BPDU guard for interface gi1.

Switch#**configure terminal**

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

Switch(config-if)# **spanning-tree bpdu-guard**



29.13 SPANNING-TREE COST

To configure the STP path cost for an interface, use the command spanning-tree cost in the Interface Configuration mode; and use the no form of the command to restore it to the default configuration.

Default setting are as follows:-

Interface Speed	STP Cost
10 Mbps	100
100 Mbps	19
1 Gbps	4
10 Gbps	2

Fig 29.6 STP costs

Switch#**configure terminal**

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

Switch(config-if)# **spanning-tree cost**

*{cost}*Switch(config-if)# **no spanning-tree**

cost*{cost}*

Syntax

spanning-tree cost *{cost}*

no spanning-tree cost*{cost}*

Parameter

Cost The port path cost. For the long path cost method, its valid range is from 0 to 200000000; and the valid range is from 0 to 65535 for the short path cost method. The value 0 indicates AUTO, which the port path cost is determined by the port speed and the path cost method.

Default

The default port path cost is 0, and it is determined by the port speed and the path cost method (long or short).

Interface	Long	Short
Gigabit Ethernet (1000Mbps)	20000	4
Fast Ethernet (100Mbps)	200000	19
Ethernet (10Mbps)	2000000	100

Mode

Interface Configuration

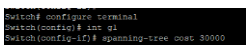
Example

The following example configures port path cost to 30000 for interface gi2.

Switch#configure terminal

Switch(config)# interface gi1

Switch(config-if)# spanning-tree cost 30000



29.14 SPANNING-TREE FORWARD-DELAY

To configure the STP bridge forward delay time, which is the amount of time that a port remains in the Listening and Learning states before it enters the Forwarding state, use the command spanning-tree forward- time in the Global Configuration mode. To restore it to the default configuration, use the "no" form of the command.

When the forward delay time is configured, the following relationship should be

maintained: 2 * (forward-time - 1) >= Max-Age

Timer	Default Value	Description
Hello	2 Seconds	How often will a BPDU be sent.
Max Age	20 Seconds (10 x *Hello* Time)	How long will a port remain in Blocking state after a topology change.
Forward Delay	15 Seconds	How long will a port remain in Listening/Learning states, before transitioning to Forwarding state. (15secs each by default, 30secs total)

Fig 29.7 Spanning Tree Default Timer

Switch#**configure terminal**

Switch(config)# **spanning-tree forward-delay** *{seconds}*

Switch(config)# **no spanning-tree forward-time***{seconds}*

Syntax

spanning-tree forward-delay*{seconds}*

no spanning-tree forward-delay *{seconds}*

Parameter *seconds* STP forward delay time. Its valid range is from 4 to 10 seconds.

Default The default forward delay time is 15

seconds. Mode Global Configuration

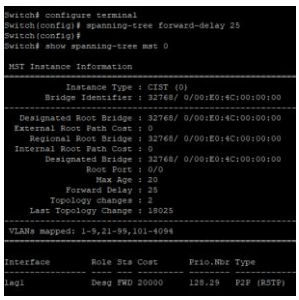
The following example configures STP forward delay time to 25.

Switch#configure terminal

Switch(config)# spanning-tree forward-delay 25

Switch# show spanning-tree mst 0

Example



29.15 SPANNING-TREE HELLO-TIME

STP hello time is the time interval to broadcast its hello message to other bridges. To configure the STP hello time, use the command spanning-tree hello-time in the Global Configuration mode; and use the **"no"** form of the command to restore the hello time to default configuration.

When the hello time is configured, the following relationship should be maintained:Max-Age >= 2 * (hello- time + 1)

Switch#**configure terminal**

Switch(config)# **spanning-tree hello-time seconds**

Switch(config)# **no spanning-tree hello-time**

Syntax	**spanning-tree hello-time seconds no spanning-tree hello-time**
Parameter	**seconds** STP hello time in second. Its valid range is from 1 to 10seconds
Default	The default STP hello time is 2 seconds.
Mode	Global Configuration
Example	The following example configures BPDU hello time to 4. Switch#**configure terminal** Switch(config)# **spanning-tree hello-time 4**

29.16 SPANNING-TREE EDGE

To enable the edge mode for an interface, use the command spanning-tree edge in the Interface Configuration mode; and use the **"no"** form of the command to restore it to the default configuration. In the edge mode, the interface would be put into the Forwarding state immediately upon link up. If the edge mode is enabled for the interface and there are BPDUs received on the interface, the loop might be occurred in the short time.

Switch#**configure terminal**

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

ID} Switch(config-if)# **spanning-tree**

edge Switch(config-if)# **no spanning-**

tree edge

Syntax

spanning-tree edge

no spanning-tree edge

Default The default configuration is

disabled. Mode Interface Configuration

Example

The following example enables the edge mode for the interface gi1.

Switch#**configure terminal**

Switch(config)# **interface**

GigabitEthernet 1 Switch(config-if)#

spanning-tree edge

29.17 SPANNING-TREE LINK-TYPE

To set the RSTP link-type for an interface, use the command spanning-tree link in the Interface Configuration mode. For the default configuration, use the **"no"** form of the command.

Switch#**configure terminal**

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

Switch(config-if)# **spanning-tree link-type (point-to-point|shared)**

Switch(config-if)# **no spanning-tree link-type(point-to-point|shared)**

Syntax	**spanning-tree link-type (point-to-point|shared)** **no spanning-tree link-type(point-to-point|shared)**
Parameter	**point-to-point** Specify the port link type is point to point. **shared** Specify the port link type is shared.
Default	The default configuration link type is point-to-point for the ports with full duplex configuration, and shared for the ports with half duplex settings.
Mode	Interface Configuration
Example	The following example configures the link-type to point-to-point for the interface GigabitEthernet 1. Switch#**configure terminal** Switch(config)# **interface** GigabitEthernet 1 Switch(config-if)# **spanning-tree link-type point-to-point**

29.18 SPANNING-TREE MAX-HOPS

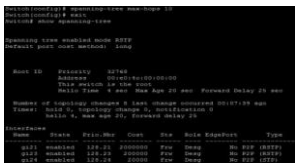
To specify the number of hops for a BPDU to be forwarded in the MSTP region, use the command spanning- tree max-hops in the Global Configuration mode and restore the setting to default configuration by the "no" form of the command.

Switch#**configure terminal**

Switch(config)# **spanning-tree max-hops** *{counts}*

Switch(config)# **no spanning-tree max-hops***{counts}*

Syntax	**spanning-tree max-hops** *{counts}* **no spanning-tree max-hops***{counts}*
Parameter	*counts* Specify the number of hops in an MSTP region before the BPDU is discarded. The valid range is 1 to 40.
Default	The default max-hops configuration
is 20 Mode	Global Configuration
Example	The following example specifies the max hops for BPDU to 10. Switch#**configure terminal** Switch(config)# **spanning-tree max-hops 10**



29.19 SPANNING-TREE MAXIMUM-AGE

To set the interval in seconds that the switch can wait without receiving the configuration messages, before attempting to redefine its own configuration, use the command spanning-tree maximum-age in the Global Configuration mode. For the default configuration, use the **"no"** form of the commands.

When the maximum age is configured, the following relationship should be

maintained: 2 * (forward-time - 1)>= Max-Age >= 2 * (hello-time + 1)

Switch#**configure terminal**

Switch(config)# **spanning-tree maximum-age** *{seconds}*

Switch(config)# **no spanning-tree maximum-age**

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

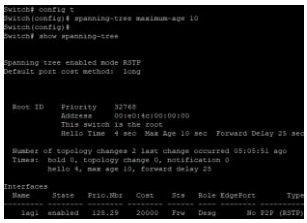
Global Configuration

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

The following example restarts the STP negotiation on the interface gi1.

Switch#**configure terminal**

Example 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.

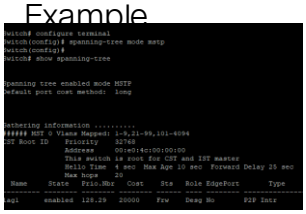
stp Enable the Spanning Tree (STP) operation.

Default The default mode is

rstp. Mode Global

Configuration

Example



T ets the STP operation to MSTP. Switch#configure terminal

h Switch(config)# spanning-tree mode mstp

e

f

o

l

l

o

w

i

n

g

e

x

a

m

p

l

e

s

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

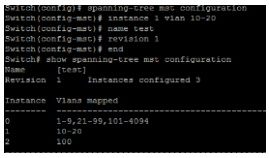
The following example modifies the MSTP configuration in the MST Configuration mode.

Example

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



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

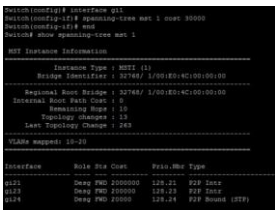
Interface Configuration

Mode

The following example configures the path cost of interface fa1 on the instance 1 to 30000 Switch#**configure terminal**

Switch(config)# **interface** gi1

Example 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.

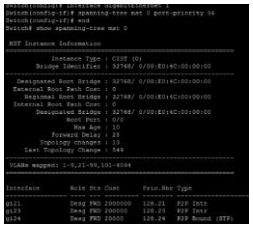
Switch#**configure terminal**

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

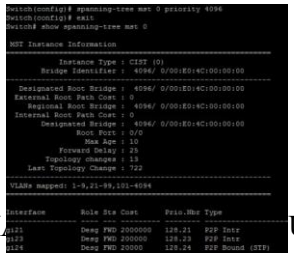
32768. Mode Global Configuration

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**

Example



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. ModeGlobal 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

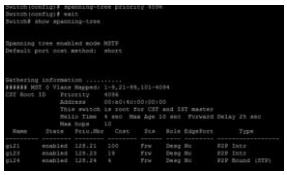
Global Configuration

Example

The following example modifies the bridge priority to 4096.

Switch#**configure terminal**

Switch(config)# **spanning-tree priority 4096**



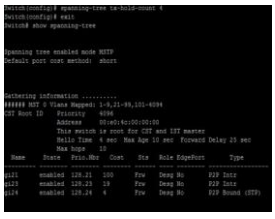
29.29 SPANNING-TREE TX-HOLD-COUNT

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** 

STORM CONTROL

Switches support rate-limiting traffic at Layer 2 using the **storm-control** commands. Storm control can be configured to set rising and falling thresholds for each of the three types of port traffic: unicast, multicast, and broadcast. Each rate limit can be configured on a per-port basis.

You can configure storm control to operate on each traffic type based on either packet rate or a percentage of the interface bandwidth. You can also specify rising and falling thresholds for each traffic type. If you don't specify a falling threshold, or if the falling threshold is the same as the rising threshold, the switch port will forward all traffic up to the configured limit and will not wait for that traffic to pass a specified falling threshold before forwarding it again.

When any of the configured thresholds is passed, the switch can take any of three additional actions, also on a per-port basis. The first, and the default, is that the switch can rate-limit by discarding excess traffic according to the configured command(s) and take no further action. The other two actions include performing the rate-limiting function and either shutting down the port or sending an SNMP trap.

30.1 SHOW STORM-CONTROL

Use **"show storm-control"** command to show all storm control related configurations including global configuration and per port configurations. Use **"show storm-control interface"** command to show selected port storm control configurations.

Switch# **show storm-control**

Switch# **show storm-control interface** *{IF_PORTS}*

show storm-control

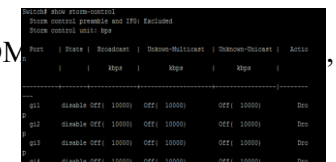
Synta x **show storm-control interface** *{IF_PORTS}*

Parameter*IF_PORTS* Specify port to

show. Mode Privileged EXEC

This example shows how to show storm control global

configuration. Switch# **show storm-control**



Example

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

This example shows how to enable storm control on interface gi1.

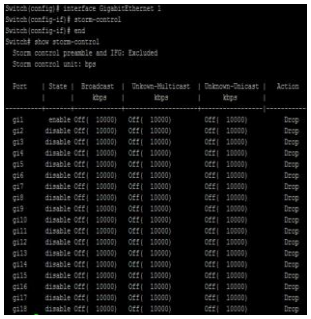
Switch#configure terminal

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.

Exampl
e



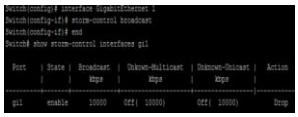
Switch#configure terminal

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.

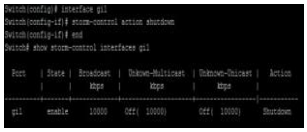
Switch#**configure terminal**

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

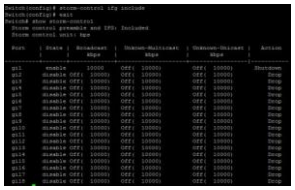
Example
This example shows how to configure storm inter frame gap to include.

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)

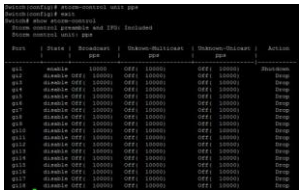
Parameter
bps Storm control rate calculates by octet-based
pps Storm control rate calculates by packet-based

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



SYSTEM FILE

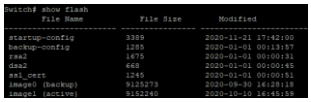
31.1 BOOT SYSTEM

Dual image allow user to have a backup image in the flash partition.Use **“boot system”** command to select the active firmware image. And another firmware image will become a backup one.

Switch#**configure terminal**

Switch(config)# **boot system (image0 | image1)**

Syntax	**boot system (image0 | image1)**
Parameter	image0 Boot from flash image partition 0 image1 Boot from flash image partition 1
Default	Default boot image is
image0. Mode	Global
Configuration	
Example	This example shows how to select image1 as active image. Switch#**configure terminal** Switch(config)# **boot system image1** Select "image1" Success This example shows how to show active image partition. Switch# **show flash**



31.2 COPY

There are many types of files in system. These files are very important for administrator to manage the switch. The most common file operation is copy. By using these copy commands, we can upgrade backup following type of files.

- Firmware Image
- Configuration Files
- Syslog Files

• Language Files
• Security Certificate

Switch# copy (flash:// | tftp://) (flash:// | tftp://)

Switch# copy tftp:// (backup-config | running-config | startup-config) copy (backup-config | running- config | startup-config) tftp://

Switch# copy (backup-config | startup-config) running-config copy (backup-config | running-config) startup-config copy (running-config | startup-config) backup-config

Syntax	copy (flash:// | tftp://) (flash:// | tftp://) copy tftp:// (backup-config | running-config | startup-config) copy (backup-config | running-config | startup-config) tftp:// copy (backup-config | startup-config) running-config copy (backup-config | running- config) startup-config copy (running-config | startup-config) backup-config
Parameter	flash:// Specify the file stored in flash to operation. Available files are: flash://startup-config flash://backup-config flash://rsa1 flash://rsa2 flash://dsa2 flash://image0 flash://image1 flash://ram.log flash://flash.log tftp:// Specify remote tftp server and remote file name. The format is “tftp://192.168.1.111/remote_file_name” running-config Running configuration file startup-config Startup configuration file backup-config Backup configuration file
Mode	Privileged EXEC

Example

This example shows how to copy running configuration to startup configuration. Switch# copy running-config startup-config

This example shows how to backup running configuration to remote tftp server 192.168.111 with file name test1.cfg.

Switch# copy running-config tftp://

Switch# copy tftp://192.168.1.111/test2.cfg startup-config

Switch# copy flash://dsa2 tftp://192.168.1.111/dsa2

31.3 DELETE

Use “delete” command to delete configuration files or use “delete system” command to delete firmware image stored in flash. The “delete startup-config” command is using to restore factory default and it is equal to command “restore-defaults”.

Switch# delete (startrup-config | backup-config | flash://)

Switch# delete system (image0 | image1)

Syntax	delete (startrup-config | backup-config | flash://) delete system (image0 | image1)
Parameter	flash://Specify the configuration file stored in flash to delete. Available files are: flash://startup-config flash://backup-config startup-config Delete startup configuration file backup-config Delete backup configuration file image0 Delete flash image0. image1 Delete flash
image1 Mode	Privileged EXEC
Example	This example shows how to delete backup configuration file. Switch# delete backup-config This example shows how to delete backup firmware image from flash. Switch# delete system image1

31.4 RESTORE-DEFAULTS

Use **“restore-defaults”** command to restore factory default of all system. The command is equal to **“delete startup-config”.**

Switch# **restore-defaults** [**interfaces** *{IF_PORTS}*]

Syntax	**restore-defaults** [**interfaces** *{IF_PORTS}*]
Parameter	interfaces *IF_PORTS* Specify port to restore its’ running config
Mode	Privileged EXEC
Example	This example shows how to restore factory defaults. Switch# **restore-defaults**

31.5 SAVE

Uses **“save”** command to save running configuration to startup configurationfile. This command is equal to
“copy running-config startup-config”.

Switch# **save**

Syntax **save**

Mode Privileged EXEC

This example shows how to save running configuration to startup configuration.

Switch# **save**

```
Switch# save
Success
```

This example shows how to show startup configuration

Example Switch# **show startup-config**

```
Switch#  show startup-config
SYSTEM CONFIG FILE ::= BEGIN
! System Description: KT-NOS RTL8382M Switc
! System Version: vSoldierOS.2K.v1.4
! System Name: Switch
! System Up Time: 0 days, 0 hours, 30 mins,
!
!
!
system location "default"
system contact "default"
no ip dhcp
ip address 192.168.0.1 mask 255.255.255.0
username "admin" secret encrypted NjI2OWM0Z
clock source local
vlan 2-100
voice-vlan oui-table 00:E0:BB "3COM"
voice-vlan oui-table 00:03:6B "Cisco"
voice-vlan oui-table 00:E0:75 "Veritel"
voice-vlan oui-table 00:D0:1E "Pingtel"
voice-vlan oui-table 00:01:E3 "Siemens"
voice-vlan oui-table 00:60:B9 "NEC/Philips"
voice-vlan oui-table 00:0F:E2 "HUC"
voice-vlan oui-table 00:09:6E "Avaya"
!
```

31.6 SHOW CONFIG

Our configuration file is text based. Therefore, we can show the configuration on terminal and read it by this command.Use **"show config"** command to show configuration files stored in system. Use **"show config interfaces"** command to show specific port configurations.

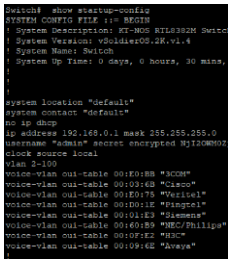
Switch#**show (running-config | startrup-config | backup-config)**

Switch#**show running-config interfaces** *{IF_PORTS}*

Syntax	**show (running-config | startrup-config | backup-config) show running-config interfaces** *{IF_PORTS}*
Parameter	running-config Show running configuration on terminal startup-config Show startup configuration on terminal backup-config Show backup configuration on terminal IF_PORTS Specify port to show its' running config
Mode	Privileged EXEC

This example shows how to show startup configuration

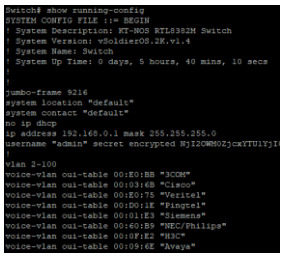
Switch# **show startup-config**



This example shows how to show running

Exampl configuration Switch# **show running-config**

e



This example shows how to display running configuration on specific port.

Switch# **show running-config interfaces gi1**

31.7 SHOW FLASH

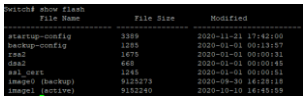
Use **"show flash"** command to show all files status which stored in flash. Switch# **show flash**

Syntax **show flash**

Mode Privileged EXEC

This example shows how to show all files status stored in flash.

Example Switch# **show flash**



SURVEILLANCE VLAN

Creating a reliable surveillance system can be a challenging task. Adding surveillance to an existing network can be problematic; periods of heavy network traffic, such as during mass data transfers or a broadcast storm, can cause your surveillance video feeds to freeze, skip frames, or even drop out completely, surveillance vlan technology that addresses the issue of how to separate data and video in a single network deployment.

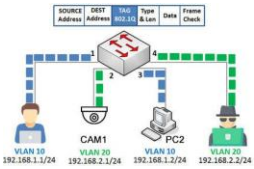


Fig 32.1 Surveillance VLAN concept

Surveillance VLAN allows quick, easy, and automatic creation of a reliable hybrid network that can handle both data and surveillance traffic. By connecting surveillance equipment such as IP cameras and NVRs, VLAN for surveillance traffic and sets Quality of Service (QoS) for that traffic to high-priority. This allows your surveillance traffic to be secure, and ensures that surveillance video continues to stream smoothly and reliably, even during periods of heavy data traffic. Doing this normally requires you to manually configure each setting and add each device to your network one by one.

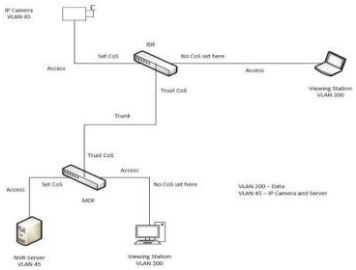


Fig 32.2 Surveillance VLAN with Trust

32.1 SURVEILLANCE-VLAN

Use the surveillance vlan global configuration command to enable the functional Surveillance VLAN on the device. Use the **"no"** form of this command to disable Surveillance VLAN function. You can verify your setting by entering the show surveillance vlan Privileged EXEC command.

Switch#**configure terminal**

Switch(config)# **surveillance-vlan**

Switch(config)# **no surveillance–vlan**

Syntax

surveillance-vlan

no surveillance –vlan

Mode Global Configuration

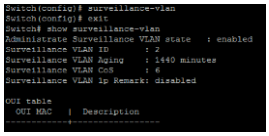
The following example shows how to enable Surveillance VLAN.

Switch#**configure terminal**

Switch(config)# **surveillance –vlan**

Example

Switch# **show surveillance –vlan**



32.2 SURVEILLANCE-VLAN (INTERFACE)

Use the surveillance vlan Interface configuration command to enable OUI surveillance VLAN configuration on an interface. Use the **"no"** form of this command to disable Surveillance VLAN on an interface. You can verify your setting by entering the show surveillance vlan Privileged EXEC command.

Syntax

surveillance-vlan

no surveillance-vlan

Mode Interface Configuration

Example

The following example how to enable Surveillance VLAN function in oui mode on an interface

Switch#**configure terminal**

Switch(config)#**interface range** GigabitEthernet 1-3

Switch(config-if)#**surveillance-vlan**

Switch# **show surveillance-vlan interfaces** gi1-3

```
Switch(config)# interface range GigabitEthernet 1-3
Switch(config-if-range)# surveillance-vlan
Switch(config-if-range)# end
Switch# show surveillance-vlan interfaces gi1-3
  Port  | State    | Port Mode   | Cos Mode
--------+----------+-------------+-----------
gi1     |  Enabled |    Auto     | Src
gi2     |  Enabled |    Auto     | Src
gi3     |  Enabled |    Auto     | Src
```

32.3 SURVEILLANCE-VLAN VLAN

Use the surveillance vlan id global configuration command to configure theVLAN identifier of the surveillance VLAN statically. Use the **"no"** form of this command to restore surveillance VLAN id to default. You can verify your setting by entering the show surveillance vlan Privileged EXEC command.

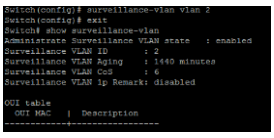
Switch#**configure terminal**

Switch(config)#**surveillance-vlan vlan** *<1-*

4094> Switch(config)#**no surveillance-vlan**

vlan

Syntax	**surveillance-vlan vlan** *<1-4094>* **no surveillance-vlan vlan**
Parameter	*<1-4094>*Specify the Surveillance VLAN
ID Default	The default Surveillance VLAN ID is
None. Mode	Global Configuration
Example	The following example shows how to set Surveillance VLAN id. The VLAN id must be created first. Switch#**configure terminal** Switch(config)# **surveillance-vlan vlan** 128 Switch# **show surveillance-vlan**



32.4 SURVEILLANCE-VLAN OUI-TABLE

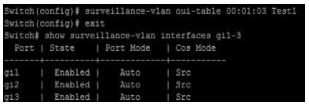
Use the surveillance vlan oui-table global configuration command to add OUI mac address to OUI Table. Use the no form of this command to remove all or specified OUI mac address. You can verify your setting by entering the show surveillance vlan Privileged EXEC command.

Switch#configure terminal

Switch(config)# surveillance-vlan oui-table A:B:C [DESCRIPTION]

Switch(config)# no surveillance-vlan oui-table [A:B:C]

Syntax	surveillance-vlan oui-table A:B:C [DESCRIPTION] no surveillance-vlan oui-table [A:B:C]
Parameter	A:B:C Specify OUI Mac address to add or remove DESCRIPTION Specify description of the specified MAC address to the surveillance VLAN OUI table
Mode	Global Configuration
Example	This following example shows how to add OUI Mac. Switch#configure terminal Switch(config)# surveillance-vlan oui-table 00:01:02 “Test” Switch# show surveillance-vlan interfaces gi1-3



32.5 SURVEILLANCE-VLAN COS (GLOBAL)

Use the surveillance vlan cos global configurations command to configure the surveillance VLAN cos value and 1p remark function.Use the **"no"** form to restore to default mode.You can verify your setting by entering the show surveillance vlan Privileged EXEC command.

Switch#**configure terminal**

Switch(config)# **surveillance-vlan cos** *<0-7>* **[remark]**

Switch(config)# **no surveillance-vlan cos**

Syntax

surveillance-vlan cos *<0-7>***[remark]**

no surveillance-vlan cos

Parameter

<0-7> Specify the surveillance VLAN Class of Service value in telephone OUI mode

remark Specify that the L2 user priority is remarked with the

CoS value DefaultThe default cos value is 6, remark is disabled.

Mode Global Configuration

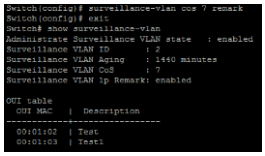
Example

The following example show how to set cos value and enable 1p remark function

Switch#**configure terminal**

Switch(config)# **surveillance-vlan cos** *7* **remark**

Switch# **show surveillance-vlan**



32.6 SURVEILLANCE-VLAN COS (INTERFACE)

Use the surveillance vlan cos mode Interface configuration command to configure OUI surveillance VLAN cos mode configuration on an interface. Use the **"no"** form to restore to default mode.You can verify your setting by entering the show surveillance-vlan interfaces Privileged EXEC command.

Switch#**configure terminal**

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

Switch(config-if)#surveillance-vlan cos (src | all)

Switch(config-if)#no surveillance-vlan cos

Syntax

surveillance-vlan cos (src | all)

no surveillance-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 Surveillance VLAN.

Default The default all port in Src

mode. Mode Interface

configuration

Example

The following example how to configure surveillance packet QoS attributes on an interface

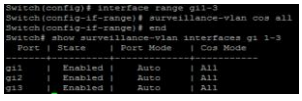
Switch#configure terminal

Switch(config)#interface range gi1-3

Switch(config-if)#surveillance-vlan cos all

Switch# show surveillance-vlan interfaces gi

1-3



32.7 SURVEILLANCE-VLAN MODE

Use the surveillance-vlan mode global configuration command to configure the surveillance VLAN mode for interface.Use the **"no"** form to restore to default mode.You can verify your setting by entering the show surveillance-vlan interfaces Privileged EXEC command.

Switch#**configure terminal**

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

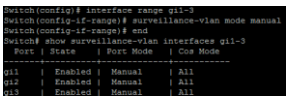
Switch(config-if)#**surveillance-vlan mode (auto|manual)**

Switch(config-if)#**no surveillance-vlan mode**

Syntax	**surveillance-vlan mode (auto|manual)** **no surveillance-vlan mode**
Parameter	auto Specifies that the port is identified as a candidate to join the surveillance VLAN. When a packet with a source OUI MAC address that identifies the remote equipment as surveillance equipment is seen on the port, the port joins the surveillance VLAN as a tagged port. manual Specifies that the port is manually assigned to the surveillance VLAN.
Default	The default is auto
mode. Mode	Interface
Configuration	
Example	The following example how to configure surveillance mode to manual Switch#**configure terminal** Switch(config)#**interface range** gi1-3 Switch(config-if)#**surveillance-vlan mode** **manual** Switch# **show surveillance-vlan**

i terfaces gi1-3

n



32.8 SURVEILLANCE-VLAN AGING-TIME

Use the surveillance vlan aging-time global configuration command to configure the surveillance VLAN aging timeout.Use the **"no"** form to restore to default time.You can verify your setting by entering the show surveillance vlan Privileged EXEC command.

Switch#**configure terminal**

Switch(config)# **surveillance-vlan aging-time** *<30-65536>*

Switch(config)# **no surveillance-vlan aging-time**

Syntax

surveillance-vlan aging-time *<30-65536>*

no surveillance-vlan aging-time

Parameter

<30-65536>
Specify the Surveillance VLAN aging timeout interval in minutes

Default The default aging-timeout value is 1440

minutes Mode Global Configuration

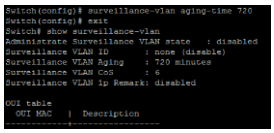
Example

The following example shows how to set aging

time. Switch#**configure terminal**

Switch(config)# **surveillance-vlan aging-time**

720 Switch# **show surveillance-vlan**



32.9 SHOW SURVEILLANCE-VLAN

Use the show surveillance vlan command in EXEC mode to display the surveillance VLAN status for all interfaces or for a specific interface if the surveillance VLAN type is OUI.

Switch#show surveillance-vlan

Switch#show surveillance-vlan interfaces [IF_PORTS]

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

NTP Version 3 (RFC 1305) allows IP hosts to synchronize their time-of-day clocks with a common source clock. For instance, routers and switches can synchronize their clocks to make event correlation from an SNMP management station more meaningful, by ensuring that any events and traps have accurate time stamps.

By design, most routers and switches use NTP *client mode*, adjusting their clocks based on the time as known by an NTP server. NTP defines the messages that flow between client and server, and the algorithms a client uses to adjust its clock. Routers and switches can also be configured as NTP servers, as well as using NTP *symmetric active mode*—a mode in which the router or switch mutually synchronizes with another NTP host. NTP servers may reference other NTP servers to obtain a more accurate clock source as defined by the *stratum level* of the ultimate source clock.

33.1 CLOCK SET

Use the clock set command to set static time. The static time won't save to configuration file. You can verify your setting by entering the show clock Privileged EXEC command.

Switch# clock set HH:MM:SS (jan|feb|mar|apr|may|jun|jul|aug|sep|oct|nov |dec) *<1-31> <2000-2035>*

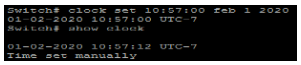
Syntax	clock set HH:MM:SS (jan|feb|mar|apr|may|jun|jul|aug|sep|oct|nov|dec) *<1-31><2000- 2035>*
Parameter	*HH:MM:SS <1-31>* (jan|feb|mar|apr|may|jun|jul|aug| sep|oct|nov|dec) *<2000-2035>* Specify static time of year, month, day, hour, minute, second
Default	No default is defined. The clock set to 2000/01/01 08:00:00 by default at startup.
Mode	Privileged EXEC

Example

The example shows how to set static time of switch.

Switch# clock set 10:57:00 feb 1 2020

Switch# show clock



33.2 Clock timezone

Use the clock timezone command to set timezone setting. Use the **"no"** form of this command to restore to default setting. You can verify your setting by entering the show clock detail Privileged EXEC command.

Switch#**configure terminal**

Switch(config)# **clock timezone ACRONYM HOUR-OFFSET** [*minutes <0-59>*]

Switch# **no clock timezone**

Synta x

clock timezone (ACRONYM HOUR-OFFSET) [*minutes <0-59>*]

no clock timezone

zone Parameter

ACRONYM Specify acronym name of time

HOUR-OFFSET Specify hour offset of

time zone

Minutes <1-59>Specify minute offset of time

zone Default Default time zone is UTC+8.

Mode Global Configuration

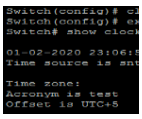
Exampl e

The example shows how to set time zone of switch and then restore to default time zone.

Switch#**configure terminal**

Switch(config)# **clock timezone** test

+5 Switch# **show clock detail**



Switch(config)# **no clock timezone**

Switch# **show clock detail**

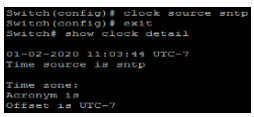
33.3 CLOCK SOURCE

Use the clock source command to set the source of time. Use the "no" form of this command to restore to default setting. You can verify your setting by entering the show clock detail Privileged EXEC command.

Switch#configure terminal

Switch(config)# clock source (local|sntp)

Syntax	clock source (local|sntp)
Parameter	local Specify to use static time sntp Specify to use sntp time
Default	Default is using local
time Mode	Global Configuration
Example	The example shows how to set clock source of switch. Switch#configure terminal Switch(config)# clock source sntp Switch(config)# show clock detail



33.4 CLOCK SUMMER-TIME

Use the clock summer-time command to set daylight saving time for system time. The **“usa”** or **“eu”** means that use the global daylight saving policy which defined by international organization. In both the **“date”**and **“recurring”**, the first part of the command specifies when summer time begins, and the second part specifies when it ends. All times are relative to the local time zone. The **“recurring”** means that adjust time every year within the month.Use the no form of this command to default setting.You can verify your setting by entering the show clock detail Privileged EXEC command.

Switch#**configure terminal**

Switch(config)# **clock summer-time ACRONYM date (jan|feb|mar|apr |may|jun|jul|aug|sep|oct|nov|dec)** *<1-31><2000-2037>*

HH:MM (jan|feb|mar|apr|may|jun|jul|aug|sep|oct|nov|dec) *<1-31><2000-2037> HH:MM [<1-1440>]*

Switch(config)# **clock summer-time ACRONYM recurring (usa|eu)** *[<1-1440>]***clock summer-time ACRONYM recurring (***<1-5>***|first|last)**

(sun|mon|tue|wed|thu|fri|sat)(jan|feb|mar|apr|may|jun|jul|aug|sep|oct|nov|dec)HH:MM **(***<1-5>* **|first|last) (sun|mon|tue|wed|thu|fri|sat)(jan|feb|mar|apr|may|jun|jul|aug|sep|oct|nov|dec)**HH:MM **[** *<1-1440>***]**

Switch(config)# **no clock summer-time**

Syntax	**clock summer-time ACRONYM date (jan|feb|mar|apr|may|jun|jul|aug|sep|oct|nov|dec)** *<1-31><2000-2037>* **HH:MM (jan|feb|mar|apr|may|jun|jul|aug|sep|oct|nov|dec)** *<1-31><2000-2037> HH:MM [<1-1440>]* **clock summer-time ACRONYM recurring (usa|eu)** *[<1-1440>]* **clock summer-time ACRONYM recurring (***<1-5>***|first|last)** **(sun|mon|tue|wed|thu|fri|sat) (jan|feb|mar|apr|may|jun|jul|aug|sep|oct|nov|dec)** HH:MM **(***<1-5>***|first|last) (sun|mon|tue|wed|thu|fri|sat) (jan|feb|mar|apr|may|jun|jul|aug|sep|oct|nov|dec)** HH:MM **[***<1-1440>***]** **no clock summer-time**

ACRONYM<1-31> Specify acronym name of time

zone (jan|feb|mar|apr| may|jun|jul|aug|sep|

oct|nov|dec)

*<2000-2037>*HH:MM Specify non-recurring daylight saving time duration.

*<1-1440>*Specify adjust offset of daylight saving time

Parameter

usa Using daylight saving time in the United States that starts on the second Sunday of March and ends on the first Sunday of November

eu Using daylight saving time in the Europe that starts on the last Sunday in March and ending on the last Sunday in October

(*<1-5>*|first|last) (sun|mon| tue|wed|thu|fri|sat) (jan|feb|mar|apr|may|jun| jul|aug|sep|oct|nov|dec) HH:MM (*<1-5>*|first|last) (sun|mon|tue|wed|thu|fri|sat) (jan|feb|mar|apr|may| jun|jul|aug|sep|oct|nov|dec) HH:MM Specify ecurring daylight saving time duration.

Mode Global Configuration

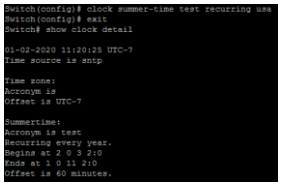
The example shows how to set clock summer time of switch. You can verify settings by the following show show clock command.

Switch#configure terminal

Switch(config)# clock summer-time test recurring usa

Example

Switch# show clock detail



33.5 SHOW CLOCK

Use the show clock command to show clock of switch. The **"detail"** means that show more information of clock such as time zone and daylight saving time.

Switch# **show clock [detail]**

Syntax **show clock [detail]**

Parameterdetail Show more detail information of

clock Mode Privileged EXEC

The example shows how to show clock of switch and detail information.

Switch#**configure terminal**

Switch(config)# **clock source sntp**

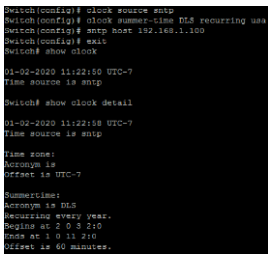
Switch(config)# **clock summer-time DLS recurring usa**

Switch(config)# **sntp host 192.168.1.100**

Example

Switch# **show clock**

Switch# **show clock detail**



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

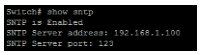
information. Switch# **show sntp**

Syntax **show sntp**

Mode Privileged EXEC

The example shows how to show remote SNTP server.

Example Switch# **show sntp**



UDLD

Virtual LANs In an Ethernet LAN, a set of devices that receive a broadcast sent by any one of the devices in the same set is called a broadcast domain. On switches that have no concept of virtual LANs (VLAN), a switch simply forwards all broadcasts out all interfaces, except the interface on which it received the frame. As a result, all the interfaces on an individual switch are in the same broadcast domain. Also, if the switch connects to other switches and hubs, the interfaces on those switches and hubs are also in the same broadcast domain.

Fig 35.1 VLAN concept

A VLAN is simply an administratively dened subset of switch ports that are in the same broadcast domain. Ports can be grouped into different VLANs on a single switch, and on multiple interconnected switches as well. By creating multiple VLANs, the switches create multiple broadcast domains. By doing so, a broadcast sent by a device in one VLAN is forwarded to the other devices in that same VLAN; however, the broadcast is not forwarded to devices in the other VLANs.

With VLANs and IP, best practices dictate a one-to-one relationship between VLANs and IP subnets. Simply put, the devices in a single VLAN are typically also in the same single IP subnet. Alternately, it is possible to put multiple subnets in one VLAN, and use secondary IP addresses on routers to route between the VLANs and subnets. Also, although not typically done, you can design a network to use one subnet on multiple VLANs, and use routers with proxy ARP enabled to forward trafc between hosts in those VLANs.

Fig 35.2 Inter VLAN communication

VLAN Conguration

Step 1 Create the VLAN.

Step 2 Associate the correct ports with that VLAN.

35.1 VLAN

Use the vlan global configuration command to create VLAN. Use the no form of this command to remove exist VLAN. You can verify your setting by entering the show vlan Privileged EXEC command.

Switch#configure terminal

Switch (config)#vlan {Vlan-ID}

Switch (config)#no vlan

Syntax

vlan

No vlan

Default VLAN 1 created by default

Mode Global

Configuration

The following example creates and removes a VLAN entry (100).

Example

Switch#configure terminal

Switch (config)# vlan 10

Switch# show vlan

35.2 NAME (VLAN)

Use the name vlan configuration command to set name of vlan. You can verify your setting by entering the show vlan Privileged EXEC command.

Switch#configure terminal

Switch (config)#vlan {Vlan-No}

Switch(config-vlan)# name

{NAME}

Syntax name *{NAME}*

ParameterNAME Specify the name of the VLAN (Max. 32 chars).

Default Default name of new vlan is VLAN xxxx. Xxxx is 4-digit vlan

number. Mode VLAN Configuration

This example sets the VLAN name of VLAN 100 to be `VLAN- one-hundred`.

Switch#configure terminal

Switch(config)# vlan 10

Example Switch(config-vlan)# name VLAN-COMMANDO1

Switch# show vlan

35.3 SWITCHPORT MODE

The VLAN mode is used to configure the port for different port role. Access port: Accepts only untagged frames and join an untagged VLAN. Hybrid port: Support all functions as defined in IEEE 802.1Q specification. Trunk port: An untagged member of one VLAN at most, and is a tagged member of zero or more VLANs. If it is an uplink port, it can recognize double tagging on this port. Tunnel port: Port-based Q- in-Q mode. Use the switch mode port configuration command to set mode of interface. You can verify your setting by entering the show interfaces switchport Privileged EXEC command.

Switch#**configure terminal**

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

Switch(config-if)# **switchport mode (access | hybrid | trunk [uplink] | tunnel)**

Syntax	**switchport mode (access | hybrid | trunk [uplink] | tunnel)**
Parameter	**access** Specify the VLAN mode to Access port. **hybrid** Specify the VLAN mode to Hybrid port. **trunk** Specify the VLAN mode to Trunk port. **uplink** Specify the Uplink property on this Trunk port. **tunnel** Specify the VLAN mode to Dot1Q Tunnel port.
Default	Default is trunk mode of all
interfaces Mode	Port Configuration
Example	This example sets VLAN mode to Access port. Switch#**configure terminal** Switch(config)# **interface** GigabitEthernet 2 Switch(config-if)# **switchport mode access**

Switch# show interfaces switchportGigabitEthernet 2

35.4 SWITCHPORT HYBRID PVID

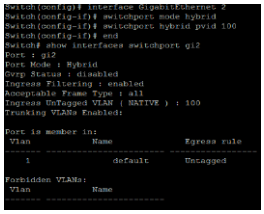
Use the switch hybrid pivd port configuration command to set pvid of interface. You can verify your setting by entering the show interfaces switchport Privileged EXEC command.

Switch#**configure terminal**

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

Switch(config-if)# **switchport hybrid pvid** *<1-4094>*

Syntax	**switchport hybrid pvid** *<1-4094>*
Parameter	*<1-4094>*Specify the port-based VLAN ID on the Hybrid port.
Default	Default pivd is 1.
Mode	Port
Configuration	
Example	This example sets PVID to 100. Switch#**configure terminal** Switch(config)# **interface** GigabitEthernet 2 Switch(config-if)# **switchport mode hybrid** Switch(config-if)# **switchport hybrid pvid** 100 Switch# **show interfaces switchport gi2**



35.5 SWITCHPORT HYBRID INGRESS-FILTERING

Use the switchport hybrid ingress-filtering port configuration command to enable vlan ingress filter. Use the **"no"** form of this command to disable. You can verify your setting by entering the s show interfaces switchport Privileged EXEC command.

Switch#**configure terminal**

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

Switch(config-if)# switchport bybrid ingress-filtering

Switch(config-if)# no switchport hybrid ingress-filtering

Syntax

switchport hybrid ingress-filtering

no switchport hybrid ingress-filtering

Mode Port Configuration

Example

This example sets ingress-filtering to disable.

Switch#configure terminal

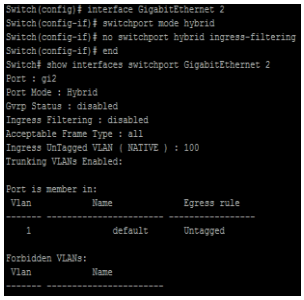
Switch(config)# interface

GigabitEthernet 2 Switch(config-if)#

switchport mode hybrid

Switch(config-if)# no switchport hybrid ingress- filtering

Switch# show interfaces switchport GigabitEthernet 2



35.6 SWITCHPORT HYBRID ACCEPTABLE-FRAME-TYPE

Use the switchport hybrid accept-frame-type port configuration command to choose which type of frame can be accepted. 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 hybrid acceptable-frame-type (all| tagged-only | untagged- only)**

Syntax **switchport hybrid acceptable-frame-type (all | tagged-only | untagged- only)**

all Specify to accept all frames.

Parameter**tagged-only** Specify to only accept tagged frames.

untagged-only Specify to only accept untagged frames.

Default Default is accept all

frames Mode Port

Configuration

This example sets acceptable-frame-type to tagged-

only. Switch#**configure terminal**

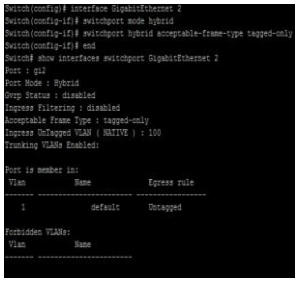
Switch(config)# **interface**

GigabitEthernet 2 Switch(config-if)#

switchport mode hybrid

Exampl e Switch(config-if)# **switchport hybrid acceptable-frame-type tagged-only**

Switch# **show interfaces switchport GigabitEthernet 2**



35.7 SWITCHPORT HYBRID ALLOWED VLAN

Use the switchport hybrid allow vlan add port configuration command to allow vlan on interface. Use the switchport hybrid allows vlan remove port configuration command to remove vlan on interface. You can verify your setting by entering the s show interfaces switchport Privileged EXEC command.

Switch#**configure terminal**

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

Switch(config-if)# **switchport hybrid allowed vlan add** *{VLAN-LIST}*

Switch(config-if)#**switchport hybrid allowed vlan remove** *{ VLAN-LIST}* **[(tagged|untagged)]**

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

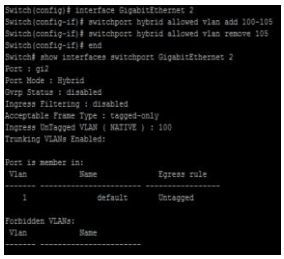
This example sets

ts 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**

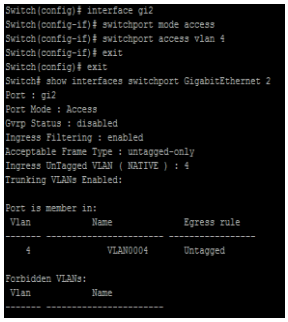
Switch (config)#**interface** {Interface-ID}

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



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**

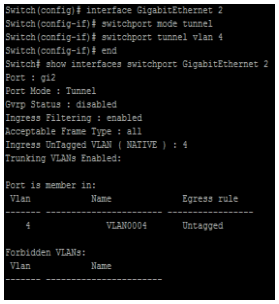
Switch(config)# **interface**

GigabitEthernet 2 Switch(config-if)#

switchport mode tunnel

Switch(config-if)# **switchport tunnel vlan** 4

Switch# **show interfaces switchport** GigabitEthernet 2



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.

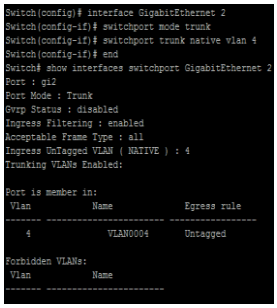
Switch#configure terminal

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



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.

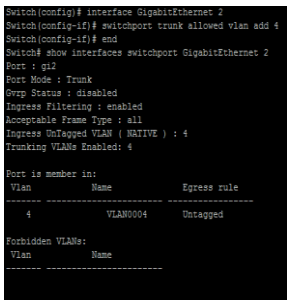
(VLAN-LIST | all) Specify the VLAN list or all VLANs to be added or removed.

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



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

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

Example

```
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**

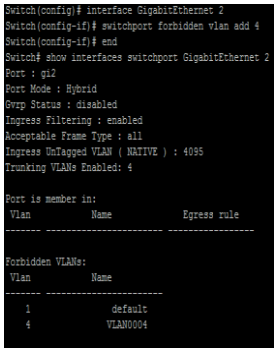
terminal

Switch(config)# **interface** GigabitEthernet 2

Switch(config-if)# **switchport forbidden vlan add**

4 Switch# **show interfaces switchport**

GigabitEthernet 2



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.

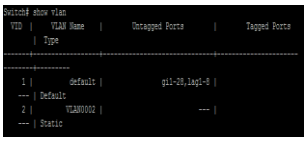
Switch(config)# **no management-vlan**

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**

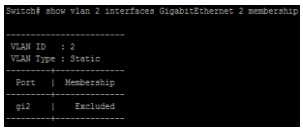
Syntax **show vlan** VLAN-LIST **interfaces** *{IF_PORTS}* **membership**

Parameter
Specify vlan to show
IF_PORTS Specify interface is to show

Mode Privileged EXEC

The following example specifies that show vlan interface membership

Example
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

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

ExampleSwitch# **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

The following example specifies that show management vlan

Example

Switch# **show management-vlan**

VLAN

Virtual LANs In an Ethernet LAN, a set of devices that receive a broadcast sent by any one of the devices in the same set is called a broadcast domain. On switches that have no concept of virtual LANs (VLAN), a switch simply forwards all broadcasts out all interfaces, except the interface on which it received the frame. As a result, all the interfaces on an individual switch are in the same broadcast domain. Also, if the switch connects to other switches and hubs, the interfaces on those switches and hubs are also in the same broadcast domain.

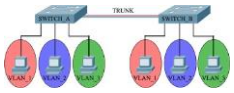


Fig 35.1 VLAN concept

A VLAN is simply an administratively dened subset of switch ports that are in the same broadcast domain. Ports can be grouped into different VLANs on a single switch, and on multiple interconnected switches as well. By creating multiple VLANs, the switches create multiple broadcast domains. By doing so, a broadcast sent by a device in one VLAN is forwarded to the other devices in that same VLAN; however, the broadcast is not forwarded to devices in the other VLANs.

With VLANs and IP, best practices dictate a one-to-one relationship between VLANs and IP subnets. Simply put, the devices in a single VLAN are typically also in the same single IP subnet. Alternately, it is possible to put multiple subnets in one VLAN, and use secondary IP addresses on routers to route between the VLANs and subnets. Also, although not typically done, you can design a network to use one subnet on multiple VLANs, and use routers with proxy ARP enabled to forward trafc between hosts in those VLANs.

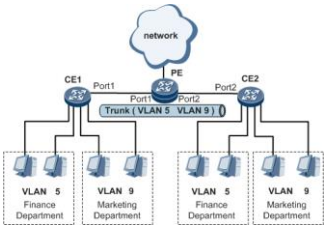


Fig 35.2 Inter VLAN communication

VLAN Conguration

Step 1 Create the VLAN.

Step 2 Associate the correct ports with that VLAN.

35.1 VLAN

Use the vlan global configuration command to create VLAN. Use the no form of this command to remove exist VLAN. You can verify your setting by entering the show vlan Privileged EXEC command.

Switch#configure terminal

Switch (config)#vlan {Vlan-ID}

Switch (config)#no vlan

Syntax

vlan

No vlan

Default VLAN 1 created by default

Mode Global

Configuration

The following example creates and removes a VLAN entry (100).

Example

Switch#configure terminal

Switch (config)# vlan 10

Switch# show vlan

35.2 NAME (VLAN)

Use the name vlan configuration command to set name of vlan. You can verify your setting by entering the show vlan Privileged EXEC command.

Switch#configure terminal

Switch (config)#vlan {Vlan-No}

Switch(config-vlan)# name

{NAME}

Syntax name *{NAME}*

ParameterNAME Specify the name of the VLAN (Max. 32 chars).

Default Default name of new vlan is VLAN xxxx. Xxxx is 4-digit vlan

number. Mode VLAN Configuration

This example sets the VLAN name of VLAN 100 to be `VLAN- one-hundred`.

Switch#configure terminal

Switch(config)# vlan 10

Example Switch(config-vlan)# name VLAN-COMMANDO1

Switch# show vlan

35.3 SWITCHPORT MODE

The VLAN mode is used to configure the port for different port role. Access port: Accepts only untagged frames and join an untagged VLAN. Hybrid port: Support all functions as defined in IEEE 802.1Q specification. Trunk port: An untagged member of one VLAN at most, and is a tagged member of zero or more VLANs. If it is an uplink port, it can recognize double tagging on this port. Tunnel port: Port-based Q- in-Q mode. Use the switch mode port configuration command to set mode of interface. You can verify your setting by entering the show interfaces switchport Privileged EXEC command.

Switch#**configure terminal**

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

Switch(config-if)# **switchport mode (access | hybrid | trunk [uplink] | tunnel)**

Syntax	**switchport mode (access | hybrid | trunk [uplink] | tunnel)**
Parameter	**access** Specify the VLAN mode to Access port. **hybrid** Specify the VLAN mode to Hybrid port. **trunk** Specify the VLAN mode to Trunk port. **uplink** Specify the Uplink property on this Trunk port. **tunnel** Specify the VLAN mode to Dot1Q Tunnel port.
Default	Default is trunk mode of all
interfaces Mode	Port Configuration
Example	This example sets VLAN mode to Access port. Switch#**configure terminal** Switch(config)# **interface** GigabitEthernet 2 Switch(config-if)# **switchport mode access**

Switch# show interfaces switchportGigabitEthernet 2

35.4 SWITCHPORT HYBRID PVID

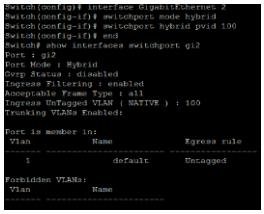
Use the switch hybrid pivd port configuration command to set pvid of interface. You can verify your setting by entering the show interfaces switchport Privileged EXEC command.

Switch#**configure terminal**

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

Switch(config-if)# **switchport hybrid pvid** *<1-4094>*

Syntax	**switchport hybrid pvid** *<1-4094>*
Parameter	*<1-4094>*Specify the port-based VLAN ID on the Hybrid port.
Default	Default pivd is 1.
Mode	Port
Configuration	
Example	This example sets PVID to 100. Switch#**configure terminal** Switch(config)# **interface** GigabitEthernet 2 Switch(config-if)# **switchport mode hybrid** Switch(config-if)# **switchport hybrid pvid** 100 Switch# **show interfaces switchport gi2**



35.5 SWITCHPORT HYBRID INGRESS-FILTERING

Use the switchport hybrid ingress-filtering port configuration command to enable vlan ingress filter. Use the **"no"** form of this command to disable. You can verify your setting by entering the s show interfaces switchport Privileged EXEC command.

Switch#**configure terminal**

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

Switch(config-if)# switchport bybrid ingress-filtering

Switch(config-if)# no switchport hybrid ingress-filtering

Syntax

switchport hybrid ingress-filtering

no switchport hybrid ingress-filtering

Mode Port Configuration

Example

This example sets ingress-filtering to disable.

Switch#configure terminal

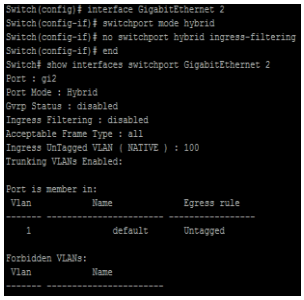
Switch(config)# interface

GigabitEthernet 2 Switch(config-if)#

switchport mode hybrid

Switch(config-if)# no switchport hybrid ingress- filtering

Switch# show interfaces switchport GigabitEthernet 2



35.6 SWITCHPORT HYBRID ACCEPTABLE-FRAME-TYPE

Use the switchport hybrid accept-frame-type port configuration command to choose which type of frame can be accepted. 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 hybrid acceptable-frame-type (all| tagged-only | untagged- only)**

Syntax **switchport hybrid acceptable-frame-type (all | tagged-only | untagged- only)**

all Specify to accept all frames.

Parameter**tagged-only** Specify to only accept tagged frames.

untagged-only Specify to only accept untagged frames.

Default Default is accept all

frames Mode Port

Configuration

This example sets acceptable-frame-type to tagged-

only. Switch#**configure terminal**

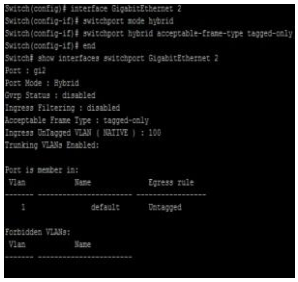
Switch(config)# **interface**

GigabitEthernet 2 Switch(config-if)#

switchport mode hybrid

Exampl e Switch(config-if)# **switchport hybrid acceptable-frame-type tagged-only**

Switch# **show interfaces switchport GigabitEthernet 2**



35.7 SWITCHPORT HYBRID ALLOWED VLAN

Use the switchport hybrid allow vlan add port configuration command to allow vlan on interface. Use the switchport hybrid allows vlan remove port configuration command to remove vlan on interface. You can verify your setting by entering the s show interfaces switchport Privileged EXEC command.

Switch#**configure terminal**

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

Switch(config-if)# **switchport hybrid allowed vlan add** *{VLAN-LIST}*

Switch(config-if)#**switchport hybrid allowed vlan remove** *{ VLAN-LIST}* **[(tagged|untagged)]**

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

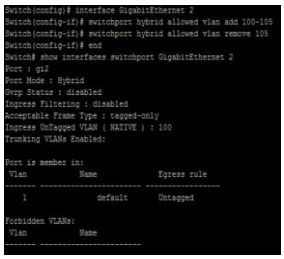
Example

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**

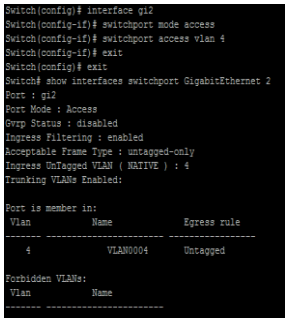
Switch (config)#**interface** {Interface-ID}

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



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**

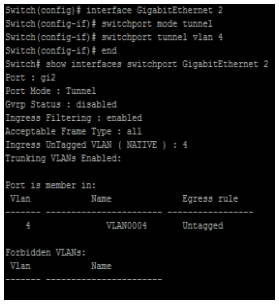
Switch(config)# **interface**

GigabitEthernet 2 Switch(config-if)#

switchport mode tunnel

Switch(config-if)# **switchport tunnel vlan** 4

Switch# **show interfaces switchport** GigabitEthernet 2



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.

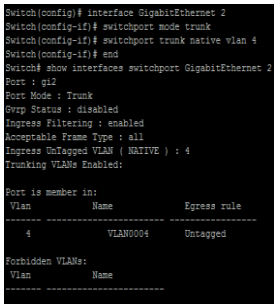
Switch#configure terminal

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



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.

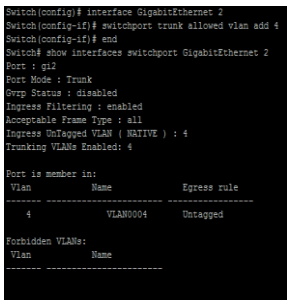
(VLAN-LIST | all) Specify the VLAN list or all VLANs to be added or removed.

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



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

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

Example

```
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**

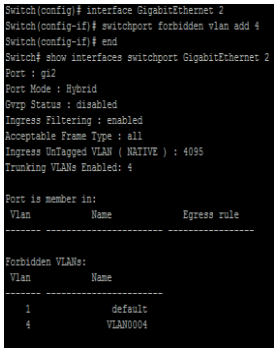
terminal

Switch(config)# **interface** GigabitEthernet 2

Switch(config-if)# **switchport forbidden vlan add**

4 Switch# **show interfaces switchport**

GigabitEthernet 2



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.

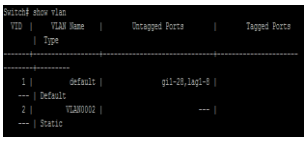
Switch(config)# **no management-vlan**

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**

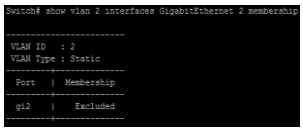
Syntax **show vlan** VLAN-LIST **interfaces** *{IF_PORTS}* **membership**

Parameter
Specify vlan to show
IF_PORTS Specify interface is to show

Mode Privileged EXEC

The following example specifies that show vlan interface membership

Example
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

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

ExampleSwitch# **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

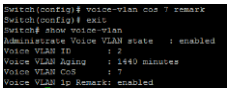
The following example specifies that show management vlan

Example

Switch# **show management-vlan**

VOICE VLAN

Syntax	voice-vlan cos *<0-7>*[remark] no voice-vlan cos
Parameter	<0-7> Specify the voice VLAN Class of Service value in telephone oui mode remark Specify that the L2 user priority is remarked with the CoS value
Default	The default cos value is 6, remark is
disabled. Mode	Global Configuration
Example	The following example show how to set cos value and enable 1p remark function Switch#configure terminal Switch(config)# voice-vlan cos 7 remark Switch# show voice-vlan



36.6 VOICE-VLAN COS (INTERFACE)

Use the voice vlan cos Interface configuration command to configure OUI voice VLAN cos mode configuration on an 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 cos (src |**

all) Switch(config-if)#**no voice-vlan cos**

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

The following example how to configure voice packet QoS attributes on an interface,

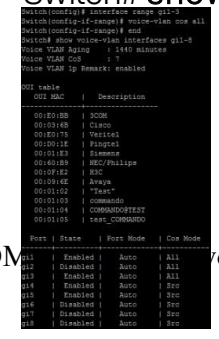
Switch#**configure terminal**

Switch(config)#**interface range** gi1-3

Switch(config-if)#**voice-vlan cos all**

Switch# **show voice-vlan interfaces**

Example



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

T llowing example how to configure voice mode to manual

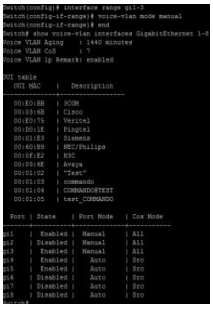
h Switch#**configure terminal**

e Switch(config)#**interface range** gi1-3

Switch(config-if)#**voice-vlan mode**

f **manual**

o Switch# **show voice-vlan interfaces** GigabitEthernet 1-8



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

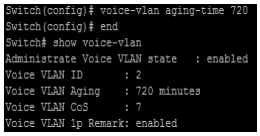
Example

The following example shows how to set aging time.

Switch#**configure terminal**

Switch(config)# **voice-vlan aging-time** 720

Switch# **show voice-vlan**



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

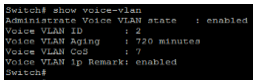
IF_PORTS Specifies interfaces to display voice VLAN settings in oui mode

Mode

Privileged EXEC

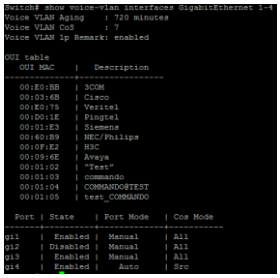
The following example show how to display voice vlan oui mode settings

Switch# **show voice-vlan**



Example

Switch# **show voice-vlan interfaces GigabitEthernet 1-4**



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

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.

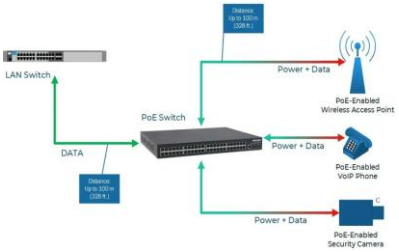


Fig 38.1 PoE Concept

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 device (PD) 4	Ultra PoE, UPoE, PoE++	Up to 100 W	2018	71 W for connected

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

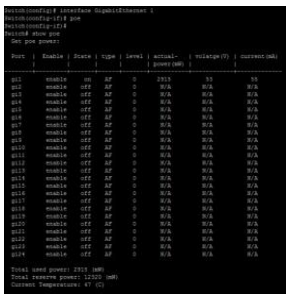
working status by using the show poe Privileged EXEC command.

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

m inutes.

```
Switch(config)# interface GigabitEthernet 1
Switch(config-if)# poe schedule week mon hour 1
```