EnGenius®

Command Line Interface User Guide

Table of Contents

Introduction

Overview

The CLI is divided into various modes. Each mode has a group of commands available in it.

Users are assigned privilege levels. Each privilege level can access the CLI modes permitted to that level. User privilege levels are described in the section below.

User (Privilege) Levels

Users may be created with one of the following user levels:

• Level 1 – Users with this level can only run User EXEC mode commands. Users at this level cannot access the web GUI.

• Level 7 – Users with this level can run commands in the User EXEC mode and a subset of commands in the Privileged EXEC mode. Users at this level cannot access the web GUI.

• Level 15 – Users with this level can run all commands. Only users at this level can access the web GUI.

A system administrator (user with level 15) can create passwords that allow a lower level user to temporarily become a higher level user. For example, the user may go from level 1 to level 7, level 1 to 15, or level 7 to level 15.

CLI Command Modes

The Command Line Interface (CLI) is divided into four command modes. The command modes are (in the order in which they are accessed):

• User EXEC mode

• Privileged EXEC mode

• Global Configuration mode

• Interface Configuration mode

Each command mode has its own unique console prompt and set of CLI commands. Entering a question mark at the console prompt displays a list of available commands for the current mode and for the level of the user. Specific commands are used to switch from one mode to another. Users are assigned privilege levels that determine the modes and commands available to them.

User EXEC Mode

Users with level 1 initially log into User EXEC mode. User EXEC mode is used for tasks that do not change the configuration, such as performing basic tests and listing system information.

The user-level prompt (default host name) is the switch's model name followed by a #. Eg.

EGS7228P#

The default host name can be changed via the hostname command in Global Configuration mode.

Privileged EXEC Mode

A user with level 7 or 15 automatically logs into Privileged EXEC mode. Users with level 1 can enter Privileged Exec mode by entering the enable command and when prompted, the password for level 15.

To return from the Privileged EXEC mode to the User EXEC mode, use the disable command.

Global Configuration Mode

The Global Configuration mode is used to run commands that configure features at the system level, as opposed to the interface level. Only users with command level of 7 or 15 can access this mode. To access Global Configuration mode from Privileged EXEC mode, enter the configure command at the Privileged EXEC mode prompt and press Enter. The Global Configuration mode prompt, consisting of the device host name followed by (config)#, is displayed:

EGS7228P(config)#

Use any of the following commands to return from Global Configuration mode to the Privileged EXEC mode:

- exit
- end
- Ctrl+Z

Interface or Line Configuration Modes

Various submodes may be entered from Global Configuration mode. These submodes enable performing commands on a group of interfaces or lines. For instance to perform several operations on a specific port or range of ports, you can enter the Interface Configuration mode for that interface.

The following submodes are available:

• Interface – Contains commands that configure a specific interface (port, VLAN, port channel, or tunnel) or range of interfaces. The Global Configuration mode command interface is used to enter the Interface Configuration mode. The interface Global Configuration command is used to enter this mode.

• Line Interface – Contains commands used to configure the management connections for the console, Telnet and SSH. These include commands such as line timeout settings, etc. The line Global Configuration command is used to enter the Line Configuration command mode.

• VLAN Database – Contains commands used to configure a VLAN as a whole. The vlan database Global Configuration mode command is used to enter the VLAN Database Interface Configuration mode.

• Management Access List – Contains commands used to define management access-lists. The management access-list Global Configuration mode command is used to enter the Management Access List Configuration mode.

• Port Channel – Contains commands used to configure port-channels; for example, assigning ports to a port-channel. Most of these commands are the same as the commands in the Ethernet interface mode, and are used to manage the member ports as a single entity. The interface port-channel Global Configuration mode command is used to enter the Port Channel Interface Configuration mode.

• QoS – Contains commands related to service definitions. The qos Global Configuration mode command is used to enter the QoS services configuration mode.

• MAC Access-List – Configures conditions required to allow traffic based on MAC addresses. The mac access-list Global Configuration mode command is used to enter the MAC access-list configuration mode.

To return from any Interface Configuration mode to the Global Configuration mode, use the exit command.

Accessing the CLI

The Switch's serial port's default settings are as follows:

- 115200 baud
- no parity
- 8 data bits
- 1 stop bit

A computer running a terminal emulation program capable of emulating a VT-100 terminal and a serial port configured as above are then connected to the Switch's Console port. With the serial port properly connected to a management computer, press the Enter key and enter the username and password.

Shortcuts

This table identifies some shortcuts in the CLI.

Key(s)	Description
(up/down arrow keys)	Scrolls through the list of recently-used commands. You can edit any command or press [ENTER] to run it again.
[TAB]	Auto-completes the keyword you are typing if possible. For example, type config, and press [TAB]. The Switch finishes the word configure.
[CTRL]+A	Moves the cursor to the beginning of the command line.
[CTRL]+E	Moves the cursor to the end of the command line.
[CTRL]+U	Clears the current command.
[CTRL]+Z / End	Returns back to the Privileged EXEC mode from any configuration mode.

EnGenius®

Chapter 1
802.1X

dot1x

Syntax

dot1x

no dot1x

Parameter

None

Default

Default is disabled

Usage

The "dot1x" command enables the global settings of IEEE 802.1X port-based network access control. Only when it is enabled, can the port-based setting work.

Use the no form of this command to disable.

Example

The following example shows how to enable 802.1X access control on port 1:

Switch(config)#

dot1x

switch(config)# interface fa1

```
switch(config-if)#
   dot1x auto
switch(config-if)#
  exit
switch(config)#
  show dot1x
802.1x protocol is: Enabled
802.1x protocol version: 2
switch(config)#
  show dot1x interfaces fa1
Port | Mode | Current State | Reauth Control | Reauth Period
fa1 Authentication | Initialize | Enabled | 3600
Quiet Period: 60 Second
Supplicant timeout: 30 Second
Max req: 2
Session Time (HH:MM:SS): 0: 0: 0: 0
```

Syntax

dot1x (auto|force-auth|force-unauth)

no dot1x

Parameter

auto	Port control will depends on the outcome of authentication.
force-auth	Force this port to be unconditional authorized.
force-unauth	Force this port to be unconditional unauthorized

Default

Default is disabled.

Mode

Interface Configuration

Usage

The "dot1x" command enables the global settings of IEEE 802.1X port-based network access control. Only when it is enabled can the port-based setting work. Use the no form of this command to disable it.

Example

The following example shows how to enable 802.1X access control on port 1:

Switch(config)#

dot1x

```
switch(config)#
  interface fa1
switch(config-if)#
   dot1x auto
switch(config-if)#
   exit
switch(config)#
  show dot1x
802.1x protocol is: Enabled
802.1x protocol version: 2
switch(config)#
  show dot1x interfaces fa1
Port | Mode | Current State | Reauth Control | Reauth Period
fa1 Authentication | Initialize | Enabled | 3600
Quiet Period: 60 Second
Supplicant timeout: 30 Second
Max req: 2
Session Time (HH:MM:SS): 0: 0: 0: 0
```

dot1x Reauthentication

Syntax

dot1x reauth

no dot1x reauth

Parameter

None

Default

Default is disabled

Mode

Interface Configuration

Usage

Use the “dot1x reauth” command to enable 802.1X periodical reauthentication function on port. Use the no form of this command to disable this function.

‘**Example**

The following example shows how to enable 802.1X access control on port 1.

switch(config)# i

nterface fa1

```
switch(config-if)#
   dot1x reauth
switch(config-if)#
   exit
switch(config)#
  show dot1x
802.1x protocol is: Enabled
802.1x protocol version: 2
switch(config)#
   show dot1x interfaces fa1
Port | Mode | Current State | Reauth Control | Reauth Period
fa1 Authentication | Initialize | Enabled | 3600
Quiet Period: 60 Second
Supplicant timeout: 30 Second
Max req: 2
Session Time (HH:MM:SS): 0: 0: 0: 0
```

dot1x Timeout Reauth-Period

Syntax

dot1x timeout reauth-period <30-65535>

no dot1x timeout reauth-period

Parameter

<30-65535> Specify the re-authentication period.

Default

3600 seconds

Mode

Interface Configuration

Usage

Use the “dot1x timeout reauth-period” command to configure the re- authentication period. Use the no form of this command to restore the period to default value.

Example

The example shows how to configure re-authentication period to 300 sec. on port 1

switch(config)#

interface fa1

```
switch(config-if)#
  dot1x timeout reauth-period 300
switch(config-if)#
   exit
switch(config)#
  show dot1x interfaces fa1
Port | Mode | Current State | Reauth Control | Reauth Period
fa1 Authentication | Initialize | Enabled | 300
Quiet Period: 60 Second
Supplicant timeout: 30 Second
Max req: 2
Session Time (HH:MM:SS): 0: 0: 0: 0
```

dot1x Timeout Quiet-Period

Syntax

dot1x timeout quiet-period <0-65535>

no dot1x timeout quiet-period

Parameter

<0-65535> Specify the quiet period

Default

60 seconds

Mode

Interface Configuration

Usage

Use the “dot1x timeout quiet-period” command to configure the quiet period. Use the no form of this command to restore the period to its default value.

Example

The example shows how to configure quiet period to 300 sec. on port 1.

switch(config)#

interface fa1

```
switch(config-if)#
   dot1x timeout quiet-period 300
switch(config-if)#
   exit
switch(config)#
  show dot1x interfaces fa1
Port | Mode | Current State | Reauth Control | Reauth Period
fa1 Authentication | Initialize | Enabled | 3600
Quiet Period: 300 Second
Supplicant timeout: 30 Second
Max req: 2
Session Time (HH:MM:SS): 0: 0: 0: 0
```

dot1x Timeout Supp-Timeout

Syntax

dot1x timeout supp-timeout <1-65535>

no dot1x timeout quiet-period

Parameter

<1-65535> Specify the supplicant period.

Default

30 seconds

Mode

Interface Configuration

Usage

Use the “dot1x timeout supp-timeout” command to configure the supplicant period. Use the no form of this command to restore the period to default value

Example

The example shows how to configure supplicant period to 300 sec. on port 1.

switch(config)#

interface fa1

```
switch(config-if)#
   dot1x timeout supp-timeout 300
switch(config-if)#
   exit
switch(config)#
  show dot1x interfaces fa1
Port | Mode | Current State | Reauth Control | Reauth Period
fa1 Authentication | Initialize | Enabled | 3600
Quiet Period: 60 Second
Supplicant timeout: 300 Second
Max req: 2
Session Time (HH:MM:SS): 0: 0: 0: 0
```

dot1x Timeout Max-Req

Syntax

dot1x max-req <1-10>

no dot1x max-req

Parameter

<1-10> Specify the maximum request retries.

Default

2 times

Mode

Interface Configuration

Usage

Use the “dot1x timeout supp-timeout” command to configure the supplicant period. Use the no form of this command to restore the period to its default value.

Example

The example shows how to configure maximum request retries to 4 times on port 1.

switch(config)#

interface fa1

```
switch(config-if)#
   dot1x max-req 4
switch(config-if)#
   exit
switch(config)#
   show dot1x interfaces fa1
Port | Mode | Current State | Reauth Control | Reauth Period
fa1 Authentication | Initialize | Enabled | 3600
Quiet Period: 60 Second
Supplicant timeout: 30 Second
Max req: 4
Session Time (HH:MM:SS): 0: 0: 0: 0
```

dot1x Guest VLAN

Syntax

dot1x guest-vlan <1-4094>

no dot1x guest-vlan

Parameter

<1-4094> Specify VLAN ID to enable 802.1X guest vlan

Default

Default is disabled

Mode

Global Configuration

Usage

Use the dot1x guest-vlan command to globally enable the guest VLAN function. Use the no form of this command to disable the guest VLAN function. For a port to become a member of thye guest VLAN after an authentication failure, you should also enable guest VLAN on that port.

Example

The example shows how to configure VLAN 2 as guest VLAN and enable guest VLAN on port 1.

switch(config)#

dot1x guest-vlan 2

```
switch(config)#
   interface fa1
switch(config-if)#
   dot1x auto
switch(config-if)#
   dot1x guest-vlan
switch(config-if)#
  exit
switch(config)#
   show dot1x guest-vlan
Guest VLAN ID: 2
Port | Guest VLAN | In Guest VLAN
fa1 | Enabled | No
fa2 | Disabled | ---
fa3 | Disabled | ---
fa4 | Disabled | ---
fa5 | Disabled | ---
fa6 | Disabled | ---
fa7 | Disabled | ---
```

Show dot1x

Syntax

show dot1x

Parameter

Default

No default value for this command.

Mode

Privileged EXEC

Usage

Use “show dot1x” command to show dot1x enabling status.

Example

This example shows how to show the dot1x enabling status.

Switch#

show dot1x

802.1x protocol is: Disabled

802.1x protocol version: 2

Show dot1x Authentication-Hosts

Syntax

show dot1x auth-hosts

Parameter

None

Default

No default value for this command.

Mode

Privileged EXEC

Usage

Use “show dot1x auth-hosts” command to show all dot1x authorized hosts.

Example

This example shows how to show the dot1x authorized hosts.

Switch#

show dot1x auth-hosts

User Name | Port | Session Time |

Authentication Method | MAC Address

8389_1 | FE3 | 0: 0: 0:20 |

Remote | 00:16:E6:D5:5C:19

Show dot1x Interface

Syntax

show dot1x interface IF_PORTS

Parameter

IF_PORTS Select port to show dot1x configurations.

Default

No default value for this command.

Mode

Privileged EXEC

Usage

Use “show dot1x interfaces” command to show dot1x information of the specified port.

Example

This example shows how to show dot1x configurations on interface fa1.

Switch#

show dot1x interfaces fa1

Port | Mode | Current State | Reauth Control | Reauth Period

fa1 | 802.1X Disabled | - | Enabled |

3600

Quiet Period: 60 Second

Supplicant timeout: 30 Second

Max req: 2

Session Time (HH:MM:SS): 0: 0: 0: 0

Show dot1x Guest VLAN

Syntax

show dot1x guest-vlan

Parameter

None

Default

No default value for this command.

Mode

Privileged EXEC

Usage

Use “show dot1x guest-vlan” command to show dot1x guest-vlan status.

Example

This example shows how to show the dot1x guest-vlan status.

Switch#: show dot1x guest-vlan

Guest VLAN ID: 2

This example shows how to show the dot1x guest-vlan status.

Switch#

show dot1x guest-vlan

Guest VLAN ID: 2

Port | Guest VLAN | In Guest VLAN

fa1 | Enabled | No

fa2 | Disabled | ---

fa3 | Disabled | ---

fa4 | Disabled | ---

fa5 | Disabled | ---

fa6 | Disabled | ---

fa7 | Disabled | ---

fa8 | Disabled | ---

fa9 | Disabled | ---

fa10 | Disabled | ---

fa11 | Disabled | ---

fa12 | Disabled | ---

fa13 | Disabled | ---

fa14 | Disabled | ---

fa15 | Disabled | ---

fa16 | Disabled | ---

fa17 | Disabled | ---

fa18 | Disabled | ---

fa19 | Disabled | ---

fa20 | Disabled | ---

fa21 | Disabled | ---

fa22 | Disabled | ---

fa23 | Disabled | ---

fa24 | Disabled | ---

gi1 | Disabled | ---

gi2 | Disabled | ---

gi3 | Disabled | ---

gi4 | Disabled | ---

EnGenius®

Chapter 2
AAA

AAA Authentication

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

Usage

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.

Local: Use local user account database to authenticate. (This method is not supported for enable authentication)

Enable: Use local enable password database to authenticate.

Tacacs+: Use remote Tacas+ server to authenticate.

Radius: Use remote Radius server to authenticate.

None: Do nothing and just make user to be authenticated.

Each list allows you to combine these methods with different orders. For example, If you want to authenticate a login user with the remote Tacacs+ server, but server may have crashed, you'll need a backup plan, such as another Radius server. You can configure the list with the Tacacs+ server as the first authentication method and the Radius server as a second one. Use the no form to delete the existing list. However, the "default" list is not allowed to be removed.

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

Login List Name | Authentication Method List

default | local

test1 | tacacs+ radius local

This example shows how to add an enable authentication list to authenticate

with order tacacs+, radius, enable.

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 List Name | Authentication Method List

default | enable

test2 | tacacs+ radius enable

Login Authentication

Syntax

login authentication LISTNAME

no login authentication

Parameter

LISTNAME Specify the login authentication list name to use.

Default

Default login authentication list for each line is “default”.

Mode

Line Configuration

Usage

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

Use no form to bind the “default” list back.

Example

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

Switch(config)#

aaa authentication login test1

tacacs+ radius local

Switch(config)#

line telnet

Switch(config-line)#

login authentication test1

This example shows how to show line binding lists.

Switch#

show line lists

Line Type | AAA Type | List Name

console | login | default

| enable | default

| exec | default

| commands | default

| accounting-exec | default

telnet | login | test1

| enable | default

| exec | default

| commands | default

| accounting-exec | default

ssh | login | default

| enable | default

| exec | default

| commands | default

| accounting-exec | default

http | login | default

https | login | default

IP http Login Authentication

Syntax

ip (http | https) login authentication LISTNAME

no ip (http | https) login authentication

http	Bind login authentication list to user access WEBUI with http protocol.
https	Bind login authentication list to user access WEBUI with https protocol.
LISTNAME	Specify the login authentication list name to use.

Default

Default login authentication list for each line is “default”.Mode

Mode

Global Configuration

Usage

Different access methods are allowed to bind different login authentication lists. Use the “ip (http | https) login authentication” command to bind the list to WEBUI access from http or https. Use no form to bind the “default” list back.

Example

This example shows how to create two new login authentication lists and bind to http and https.

This example shows how to create two new login authentication lists and bind to http and https.

```
Switch(config)#
  aaa authentication login test1
tacacs+ radius local
Switch(config)#
  aaa authentication login test2
radius local
Switch(config)#
  ip http login authentication test1
Switch(config)#
  ip https login authentication test2
```

This example shows how to show line binding lists.

```
Switch#
  show line lists
Line Type | AAA Type | List Name
console | login | default
| enable | default
| exec | default
```

| commands | default

| accounting-exec | default

telnet | login | default

| enable | default

| exec | default

| commands | default

| accounting-exec | default

ssh | login | default

| enable | default

| exec | default

| commands | default

| accounting-exec | default

http | login | test1

https | login | test2

Enable Authentication

Syntax

enable authentication LISTNAME

no enable authentication

Parameter

LISTNAME Specify the enable authentication list name to use.

Default

Default enable authentication list for each line is “default”.

Mode

Line Configuration

Usage

Different access methods are allowed to bind different enable authentication lists. Use the “enable authentication” command to bind the list to specific line (console, telnet, ssh). Use no form to bind the “default” list back.

Example

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

Switch(config)#

aaa authentication enable test1

tacacs+ radius enable

Switch(config)#

line telnet

Switch(config-line)#

enable authentication test1

This example shows how to show line binding lists.

Switch#

show line lists

Line Type | AAA Type | List Name

console | login | default

| enable | default

| exec | default

| commands | default

| accounting-exec | default

telnet | login | default

| enable | test1

| exec | default

| commands | default

| accounting-exec | default

ssh | login | default

| enable | default

| exec | default

| commands | default

| accounting-exec | default

http | login | default

https | login | default

Show AAA Authentication

Syntax

show aaa authentication (login | enable) lists

Parameter

login	Show login authentication list
enable	Show enable authentication list

Default

No default value for this command

Mode

Privileged EXEC

Usage

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

Example

This example shows how to show existing login authentication lists.

Switch#

show aaa authentication login lists

Login List Name | Authentication Method List

default | local

test1 | tacacs+ radius local

This example shows how to show existing enable authentication lists

Switch#

show aaa authentication login lists

Enable List Name | Authentication Method List

default | enable

test2 | tacacs+ radius enable

Show Line Lists

Syntax

Show line lists

Parameter

Default

No default value for this command

Mode

Privileged EXEC

Usage

Use the “show line lists” command to show all of the lines’ binding list of all authentication, authorization, and accounting functions.

Example

This example shows how to show line binding lists.

Switch#

show line lists

Line Type | AAA Type | List Name

console | login | default

| enable | default

| exec | default

| commands | default

| accounting-exec | default

telnet | login | default

| enable | default

| exec | default

| commands | default

| accounting-exec | default

ssh | login | default

| enable | default

| exec | default

| commands | default

| accounting-exec | default

http | login | default

https | login | default

tacacs Default-Config

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

Usage

Use the “tacacs default-config” command to modify the default values of the tacacs+ server. These default values will be used when a user tries to create a new tacacs+ server and doesn’t assign these values.

Example

This example shows how modify default tacacs+ configuration

This example shows how modify default tacacs+ configuration

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

Timeout | Key

10 | tackey

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

Switch(config)#

tacacs host 192.168.1.111

Switch#

show tacacs

Prio | Timeout | IP Address | Port |

Key

1 | 10 | 192.168.1.111 | 49 |

tackey

tacacs Host

Syntax

tacacs host HOSTNAME [port <0-65535>] [key TACPLUSKEY] [priority <0-65535>] [timeout <1-30>]

no tacacs [host HOSTNAME]

Parameter

Host	HOSTNAME Specify tacacs+ server host name, both IP address and domain name are available.
Port<0-65535>	Specify tacacs+ server udp port
Key	TACPLUSKEY Specify tacacs+ server key string
Priority<0-65535>	Specify tacacs+ server priority
Timeout <1-30>	Specify tacacs+ server timeout value

Default

Default tacacs+ key is “”.

Default tacacs+ timeout is 5 seconds

Mode

Global Configuration

Usage

Use “tacacs host” command to add or edit tacacs+ server for authentication, authorization or accounting. Use no form to delete one or all tacacs+ servers from database.

Example

This example shows how to create a new tacacs+ server

Switch(config)#

tacacs host 192.168.1.111 port 12345

key tacacs+ priority 100 timeout 10

This example shows how to show existing tacacs+ server.

Switch#

show tacacs

Prio | Timeout | IP Address | Port | Key

100 | 10 | 192.168.1.111 | 12345 |

tacacs+

Show tacacs Default-Config

Syntax

show tacacs default-config

Parameter

None

Default

No default value for this command

Mode

Privileged EXEC

Usage

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

Example

This example shows how to show default tacacs+ configurations.

Switch#

show tacacs default-config

Timeout | Key

10 | tackey

Show tacacs

Syntax

Show tacacs

Parameter

None

Default

No default value for this command

Mode

Privileged EXEC

Usage

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

Example

This example shows how to show existing tacacs+ server.

Switch#

show tacacs

Prio | Timeout | IP Address | Port | Key

100 | 10 | 192.168.1.111 | 12345 |tacacs+

Radius Default-Config

Syntax

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

Parameter

Key	RADIUSKEY Specify default radius server key string
Retransmit	<1-10> Specify default radius server retransmit value
Timeout	<1-30> Specify default radius server timeout value

Default

Default radius key is “”.

Default radius retransmit is 3 times.

Default radius timeout is 3 seconds.

Mode

Global Configuration

Usage

Use the “radius default-config” command to modify the default values of the radius server. These default values will be used when a user tries to create a new radius server and isn’t assigned these values.

Example

This example shows how modify default radius configuration

Switch(config)#

radius default-config timeout 20

Switch(config)#

radius default-config key radiuskey

Switch(config)#

radius default-config retransmit 5

This example shows how to show default radius configurations.

Switch#

show radius default-config

Retries| Timeout| Key

5 | 20 | radiuskey

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

Switch(config)#

radius host 192.168.1.111

Switch#

show radius

Prio | IP Address | Auth-Port| Retries|

Timeout| Usage-Type| Key

1 | 192.168.1.111 | 1812 | 5 |

20 | All | radiuskey

Radius Host

Syntax

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

no radius [host HOSTNAME]

Parameter

Host	HOSTNAME Specify radius server host name, both IP address and domain name are available.
Auth-port <0- 65535>	Specify radius server udp port
Key RADIUSKEY	Specify radius server key string
priority <0-65535>	Specify radius server priority
Retransmit <1-10>	Specify radius server retransmit times
Timeout <1-30>	Specify radius server timeout value
Type	Usage type of this server
Login	Use for login
802.1X	Use for 802.1X authentication
All	Use for both login and 802.1X authentication

Default

Default radius key is “”.

Default radius timeout is 3 seconds.

Mode

Global Configuration

Usage

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

Example

This example shows how to create a new radius server

Switch(config)#

radius host 192.168.1.111 auth-port 12345 key radiuskey priority 100 retransmit 5 timeout 10 type all

This example shows how to show existing radius server.

Switch#

show radius

Prio | IP Address | Auth-Port| Retries|

Timeout| Usage-Type| Key

100 | 192.168.1.111 | 12345 | 5 | 10

| All |radiuskey

Show Radius Default-Config

Syntax

show radius default-config

Parameter

None

Default

No default value for this command

Mode

Privileged EXEC

Usage

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

Example

This example shows how to show default radius configurations.

Switch#

show radius default-config

Retries| Timeout| Key

5 | 20 | radiuskey

Show Radius

Syntax

Show radius

Parameter

None

Default

No default value for this command

Mode

Privileged EXEC

Usage

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

Example

This example shows how to show existing radius server.

Switch#

show radius

Prio | IP Address | Auth-Port| Retries|

Timeout| Usage-Type| Key

100 | 192.168.1.111 | 12345 | 5 | 10

| All |radiuskey

EnGenius®

Chapter 3
ACL

MAC ACL

Syntax

mac acl NAME

no mac acl NAME

Parameter

NAME Specify the name of MAC ACL

Default

No default is defined

Mode

Global Configuration

Usage

Use the mac acl command to create a MAC access list and to enter mac-acl configuration mode. The name of the ACL must be unique and cannot have same name as another ACL or QoS policy. Once an ACL is created, an implicit “deny any” ACE is 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 it.

Example

The example shows how to create a ip acl. You can verify settings by the following show acl commands:

```
Switch334455(config)#
  mac acl test
Switch334455(mac-al)#
  show acl
MAC access list test
```

Permit (MAC)

Syntax

[sequence <1-2147483647>] permit (A:B:C:D:E:F/A:B:C:D:E:F|any) (A:B:C:D:E:F/A:B:C:D:E:F|any) [vlan <1-4094>] [cos <0-7> <0-7>]

[ethtype <1501-65535>]

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 <1501-65535>]	(Optional) Specify Ethernet protocol number of packet

Default

No default is defined.

Mode

MAC ACL Configuration

Usage

Usage

Use the permit command to add permit conditions for a mac ACE that bypass those packets that hit the ACE. The “sequence” also represents the hit priority when an ACL binds to an interface. An ACE that doesn’t specify a “sequence” index would assign a sequence index which is the largest existed index plus 20. If the packet content can match more than one ACE, the lowest sequence ACE is hit. An ACE can not be added if it has the same conditions as existing ACE.

Example

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

Switch334455(config)#

mac acl test

Switch334455(mac-al)#

sequence 999 permit

22:33:44:55:66:77/FF:FF:FF:FF:FF:FF any vlan 3 ethtype 1999

Switch334455(mac-al)#

show acl

MAC access list test

sequence 999 permit 22:33:44:55:66:77/FF:FF:FF:FF:FF:FF any vlan 3 ethtype 1999

Deny (MAC)

Syntax

[sequence <1-2147483647>] deny (A:B:C:D:E:F/A:B:C:D:E:F|any) (A:B:C:D:E:F/A:B:C:D:E:F|any) [vlan <1-4094>] [cos <0-7> <0-7>]

[ethtype <1501-65535>] [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 <1501-65535>]	(Optional) Specify Ethernet protocol number of packet.
[shutdown]	(Optional) Shutdown interface while ACE hit.

Default

No default is defined

Mode

MAC ACL Configuration

Usage

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

Example

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

Switch334455(config)#

mac acl test

Switch334455(mac-al)#

sequence 30 permit any any

Switch334455(mac-al)# deny any aa:bb:cc:00:0:00/FF:FF:FF:00:00:00 vlan 9 shutdown

Switch334455(mac-al)#

show acl

MAC access list test

sequence 30 permit any any

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

IP ACL

Syntax

IP acl NAME

no IP acl NAME

Parameter

NAME Specify the name of IPv4 ACL

Default

No default is defined

Mode

Global Configuration

Usage

Use the ip acl command to create an IPv4 access list and to enter the ip-acl configuration mode. The name of the ACL must be unique and cannnot have same name with as another 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 it.

Example

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

```
Switch334455(config)#
  ip acl iptest
Switch334455(ip-al)#
  show acl
IP access list iptest
```

Permit (IP)

Syntax

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

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

router-advertisement|router-solicitation|time-exceeded|timestamp| timestampreply| traceroute|any) (<0-255>|any) [(dscp|precedence) VALUE]

[sequence <1-2147483647>] permit igmp (A.B.C.D/A.B.C.D|any) (A.B.C.D/A.B.C.D|any) (<0-255>|host-query|host-report|dvmrp|pim| cisco-trace|host-report-v2|host-leave-v2|host-report-v3|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|ftpdata| ftp|telnet|smtp|time|hostname|whois| tacacs-

ds| domain|www|pop2 pop3| syslog|talk| klogin|kshell|sunrpc|drip|PORT_RANGE|any) [match-all TCP_FLAG] [(dscp|precedence) VALUE]

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

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

no sequence <1-2147483647>

Parameter

<1-2147483647>	(Optional) Specify sequence index of ACE, the sequence index represent the priority of an ACE in ACL.
(A.B.C.D/A.B.C.D|any)	Specify the source IPv4 address and mask of packet or any IPv4 address.
(A.B.C.D/A.B.C.D|any)	Specify the destination IPv4 address and mask of packet or any IPv4 address.
[dscp VALUE]	(Optional) Specify the DSCP of packet.
[precedence VLAUE]	(Optional) Specify the IP precedence of packet.
icmp-type	Specify ICMP message type for filtering ICMP packet. Enter a type name of list or a number of ICMP message type.
icmp-code	Specify ICMP message code for filtering ICMP packet.
igmp-type	Specify IGMP type for filtering IGMP packet. Enter a type name of list or a number of IGMP type.
l4-source-port	Specify TCP/UDP source port of for filtering TCP/UDP packet. Enter a port name of list or a number of TCP/UDP port.
l4-destination-port	Specify TCP/UDP destination port of for filtering TCP/UDP packet. Enter a port name of list or a number of TCP/UDP port.
match-all	Specify tcp flag for TCP packet. If a flag should be set it is prefixed by \"+\".If a flag should be unset it is prefixed by \"-\". Available options are +urg, +ack, +psh, +rst, +syn, +fin, -urg, -ack, -psh, -rst, -syn and -fin.To define more than 1 flag-enter additional flags one after another without a space (example +syn-ack).

Default

No default is defined.

Mode

IP ACL Configuration

Usage

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

Example

The example shows how to add 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.

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

Switch334455(ip-al)#

permit ip 192.168.1.0/255.255.255.0

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

Switch334455(ip-al)#

permit icmp any any echo-request any

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

Switch334455(ip-al)#

permit tcp any any any www dscp 5

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

Switch334455(ip-al)#

permit udp any any 192.168.1.1/255.255.255.255 snmp

Switch334455(ip-al)#

show acl

IP access list iptest

sequence 1 permit ip 192.168.1.0/255.255.255.0 any

sequence 21 permit icmp any any echo-request any

sequence 41 permit tcp any any any www dscp 5

sequence 61 permit udp any any 192.168.1.1/255.255.255.255 snmp

Deny (IP)

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 igmp (A.B.C.D/A.B.C.D|any) (A.B.C.D/A.B.C.D|any) (<0-255>|host-query|host-report|dvmrp|pim| cisco-trace|host-report-v2|host-leave-v2|host-report-v3|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-da ta|ftp|telnet|smtp|time|hostname|whois|tacacs-ds| domain|www|pop2|pop3|syslog|talk|klogin|kshell kshell|sunrpc|drip|PORT_RANGE|any) (A.B.C.D/A.B.C.D|any) (<0-65535>|echo|discard|daytime|ftp-data|ftp|telnet| smtp|time|hostname|whois|tacacs-ds|domain|www|pop2|pop3|syslog|talk| klogin|kshell|sunrpc|drip|PORT_RANGE|any) [match-all TCP_FLAG] [(dscp|precedence) VALUE] [shutdown]

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

no sequence <1-2147483647>

Parameter

<1-2147483647>	(Optional) Specify sequence index of ACE, the sequence index represent the priority of an ACE in ACL.
(A.B.C.D/A.B.C.D|any)	Specify the source IPv4 address and mask of packet or any IPv4 address.
(A.B.C.D/A.B.C.D|any)	Specify the destination IPv4 address 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.
igmp-type	Specify IGMP type for filtering IGMP packet. Enter a type name of list or a number of IGMP type.
l4-source-port	Specify TCP/UDP source port of for filtering TCP/UDP packet. Enter a port name of list or a number of TCP/UDP port.
l4-destination-port	Specify TCP/UDP destination port of for filtering TCP/UDP packet. Enter a port name of list or a number of TCP/UDP port
match-all	Specify tcp flag for TCP packet. If a flag should be set it is prefixed by \"+\".If a flag should be unset it is prefixed by \"-\". Available options are +urg, +ack, +psh, +rst, +syn, +fin, -urg, -ack, - psh, -rst, -syn and -fin.To define more than 1 flag - enter additional flags one after another without a space (example +syn-ack).
[shutdown]	(Optional) Shutdown interface while ACE hit

Default

No default is defined.

Mode

IP ACL Configuration

Usage

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 can not be added if has the same conditions as existed ACE. Use “shutdown” to shutdown interface while ACE hit.

Example

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

```
Switch334455(config)#
  ip acl iptest
Switch334455(ip-al)#
  deny ip 192.168.1.80/255.255.255.255 any
Switch334455(ip-al)#
  show acl
IP access list iptest
sequence 1 deny ip 192.168.1.80/255.255.255.255 any
```

IPv6 ACL

Syntax

ipv6 acl NAME

no ipv6 acl NAME

Parameter

NAME Specify the name of IPv6 ACL

Default

No default is defined

Mode

Global Configuration

Usage

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

Example

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

```
Switch334455(config)#
  ipv6 acl ipv6test
Switch334455(ipv6-al)#
  show acl
IPv6 access list iptest
```

Permit (IPv6)

Syntax

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

[sequence <1-2147483647>] permit icmp (X:X::X:X/<0-128>|any) (X:X::X:X/<0-128>|any) (<0-255>|destination-unreachable|packet-toobig|

time-exceeded|parameter-problem|echo-request|echo-reply| mldquery| mld-report|mldv2-report|mld-done| router-solicitation|routeradvertisement| 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-all TCP_FLAG] [(dscp|precedence) VALUE]

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

no sequence <1-2147483647>

Parameter

<1-2147483647> (Optional)	Specify sequence index of ACE, the sequence index represent the priority of an ACE in ACL.
(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.
igmp-type	Specify IGMP type for filtering IGMP packet. Enter a type name of list or a number of IGMP type.
l4-source-port	Specify TCP/UDP source port of for filtering TCP/UDP packet. Enter a port name of list or a number of TCP/UDP port
l4-destination-port	Specify TCP/UDP destination port of for filtering TCP/UDP packet. Enter a port name of list or a number of TCP/UDP port.
match-all	Specify tcp flag for TCP packet. If a flag should be set it is prefixed by \"+\".If a flag should be unset it is prefixed by \"-\". Available options are +urg, +ack, +psh, +rst, +syn, +fin, -urg, -ack, - psh, -rst, -syn and -fin.To define more than 1 flag - enter additional flags one after another without a space (example +syn-ack).

Default

No default is defined.

Mode

IP ACL Configuration

Usage

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

Example

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

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

Switch334455(ipv6-al)#

permit permit ipv6 fe80:1122:3344:5566::1/64 any

Switch334455(ipv6-al)#

show acl

IPv6 access list ipv6test

sequence 1 permit ipv6 fe80:1122:3344:5566::1/64 any

Deny IP

Syntax

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

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

[sequence <1-2147483647>] deny igmp (A.B.C.D/A.B.C.D|any) (A.B.C.D/A.B.C.D|any) (<0-255>|host-query|host-report|dvmrp|pim| cisco-trace|host-report-v2|host-leave-v2|host-report-v3|any) [(dscp|precedence) VALUE] [shutdown]

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

[sequence <1-2147483647>] deny udp (A.B.C.D/A.B.C.D|any) (<0-65535>|echo|discard|time|nameserver|tacacs-ds|domain|bootps|bootpc|tftp|sunrpc|ntp|netbios-ns|snmp|snmptrap|who|syslog|talk|rip|PORT_RANGE|any) (A.B.C.D/A.B.C.D|any) (<0-65535>|echo|discard|time|nameserver|tacacs-ds|domain|bootps|bootpc|tftp|sunrpc|ntp| netbios-ns|snmp|snmptrap|who|syslog|PORT_RANGE|any)[(dscp|precedence) VALUE] [shutdown]no sequence <1-2147483647>

Parameter

<1-2147483647> (Optional)	Specify sequence index of ACE, the sequence index represent the priority of an ACE in ACL.
(A.B.C.D/ A.B.C.D|any)	Specify the source IPv4 address and mask of packet or any IPv4 address.
(A.B.C.D/ A.B.C.D|any)	Specify the destination IPv4 address 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.
igmp-type	Specify IGMP type for filtering IGMP packet. Enter a type name of list or a number of IGMP type.
l4-source-port	Specify TCP/UDP source port of for filtering TCP/UDP packet. Enter a port name of list or a number of TCP/UDP port.
l4-destination-port	Specify TCP/UDP destination port of for filtering TCP/UDP packet. Enter a port name of list or a number of TCP/UDP port.
match-all	Specify tcp flag for TCP packet. If a flag should be set it is prefixed by \"+\".If a flag should be unset it is prefixed by \"-\". Available options are +urg, +ack, +psh, +rst, +syn, +fin, -urg, -ack, - psh, -rst, -syn and -fin.To define more than 1 flag - enter additional flags one after another without a space (example +syn-ack).
[shutdown] (Optional)	Shutdown interface while ACE hit

Default

No default is defined.

Mode

IP ACL Configuration

Usage

Use the deny command to add deny conditions for an IPv6 ACE that then drops those packets that hit the ACE. The "sequence" also represents hit priority when the ACL binds to an interface. An ACE that doesn not specify the "sequence" index would assign a sequence index which is the largest existed index plus 20. If packet content can match more than one ACE, the lowest sequence ACE is hit. An ACE can not be added if it has the same conditions as existing ACEs. Use "shutdown" to shutdown the interface while ACE hits

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

Switch334455(config)#

ipv6 acl ipv6test

Switch334455(ip-al)#

deny ipv6 any fe80::abcd/128

Switch334455(ip-al)#

show acl.

IPv6 access list ipv6test

sequence 1 deny ipv6 any fe80::abcd/128

Bind ACL

Syntax

(mac|ip|ipv6) acl NAME

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

Parameter

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

Default

No default is defined

Mode

Interface Configuration

Usage

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

Example

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

switch(config)#

interface fa1

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

Show ACL

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 the ACL

Default

No default is defined

Mode

Global Configuration

Context Configuration

Usage

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

Example

The example shows how to show all IP ACL.

```
Switch334455(config)#
  show ip acl
IP access list iptest
sequence 1 deny ip 192.168.1.80/255.255.255.255 any
```

Show ACL Utilization

Syntax

show acl utilization

Parameter

None

Default

No default is defined

Mode

Global Configuration

Usage

Use the show acl utilization command to show the usage of PIE of ASIC. When a ACL bind to interface, it needs ASIC PIE resource to help to filter packet. An ASIC has limited PIE resource. This command help user to know the PIE usage of AISC.

Example

The example shows how to show PIE utilization.

Switch334455(config)#

show acl utilization

Group Index : 1

Group Assign to : Mac-based ACL and IPv4-based ACL

Group Maximun ACEs : 128

Group Remain ACEs : 125

Group Used ACEs : 3

ACEs Used by ACL : 3

ACEs Used by QoS : 0

Group Index : 2

Group Assign to : None

Group Maximun ACEs : 128

Group Remain ACEs : 128

Group Used ACEs : 0

ACEs Used by ACL : 0

ACEs Used by QoS : 0

Group Index : 3

Group Assign to : None

Group Maximun ACEs : 128

Group Remain ACEs : 128

Group Used ACEs : 0

ACEs Used by ACL : 0

ACEs Used by QoS : 0

Group Index : 4

Group Assign to : None

Group Maximun ACEs : 128

Group Remain ACEs : 128

Group Used ACEs : 0

ACEs Used by ACL : 0

ACEs Used by QoS : 0

EnGenius®

Chapter 4
Administration

Enable

Syntax

enable [<1-15>]

disable [<1-14>]

Parameter

<1-15>	Specify privileged level to enable
<1-14>	Specify privileged level to disable

Default

Default privilege level is 15 if no privilege level is specified on enable command.

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

Mode

User EXEC

Usage

In User EXEC mode, user only allows to do a few actions. Most of commands are only available in privileged EXEC mode. Use “enable” command to enter the privileged mode to do more actions on switch. In privileged EXEC mode, use “exit” command is able to go back to user EXEC mode with original user privilege level. If you need to go back to user EXEC mode with different privilege level, use “disable” command to specify the privilege level you need. In privileged EXEC mode, the prompt will show “Switch#”

Example

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

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

This example show how to enter user EXEC mode with privilege 3.

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

Exit

Syntax

exit

Parameter

None

Default

No default value for this command.

Mode

User EXEC

Privileged EXEC

Global Configuration

Interface Configuration

Line Configuration

Usage

In User EXEC mode, “exit” command will close current CLI session. In other modes, “exit” command will go to the parent mode. And every mode has the “exit” command.

Example

This example shows how to enter privileged EXEC mode and use exit command to go back to user EXEC mode.

```
Switch>
  enable
Switch#
  exit
Switch>
```

Configure

Syntax

configure

Parameter

None

Default

No default value for this command

Mode

Privileged EXEC

Usage

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

Example

This example shows how to enter global configuration mode.

```
Switch#
  configure
Switch(config)#
```

Interface

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:

fa1

FastEthernet3

Gigabit4

If port range is specified, the list format is also available. For Example:

fa1,3,5

fa2,gi1-3

Default

No default value for this command

Mode

Global Configuration

Usage

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

Example

This example shows how to enter Interface Configuration mode.

```
Switch#
  configure
Switch(config)#
  interface fa1
Switch(config-if)#
```

Line

Syntax

line (console | telnet | ssh)

Parameter

console	Select console line to configure.
telnet	Select telnet line to configure.
ssh	Select ssh line to configure.

Default

No default value for this command.

Mode

Global Configuration

Usage

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

Example

This example shows how to enter Interface Configuration mode.

```
Switch#
  configure
Switch(config)#
  line console
Switch(config-line)#
```

End

Syntax

end

Parameter

None

Default

No default value for this command.

Mode

Privileged EXEC

Global Configuration

Interface Configuration

Line Configuration

Usage

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

Example

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

```
Switch#
   configure
Switch(config)#
  interface fa1
Switch(config-if)#
  end
Switch#
```

Reboot

Syntax

reboot

Parameter

None

Default

No default value for this command.

Mode

Privileged EXEC

Usage

Use the “reboot” command to make the system do a hot restart.

Example

This example shows how to restart the system

Switch#

reboot

System Name

Syntax

system name NAME

Parameter

NAME Specify system name string.

Default

Default name string is “Switch”.

Mode

Global Configuration

Usage

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

Example

This example shows how to modify contact information

Switch(config)#

system name myname

myname(config)#

This example shows how to show system name information

```
Switch#
  show info
System Name : myname
System Location : Default Location
System Contact : Default Contact
MAC Address : DE:AD:BE:EF:01:02
IP Address : 192.168.1.1
Subnet Mask : 255.255.255.0
Loader Version : 1.3.0.26225
Loader Date : Thu May 17 15:19:42 CST 2012
Firmware Version : 2.5.0-beta.32811
Firmware Date : Mon Sep 24 19:33:42 CST 2012
System Object ID : 1.3.6.1.4.1.27282.3.2.10
System Up Time : 0 days, 0 hours, 2 mins, 37 secs
```

System Contact

Syntax

system contact CONTACT

Parameter

CONTACT Specify contact string.

Default

Default contact string is “Default Contact”.

Mode

Global Configuration

Usage

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

Example

This example shows how to modify contact information

Switch(config)#

system contact callme

This example shows how to show system contact information

```
Switch#
  show info
System Name : Switch
System Location : Default Location
System Contact : callme
MAC Address : DE:AD:BE:EF:01:02
IP Address : 192.168.1.1
Subnet Mask : 255.255.255.0
Loader Version : 1.3.0.26225
Loader Date : Thu May 17 15:19:42 CST 2012
Firmware Version : 2.5.0-beta.32811
Firmware Date : Mon Sep 24 19:33:42 CST 2012
System Object ID : 1.3.6.1.4.1.27282.3.2.10
System Up Time : 0 days, 0 hours, 2 mins, 37 secs
```

System Location

Syntax

CONTACT Specify location string.

Parameter

None

Default

Default location string is “Default Location”.

Mode

Global Configuration

Usage

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

Example

This example shows how to modify contact information

Switch(config)#

system location home

This example shows how to show system location information

```
Switch#
  show info
System Name :
System Location : home
System Contact : Default Contact
MAC Address : DE:AD:BE:EF:01:02
IP Address : 192.168.1.1
Subnet Mask : 255.255.255.0
Loader Version : 1.3.0.26225
Loader Date : Thu May 17 15:19:42 CST 2012
Firmware Version : 2.5.0-beta.32811
Firmware Date : Mon Sep 24 19:33:42 CST 2012
System Object ID : 1.3.6.1.4.1.27282.3.2.10
System Up Time : 0 days, 0 hours, 2 mins, 37 secs
```

Username

Syntax

username WORD<0-32> [privilege (admin | user | <0-15>)] (password | secret) WORD<0-32>

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 WORD<0-32>	Specify password string and make it not encrypted. secret WORD<0-32>

Default

Default username "" has password "" with privilege 1. Default username "admin" has password "admin" with privilege 15.

Mode

Global Configuration

Usage

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

Example

Example

This example shows how to add a new user account.

Switch(config)#

username test secret passwd

This example shows how to show existing user accounts.

Switch#

show username

Priv | Type | User Name |

Password

01 | secret | |

dnXencJRwfIV6

15 | secret | admin |

FzjrGO6vfbERY

15 | secret | test |

7p57T9yMkViSUS

Enable Password

Syntax

enable [privilege <0-15>] (password | secret) WORD<032>

no enable [privilege <0-15>]

Parameter

privilege <0-15>	Specify the privilege level to configure. If no privilege level is specified, default is 15.
passwordWORD<0-32>	Specify password string and make it not encrypted.
secret WORD<0-32>	Specify password string and make it encrypted.

Default

Default enable password for all privilege levels are "".

Mode

Global Configuration

Usage

Use the "enable password" command to edit passwords for each privilege level for enabling authentication. Use the "no enable" command to restore password enabling to a default empty value. The only way to show this configuration is using "show running-config".

Example

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

Example

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

Switch(config)#

enable secret enblpasswd

IP Address

Syntax

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

Parameter

address A.B.C.D	Specify IPv4 address for switch
mask A.B.C.D	Specify net mask address for switch

Default

Default IP address is 192.168.1.1 and default net mask is 255.255.255.0.

Mode

Global Configuration

Usage

Use the “ip address” command to modify administration ipv4 addresses. This address is very important. When you try to use telnet, ssh, http, https, snmp, etc. to connect to the switch, you need to use this ip address to access it.

Example

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

Switch(config)# ip address 192.168.1.200 mask 255.255.255.0

This example shows how to show current ipv4 address of the switch.

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

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 192.168.1.254.

Mode

Global Configuration

Usage

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

Example

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

Switch#

show ip

IP Address: 192.168.1.1

Subnet Netmask: 255.255.255.0

Default Gateway: 192.168.1.100

IP DNS

Syntax

ip dns A.B.C.D [A.B.C.D]

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

Parameter

A.B.C.D Specify the DNS server ip address.

Default

Default IP address of DNS server is 168.95.1.1 and 168.95.192.1

Mode

Global Configuration

Usage

Use “ip dns” command to modify DNS server address. And use “no ip dns” to delete existing DNS server.

Example

This example shows how to modify the DNS server of the switch.

Switch(config)#

ip dns 111.111.111.111 222.222.222.222

This example shows how to show current DNS server of the switch.

```
Switch#
  show ip dns
DNS Server 1 : 111.111.111.111
DNS Server 2 : 222.222.222.222
```

IP DHCP

Syntax

ip dhcp

no ip dhcp

Parameter

None

Default

.Default DHCP client is disabled.

Mode

Global Configuration

Usage

Use “ip dhcp” command to enabled dhcp client to get IP address from remote DHCP server. Use “no ip dhcp” command to disabled dhcp client and use static ip address.

Example

This example shows how to enable dhcp client.

Switch(config)#

ip dhcp

This example shows how to show current dhcp client state of the switch.

```
Switch#
  show ip dhcp
DHCP Status : enabled
```

IPv6 Autoconfig

Syntax

ipv6 autoconfig

no ipv6 autoconfig

Parameter

None

Default

Default IPv6 auto config is enabled.

Mode

Global Configuration

Usage

Use the “ipv6 autoconfig” command to enable the IPv6 auto configuration feature. Use “no ipv6 autoconfig” command to disable the IPv6 auto configuration feature.

Example

This example shows how to disable IPv6 auto config.

Switch(config)# no ipv6 autoconfig

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

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

IPv6 Address

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

Default

No default ipv6 address on the switch.

Mode

Global Configuration

Usage

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

Example

This example shows how to add static ipv6 address of the switch.

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

IPv6 Default Gateway

Syntax

ipv6 default-gateway X:X::X:X

Parameter

X:X::X:X Specify default gateway IPv6 address for switch

Default

No default ipv6 default gateway address on the switch.

Mode

Global Configuration

Usage

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

Example

This example shows how to modify the ipv6 default gateway address of the switch.

Switch(config)#

ipv6 default-gateway fe80::dcad:beff:feef:103

Switch#

show ipv6

IPv6 DHCP Configuration : Disabled

IPv6 DHCP DUID :

IPv6 Auto Configuration : Enabled

IPv6 Link Local Address :

fe80::dcad:beff:feef:102/64

IPv6 static Address :

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

IPv6 static Gateway Address : ::

IPv6 in use Address :

fe80::dcad:beff:feef:102/64

IPv6 in use Gateway Address : ::

IPv6 DHCP

Syntax

ipv6 dhcp

no ipv6 dhcp

Parameter

None

Default

Default DHCPv6 client is disabled.

Mode

Global Configuration

Usage

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

Example

This example shows how to enable dhcp client.

Switch(config)#

ipv6 dhcp

This example shows how to show current dhcpv6 client state of the switch.

```
Switch#
  show ipv6 dhcp
DHCPv6 Status : enabled
```

IP Service

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

Usage

Use “ip service” command to enable all kinds of ip services. Such as telnet, ssh, http and https. Use no form to disable service.

Example

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

Switch(config)#

ip telnet

Telnetd daemon enabled.

Switch(config)#

exit

Switch#

show line telnet

Telnet

Telnet Server : enabled

Session Timeout : 10 (minutes)

History Count : 128

Password Retry : 3

Silent Time : 0 (seconds)

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

service status.

Switch(config)#

ip https

Switch(config)#

exit

Switch# show ip https

HTTPS daemon : enabled

Session Timeout : 10 (minutes)

IP Session Timeout

Syntax

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

Parameter

http	Specify session timeout for http service.
https	Specify session timeout for https service.
<0-86400>	Specify session timeout minutes. 0 means never timeout.

Default

Default session timeout for http and https is 10 minutes.

Mode

Global Configuration

Usage

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

Example

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

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

HTTPS daemon : enabled

Session Timeout : 15 (minutes)

Switch#

show ip https

HTTPS daemon : disabled

Session Timeout : 20 (minutes)

Exec-Timeout

Syntax

exec-timeout <0-65535>

Parameter

<0-65535> Specify session timeout minutes. 0 means never timeout

Default

Default session timeout for all lines are 10 minutes.

Mode

Line Configuration

Usage

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

Example

This example shows how to change console session timeout to 15min ,telnet session timeout to 20 min and ssh session timeout to 25 min.

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

Console

Session Timeout : 15 (minutes)

History Count : 128

Password Retry : 3

Silent Time : 0 (seconds)

Telnet

Telnet Server : disabled

Session Timeout : 20 (minutes)

History Count : 128

Password Retry : 3

Silent Time : 0 (seconds)

SSH

SSH Server : disabled

Session Timeout : 25 (minutes)

History Count : 128

Password Retry : 3

Silent Time : 0 (seconds)

Password-Thresh

Syntax

password-thresh <0-120>

Parameter

<0-120> Specify password fail retry number. 0 means no limit.

Default

Default password fail retry number is 3.

Mode

Line Configuration

Usage

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

Example

This example shows how to change the console fail retry number to 4, the telnet fail retry number to 5 and the ssh fail retry number to 6.

```
Switch(config)#
  line console
Switch(config-line)#
   password-thresh 4
Switch(config-line)#
   exit
Switch(config)#
   line telnet
Switch(config-line)#
  password-thresh 5
Switch(config-line)#
  exit
Switch(config)#
  line ssh
Switch(config-line)#
  password-thresh 6
Switch(config-line)#
   exit
```

This example shows how show line information.

```
Switch#
  show line
Console
Session Timeout : 10 (minutes)
History Count : 128
Password Retry : 4
Silent Time : 0 (seconds)
Telnet
Telnet Server : disabled
Session Timeout : 10 (minutes)
History Count : 128
Password Retry : 5
Silent Time : 0 (seconds)
SSH
SSH Server : disabled
Session Timeout : 10 (minutes)
History Count : 128
Password Retry : 6
```

Silent Time : 0 (seconds)

Silent-Time

Syntax

silent-time <0-65535>

Parameter

<0-65535> Specify silent time with unit seconds. 0 means do not silent.

Default

Default silent time is 0.

Mode

Line Configuration

Usage

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

Example

This example shows how to change the console silent time to 10, the telnet silent time to 15, and the ssh silent time to 20.

Switch(config)#

line console

```
Switch(config-line)#
  silent-time 10
Switch(config-line)#
   exit
Switch(config)#
   line telnet
Switch(config-line)#
  silent-time 15
Switch(config-line)#
  exit
Switch(config)#
   line ssh
Switch(config-line)#
  silent-time 20
Switch(config-line)#
  exit
```

This example shows how show line information.

```
Switch#
  show line
```

Console

Session Timeout : 10 (minutes)

History Count : 128

Password Retry : 3

Silent Time : 10 (seconds)

Telnet

Telnet Server : disabled

Session Timeout : 10 (minutes)

History Count : 128

Password Retry : 3

Silent Time : 15 (seconds)

SSH

SSH Server : disabled

Session Timeout : 10 (minutes)

History Count : 128

Password Retry : 3

Silent Time : 20 (seconds)

History

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

Usage

Use the “history” command to specify the maximum commands of history numbers for the CLI running on the console, telnet, or ssh service. Every command input by the user will record in the history buffer. If all history commands exceed the configured history number, older commands will be deleted from the buffer. Use the “no history” to disable the history feature. Use the “show history” to show all history commands.

Example

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

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

This example shows how show line information.

```
Switch#
   show line
Console
Session Timeout : 10 (minutes)
History Count : 100
Password Retry : 3
Silent Time : 0 (seconds)
Telnet
Telnet Server : disabled
Session Timeout : 10 (minutes)
History Count : 150
Password Retry : 3
Silent Time : 0 (seconds)
SSH
SSH Server : disabled
Session Timeout : 10 (minutes)
History Count : 200
Password Retry : 3
```

Silent Time : 0 (seconds)

Switch#

show history

Maximun History Count: 100

1. enable
2. configure
3. line console
4. exit
5. show history
6. line
7. exit
8. show history
9. configure
10. line
11. line console
12. exit
13. line console
14. history 100
15. exit

16. show history
17. exit
18. show history

Clear Service

Syntax

clear (telnet | ssh)

Parameter

telnet	Clear all telnet sessions.
ssh	Clear all ssh sessions

Default

No default value for this command.

Mode

Privileged EXEC

Usage

Use “clear service” command to kill all existing sessions for the select service.

Example

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

Switch#

clear telnet

SSL

Syntax

ssl

Parameter

Default

No default value for this command.

Mode

Global Configuration

Usage

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

Example

This example shows how to generate certificate files.

Switch(config)#

ssl

This example shows how to show the certificate file lists.

```
Switch#
    show flash
File Name File Size Modified
startup-config 1191 2000-01-01 00:00:23
rsa1 974 2000-01-01 00:00:18
rsa2 1675 2000-01-01 00:00:18
dsa2 668 2000-01-01 00:00:18
ssl_cert 993 2000-01-01 00:00:18
image0 (active) 4372401 2012-09-24 01:57:29
image1 (backup) 0
```

Ping

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.

Default

No default value for this command.

Mode

Privileged EXEC

Usage

Use “ping” command to do network ping diagnostic.

Example

This example shows how to ping remote host 192.168.1.111.

Switch#

ping 192.168.1.111

PING 192.168.1.111 (192.168.1.111): 56 data bytes

64 bytes from 192.168.1.111: icmp_seq=0 ttl=128time=10.0 ms time=10.0 ms

64 bytes from 192.168.1.111: icmp_seq=1 ttl=128 time=0.0 ms

64 bytes from 192.168.1.111: icmp_seq=2 ttl=128 time=0.0 ms

64 bytes from 192.168.1.111: icmp_seq=3 ttl=128 time=0.0 ms

192.168.1.111 ping statistics

4 packets transmitted, 4 packets received, 0% packet loss

round-trip min/avg/max = 0.0/2.5/10.0 ms

Traceroute

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.

Default

.No default value for this command.

Mode

User EXEC

Privileged EXEC

Usage

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

Example

This example shows how to trace route host 192.168.1.111.

Switch#

traceroute 192.168.1.111

traceroute to 192.168.1.111 (192.168.1.111), 30 hops

max, 40 byte packets

1 192.168.1.111 (192.168.1.111) 0 ms 10 ms 0 ms

Clear ARP

Syntax

clear arp [A.B.C.D]

show arp

Parameter

A.B.C.D Specify specific arp entry to clear.

Default

No default value for this command.

Mode

User EXEC

Privileged EXEC

Usage

Use the “clear arp” command to clear all or specific one arp entry. Use the “show arp” command to show all arp entries.

Example

This example shows how to show arp entries.

Switch#

show arp

Address HWtype HWaddress Flags

Mask Iface

192.168.1.111 ether 00:0E:2E:F1:4B:3C C eth0

This example shows how to clear all arp entries.

Switch(config)#

clear arp

Show Version

Syntax

show version

Parameter

None

Default

No default value for this command.

Mode

User EXEC

Privileged EXEC

Usage

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

Example

This example shows how to show system version.

Switch#

show version

Loader Version : 1.3.0.26225

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

Firmware Version : 2.5.0-beta.32811

Firmware Date : Mon Sep 24 19:33:42 CST 2012

Show Info

Syntax

show info

Parameter

None

Default

No default value for this command.

Mode

User EXEC

Privileged EXEC

Usage

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

Example

This example shows how to show system version.

Switch#

show info

System Name : Switch

System Location : Default Location

System Contact : Default Contact

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

IP Address : 192.168.1.1

Subnet Mask : 255.255.255.0

Loader Version : 1.3.0.26225

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

Firmware Version : 2.5.0-beta.32811

Firmware Date : Mon Sep 24 19:33:42 CST 2012

System Object ID : 1.3.6.1.4.1.27282.3.2.10

System Up Time : 0 days, 1 hours, 49 mins, 29 secs

Show History

Syntax

show history

Parameter

None

Default

No default value for this command.

Mode

User EXEC

Privileged EXEC

Global Configuration

Usage

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

Example

This example shows how show history commands.

Switch#

show history

Maximun History Count: 100

1. enable
2. configure
3. line console
4. exit
5. show history
6. line
7. exit
8. show history
9. configure
10. line
11. line console
12. exit
13. line console
14. history 100
15. exit
16. show history
17. exit
18. show history

Show Username

Syntax

show username

Parameter

None

Default

No default value for this command.

Mode

Privileged EXEC

Usage

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

Example

This example shows how to show existing user accounts.

Switch#

show username

Priv | Type | User Name |

Password

01 | secret | |

dnXencJRwflV6

15 | secret | admin |

FzjrGO6vfbERY

15 | secret | test |

7p57T9yMkViSUS

Show IP

Syntax

show ip

Parameter

None

Default

No default value for this command

Mode

User EXEC

Privileged EXEC

Usage

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

Example

This example shows how to show current ipv4 address of the switch.

Switch#

show ip

IP Address: 192.168.1.200

Subnet Netmask: 255.255.255.0

Default Gateway: 192.168.1.254

Show IP DHCP

Syntax

show ip dhcp

Parameter

None

Default

No default value for this command.

Mode

User EXEC

Privileged EXEC

Usage

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

Example

This example shows how to show current dhcp client state of the switch.

Switch#

show ip dhcp

DHCP Status : enabled

Show IPv6

Syntax

show ipv6

Parameter

None

Default

No default value for this command.

Mode

User EXEC

Privileged EXEC

Usage

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

Example

This example shows how to show current ipv6 address of the switch.

Switch#

show ipv6

IPv6 DHCP Configuration : Disabled

IPv6 DHCP DUID :

IPv6 Auto Configuration : Enabled

IPv6 Link Local Address :

fe80::dcad:beff:feef:102/64

IPv6 static Address :

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

IPv6 static Gateway Address : ::

IPv6 in use Address :

fe80::dcad:beff:feef:102/64

IPv6 in use Gateway Address : ::

Show IPv6 DHCP

Syntax

show ipv6 dhcp

Parameter

Default

No default value for this command

Mode

User EXEC

Privileged EXEC

Usage

Use “show ipv6 dhcp” command to show system IPv6 dhcp client enable state.

Example

This example shows how to show current dhcpv6 client state of the switch.

Switch#

show ipv6 dhcp

DHCPv6 Status : enabled

Show Line

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.

Default

No default value for this command

Mode

Privileged EXEC

Usage

Use “show line” command to show all line configurations including session timeout, history count, password retry number and silent time. For telnet and ssh, it also shows the service enable/disable state.

Example

This example shows how show all lines’ information.

Switch#

show line

Console

Session Timeout : 15 (minutes)

History Count : 128

Password Retry : 3

Silent Time : 0 (seconds)

Telnet

Telnet Server : disabled

Session Timeout : 20 (minutes)

History Count : 128

Password Retry : 3

Silent Time : 0 (seconds)

SSH

SSH Server : disabled

Session Timeout : 25 (minutes)

History Count : 128

Password Retry : 3

Silent Time : 0 (seconds)

EnGenius®

Chapter 5
Cable Diagnostics

Show Cable-Diag Interfaces

Syntax

logging

no logging

Parameter

N/A

Default

logging

Mode

Global Configuration

Usage

Display the estimated length of copper cable attached to the ports.

show cable-diag interface all

Display the estimated length of copper cables attached to all ports.

show cable-diag interface

Disable the estimated length of copper cable attached to port fa1.

Example

```
 Switch(config)#
   show cable-diag interfaces fa1
Port | Length [meters]
fa1 | 5.55
```

Chapter 6
DHCP Snooping

IP DHCP Snooping

Syntax

ip dhcp snooping

no ip dhcp snooping

Parameter

None

Default

DHCP snooping is disabled

Mode

Global Configuration

Usage

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

Example

The example shows how to enable DHCP Snooping on VLAN 1. You can verify settings by the following show ip dhcp snooping command.

switch(config)#

ip dhcp snooping

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

IP DHCP Snooping VLAN

Syntax

ip dhcp snooping vlan VLAN-LIST

Parameter

VLAN-LIST Specify VLAN ID or a range of VLANs to enable or disable dynamic Arp inspection

Default

Default is disabled on all VLANs

Mode

Global Configuration

Usage

Use the ip arp inspection vlan command to enable VLANs on DHCP Snooping function. Use the no form of this command to disable VLANs on DHCP Snooping function

Example

The example shows how to enable VLAN 1-100 on DHCP Snooping, and then disable VLAN 30- 40 on DHCP Snooping. You can verify settings by the following show ip dhcp snooping command.

switch(config)#

vlan 1-100

```
switch(config)#
   exit
switch(config)#
   ip dhcp snooping
switch(config)#
   ip dhcp snooping vlan 1-100
switch(config)#
  show ip dhcp snooping
DHCP Snooping : enabled
Enable on following Vlans : 1-100
circuit-id default format: vlan-port
remote-id: : 00:11:22:33:44:55 (Switch Mac in Byte Order)
switch(config)#
  no ip dhcp snooping vlan 30-40
switch(config)#
   show ip dhcp snooping
DHCP Snooping : enabled
Enable on following Vlans : 1-29,41-100
circuit-id default format: vlan-port
```

remote-id: : 00:11:22:33:44:55 (Switch Mac in Byte Order)

IP DHCP Snooping Trust

Syntax

ip dhcp snooping trust

no ip dhcp snooping trust

Parameter

None

Default

DHCP snooping trust is disabled

Mode

Interface Configuration

Usage

Use the ip dhcp snooping trust command to set trusted interface. The switch does not check DHCP packets that are received on the trusted interface; it simply forwards it. Use the no form of this command to set untrusted interface.

Example

The example shows how to set interface gi1 to trust. You can verify settings by the following show ip dhcp snooping interface command.

switch(config)#

interface gi1

```
switch(config)#
   ip dhcp snooping trust
switch(config)#
  do show ip dhcp snooping interface gi1
Interfaces | Trust State | Rate (pps) | hwaddr Check | Insert Option82 |
gi1 | Trusted | None | disabled | disabled |
```

IP DHCP Snooping Verify

Syntax

ip dhcp snooping verify mac-address

[no] ip dhcp snooping verify mac-address

Parameter

None

Default

DHCP snooping verify mac-address is disabled.

Mode

Interface Configuration

Usage

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

Example

The example shows how to set interface gi1 to validate “mac-address”. You can verify settings by the following show ip dhcp snooping interface command.

switch(config)#

interface gi1

```
switch(config-if)#
    ip dhcp snooping verify mac-address
switch(config)#
   do show ip dhcp snooping interface gi1
Interfaces | Trust State | Rate (pps) | hwaddr Check | Insert Option82 |
gi1 | Untrusted | None | enabled | disabled |
```

IP DHCP Snooping Rate Limit

Syntax

ip dhcp snooping rate-limit <1-50>

[no] ip dhcp snooping rate-limit

Parameter

<1-50> Set 1 to 50 PPS of DHCP packet rate limitation

Default

Default is un-limited of DHCP packet

Mode

Interface Configuration

Usage

Use the ip dhcp snooping rate-limit command to set rate limitation on interface. The switch drop DHCP packets after receives more than configured rate of packets per second. Use the no form of this command to return to default settings.

Example

The example shows how to set rate limit to 30 pps on interface gi1. You can verify settings by the following show ip dhcp snooping interface command.

switch(config)#

interface gi1

```
switch(config)# ip dhcp snooping rate-limit 30
switch(config)# do show ip dhcp snooping interface gi1
Interfaces | Trust State | Rate (pps) | hwaddr Check | Insert Option82 |
gi1 | Untrusted | 30 | disabled | disabled |
```

Clear IP DHCP Snooping Statistics

Syntax

clear ip dhcp snooping interfaces IF_PORTS statistics

Parameter

IF_PORTS specifies ports to clear statistics

Default

No default is defined

Mode

Global Configuration

Usage

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

Example

The example shows how to clear statistics on interface gi1. You can verify settings by the following show ip dhcp snooping interface statistics command.

switch#

clear ip dhcp snooping interfaces gi1 statistics

switch#

show ip dhcp snooping interfaces gi1 statistics

Interfaces | Forwarded | Chaddr Check Dropped | Untrust Port Dropped |

Untrust Port With Option82 Dropped | Invalid Drop

gi1 | 0 | 0 | 0 | 0 | 0

Show IP DHCP Snooping

Syntax

show ip dhcp snooping

Parameter

None

Default

No default is defined

Mode

Global Configuration

Usage

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

Example

The example shows how to show settings of DHCP Snooping

```
switch(config)#
  show ip dhcp snooping
DHCP Snooping : enabled
Enable on following Vlans : 1
```

circuit-id default format: vlan-port

remote-id: : 00:11:22:33:44:55 (Switch Mac in Byte Order)

IP Show IP DHCP Snooping Interface

Syntax

show ip dhcp snooping interfaces IF_PORTS

show ip dhcp snooping interfaces IF_PORTS statistics

Parameter

IF_PORTS specifies ports to show statistics

Default

No default is defined

Mode

Global Configuration

Usage

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

Example

The example shows how to show settings of interface gi1.

switch#

show ip dhcp snooping interface gi1

Interfaces | Trust State | Rate (pps) | hwaddr Check | Insert Option82 |

gi1 | Untrusted | None | enabled | disabled |

The example shows how to show statistics of interface gi1.

switch#

show ip dhcp snooping interfaces gi1 statistics

Interfaces | Forwarded | Chaddr Check Dropped | Untrust Port Dropped |

Untrust Port With Option82 Dropped | Invalid Drop

gi1 | 0 | 0 | 0 | 0 | 0

Show IP DHCP Snooping Binding

Syntax

show ip dhcp snooping binding

Parameter

None

Default

No default is defined

Mode

Global Configuration

Usage

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

Example

The example shows how to show binding entries that learned by DHCP Snooping.

switch#

show ip dhcp snooping binding

Bind Table: Maximun Binding Entry Number 192

Port | VID | MAC Address | IP | Type | Lease Time

fa1 | 1 | 48:5B:39:C7:12:62 | 192.168.1.100(255.255.255.255)|DHCP Snooping | 86400

IP DHCP Snooping Option

Syntax

ip dhcp snooping option

no ip dhcp snooping option

Parameter

None

Default

DHCP snooping option82 is disabled

Mode

Interface Configuration

Usage

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

Example

The example shows how to enable option82 insertion. You can verify settings by the following show ip dhcp snooping interface command.

```
switch(config)#
  interface gi1
```

```
switch(config)#
  ip dhcp snooping option
switch(config)#
  do show ip dhcp snooping interface gi1
Interfaces | Trust State | Rate (pps) | hwaddr Check | Insert Option82 |
gi1 | Untrusted | None | disabled | enabled |
```

IP DHCP Snooping Option Action

Syntax

ip dhcp snooping option action (drop|keep|replace)

no ip dhcp snooping option action

Parameter

Drop	Drop packets with option82 that are received from un trusted port.
Keep	Keep original option82 content in packet.
Replace	Replace option82 content by switch setting op Drop packets with option82 that are received from un trusted port.

Default

DHCP snooping option82 is drop

Mode

Interface Configuration

Usage

Use the ip dhcp snooping option action command to set the action when it receives packets with the option82 content. Use the no form of this command to restore to the default settings.

Example

The example shows how to set action to replace option82 content. You can verify settings by the following show running-config command.

```
switch(config)#
  interface gi1
switch(config)#
  ip dhcp snooping option action replace
```

IP DHCP Snooping Option Circuit-ID

Syntax

ip dhcp snooping [vlan <1-4094>] option circuit-id STRING

no ip dhcp snooping [vlan <1-4094>] option circuit-id

Parameter

Vlan <1-4094>	VLAN ID to set user defined circuit-id string
STRING	Circuit-id string, 1 to 63 ASCII characters, no spaces.

Default

Default circuit-id is port id + vlan id in byte format

Mode

Interface Configuration

Usage

Use the ip dhcp snooping option circuit-id command to set the user-defined circuit-id string. The Circuit-id is per port per VLAN setting. If a VLAN is not found to use a user-defined circuit-id, then it will use it per port circuit-id string. Use the no form of this command to default setting.

Example

The example shows how to set a user-defined circuit-id string on interface gi1 and VLAN 1. You can verify settings by the following show running-config command.

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

IP DHCP Snooping Option Remote-ID

Syntax

ip dhcp snooping option remote-id STRING

no ip dhcp snooping option remote-id

Parameter

STRING Remote-id string, 1 to 63 ASCII characters, no spaces.

Default

Default remote-id is the switch MAC address in byte order.

Mode

Global Configuration

Usage

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

Example

The example shows how to set a user-defined remote-id string on switch. You can verify settings by the following show ip dhcp snooping option remote-id.

switch(config)#

ip dhcp snooping option remote-id test_remote

```
switch(config)#
  show ip dhcp snooping option remote-id
Remote ID: test_remote
```

Show IP DHCP Snooping Option

Syntax

show ip dhcp snooping option remote-id

Parameter

None

Default

No default is defined

Mode

Global Configuration

Usage

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

Example

The example shows how to show remote-id string.

```
switch(config)#
  show ip dhcp snooping option remote-id
Remote ID: test_remote
```

IP DHCP Snooping Database

Syntax

ip dhcp snooping database flash

ip dhcp snooping database tftp (A.B.C.D|HOSTNAME) NAME

no ip dhcp snooping database

Parameter

(A.B.C.D|HOSTNAME)	Specify the IP address or hostname of remote TFTP server
NAME	Input name of backup file

Default

DHCP snooping database is disabled

Mode

Global Configuration

Usage

Use the ip dhcp snooping database command to enable the DHCP Snooping database agent. The “flash” means that it will write a backup file to the switch local drive. The “tftp” means that it will write a backup file to the remote TFTP server. Use the no form of this command to disable it.

Example

The example shows how to enable DHCP Snooping database agent and write backup file to remote TFTP server with file name “backup_file”. You can verify settings by the following show ip dhcp snooping database command.

```
switch(config)#
  ip dhcp snooping database tftp 192.168.1.50 backup_file
switch(config)#
  show ip dhcp snooping database
Type : tftp: 192.168.1.50
FileName : backup_file
Write delay Timer : 300 seconds
Abort Timer : 300 seconds
Agent Running : Running
Delay Timer Expiry : 300 seconds
Abort Timer Expiry : 299
Last Succeded Time : None
Last Failed Time : None
Last Failed Reason : No failure recorded.
Total Attempts : 1
Successful Transfers : 0 Failed Transfers : 0
Successful Reads : 0 Failed Reads : 0
Successful Writes : 0 Failed Writes : 0
```

IP DHCP Snooping Database Write-Delay

Syntax

ip dhcp snooping database write-delay <15-86400>

Parameter

<15-86400> specifies the seconds of the timeout. Specify the duration for which the transfer should be delayed after the binding database changes.

Default

DHCP snooping database write-delay is 300 seconds

Mode

Global Configuration

Usage

Use the ip dhcp snooping database write-delay command to modify the write-delay timer. Use the no form of this command to set the default settings.

Example

The example shows how to set write-delay timer to 60 seconds. You can verify settings by the following show ip dhcp snooping database command.

switch(config)#

ip dhcp snooping database write-delay 60

```
switch(config)#
  show ip dhcp snooping database
Type : tftp: 192.168.1.50
FileName : backup_file
Write delay Timer : 60 seconds
Abort Timer : 300 seconds
Agent Running : Running
Delay Timer Expiry : 300 seconds
Abort Timer Expiry : 299
Last Succeded Time : None
Last Failed Time : None
Last Failed Reason : No failure recorded.
Total Attempts : 1
Successful Transfers : 0 Failed Transfers : 0
Successful Reads : 0 Failed Reads : 0
Successful Writes : 0 Failed Writes : 0
```

```
switch(config)#
  show ip dhcp snooping database
Type : tftp: 192.168.1.50
FileName : backup_file
Write delay Timer : 60 seconds
Abort Timer : 300 seconds
Agent Running : Running
Delay Timer Expiry : 300 seconds
Abort Timer Expiry : 299
Last Succeded Time : None
Last Failed Time : None
Last Failed Reason : No failure recorded.
Total Attempts : 1
Successful Transfers : 0 Failed Transfers : 0
Successful Reads : 0 Failed Reads : 0
Successful Writes : 0 Failed Writes : 0
```

IP DHCP Snooping Database Timeout

Syntax

ip dhcp snooping database timeout <0-86400>

Parameter

<15-86400> specifies the seconds of timeout Specify (in seconds) how long to wait for the database transfer process to finish before stopping the process. Use 0 to define an infinite duration, which means to continue trying the transfer indefinitely

Default

DHCP snooping database timeout is 300 seconds

Mode

Global Configuration

Usage

Use the ip dhcp snooping database timeout command to modify the timeout timer. Use the no form of this command to set the default settings.

Example

The example shows how to set timeout timer to 60 seconds. You can verify settings by the following show ip dhcp snooping database command.

switch(config)#

ip dhcp snooping database timeout 60

```
switch(config)#
  show ip dhcp snooping database
Type : tftp: 192.168.1.50
FileName : backup_file
Write delay Timer : 300 seconds
Abort Timer : 60 seconds
Agent Running : Running
Delay Timer Expiry : 300 seconds
Abort Timer Expiry : 299
Last Succeded Time : None
Last Failed Time : None
Last Failed Reason : No failure recorded.
Total Attempts : 1
Successful Transfers : 0 Failed Transfers : 0
Successful Reads : 0 Failed Reads : 0
Successful Writes : 0 Failed Writes : 0
```

Clear IP DHCP Snooping Database Statistics

Syntax

clear ip dhcp snooping database statistics

Parameter

None

Default

No default is defined.

Mode

Global Configuration

Usage

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

Example

The example shows how to clear statistics of DHCP Snooping agent. You can verify settings by the following show ip dhcp snooping database command.

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

Type : tftp: 192.168.1.50

FileName : backup_file

Write delay Timer : 300 seconds

Abort Timer : 60 seconds

Agent Running : Running

Delay Timer Expiry : 300 seconds

Abort Timer Expiry : 299

Last Succeded Time : None

Last Failed Time : None

Last Failed Reason : No failure recorded.

Total Attempts : 0

Successful Transfers : 0 Failed Transfers : 0

Successful Reads : 0 Failed Reads : 0

Successful Writes : 0 Failed Writes : 0

Renew IP DHCP Snooping Database

Syntax

renew ip dhcp snooping database

Parameter

None

Default

No default is defined

Mode

Global Configuration

Usage

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

Example

The example shows how to renew the DHCP Snooping database. You can verify settings by the following show ip dhcp snooping database and show ip dhcp snooping binding commands.

switch(config)#

show ip dhcp snooping database

Type : tftp: 192.168.1.50

FileName : backup_file

Write delay Timer : 300 seconds

Abort Timer : 60 seconds

Agent Running : Running

Delay Timer Expiry : 300 seconds

Abort Timer Expiry : 299

Last Succeded Time : None

Last Failed Time : None

Last Failed Reason : No failure recorded.

Total Attempts : 1

Successful Transfers : 1 Failed Transfers : 0

Successful Reads : 1 Failed Reads : 0

Successful Writes : 0 Failed Writes : 0

switch# show ip dhcp snooping binding

Bind Table: Maximun Binding Entry Number 192

Port | VID | MAC Address | IP | Type | Lease Time

fa1 | 1 | 48:5B:39:C7:12:62 | 192.168.1.100(255.255.255.255)|DHCP Snooping | 86400

Show IP DHCP Snooping Database

Syntax

show ip dhcp snooping database

Parameter

None

Default

No default is defined

Mode

Global Configuration

Usage

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

Example

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

```
switch(config)#
  show ip dhcp snooping database
Type : tftp: 192.168.1.50
FileName : backup_file
```

Write delay Timer : 300 seconds

Abort Timer : 60 seconds

Agent Running : Running

Delay Timer Expiry : 300 seconds

Abort Timer Expiry : 299

Last Succeded Time : None

Last Failed Time : None

Last Failed Reason : No failure recorded.

Total Attempts : 1

Successful Transfers : 1 Failed Transfers : 0

Successful Reads : 1 Failed Reads : 0

Successful Writes : 0 Failed Writes : 0

EnGenius®

Chapter 7
DOS

DoS

Syntax

dos (syn-fin | xma | null-scan | sport-less1024 | icmp-frag-pkts | pod | tcpblat | udp-blat | land | da-eq-sa)

no dos (syn-fin | xma | null-scan | sport-less1024 | icmp-frag-pkts | pod | tcp-blat | udp-blat | land | da-eq-sa)

dos smurf <0-31>

dos tcp-hdr-min <0-255>

dos icmp-ping-max <0-65535>

dos ipv6-min-frag <0-65535>

no dos smurf <0-31>

no dos tcp-hdr-min <0-255>

no dos icmp-ping-max <0-65535>

no dos ipv6-min-frag <0-65535>

Parameter

syn-fin	Enable/Disable syn-fin protection.
xma	Enable/Disable xma protection.
null-scan	Enable/Disable null-scan protection.
sport-less1024	Enable/Disable sport-less1024 protection.
icmp-frag-pkts	Enable/Disable icmp-grag-pkts protection.
pod	Enable/Disable pod protection.
tcp-blat	Enable/Disable tcp-blat protection.
udp-blat	Enable/Disable udp-blat protection.
land	Enable/Disable land protection.
da-eq-sa	Enable/Disable da-eq-sa protection.
smurf	<0-31> Specify smurf length.
tcp-hdr-min **<0-255>**	Specify tcp-hdr-min length.
icmp-ping-max **<0-65535>**	Specify icmp-ping-max size.
ipv6-min-frag <0-65535>	Specify ipv6-min-frag length.

Default

Default enable state of all DoS types are disabled.

Default smurf length is 24.

Default tcp-hdr-min length is 20.

Default icmp-ping-max size is 512.

Default

Default enable state of all DoS types are disabled.

Default smurf length is 24.

Default tcp-hdr-min length is 20.

Default icmp-ping-max size is 512.

Default ipv6-min-frag length is 1280

Mode

Global Configuration

Usage

DoS is using to protect malicious attack from other devices. This command can configure DUT to enable/disable following types of attacks.

syn-fin: A TCP packet with the SYN and FIN flags set.

xma: TCP sequence number is zero, and the FIN/URG/PSH flags areset.

null-scan: TCP sequence number is zero, and all control flags are zeroes.

sport-less1024: TCP SYN packets with source port less than 1024.

icmp-frag-pkts: Fragmented ICMP packets.

Pod: Ping packets that length are larger than 65535 bytes.

tcp-blat: Both the source and the destination TCP port are the same.

udp-blat: Both the source and the destination UDP port are the same.

land: Both the source and the destination IPv4/IPv6 addresses are the same.

da-eq-sa: Both the source and the destination MAC addresses are the same.

smurf: ICMP echo request packet that destination IPv4 address is broadcast address.

tcp-hdr-min: TCP packet that header length is less than the configured value.

icmp-ping-max: PING packet with the length.

ipv6-min-frag: IPv6 fragmented packets (not including the last one) that payload length less than 1240 bytes.

Example

This example shows how to enable syn-fin and smurf with length 30 on interface fa1.

```
Switch(config)#
  interface fa1
Switch(config-if)#
   dos syn-fin
Switch(config-if)#
  dos smurf 30
```

This example shows how to show current dos state on interface fa1

```
Switch#
  show dos interfaces fa1
Port | Type | State (Length)
fa1 |
```

| syn-fin | enabled

| xma | disabled

| null-scan | disabled

| sport-less1024 | disabled

| lcmp-frag-pkts | disabled

| pod | disabled

| tcp-blat | disabled

| udp-blat | disabled

| land | disabled

| da-eq-sa | disabled

| smurf | enabled (30)

| tcp-hdr-min | disabled

| icmp-ping-max | disabled

| ipv6-min-frag | disabled

Show DoS

Syntax

show dos interfaces IF_PORTS

Parameter

IF_PORTS Enable/Disable syn-fin protection

Default

No default value for this command.

Mode

Privileged EXEC

Usage

Use “show dos” command to show dos configuration on selected ports.

Example

This example shows how to show current dos state on interface fa1.

This example shows how to show current dos state on interface fa1

Switch#

show dos interfaces fa1

Port | Type | State (Length)

fa1 |

| syn-fin | enabled

| xma | disabled

| null-scan | disabled

| sport-less1024 | disabled

| lcmp-frag-pkts | disabled

| pod | disabled

| tcp-blat | disabled

| udp-blat | disabled

| land | disabled

| da-eq-sa | disabled

| smurf | enabled (30)

| tcp-hdr-min | disabled

| icmp-ping-max | disabled

| ipv6-min-frag | disabled

Chapter 8
Dynamic ARP Inspection

IP ARP Inspection

Syntax

ip arp inspection

no ip arp inspection

Parameter

None

Default

Dynamic Arp inspection is disabled

Mode

Global Configuration

Usage

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

Example

The example shows how to enable Dynamic Arp Inspection on VLAN 1. You can verify settings by the following show ip arp inspection command.

switch(config)#

ip arp inspection

```
switch(config)#
  ip arp inspection vlan 1
switch(config)#
  show ip arp inspection
Dynamic ARP Inspection: enabled
Enable on Vlans: 1
```

IP ARP Inspection VLAN

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

Usage

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

Example

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

```
switch(config)#
  vlan 1-100
switch(config)#
  exit
switch(config)#
  ip arp inspection
switch(config)#
  ip arp inspection vlan 1-100
switch(config)#
  show ip arp inspection
Dynamic ARP Inspection : enabled
Enable on Vlans : 1-100
switch(config)#
  no ip arp inspection vlan 30-40
switch(config)#
  show ip arp inspection
Dynamic ARP Inspection : enabled
Enable on Vlans : 1-29, 41-100
```

IP ARP Inspection Trust

Syntax

ip arp inspection trust

no ip arp inspection trust

Parameter

None

Default

Dynamic Arp inspection trust is disabled

Mode

Interface Configuration

Usage

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

Example

The example shows how to set interface gi1 to trust. You can verify settings by the following show ip arp inspection interface command.

```
switch(config)#
  interface gi1
```

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

IP ARP Inspection Validate

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]

Parameter

None

Default

Default is disabled of all validation

Mode

Interface Configuration

Usage

Use the ip arp inspection validate command to enable validate function on interface. The “src-mac” drop ARP requests and reply packets that arp-sender-mac and ethernetsource-mac is not match. The “dst-mac” drop ARP reply packets that arp-target-mac and ethernet-dst-mac is not match. The “ip” drop ARP request and reply packets that sender-ip is invalid

such as broadcast multicast all zero IP address and drop ARP reply packets that target-ip is invalid. The “allow-zeros” means won’t drop all zero IP address. Use the no form of this command to disable validation.

Example

The example shows how to set interface gi1 to validate “src-mac” “dst-mac” and “ip allow zeros”. You can verify settings by the following show ip arp inspection interface command.

```
switch(config)#
  interface gi1
switch(config-if)#
  ip arp inspection validate src-mac
switch(config-if)#
  ip arp inspection validate dst-ma
switch(config-if)#
  ip arp inspection validate ip allow-zeros
switch(config)#
  do show ip arp inspection interface gi1
Interfaces | Trust State | Rate (pps) | SMAC Check | DMAC Check | IP Check/Allow Zero |
gi1 | Untrusted | 30 | disabled | disabled | disabled/disabled
```

IP ARP Inspection Rate Limit

Syntax

ip arp inspection rate-limit <1-50>

[no] ip arp inspection rate-limit

Parameter

<1-50> Set 1 to 50 PPS of DHCP packet rate limitation

Default

Default is un-limited of ARP packet

Mode

Interface Configuration

Usage

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

Example

The example shows how to set rate limit to 30 pps on interface gi1. You can verify settings by the following show ip arp inspection interface command.

```
switch(config)#
  interface gi1
switch(config)#
  ip arp inspection rate-limit 30
switch(config)#
  do show ip arp inspection interface gi1
Interfaces | Trust State | Rate (pps) | SMAC Check | DMAC Check | IP Check/Allow Zero |
gi1 | Untrusted | 30 | disabled | disabled | disabled/disabled
```

Clear IP ARP Inspection Statistics

Syntax

clear ip arp inspection interfaces IF_PORTS statistics

Parameter

IF_PORTS specifies ports to clear statistics

Default

No default is defined

Mode

Global Configuration

Usage

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

Example

The example shows how to clear statistics on interface gi1. You can verify settings by the following show ip arp inspection interface statistics command.

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

Port| Forward |Source MAC Failures|Dest MAC Failures|

SIP Validation Failures|DIP Validation Failures|IP-MAC Mismatch Failures

gi1| 0 | 0 | 0 | 0 | 0 | 0

Show IP ARP Inspection

Syntax

show ip dhcp snooping

Parameter

None

Default

No default is defined

Mode

Global Configuration

Usage

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

Example

The example shows how to show settings of Dynamic Arp Inspection

```
switch(config)#
  show ip arp inspection
Dynamic ARP Inspection : enabled
Enable on Vlans : 1
```

Show IP ARP Inspection Interface

Syntax

show ip arp inspection interfaces IF_PORTS

show ip arp inspection interfaces IF_PORTS statistics

Parameter

IF_PORTS specifies ports to show statistics

Default

No default is defined

Mode

Global Configuration

Usage

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

Example

The example shows how to show settings of interface gi1.

switch#

show ip arp inspection interface gi1

Interfaces | Trust State | Rate (pps) | SMAC Check | DMAC Check | IP Check/Allow Zero |

gi1 | Trusted | None | disabled | disabled | disabled/disabled

The example shows how to show statistics of interface gi1.

switch#

show ip arp inspection interfaces gi1 statistics

Port| Forward |Source MAC Failures|Dest MAC Failures|

SIP Validation Failures|DIP Validation Failures|IP-MAC Mismatch Failures

gi1| 0 | 0 | 0 | 0 | 0 | 0

EnGenius®

Chapter 9
IGMP Snooping

IP IGMP Snooping

Syntax

ip igmp snooping

no ip igmp snooping

Parameter

None

Default

ip igmp snooping

Mode

Global Configuration

Usage

“no ip igmp snooping” will clear all ip igmp snooping dynamic group and dynamic router port, and make the static ip igmp group invalid. Then do not learning the dynamic group and router port by igmp message. The configure can use “show ip igmp snooping”.

Example

The following example specifies that set ip igmp snooping test.

Switch(config)#

ip igmp snooping

Switch#

show ip igmp snooping

IGMP Snooping Status

Snooping : Enabled

Report Suppression : Enabled

Operation Version : v2

Forward Method : mac

Unknown Multicast Action : Flood

Switch(config)#

no ip igmp snooping

Switch#

show ip igmp snooping

IP IGMP Snooping Report-Suppression

Syntax

[no] ip igmp snooping report-suppression

Parameter

none

Default

ip igmp snooping report-suppression

Mode

Global Configuration

Usage

“no ip igmp snooping report-suppression” will disable the igmp v1/v2 igmp report suppression function. The receive report will fthen orward to the vlan router ports. The configuration can use “show ip igmp snooping”.

Example

The following example specifies the disable ip igmp snooping report-suppression test.

Switch(config)#

no ip igmp snooping report-suppression

Switch#

show ip igmp snooping

IGMP Snooping Status

Snooping : Enabled

Report Suppression : Disabled

Operation Version : v2

Forward Method : mac

Unknown Multicast Action : Flood

IP IGMP Snooping Version

Syntax

ip igmp snooping version (2|3)

Parameter

(2|3) Ip igmp snooping running version 2 or 3

Default

ip igmp snooping version 2

Mode

Global Configuration

Usage

“ip igmp snooping version 3” will remove all ipv4 group entries when the forward method is src-dst-ip. When the forward method is mac, it will remove the dynamic group entry. The same is from v3 change to v2. For this, all querier versions will update to version 2. The configuration can use “show ip igmp snooping”.

Example

The following example specifies that set ip igmp snooping version 3 test.

Switch(config)#

ip igmp snooping version 3

Switch#

show ip igmp snooping

IP IGMP Snooping Unknown-Multicast Action

Syntax

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

Parameter

(drop | flood | routerport) Unknown multicast action for drop|flood|router-port

Default

ip igmp snooping unknown-multicast action flood

Mode

Global Configuration

Usage

When igmp snooping and mld snooping are disabled, it can't set an action to drop or router-port. When disabling igmp snooping & mld snooping, it sets unknown multicast action flood. When the action is router-port to flood or drop, it will delete the unknown multicast group entry. If the lookup mode is src-dst-ip, when changed, the unknown action will delete all the dynamic groupd. The configuration can use "show ip igmp snooping".

Example

The following example specifies that set ip igmp unknown multicast action router-port test.

Switch(config)#

ip igmp snooping

Switch(config)#

ip igmp snooping unknown-multicast action router-port

Switch#

show ip igmp snooping

IGMP Snooping Status

Snooping : Enabled

Report Suppression : Disabled

Operation Version : v2

Forward Method : mac

Unknown Multicast Action : Router Port

Switch#

show ip igmp snooping

Switch(config)#

no ip igmp snooping

IGMP Snooping Status

Snooping : Disabled

Report Suppression : Disabled

Operation Version : v2

Forward Method : mac

Unknown Multicast Action : Flood

IP IGMP Snooping Forward-Method

Syntax

ip igmp snooping forward-method (mac |src-dst-ip)

Parameter

(mac | src-dst-ip) Multicast lookup method is DMAC OR DIP+SIP

Default

ip igmp snooping forward-method mac

Mode

Global Configuration

Usage

When changing the lookup method, it will remove all groups. The configuration can use “show ip igmp snooping”.

Example

The following example specifies that set ip igmp lookup method is src-dst-ip test.

Switch(config)#

ip igmp forward-method src-dst-ip

Switch#

show ip igmp snooping

IGMP Snooping Status

Snooping : Disabled

Report Suppression : Disabled

Operation Version : v2

Forward Method : src-dst-ip

IP IGMP Snooping Querier

Syntax

ip igmp snooping vlan <VLAN-LIST> querier

no ip igmp snooping [vlan <VLAN-LIST>] querier

ip igmp snooping vlan <VLAN-LIST> querier version (2|3)

Parameter

VLAN-LIST	specifies VLAN ID list to set
(2|3)	Query version 2 or 3

Default

no ip igmp snooping querier

Mode

Global Configuration

Usage

When enabling ip igmp vlan querier, there will be a process router selection. The selection will send general and specific queries. The configuration can use “show ip igmp snooping querier”.

Example

Example

The following example specifies that set ip igmp snooping querier test. test must be create static vlan firstly.

```
Switch(config)#
  vlan 2
Switch(config-vlan)#
  exit
Switch(config)#
  ip igmp snooping vlan 2 querier
Switch(config)#
  exit
Switch#
  show ip igmp snooping querier
VID | State | Status | Version | Querier IP
1 | Disabled | Non-Querier | No | ------
2 | Enabled | Querier | v2 | 192.168.1.254
Switch#
  configure
Switch(config)#
  ip igmp snooping version 3
```

```
Switch(config)#
  ip igmp snooping vlan 2 querier version 3
Switch(config)#
  do show ip igmp snooping queier
VID | State | Status | Version | Querier IP
1 | Disabled | Non-Querier | No | ------
2 | Enabled | Querier | v3 | 192.168.1.254
Switch(config)#
  no ip igmp snooping queier
Switch(config)#
  do show ip igmp snooping queier
```

IP IGMP Snooping VLAN

Syntax

ip igmp snooping vlan VLAN-LIST

no ip igmp snooping vlan VLAN-LIST

Parameter

VLAN-LIST specifies VLAN ID list to set

Default

no ip igmp snooping vlan 1-4094

Mode

Global Configuration

Usage

“No ip igmp snooping vlan 1” will clear vlans for all ip igmp snooping dynamic groups and dynamic router ports, and make the static ip igmp group invalid depending on which vlan ID is vlan 1. Then there is no learning of the dynamic group and router port by igmp messages for vlan 1. The configuration can use show ip igmp snooping vlan 1.

Example

The following example specifies that set ip igmp snooping vlan test. The test must enable ip igmp snooping first.

Switch(config)#

ip igmp snooping

Switch(config)#

IGMP Snooping query interval: admin 125 sec oper 125 sec

IGMP Snooping query max response : admin 10 sec oper 10 sec

IGMP Snooping last member query counter: admin 2 oper 2

IGMP Snooping last member query interval: admin 1 sec oper 1 sec

IGMP Snooping last immediate leave: disabled

IGMP Snooping mrouter port learn by pim-dvmrp: enabled

Switch(config)#

no ip igmp snooping vlan 1

Switch#

show ip igmp snooping vlan 1

IGMP Snooping is globaly enabled

IGMP Snooping VLAN 1 admin : disabled

IGMP Snooping operation mode : disabled

IGMP Snooping robustness: admin 2 oper 2

IGMP Snooping query interval: admin 125 sec oper 125 sec

IGMP Snooping query max response : admin 10 sec oper 10 sec

IGMP Snooping last member query counter: admin 2 oper 2

IGMP Snooping last member query interval: admin 1 sec oper 1 sec

IGMP Snooping last immediate leave: disabled

IGMP Snooping mrouter port learn by pim-dvmrp: enabled

IP IGMP Snooping VLAN Parameters

Syntax

ip igmp snooping vlan <VLAN-LIST> last-member-query-count <1-7>

no ip igmp snooping vlan <VLAN-LIST> last-member-query-count

ip igmp snooping vlan <VLAN-LIST> last-member-query-interval <1- 60>

no ip igmp snooping vlan <VLAN-LIST> last-member-query-interval

[no] ip igmp snooping vlan <VLAN-LIST> mrouter learn pim-dvmrp

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

ip igmp snooping vlan <VLAN-LIST> query-interval <30-18000>

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

ip igmp snooping vlan <VLAN-LIST> response-time <5-20>

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

ip igmp snooping vlan <VLAN-LIST> robustness-variable <1-7>

no ip igmp snooping vlan <VLAN-LIST> robustness-variable

Parameter

VLAN-LIST	specifies VLAN ID list to set
last-member-query-count <1-7>	specifies last member query count to set. Default is 2
last-member-queryinterval <1-60>	specifies last member query interval to set. Default is 1
query-interval <30-18000>	specifies query interval to set. Default is 125
response-time <5- 20>	specifies a response time to set. default is 10
robustness-variable <1-7>	specifies a robustness value to set, default is 2

Default

no ip igmp snooping vlan 1-4094 last-member-query-count

no ip igmp snooping vlan 1-4094 last-member-query-interval

ip igmp snooping vlan 1-4094 mrouter learn pim-dvmrp

no ip igmp snooping vlan 1-4094 fastleave

no ip igmp snooping vlan 1-4094 query-interval

no ip igmp snooping vlan 1-4094 response-time

no ip igmp snooping vlan 1-4094 robustness-variable

Mode

Global Configuration

Usage

“no ip igmp snooping vlan 1 (last-member-query-count | last-member-queryinterval | query-interval | response-time | robustness-variable)” will set the vlan parameters to default. The cli settings will change the ip igmp vlan parameters to the admin settings. The configuration can use show ip igmp snooping vlan 1.

Example

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

Switch(config)#

ip igmp snooping vlan 1 fastleave

Switch(config)#

ip igmp snooping vlan 1 last-member-query-count 5

Switch(config)#

ip igmp snooping vlan 1 last-member-query-interval 3

Switch(config)#

ip igmp snooping vlan 1 query-interval 100

Switch(config)#

ip igmp snooping vlan 1 response-time 12

Switch(config)#

ip igmp snooping vlan 1 robustness-variable 4

```
Switch#
  show ip igmp snooping vlan 1
IGMP Snooping is globaly enabled
IGMP Snooping VLAN 1 admin : enabled
IGMP Snooping operation mode : enabled
IGMP Snooping robustness: admin 4 oper 2
IGMP Snooping query interval: admin 100 sec oper 125 sec
IGMP Snooping query max response : admin 12 sec oper 10 sec
IGMP Snooping last member query counter: admin 5 oper 2
IGMP Snooping last member query interval: admin 3 sec oper 1 sec
IGMP Snooping last immediate leave: enabled
IGMP Snooping mrouter port learn by pim-dvmrp: enabled
```

IP IGMP Snooping Static Port

Syntax

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

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

Parameter

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

Default

None static/forbidden ports

Mode

Global Configuration

Usage

'ip igmp snooping vlan 1 static-port fa1-2' will add static port fa1-2 for vlan 1. The all known vlan 1 ipv4 group will add the static ports. "ip igmp snooping vlan 1 forbidden-port fa3-4" will add forbidden port fa3-4. for vlan 1. The all known vlan 1 ipv4 group will remove the forbidden ports.

The configuration can use "show ip igmp snooping forward-all".

Example

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

```
Switch(config)#
  ip igmp snooping vlan 1 static -port fa1-2
Switch(config)#
  ip igmp snooping vlan 1 forbidden -port fa3-4
Switch#
  show ip igmp snooping forward-all vlan 1
IGMP Snooping VLAN : 1
IGMP Snooping static port : fa1-2
IGMP Snooping forbidden port : fa3-4
```

IP IGMP Snooping Static Router Port

Syntax

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

[no] ip igmp snooping vlan <VLAN-LIST> forbidden-router-port IF_PORTS

Parameter

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

Default

None static/forbidden router ports

Mode

Global Configuration

Usage

“ip igmp snooping vlan 1 static-router-port fa1-2” will add static the router port fa1-2 for vlan 1. “ip igmp snooping vlan 1 forbidden-router-port fa2” will add the forbidden router port fa2 for vlan 1. This will also remove fa2 from static the router port. The forbidden router port receive query will not forward. The configuration can use ‘show ip igmp snooping router’.

Example

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

Switch(config)#

ip igmp snooping vlan 1 static-router-port fa1-2

Switch(config)#

ip igmp snooping vlan 1 forbidden-router-port fa2

Switch#

show ip igmp snooping router

Dynamic Router Table

VID | Port | Expiry Time(Sec)

Total Entry 0

Static Router Table

Static Router Table

VID | Port Mask

1 | fa1

Total Entry 1

Forbidden Router Table

VID | Port Mask

1 | fa2

Total Entry 1

IP IGMP Snooping Static Group

Syntax

[no] ip igmp snooping vlan <VLAN-LIST> static-group <ip-addr> interface IF_PORT

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

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

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

Parameter

VLAN-LIST	specifies VLAN ID list to set
ip-addr	specifies multicast group ipv4 address
IF_PORT	specifies port id to set or remove

Default

None

Mode

Global Configuration

Usage

'ip igmp snooping vlan 1 static-group 224.1.1.1 interface fa1' will add static group. The static group will not learn from other dynamic ports. If the dynamic group exists, then the static group will overlap with the dynamic group. If you remove the last member of static group, the static group will be deleted. If the static group wants to validate itself , you must enable igmp snooping vlan and ip igmp snooping. The configuration can use "show ip igmp snooping group [(dynamic |

static)]" to display. You can also use "no ip igmp snooping vlan 1 group 224.1.1.1" to delete the static group. In addition, you can use clear ip igmp snooping groups to delete the static group.

Example

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

Switch(config)#

ip igmp snooping vlan 1 static-group 224.1.1.1 interface

fa1

Switch(config)#

ip igmp snooping vlan 1 static-group 224.1.1.1 interface

fa2

Switch#

show ip igmp snooping groups

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

1 | 224.1.1.1 | Static| -- | fa1-2

Total Number of Entry = 1

Switch#

clear ip igmp snooping groups static

Switch# s

how ip igmp snooping groups

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

Total Number of Entry = 0

IP IGMP Profile

Syntax

ip igmp profile <1-128>

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

show ip igmp profile [<1-128>]

Parameter

<1-128>	specifies profile ID
<ip-addr>	Start ipv4 multicast address
[ip-addr]	End ipv4 multicast address
(permit | deny)	Permit: Allow Multicast address range ip address learning Deny: Do not allow Multicast address range ip address learning

Default

None

Mode

ip igmp profile <1-128>: Global Configuration

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

igmp profile config mode

Usage

Use the ‘ip igmp profile 1’ entry for the igmp profile config mode. Use ‘profile range ip 224.1.1.1 224.1.1.8 action permit’ to configure the profile entry. The profile entry is used by the port filter. The configuration can use ‘show ip igmp profile [<1-128>]’ to display.

Example

The following example specifies that set ip igmp profile test:

Switch(config) #

ip igmp profile 1

Switch(config-igmp-profile)#

profile range ip 224.1.1.1 224.1.1.8 action permit

Switch(config-igmp-profile)#

show ip igmp profile

IP igmp profile index: 1

IP igmp profile action: permit

Range low ip: 224.1.1.1

Range high ip: 224.1.1.8

Switch(config-igmp-profile)#

exit

```
Switch(config)#
  ip igmp profile 10
Switch(config-igmp-profile)#
  profile range ip 224.1.1.5 224.1.1.10 action
deny
Switch(config-igmp-profile)#
  show ip igmp profile
IP igmp profile index:
  10
IP igmp profile action:
  deny
Range low ip:
  224.1.1.5
Range high ip:
  224.1.1.10
Switch(config-igmp-profile)#
  exit
Switch(config)#
  exit
```

```
Switch#
  show ip igmp profile
IP igmp profile index:
  1
IP igmp profile action:
  permit
Range low ip:
  224.1.1.1
Range high ip:
  224.1.1.8
IP igmp profile index:
  10
IP igmp profile action:
  deny
Range low ip:
  224.1.1.5
Range high ip:
  224.1.1.10
```

IP IGMP Filter

Syntax

ip igmp filter <1-128>

[no] ip igmp filter

Show ip igmp filter [interfaces IF_PORTS]

Parameter

<1-128>	Specifies profile ID
[interfaces IF_PORTS]	Specifies interfaces to display

Default

None

Mode

Interface mode

Usage

After creating the ip igmp profile entry, you can use 'ip igmp filter 1' to bind a profile for a port. When the port binds a profile, then the port learning group will update. If the group is not matched to the profile rule it will remove the port from the group. Static groups are excluded. The configuration can use 'show ip igmp filter' to display.

Example

The following example specifies that set ip igmp filter test.

The configure must create ip igmp profile firstly.

```
Switch(config)#
  ip igmp profile 1
Switch(config-igmp-profile)#
  profile range ip 224.1.1.1 224.1.1.8 action permit
Switch(config-igmp-profile)#
  exit
Switch(config)#
  interface fa1
Switch(config-if)#
  ip igmp filter 1
Switch(config-if)#
  exit
Switch(config)#
  exit
Switch#
  show ip igmp filter
Port ID | Profile ID
fa1 : 1
fa2 : None
```

fa3 : None

IP IGMP Max-Groups

Syntax

ip igmp max-groups <0-512>

no ip igmp max-groups

ip igmp max-groups action (deny | replace)

Show ip igmp max-group [interfaces IF_PORTS]

Show ip igmp max-group action [interfaces IF_PORTS]

Parameter

<1-128>	Specifies profile ID
(deny | replace)	Deny: Current port igmp group arrived max-groups, don't add group. Replace: Current port igmp group arrived max-groups, remove port form rand group, and add port to group.

Default

no ip igmp max-groups

ip igmp max-groups action deny

Mode

Interface mode

Usage

Use ‘ip igmp max-groups 10’ to limit port learning. The max group number is 10. When the port haslearned more than 10 groups, then the rest of the groups will be removes from the port form the group. Static groups are excluded. The configuration can use ‘show ip igmp max-group & show ip igmp max-group action ’ to display.

Example

The following example specifies that set ip igmp max-groups and action is replace test.

Switch(config)#

interface fa1

Switch(config-if)#

ip igmp max-groups 10

Switch(config-if)#

ip igmp max-groups action replace

Switch(config-if)#

exit

Switch(config)#

exit

Switch#

show ip igmp max-group

Port ID | Max Group

fa1 : 10

fa2 : 1024

fa3 : 1024

--More--

Switch#

show ip igmp max-group action

Port ID | Max-groups Action

fa1 : replace

fa2 : deny

fa3 : deny

fa4 : deny

fa5 : deny

fa6 : deny

--More--

Clear IP IGMP Snooping Groups

Syntax

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

Parameter

none	Clear ip igmp groups include dynamic and static
(dynamic | static)	Ip igmp group type is dynamic or static

Default

Clear all ip igmp groups

Mode

privileged mode

Usage

This command will clear the ip igmp groups for dynamic or static or all of type. The configuration can use 'show ip igmp snooping groups' to check.

Example

Switch#

clear ip igmp snooping groups static

Switch#

show ip igmp snooping groups

```
Switch#
  clear ip igmp snooping groups
Switch#
  show ip igmp snooping groups
```

Clear IP IGMP Snooping Statistics

Syntax

clear ip igmp snooping statistics

Parameter

none

Default

none

Mode

privileged mode

Usage

This command will clear the igmp statistics. The configuration can use show ip igmp snooping.

Example

The following example specifies that clear ip igmp snooping statistics test.

Switch#

clear ip igmp snooping statistics

Switch#

show ip igmp snooping

Show IP IGMP Snooping Counters

Syntax

show ip igmp snooping groups counters

Parameter

none

Default

none

Mode

privileged mode

Usage

This command will display the ip igmp group counter include static group.

Example

The following example specifies that display ip igmp snooping group counter test.

Switch#

show ip igmp snooping counters

Total ip igmp snooping group number: 0

Show IP IGMP Snooping Groups

Syntax

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

Parameter

none	Show ip igmp groups include dynamic and static]
(dynamic | static)	Display Ip igmp group type is dynamic or static

Default

display all ip igmp groups

Mode

privileged mode

Usage

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

Example

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

Switch#

show ip igmp snooping groups

```
Switch#
  show ip igmp snooping groups dynamic
Switch#
  show ip igmp snooping groups static
```

Show IP IGMP Snooping Router

Syntax

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

Parameter

none	Show ip igmp router include dynamic and static and forbidden
(dynamic | forbidden | static)	Display Ip igmp router info for different type

Default

display all router info

Mode

privileged mode

Usage

This command will display the ip igmp router info.

Example

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

Switch#

show ip igmp snooping router

Switch#

show ip igmp snooping router dynamic

Switch#

show ip igmp snooping rotuer static

Switch#

show ip igmp snooping rotuer forbidden

Show IP IGMP Snooping Querier

Syntax

show ip igmp snooping querier

Parameter

none Show all vlan ip igmp querier info.

Default

none

Mode

privileged mode

Usage

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

Example

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

Switch#

show ip igmp snooping querier

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

Show IP IGMP Snooping

Syntax

show ip igmp snooping

Parameter

none Show ip igmp snooping global info.

Default

none

Mode

privileged mode

Usage

This command will display ip igmp snooping global info.

Example

The following example specifies that show ip igmp snooping test.

Switch#

show ip igmp snooping

IGMP Snooping Status

Snooping : Enabled

General Query Rx : 0

General Query Tx : 0

GS Query Rx : 0

GS Query Tx : 0

Report Rx : 0

Report Tx : 0

Packet Statistics

Total Rx : 0

Valid Rx : 0

Invalid Rx : 0

Other Rx : 0

General Query Rx : 0

General Query Tx : 0

GS Query Rx : 0

GS Query Tx : 0

Report Rx : 0

Report Tx : 0

Leave Rx : 0

Leave Tx : 0

Show IP IGMP Snooping VLAN

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

Default

Show all ip igmp snooping vlan info

Mode

privileged mode

Usage

This command will display ip igmp snooping vlan info.

Example

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

```
Switch#
        show ip igmp snooping vlan
IGMP Snooping is globaly enabled
```

IGMP Snooping VLAN 1 admin : disabled

IGMP Snooping operation mode : disabled

IGMP Snooping robustness: admin 2 oper 2

IGMP Snooping query interval: admin 125 sec oper 125 sec

IGMP Snooping query max response : admin 10 sec oper 10 sec

IGMP Snooping last member query counter: admin 2 oper 2

IGMP Snooping last member query interval: admin 1 sec oper 1 sec

IGMP Snooping last immediate leave: disabled

IGMP Snooping mrouter port learn by pim-dvmrp: enabled

Show IP IGMP Snooping Forward-All

Syntax

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

Parameter

none Show all ip igmp snooping vlan forward-all info

[vlan VLAN-LIST] Show specifies vlan of ip igmp forward info.

Default

Show all vlan ip igmp forward all info

Mode

privileged mode

Usage

This command will display ip igmp snooping forward all info.

Example

The following example specifies that show ip igmp snooping forward-all test.

Switch#

show ip igmp snooping forward-all

IGMP Snooping VLAN : 1

IGMP Snooping static port : None

IGMP Snooping forbidden port : None

Show IP IGMP Snooping Profile

Syntax

show ip igmp profile [<1-128>]

Parameter

none Show all ip igmp snooping profile info

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

Default

Show all ip igmp profile info

Mode

privileged mode

Usage

This command will display ip igmp profile info.

Example

The following example specifies that show ip igmp profile test.

Switch#

show ip igmp profile

IP igmp profile index: 1

IP igmp profile action: permit

Range low ip: 224.1.1.1

Range high ip: 224.1.1.8

IP igmp profile index: 2

IP igmp profile action: deny

Range low ip: 225.1.1.0

Range high ip: 225.1.2.1

Show IP IGMP Snooping Port Filter

Syntax

show ip igmp filter [interfaces IF_PORTS]

Parameter

none	Show all port filter
[interfaces IF_PORTS]	Show specifies ports filter

Default

Show all ports ip igmp filter

Mode

privileged mode

Usage

This command will display ip igmp port filter info.

Example

The following example specifies that show ip igmp filter test.

Switch#

show ip igmp filter

Port ID | Profile ID

fa1 : 1

fa2 : None

fa3 : None

fa4 : None

fa5 : None

--More--

Show IP IGMP Snooping Port Max-Group

Syntax

show ip igmp max-group [interfaces IF_PORTS]

Parameter

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

Default

Show all ports ip igmp max-group

Mode

privileged mode

Usage

This command will display ip igmp port max-group.

Example

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

Switch(config)#

interface fa1

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

```
Switch(config-if)#
  ip igmp max-groups 50
Switch(config-if)#
  exit
Switch(config)#
  exit
Switch#
  show ip igmp max-group
Port ID | Max Group
fa1 : 50
fa2 : 1024
fa3 : 1024
fa4 : 1024
fa5 : 1024
```

Show IP IGMP Snooping Port Max-Group Action

Syntax

show ip igmp max-group action [interfaces IF_PORTS]

Parameter

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

Default

Show all ports ip igmp max-group action

Mode

privileged mode

Usage

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

Example

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

Switch(config)#

interface fa1

Switch(config-if)#

ip igmp max-groups action replace

```
Switch(config-if)#
  exit
Switch(config)#
  exit
Switch#
  show ip igmp max-group action
Port ID | Max-groups Action
fa1 : replace
fa2 : deny
fa3 : deny
fa4 : deny
fa5 : deny
```

EnGenius®

Chapter 10
IP Source Guard

IP Source Verify

Syntax

ip source verify

ip source verify mac-and-ip

no ip source verify

Parameter

None

Default

IP Source Guard is disabled

Mode

Interface Configuration

Usage

Use the ip source verify command to enable IP Source Guard function. Default IP Source Guard filter source IP address. The “mac-and-ip” filters not only source IP address but also source IP address. Use the no form of this command to disable.

Example

The example shows how to enable IP Source Guard with source IP address filtering on interface gi1.

Switch(config)# interface gi1

switch(config-if)#

ip source verify

The example shows how to enable IP Source Guard with source IP and MAC address filtering on interface gi2. You can verify settings by the following show ip source interfaces command.

Switch(config)#

interface gi2

switch(config-if)#

ip source verify mac-and-ip

switch(config-if)#

do show ip source interfaces gi1-2

Port | Status | Max Entry | Current Entry

gi1 | Verify MAC+IP | No Limit | 0

gi2 | disabled | No Limit | 0

IP Source Binding

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.

Default

Default is no binding entry.

Mode

Global Configuration

Usage

Use the ip source binding command to create a static IP source binding entry has an IP address, its associated MAC address AVLAN ID Ainterface. Use the no form of this command to delete static entry.

Example

The example shows how to add a static IP source binding entry. You can verify settings by the following show ip source binding command.

Switch(config)#

ip source binding 00:11:22:33:44:55 vlan 1 192.168.1.55 interface fa1

switch(config)#

do show ip source binding

Bind Table: Maximun Binding Entry Number 192

Port | VID | MAC Address | IP | Type | Lease Time

fa1 | 1 | 00:11:22:33:44:55 | 192.168.1.55(255.255.255.255)| Static | NA

Show IP Source Interface

Syntax

show ip source interfaces IF_PORTS

Parameter

IF_PORTS specifies ports to show

Default

No default is defined

Mode

Global Configuration

Usage

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

Example

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

switch#

show ip source interfaces gi1

Port | Status | Max Entry | Current Entry

gi1 | Verify MAC+IP | No Limit | 0

Show IP Source Binding

Syntax

show ip source binding [(dynamic|static)]

Parameter

dynamic	Show entries that added by DHCP snooping learn
static	Show entries that added by user

Default

No default is defined

Mode

Global Configuration

Usage

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

Example

The example shows how to show static binding entries of IP Source Guard.

switch#

show ip source binding

Bind Table: Maximun Binding Entry Number 192

Port | VID | MAC Address | IP | Type | Lease Time

fa1 | 1 | 00:11:22:33:44:55 | 192.168.1.55(255.255.255.255)| Static | NA

EnGenius®

Chapter 11
Link Aggregation

Lag Load-balance

Syntax

lag load-balance (src-dst-mac | src-dst-mac-ip)

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

Usage

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

Example

This example shows how to change load balance algorithm to src-dst-mac-ip.

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

This example shows how to show current load balance algorithm.

```
Switch#
        show lag
Load Balancing: src-dst-mac-ip.

Group ID | Type | Ports

1 | --------- |
2 | --------- |
3 | --------- |
4 | --------- |
5 | --------- |
6 | --------- |
7 | --------- |
8 | --------- |
```

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 1.

Mode

Global Configuration

Usage

LACP system priority is used for two connected DUT to select the master switch. A lower system priority value has a higher priority. And the DUT with a higher priority can decide which ports are able to join the LAG. Use “no lacp system-priority” to restore to the default priority value. The only way to show this configuration is using the “show running-config”command.

Example

This example shows how to configure lacp system priority to 1000.

Switch(config)#

LACP Port-Priority

Syntax

lacp port-priority <1-65535>

Parameter

<1-65535> Specify port priority value

Default

Default port priority is 1.

Mode

Interface Configuration

Usage

LACP port priority is used for two connected DUT to select aggregation ports. A lower port priority value has a higher priority. And the port with the higher priority will be selected into LAG first. The only way to show this configuration is using the “show running-config” command.

Example

This example shows how to configure interface fa1 lacp port priority to 100.

Switch(config)#

interface fa1

```
Switch(config-if)#
  lacp port-priority 100
```

LACP Timeout

Syntax

lacp timeout (long | short)

Parameter

long Send LACP packet every 30 seconds.

short Send LACP packet every 1 second.

Default

Default LACP timeout is long.

Mode

Interface Configuration

Usage

LACP need to send LACP packet to partner switch to check the link status. This command configures the interval of sending LACP packets. The only way to show this configuration is using the “show running-config” command.

Example

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

Switch(config)# interface fa1

```
Switch(config-if)#
  lacp timeout short
```

LAG

Syntax

lag <1-8> mode (static | active | passive)

no lag

Parameter

<1-8>	Specify the LAG id for the interface
static	Specify the LAG to be static mode and join the interface into this LAG.
active	Specify the LAG to be dynamic mode and join the interface into this LAG with LACP active port.
passive	Specify the LAG to be dynamic mode and join the interface into this LAG with LACP passive port.

Default

There is no LAG in default

Mode

Interface Configuration

Usage

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

Example

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

```
Switch(config)#
  interface range fa1-3
Switch(config-if)#
  lag 1 mode active
```

This example shows how to show current LAG status.

```
Switch#
  show lag
Load Balancing: src-dst-mac-ip.
Group ID | Type | Ports

1 | LACP | Inactive: fa1-3
2 | ------ |
3 | ------ |
4 | ------ |
5 | ------ |
6 | ------ |
7 | ------ |
8 | ------ |
```

Show Lag

Syntax

show lag

Parameter

None

Default

No default values for this command.

Mode

Privileged EXEC

Usage

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

Example

This example shows how to show current LAG status.

Switch#

show lag

Load Balancing: src-dst-mac-ip.

Group ID | Type | Ports

1 | LACP | Inactive: fa1-3
2 | ------ |
3 | ------ |
4 | ------ |
5 | ------ |
6 | ------ |
7 | ------ |
8 | ------ |

Chapter 12
LLDP

LLDP

Syntax

lldp

no lldp

Default

lldp

Mode

Global Configuration

Usage

The “lldp” command globally enables the LLDP RX/TX ability. The “no lldp run” command disables the LLDP RX/TX ability and the behavior when receiving a LLDP PDU would then be decided by the “lldp lldpdu” command. The LLDP enabling status is displayed by the “show lldp” command.

Example

The following example sets LLDP enable/disable.

Switch121212(config)#

show lldp

Switch121212(config)#

lldp

State: Enabled

Timer: 30 Seconds

Hold multiplier: 4

Reinit delay: 2 Seconds

Tx delay: 2 Seconds

LLDP packet handling: Flooding

Switch121212(config)#

no lldp

Switch121212(config)#

show lldp

State: Disabled

Timer: 30 Seconds

Hold multiplier: 4

Reinit delay: 2 Seconds

Tx delay: 2 Seconds

LLDP packet handling: Flooding

LLDP Tx-Interval

Syntax

lldp tx-interval <5-32768>

Parameter

<5-32768> Specify the LLDP PDU TX interval in unit of second.

Default

lldp tx-interval 30

Mode

Global Configuration

Usage

This command globally configures the LLDP TX interval. It should be noticed that both “lldp tx-interval” and “lldp tx-delay” affects the LLDP PDU TX time. The larger value of the two configurations decides the TX interval. The configuration could be shown by the “show lldp” command.

Example

This example sets LLDP TX interval to 10 seconds.

Switch121212(config)#

lldp tx-interval 10

```
Switch121212(config)#
  show lldp
State: Disabled
Timer: 10 Seconds
Hold multiplier: 4
Reinit delay: 2 Seconds
Tx delay: 2 Seconds
LLDP packet handling: Flooding
```

LLDP Reinit-Delay

Syntax

lldp reinit-delay <1-10>

Parameter

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

Default

lldp reinit-delay 2

Mode

Global Configuration

Usage

This command globally configures the LLDP re-initial delay. This delay avoids the LLDP from generating too many PDUs if the port is up and down frequently. The delay starts to count down when the port links down. The port would not generate a LLDP PDU until the delay counts to zero. The configuration could be shown by the “show lldp” command.

Example

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

Switch121212(config)#

lldp reinit-delay 5

```
Switch121212(config)#
  show lldp
State: Disabled
Timer: 10 Seconds
Hold multiplier: 4
Reinit delay: 5 Seconds
Tx delay: 2 Seconds
LLDP packet handling: Flooding
```

LLDP Holdtime-Multiplier

Syntax

lldp holdtime-multiplier <2-10>

Parameter

<2-10> Specify the LLDP hold time multiplier.

Default

lldp holdtime-multiplier 4

Mode

Global Configuration

Usage

This command globally configures the LLDP PDU hold multiplier that decides the time-to-live (TTL) value sent in LLDP advertisements: TTL = (txinterval * holdtime-multiplier). The configuration could be shown by the “show lldp” command.

Example

This example sets LLDP hold time multiplier to 3.

Switch121212(config)#

lldp holdtime-multiplier 3

```
Switch121212(config)#
  show lldp
State: Disabled
Timer: 10 Seconds
Hold multiplier: 3
Reinit delay: 2 Seconds
Tx delay: 2 Seconds
LLDP packet handling: Flooding
```

LLDP Tx-Delay

Syntax

lldp tx-delay <1-8192>

Parameter

<1-8192> Specify the LLDP tx delay in unit of seconds.

Default

lldp tx-delay 2

Mode

Global Configuration

Usage

This command globally configures the delay in seconds between successive LLDP frame transmissions. The delay starts to count in any case that a LLDP PDU is sent by, such as a LLDP PDU advertise routine, LLDP PDU content change, port link up, etc. The configuration could be shown by the “show lldp” command.

Example

This example sets LLDP PDU TX delay to 10.

Switch121212(config)#

  lldp tx-delay 10

```
Switch121212(config)#
  show lldp
State: Disabled
Timer: 10 Seconds
Hold multiplier: 4
Reinit delay: 2 Seconds
Tx delay: 10 Seconds
LLDP packet handling: Flooding
```

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), maxframe- size (802.3 max frame size), and managementaddr (management address).

Default

no lldp tlv-select

Mode

Port Configuration

Usage

This command per port configures the selected TLV attaching in PDU. The “no lldp tlv-select” command would remove all selected TLVs. The configuration could be shown by the “show lldp” command.

Example

This example selects the system name, system description, system capability, 802.3 MAC-PHY, 802.3 link aggregation, 802.3 max frame size, and management address TLVs for interfaces fa1 and fa3.

```
Switch121212(config)#
  interface range fa1,3
Switch121212(config-if-range)#
   lldp tlv-select port-desc sys-name sys-desc sys-cap mac-phy lag max-frame-size management-addr
Switch121212(config-if-range)#
  exit
Switch121212(config)#
  show lldp interfaces fa1,3
State: Disabled
Timer: 10 Seconds
Hold multiplier: 3
Reinit delay: 2 Seconds
Tx delay: 2 Seconds
LLDP packet handling: Flooding
Port | State | Optional TLVs | Address
fa1 | RX,TX | PD, SN, SD, SC |192.168.1.254
fa3 | RX,TX | PD, SN, SD, SC |192.168.1.254
Port ID: fa1
```

802.3 optional TLVs: 802.3-mac-phy, 802.3-lag, 802.3-max-frame-size,

management-addr

802.1 optional TLVs

PVID: Enabled

Port ID: fa3

802.3 optional TLVs: 802.3-mac-phy, 802.3-lag, 802.3-max-frame-size,

management-addr

802.1 optional TLVs

PVID: Enabled

LLDP TLV-Select PVID

Syntax

lldp tlv-select pvid (disable|enable)

Parameter

(disable|enable) Specifies the LLDP 802.1 PVID TLV attach enable status.

Default

lldp tlv-select pvid enable

Mode

Port Configuration

Usage

This command per port configures the 802.1 PVID TLV attach enable status. The configuration could be shown by the “show lldp” command.

Example

This example sets the port gi1 PVID TLV attach status to disabled and the port gi2 to enabled.

```
Switch121212(config)#
  interface gi1
Switch121212(config-if-range)#
  lldp tlv-select pvid disable
```

```
Switch121212(config-if-range)#
  exit
Switch121212(config)#
  interface gi2
Switch121212(config-if-range)#
  lldp tlv-select pvid enable
Switch121212(config-if-range)#
  exit
Switch121212(config)#
  show lldp interfaces gi1,gi2
State: Disabled
Timer: 10 Seconds
Hold multiplier: 3
Reinit delay: 2 Seconds
Tx delay: 2 Seconds
LLDP packet handling: Flooding
```

Port | State | Optional TLVs | Address

gi1 | RX,TX | |192.168.1.254

gi2 | RX,TX | |192.168.1.254

Port ID: gi1

802.3 optional TLVs:

802.1 optional TLVs

PVID: Disabled

Port ID: gi2

802.3 optional TLVs:

802.1 optional TLVs

PVID: Enabled

LLDP TLV-Select VLAN-Name

Syntax

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

Parameter

(add|remove)	Specifies to add or remove VLAN list for LLDP 802.1 VLAN-NAME TLV.
VLAN-LIST	Specify VLAN list. The configured ports should be member of all the specified VLANs or the VLAN-LIST is not valid.

Default

In default no VLAN is added

Mode

Port Configuration

Usage

The commands per port configuration to add or remove the VLAN list for 802.1 VLAN-NAME TLV. The configuration could be shown by the “show lldp” command

Example

This example adds VLAN 1, 100, 4000 to VLAN-NAME TLV for port fa10.

```
Switch121212(config)#
  vlan 100
Switch121212(config-vlan)#
  exit
Switch121212(config)#
  vlan 4000
Switch121212(config-vlan)#
  exit
Switch121212(config)#
  interface fa10
Switch121212(config-if-range)#
  switchport trunk allowed vlan add all
Switch121212(config-if-range)#
  lldp tlv-select pvid enable
Switch121212(config-if-range)#
  exit
Switch121212(config)#
  show lldp interfaces gi1,gi2
State: Disabled
```

Timer: 10 Seconds

Hold multiplier: 3

Reinit delay: 2 Seconds

Tx delay: 2 Seconds

LLDP packet handling: Flooding

Port | State | Optional TLVs | Address

gi1 | RX,TX | |192.168.1.254

gi2 | RX,TX | |192.168.1.254

Port ID: gi1

802.3 optional TLVs:

802.1 optional TLVs

PVID: Disabled

Port ID: gi2

802.3 optional TLVs:

802.1 optional TLVs

PVID: Enabled

LLDP LLDPDU

Syntax

lldp lldpdu (filtering|flooding|bridging)

Parameter

(filtering | flooding | bridging) Specifies that when LLDP is globally disabled, received LLDP packets are filtered (dropped), flooded (forwarded to all interfaces) or bridged (flooded to VLAN member ports).

Default

lldp lldpdu flooding

Mode

Global Configuration

Usage

This command globally configures the LLDP PDU handling behavior when LLDP is globally disabled. It should be noted that if LLDP is globally enabled and the per port LLDP RX status is configured to disabled, the received LLDP PDU would be dropped instead of taking the globally disabled behavior. The configuration could be shown by the “show lldp” command.

Example

This example sets LLDP disable action to bridging.

```
Switch121212(config)#
  lldp lldpdu bridging
Switch121212(config)#
  show lldp
State: Enabled
Timer: 30 Seconds
Hold multiplier: 4
Reinit delay: 2 Seconds
Tx delay: 2 Seconds
LLDP packet handling: Bridging
```

LLDP Rx LLDP Tx

Syntax

lldp rx

no lldp rx

lldp tx

no lldp tx

Default

lldp rx

lldp tx

Mode

Port Configuration

Usage

The commands per port configures the LLDP PDU RX and TX ability. The configuration could be shown by the “show lldp” command.

Example

This example sets port fa1 to enable LLDP RX and TX, port fa2 to disable RX but enable TX, port fa3 to enable RX but disable TX, port fa4 to disable RX and TX.

```
Switch121212(config)#
   interface fa1
Switch121212(config-if)#
  lldp rx
Switch121212(config-if)#
   lldp tx
Switch121212(config-if)#
   exit
Switch121212(config)#
  interface fa2
Switch121212(config-if)#
   no lldp rx
Switch121212(config-if)#
   lldp tx
Switch121212(config-if)#
   exit
Switch121212(config)#
  interface fa3
```

```
Switch121212(config-if)#
  lldp rx
Switch121212(config-if)#
  no lldp tx
Switch121212(config-if)#
  exit
Switch121212(config)#
  interface fa4
Switch121212(config-if)#
  no lldp rx
Switch121212(config-if)#
  no lldp tx
Switch121212(config-if)#
  exit
Switch121212(config)#
  show lldp interfaces fa1-4
State: Enabled
Timer: 30 Seconds
```

Hold multiplier: 4

Reinit delay: 2 Seconds

Tx delay: 2 Seconds

LLDP packet handling: Bridging

Port | State | Optional TLVs | Address

fa1 | RX,TX | |192.168.1.254

fa2 | TX | |192.168.1.254

fa3 | RX | |192.168.1.254

fa4 |Disable | |192.168.1.254

LLDP Med

Syntax

lldp med

no lldp med

Default

lldp med

Mode

Port Configuration

Usage

The commands per port configures the LLDP MED enable status. If LLDP MED is enabled, the LLDP MED capability TLV and other selected MED TLV would be attached. The configuration could be shown by the “show lldp med” command.

Example

This example sets ports fa1-4 to enable LLDP MED and ports fa5-8 to disable LLDP MED.

```
Switch121212(config)#
  interface range fa1-4
Switch121212(config-if)#
   lldp med
```

```
Switch121212(config-if)#
  exit
Switch121212(config)#
  interface range fa5-8
Switch121212(config-if)#
  no lldp med
Switch121212(config-if)#
  exit
Switch121212(config)#
  show lldp interfaces fa1-8 med
Port | Capabilities | Network Policy | Location | Inventory | POE
fa1 | Yes | Yes | No | No | No
fa2 | Yes | Yes | No | No | No
fa3 | Yes | Yes | No | No | No
fa4 | Yes | Yes | No | No | No
fa5 | No | Yes | No | No | No
fa6 | No | Yes | No | No | No
fa7 | No | Yes | No | No | No
```

fa8 | No | Yes | No | No | 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

lldp med tlv-select network-policy

Mode

Port Configuration

Usage

The commands per port configures the LLDP MED TLV selection. The “no lldp med tlv-select” command would remove all selected MED TLVs over the dedicated ports. It should be noted that even if no MED TLV is selected, the MED capability TLV would be attached if a LLDP MED is enable. The configuration could be shown by the “show lldp med” command.

Example

This example sets ports fa1-2 to select the LLDP MED network policy, location, POE-PSE, inventory TLVs, and sets ports fa3-4 to deselect all LLDP MED TLVs.

```
Switch121212(config)#
  interface range fa1-2
Switch121212(config-if)#
  lldp med tlv-select network-policy location poe-pse inventory
Switch121212(config-if)#
  exit
Switch121212(config)#
   interface range fa3-4
Switch121212(config-if-range)#
   no lldp med tlv-select
Switch121212(config-if-range)#
  exit
Switch121212(config)#
  show lldp interfaces fa1-4 med
Port | Capabilities | Network Policy | Location | Inventory | POE
fa1 | Yes | Yes | Yes | Yes | Yes
fa2 | Yes | Yes | Yes | Yes | Yes
fa3 | Yes | No | No | No | No
```

fa4 | Yes | No | No | No | No

LLDP Med Fast-Start-Repeat-Count

Syntax

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

Parameter

<1-10> LLDP PDU fast start TX repeat counts.

Default

lldp med fast-start-repeat-count 3

Mode

Global Configuration

Usage

The commands globally configures the LLDP PDU fast start TX repeat count. When the port links are up, it will send a LLDP PDU immediately to notify the link partner. The number of LLDP PDUs sent when it links up depends on the fast -start-repeat-count configuration. The LLDP PDU fast-start transmits in intervals of one second. The fast start behavior works no matter whether the LLDP MED is enabled or not. The configuration could be shown by the “show lldp med” command.

Example

This example sets fast start repeat count to 10.

Switch121212(config)#

lldp med fast-start-repeat-count 10

```
Switch121212(config)#
  show lldp med
Fast Start Repeat Count: 10
lldp med network-policy voice: auto
```

LLDP Med Network-Policy

Syntax

lldp med network-policy <1-32> app (voice|voice-signaling|guestvoice| guest-voice-signaling|softphone-voice|

video-conferencing|streaming-video|video-signaling) vlan <1-4094> vlantype

(tag|untag) priority <0-7> dscp <0-63>

no lldp med network-policy <1-32>

Parameter

<1-32>	Specify the network policy index
(voice|voicesignaling| guest-voice| guest-voicesignaling| softphonevoice| videoconferencing| streamingvideo| video-signaling)	Specify the network policy application type.
<1-4094>	Specify the VLAN ID
(tag|untag)	Specify the VLAN tag status
<0-7>	Specify the L2 priority
<0-63>	Specify the DHCP value

Default

In default all network policy are cleared.

Mode

Global Configuration

Usage

The command globally configures the LLDP MED network policy table. The “lldp med network-policy” command creates a network policy entry that can be bound to ports. If the LLDP MED network policy voice auto mode is enabled, the “voice” type network policy can not be created since it is in auto mode. The “no lldp med network-policy” command clears the network policy entry of the specified index. A network policy can be cleared only when it is not bound to any port. The network policy table configuration could be shown by the “show lldp med” command.

Example

This example creates 2 network policies.

Switch121212(config)#

lldp med network-policy 1 app voice-signaling vlan 2

vlan-type tag priority 3 dscp 4

Switch121212(config)#

lldp med network-policy 32 app video-conferencing

vlan 5 vlan-type tag priority 1 dscp 63

Switch121212(config)#

show lldp med

Fast Start Repeat Count: 10

lldp med network-policy voice: auto

Network policy 1

Application type: Voice Signaling

VLAN ID: 2 tagged

Layer 2 priority: 3

DSCP: 4

Network policy 32

Application type: Conferencing

VLAN ID: 5 tagged

Layer 2 priority: 1

DSCP: 63

LLDP Med Network-Policy Add|Remove

Syntax

lldp med network-policy (add|remove) <1-32>

Parameter

(add | remove)	Add or remove network policy binding for ports.
<1-32>	Specify the network policy index

Default

lldp med fast-start-repeat-count 3

Mode

Port Configuration

Usage

The command per port configures the network policy binding for port interface. The bound network policy of one port should be configured with different types. If a network policy TLV is selected over a port, the bound network policies would be attached in LLDP MED PDU. The configuration of network policy binding could be shown by the “show lldp med” command.

Example

This example binds network policy for interface fa1 and fa2.

Switch121212(config)#

show lldp med

Fast Start Repeat Count: 10

lldp med network-policy voice: auto

Network policy 1

Application type: Voice Signaling

VLAN ID: 2 tagged

Layer 2 priority: 3

DSCP: 4

Network policy 32

Application type: Conferencing

VLAN ID: 5 tagged

Layer 2 priority: 1

DSCP: 63

Switch121212(config)#

interface range fa1,2

```
Switch121212(config-if-range)#
  lldp med network-policy add 1,32
Switch121212(config)#
  show lldp interfaces fa1,2 med
Port | Capabilities | Network Policy | Location | Inventory | POE
fa1 | Yes | Yes | Yes | Yes | Yes
fa2 | Yes | Yes | Yes | Yes | Yes
Port ID: fa1
Network policies: 1, 32
Port ID: fa2
Network policies: 1, 32
```

LLDP Med Network-Policy Auto

Syntax

lldp med network-policy auto

no lldp med network-policy auto

Default

lldp med network-policy auto

Mode

Global Configuration

Usage

The command globally configures the network policy voice auto mode enabling status. In voice auto mode, if a network-policy TLV is selected, a voice type network policy would be attached to a PDU for which the contents come from voice VLAN configuration. This works for a voice VLAN module to exchange voice VLAN information with a link partner. If the voice auto mode is enabled, a user cannot manually create a voice type network policy; if a voice type network policy is created, the voice auto mode can not be enabled. The configuration of network policy auto mode could be shown by the “show lldp med” command.

Example

This example sets the network policy auto mode to enabled and then to disabled.

```
Switch121212(config)#
  lldp med network-policy auto
Switch121212(config)#
   show lldp med
Fast Start Repeat Count: 10
lldp med network-policy voice: auto
Switch121212(config)#
  no lldp med network-policy auto
Switch121212(config)#
  show lldp med
Fast Start Repeat Count: 10
lldp med network-policy voice: manual
```

LLDP Med Location

Syntax

lldp med location (coordination|civic-address|ecs-elin) ADDR

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

Parameter

(coordination | civic-address | ecselin)	Location type to be configured. “ecs-elin” is abbreviation of emergency call service – emergency location identifier number
ADDR	Specify the location data. Input format is hexadecimal values without colon (for example: 1234AB). For coordination location type, the length of ADDR is 16 bytes. For civic-address, the length is 6 to 160 bytes. For ecs-elin, the length is 10 to 25 bytes.

Default

In default all locations are cleared

Mode

Port Configuration

Usage

The command per port configures the LLDP MED location data. The “no lldp med location” command clears the location data. The “coordinate”, “civicaddress”, “ecs-elin” locations are independent, so at most three location TLVs could be sent if their data are not empty. The configuration of the location could be shown by the “show lldp interface PORT med” command.

Example

This example sets the location data for interface fa1.

```
Switch121212(config)#
  interface fa1
Switch121212(config-if)#
   lldp med location coordinate1122334455667788 99AABBCCDDEEFF00
Switch121212(config-if)#
   lldp med location civic-address 112233445566
Switch121212(config-if)#
  lldp med location ecs-elin1122334455667788 99AA
Switch121212(config)#
  show lldp interfaces fa1 med
Port | Capabilities | Network Policy | Location | Inventory | POE
fa1 | Yes | Yes | Yes | Yes | Yes
Port ID: fa1
Network policies: 1, 32
Location:
Coordinates: 1122334455667788 99AABBCCDDEEFF00
```

Civic-address: 112233445566

Ecs-elin: 1122334455667788 99AA

Show LLDP

Syntax

show lldp

show lldp interface IF_NMLPORTS

Parameter

IF_NMLPORTS Specify the ports to display information

Default

This command has no default value.

Mode

Privileged, Global Configuration

Usage

The “show lldp” and “show lldp interface” command displays LLDP global information including the LLDP enabling status, LLDP PDU TX interval, hold time multiplier, re-initial delay, TX delay, and LLDP packet handling when a LLDP is disabled. The per port information displayed includes the port LLDP RX/TX enabling status and the selected TLV to TX and IP address. The abbreviations in the optional TLVs are: port description (PD), system name (SN), system description (SD), and system capability (SC).

Example

This example displays lldp information of port fa1 and gi1

```
Switch121212#
  show lldp interfaces fa1,gi1
State: Disabled
Timer: 30 Seconds
Hold multiplier: 4
Reinit delay: 2 Seconds
Tx delay: 2 Seconds
LLDP packet handling: Flooding
Port | State | Optional TLVs | Address
fa1 | RX,TX | PD, SN, SD, SC |192.168.1.254
gi1 | RX,TX | |192.168.1.254
Port ID: fa1
802.3 optional TLVs: 802.3-mac-phy, 802.3-lag, 802.3-max-frame-size,
management-addr
802.1 optional TLVs
PVID: Enabled
```

Port ID: gi1

802.3 optional TLVs:

802.1 optional TLVs

PVID: Enabled

Show LLDP Local-Device

Syntax

show lldp local-device

show lldp interfaces IF_NMLPORTS local-device

Parameter

IF_NMLPORTS Specify the ports to display information

Default

There is no default configuration for this command.

Mode

Privileged, Global Configuration

Usage

The commands show the local configuration of LLDP PDU. By the commands, a user can view the contents of LLDP/ LLDP-MED TLVs that would be attached in LLDP PDU.

Example

This example display the local device information.

```
Switch121212(config)#
  show lldp local-device
LLDP Local Device Information:
Chassis Type : Mac Address
Chassis ID : 00:12:12:12:12:12
System Name : Switch121212
System Description :
System Capabilities Support : Bridge
System Capabilities Enable : Bridge
Management Address : 192.168.1.254(IPv4)
Switch121212(config)#
  show lldp interfaces fa1 local-device
Device ID: 00:12:12:12:12:12
Port ID: fa1
System Name: Switch121212
Capabilities: Bridge
```

System description:

Port description:

Management address: 192.168.1.254

Time To Live: 120

802.3 MAC/PHY Configur/Status

Auto-negotiation support: Supported

Auto-negotiation status: Enabled

Auto-negotiation Advertised Capabilities: 10BASE-T half duplex, 10BASET

full duplex, 100BASE-TX half duplex, 100BASE-TX full duplex

Operational MAU type: Other or unknown

802.3 Link Aggregation

Aggregation capability: Capable of being aggregated

Aggregation status: Not currently in aggregation

Aggregation port ID: 0

802.3 Maximum Frame Size: 1522

802.1 PVID: 1

LLDP-MED capabilities: Capabilities, Network Policy, Location, Extended

PSE, Inventory

LLDP-MED Device type: Network Connectivity

LLDP-MED Network policy

Application type: Voice Signaling

Flags: Unknown Policy

VLAN ID: 2

Layer 2 priority: 3

DSCP: 4

LLDP-MED Network policy

Application type: Conferencing

Flags: Unknown Policy

VLAN ID: 5

Layer 2 priority: 1

DSCP: 63

Hardware revision: 1123

Firmware revision: 2.5.0-beta.32801

Software revision: 2.5.0-beta.32801

Serial number: abc

Manufacturer Name:

Model name:

Asset ID:

LLDP-MED Location

Coordinates: 11:22:33:44:55:66:77:88:99:AA:BB:CC:DD:EE:FF:00

Civic-address: 11:22:33:44:55:66

Ecs-elin: 11:22:33:44:55:66:77:88:99:AA

Show LLDP Neighbor

Syntax

show lldp neighbor

show lldp interfaces IF_NMLPORTS neighbor

Parameter

IF_NMLPORTS Specify the ports to display information

Default

There is no default configuration for this command

Mode

Privileged, Global Configuration

Usage

When a LLDP PDU is received on LLDP RX enabled ports, the system would store the PDU information in a database until the time to live of the PDU counts down to zero. The command displays the received neighbor LLDP PDU information.

Example

This example display the neighbor information.

Switch121212(config)#

  show lldp neighbor

Port | Device ID | Port ID | SysName | Capabilities | TTL

fa3 | 00:12:12:12:12:12 | fa1 | Switch121212 | Bridge | 111

fa11 | TREEBASE |00:1A:4D:26:EB:E8 | TREEBASE | Station

Only | 33

Switch121212(config)#

show lldp interfaces fa3 neighbor

Device ID: 00:12:12:12:12:12

Port ID: fa1

System Name: Switch121212

Capabilities: Bridge

System description:

Port description:

Management address: 192.168.1.254

Time To Live: 98

802.3 MAC/PHY Configur/Status

Auto-negotiation support: Supported

Auto-negotiation status: Enabled

Auto-negotiation Advertised Capabilities: 10BASE-T half duplex, 10BASET

full duplex, 100BASE-TX half duplex, 100BASE-TX full duplex

Operational MAU type: 100BASE-TX full duplex mode

802.3 Link Aggregation

Aggregation capability: Capable of being aggregated

Aggregation status: Not currently in aggregation

Aggregation port ID: 0

802.3 Maximum Frame Size: 1522

802.1 PVID: 1

LLDP-MED capabilities: Capabilities, Network Policy, Location, Extended

PSE, Inventory

LLDP-MED Device type: Network Connectivity

LLDP-MED Network policy

Application type: Voice Signaling

Flags: Unknown Policy

VLAN ID: 2

Layer 2 priority: 3

DSCP: 4

LLDP-MED Network policy

]Application type: Conferencing

Flags: Unknown Policy

VLAN ID: 5

Layer 2 priority: 1

DSCP: 63

LLDP-MED Power over Ethernet

Device Type: Power Sourcing Entity

Power Source: Primary Power Source

Power priority: Low

Power value: 13.0 Watts

Hardware revision: 1123

Firmware revision: 2.5.0-beta.32801

Software revision: 2.5.0-beta.32801

Serial number: abc

Manufacturer Name:

Model name:

Asset ID:

LLDP-MED Location

Coordinates: 11:22:33:44:55:66:77:88:99:AA:BB:CC:DD:EE:FF:00

Civic-address: 11:22:33:44:55:66

Ecs-elin: 11:22:33:44:55:66:77:88:99:AA

Show LLDP Med

Syntax

show lldp med

show lldp interfaces IF_NMLPORTS med

Parameter

IF_NMLPORTS Specify the ports to display information

Default

There is no default configuration for this command

Mode

Privileged, Global Configuration

Usage

The commands displays the LLDP MED configuration information

Example

This example display the LLDP MED information.

Switch121212(config)#

show lldp med

Fast Start Repeat Count: 10

lldp med network-policy voice: manual

Network policy 1

Application type: Voice Signaling

VLAN ID: 2 tagged

Layer 2 priority: 3

DSCP: 4

Network policy 32

Application type: Conferencing

VLAN ID: 5 tagged

Layer 2 priority: 1

DSCP: 63

Port | Capabilities | Network Policy | Location | Inventory | POE

fa1 | Yes | Yes | Yes | Yes | Yes

fa2 | Yes | Yes | Yes | Yes | Yes

fa3 | Yes | No | No | No | No

fa4 | Yes | No | No | No | No

fa5 | No | Yes | No | No | No

fa6 | No | Yes | No | No | No

fa7 | No | Yes | No | No | No

fa8 | No | Yes | No | No | No

fa9 | Yes | Yes | No | No | No

fa10 | Yes | Yes | No | No | No

fa11 | Yes | Yes | No | No | No

fa12 | Yes | Yes | No | No | No

fa13 | Yes | Yes | No | No | No

fa14 | Yes | Yes | No | No | No

fa15 | Yes | Yes | No | No | No

fa16 | Yes | Yes | No | No | No

fa17 | Yes | Yes | No | No | No

fa18 | Yes | Yes | No | No | No

fa19 | Yes | Yes | No | No | No

fa20 | Yes | Yes | No | No | No

fa21 | Yes | Yes | No | No | No

fa22 | Yes | Yes | No | No | No

fa23 | Yes | Yes | No | No | No

fa24 | Yes | Yes | No | No | No

gi1 | Yes | Yes | No | No | No

gi2 | Yes | Yes | No | No | No

gi3 | Yes | Yes | No | No | No

gi4 | Yes | Yes | No | No | No

Switch121212(config)#

show lldp interfaces fa1 med

Port | Capabilities | Network Policy | Location | Inventory | POE

fa1 | Yes | Yes | Yes | Yes | Yes

Port ID: fa1

Network policies: 1, 32

Location:

Coordinates: 11223344556677889AABBCCDDEEFF00

Civic-address: 112233445566

Ecs-elin: 1122334455667788 99AA

Switch121212(config)#

Show LLDP Statistics

Syntax

show lldp statistics

show lldp interfaces IF_NMLPORTS statistics

Parameter

IF_NMLPORTS Specify the ports to display information

Default

There is no default configuration for this command

Mode

Privileged, Global Configuration

Usage

The command displays the LLDP RX/TX statistics.

Example

This example display the LLDP statistics.

witch121212(config)#

show lldp statistics

LLDP Global Statistics:

Insertions : 3

Deletions : 0

Drops : 0

Age Outs : 1

| TX Frames | RX Frames | RX TLVs | RX Ageouts

Port | Total | Total | Discarded | Errors | Discarded | Unrecognized |

Total

fa1 | 50 | 0 | 0 | 0 | 0 | 0 | 0

fa2 | 0 | 0 | 0 | 0 | 0 | 0 | 0

fa3 | 0 | 50 | 0 | 0 | 0 | 0 | 1

fa4 | 0 | 0 | 0 | 0 | 0 | 0 | 0

fa5 | 0 | 0 | 0 | 0 | 0 | 0 | 0

fa6 | 0 | 0 | 0 | 0 | 0 | 0 | 0

fa7 | 0 | 0 | 0 | 0 | 0 | 0 | 0

fa8 | 0 | 0 | 0 | 0 | 0 | 0 | 0

fa9 | 0 | 0 | 0 | 0 | 0 | 0 | 0

fa10 | 0 | 0 | 0 | 0 | 0 | 0 | 0

fa11 | 3377 | 10129 | 0 | 0 | 0 | 0 | 0

fa12 | 0 | 0 | 0 | 0 | 0 | 0 | 0

fa13 | 0 | 0 | 0 | 0 | 0 | 0 | 0

fa14 | 0 | 0 | 0 | 0 | 0 | 0 | 0

fa15 | 0 | 0 | 0 | 0 | 0 | 0 | 0

fa16 | 0 | 0 | 0 | 0 | 0 | 0 | 0

fa17 | 0 | 0 | 0 | 0 | 0 | 0 | 0

fa18 | 0 | 0 | 0 | 0 | 0 | 0 | 0

fa19 | 0 | 0 | 0 | 0 | 0 | 0 | 0

fa20 | 0 | 0 | 0 | 0 | 0 | 0 | 0

fa21 | 0 | 0 | 0 | 0 | 0 | 0 | 0

fa22 | 0 | 0 | 0 | 0 | 0 | 0 | 0

fa23 | 0 | 0 | 0 | 0 | 0 | 0 | 0

fa24 | 0 | 0 | 0 | 0 | 0 | 0 | 0

gi1 | 3377 | 0 | 0 | 0 | 0 | 0 | 0

gi2 | 3377 | 0 | 0 | 0 | 0 | 0 | 0

gi3 | 0 | 0 | 0 | 0 | 0 | 0 | 0

gi4 | 0 | 0 | 0 | 0 | 0 | 0 | 0

```
Switch121212(config)#
  show lldp interfaces fa1 statistics
LLDP Port Statistics:
| TX Frames | RX Frames | RX TLVs | RX Ageouts
Port | Total | Total | Discarded | Errors | Discarded | Unrecognized |
Total
fa1 | 51 | 0 | 0 | 0 | 0 | 0 | 0
```

Show LLDP TLV-Overloading

Syntax

show lldp interfaces IF_NMLPORTS tlvs-overloading

Parameter

IF_NMLPORTS Specify the ports to display information

Default

There is no default configuration for this command.

Mode

Privileged, Global Configuration

Usage

The LLDP PDU is composed by TLVs and a selected number TLVs may compose a large PDU that the system cannot handle. The maximum PDU length is to take the smaller jumbo frame size minus 30 bytes (30 bytes kept for a header) or 1488 bytes. The command displays the length of LLDP TLVs and if a TLV overloads the PDU length then the TLVs with a status marked “overload” would not be transmitted.

Example

This example display the LLDP TLVs overloading status of port fa1.

Switch121212(config)#

show lldp interfaces fa1 tlvs-overloading

fa1:

TLVs Group | Bytes | Status

Mandatory | 21 | Transmitted

LLDP-MED Capabilities | 9 | Transmitted

LLDP-MED Location | 53 | Transmitted

LLDP-MED Network Policies | 20 | Transmitted

LLDP-MED POE | 9 | Transmitted

802.3 | 30 | Transmitted

Optional | 38 | Transmitted

LLDP-MED Inventory | 97 | Transmitted

802.1 | 8 | Transmitted

Total: 285 bytes

Left: 1203 bytes

EnGenius®

Chapter 13
Logging

Logging

Syntax

logging

no logging

Parameter

None

Default

logging

Mode

Global Configuration

Usage

Enable/Disable the logging service.

Logging

Enable the logging service. It is the global option for the logging service. The status of the logging service is available from the command “show logging”.

No logging

Disable the logging service. When the logging service is disabled, all messages will stop logging to the system.

Show logging

Display the global logging status. It will show the logging configuration of the system, including the global logging status, and the lists of logging services.

Example

```
Switch(config)#
  show logging
Switch(config)#
  no logging
Switch(config)#
  show logging
Logging service is disabled
TARGET | STATUS | Server (PORT) | FACILITY | LOG LEVEL
buffered | enabled | | |emerg, alert, crit, error, warning, notice, info
Switch(config)#
  logging
Switch(config)#
  show logging
Logging service is enabled
```

TARGET | STATUS | Server (PORT) | FACILITY | LOG LEVEL

buffered | enabled | | |emerg, alert, crit, error, warning, notice, info

Logging Flash|Buffered

Syntax

logging (flash|buffered) [severity <0-7>]

no logging (flash|buffered)

Parameter

flash	Specify logging to flash.
buffer	Specify logging to RAM.
severity	Specify the minimum severity mask of logging message.

Default

logging buffered

no logging flash

Parameter:

severity 6: (emerg, alert, crit, error, warning, notice, info)

Mode

Global Configuration

Usage

Enable/Disable the local capability to log messages to RAM/flash with the minimum severity. The minimum severity value is “6”, including messages of severity emergency, alert, critical, error, warning, notice, and info.

Logging flash

Enables the capability to log message to flash. The default minimum severity is 6. When the service is enabled, messages will start to be logged to the flash. All logging messages will be saved when the system shuts down. Only when the local logging capability of flash is enabled will the status of logging the flash service will be shown by the command “show logging”.

Logging buffered

Enables the capability to log messages to RAM. The default minimum severity is 6. When the service is enabled, the messages will start to be logged to RAM. All logging message will be lost when the system shuts down.

No logging flash

Disables the capability to log messages to flash. Once the logging capability of flash is disabled, the status of logging the flash service will be removed from the service list shown by the command “show logging”.

No logging buffered

Disables the capability to log messages to RAM.

Show logging

Displays the logging status. It will show the logging configuration of the system, including the global logging status and the lists of logging services. When the local logging capability is enabled, the status of the local logging (flash or buffered) will be shown by the command “show logging”; Otherwise, the logging entry will be removed from the service list.

Example

```
Switch(config)#
  show logging
Logging service is enabled
TARGET | STATUS | Server (PORT) | FACILITY | LOG LEVEL
buffered | enabled | | |emerg, alert, crit, error, warning, notice, info
Switch(config)#
  no logging buffer
Switch(config)#
  show logging
Logging service is enabled
TARGET | STATUS | Server (PORT) | FACILITY | LOG LEVEL
Switch(config)#
  logging buffered
Switch(config)#
  logging flash severity 5
Switc(config)h#
  show logging
```

Logging service is enabled

TARGET | STATUS | Server (PORT) | FACILITY | LOG LEVEL

buffered | enabled | | |emerg, alert, crit, error, warning, notice, info

flash | enabled | | |emerg, alert, crit, error, warning, notice

Logging Host

Syntax

logging host <ip-addr> [port <0-65535>] [severity <0-7>] [facility(local0|local1|local2|local3|local4|local5|local6|local7)]

no logging <ip-addr>

Parameter

ip-addr	Specify the IP address of remote logging server.
port	Specify the port number of remote logging server.
severity	Specify the minimum severity mask of logging message.
facility	Specify the facility of logging messages.

Default

N/A

Parameter:

port 514:

severity 6: (emerg, alert, crit, error, warning, notice, info)

facility: Local7

Mode

Global Configuration

Usage

Enable/Disable the capability to log message to the remote syslog server.

Logging host 192.168.1.100

Enables the capability to log messages to the remote server. The default values of the parameter port is “514”. The severity is “6” (emerg, alert, crit, error, warning, notice, info), and the facility is “local7”. All logging messages will be sent to the remote server. Only when the remote logging capability is enabled will the status of remote logging service will be shown by the command “show logging”. When an existing entry is set twice, the old setting will be replaced and modified with the new one.

No logging host 192.168.1.100

Disables the capability to log messages to the remote server. When the remote logging service is disabled, the log will not be sent to the remote syslog server, and the status of remote logging entry will be removed from service list shown by the command “show command”.

Show logging

Displays the logging status. It will show the logging configuration of the system, including the global logging status and the lists of logging services. When the remote logging capability is enabled, the status of remote logging will be shown by the command “show logging”. Otherwise, the remote logging entry will be removed from the service list.

Example

Switch(config)#

logging host 192.168.1.100

Switch(config)#

logging host 192.168.1.100 port 2048 severity

```
3 facility local1
Switch(config)# s
  how logging
Logging service is enabled
TARGET | STATUS | Server (PORT) | FACILITY | LOG LEVEL
buffered | enabled | | |emerg, alert, crit, error, warning, notice, info
flash | enabled | | |emerg, alert, crit, error, warning, notice
host | enabled | 192.168.1.100( 2048)| local1 |emerg, alert, crit, error
Switch(config)#
  no logging host 192.168.1.100
Switch(config)#
  show logging
Logging service is enabled
TARGET | STATUS | Server (PORT) | FACILITY | LOG LEVEL
buffered | enabled | | |emerg, alert, crit, error, warning, notice, info
flash | enabled | | |emerg, alert, crit, error, warning, notice
```

Show Logging

Syntax

show logging

Parameter

None

Default

None

Mode

Privileged, Global Configuration

Usage

show logging

Shows the logging configuration. The information includes the global logging service status, and the list of logging service. Status of the global logging service can be determined by the command “logging/no logging”. The list of logging services shows all the active logging services.

Example

Switch(config)#

show logging

Logging service is enabled

TARGET | STATUS | Server (PORT) | FACILITY | LOG LEVEL

buffered | enabled | | |emerg, alert, crit, error, warning, notice, info

Show Logging Flash|Buffered

Syntax

show logging (flash|buffered)

Parameter

Flash Specify showing the messages logged to flash.

Buffered Specify showing the messages logged to RAM.

Default

None

Mode

Privileged, Global Configuration

Usage

Shows the messages logged to flash/RAM.

Show logging flash

Shows the messages logged to the flash. When the capability of the service is enabled, it will show all messages logged to flash. All messages will be logged in an inverse chronological order.

Show logging buffered

Shows the messages logged to RAM. When the capability of the service is enabled, it will show all messages logged to RAM. Logs will be lost after a system shutdown. All messages will be logged in an inverse chronological order.

Example

```
 Switch(config)#
   show logging buffered
Log messages in buffered
NO.| Timestamp | Category | Severity | Message
1| Jan 01 08:00:57| STP| info| Port 1 STP port state is set to Forwarding
2| Jan 01 08:00:42| STP| info| Port 1 STP port state is set to Learning
3| Jan 01 08:00:30| AAA| info| User '' enter privileged mode from console with level '15' success
4| Jan 01 08:00:28| AAA| info| User '' is authorized with privilege level 1
5| Jan 01 08:00:28| AAA| info| User '' login from console success
6| Jan 01 08:00:24| System| info| Sysinfo variable 'resetdefault' is set to value '0'
7| Jan 01 08:00:23| System| notice| System Startup!
```

Clear Logging Flash|Buffered

Syntax

clear logging (flash|buffered)

Parameter

flash	Specify clearing the messages logged to flash.
Buffered	Specify clearing the messages logged to RAM.

Default

None

Mode

Privileged, Global Configuration

Usage

Clear the message logged to flash/RAM.

Clear logging flash

Clear the messages logged to flash.

Clear logging buffered

Clear the messages logged to RAM.

Example

Switch#

show logging buffered

Log messages in buffered

NO.| Timestamp | Category | Severity | Message

1| Jan 01 08:00:57| STP| info| Port 1 STP port state is set to Forwarding

2| Jan 01 08:00:42| STP| info| Port 1 STP port state is set to Learning

3| Jan 01 08:00:30| AAA| info| User '' enter privileged mode from console with level '15' success

4| Jan 01 08:00:28| AAA| info| User '' is authorized with privilege level 1

5| Jan 01 08:00:28| AAA| info| User '' login from console success

6| Jan 01 08:00:24| System| info| Sysinfo variable 'resetdefault' is set to value '0'

7| Jan 01 08:00:23| System| notice| System Startup!

Switch#

clear logging buffered

Switch#

show logging buffered

Log messages in buffered

NO.| Timestamp | Category | Severity | Message

EnGenius®

Chapter 14
MAC Address Table

Clear MAC Address-Table

Syntax

clear mac address-table dynamic [interfaces IF_PORTS] [vlan <1-4094>]

Parameter

IF_PORTS Delete all dynamic addresses on the specified interface.

<1-4094> Delete all dynamic addresses on the specified VLAN

Default

None

Mode

Privileged EXEC

Usage

Use the clear mac address-table Privileged EXEC command to delete a dynamic mac entry on a specified interface or VLAN, or all dynamic mac entries in a mac address table. You can verify your settings by entering the show mac address-table dynamic Privileged EXEC command.

Example

This example shows how to delete dynamic MAC address entries on gi1

switch#

show mac address-table dynamic

VID | MAC Address | Type | Ports

1 | 00:00:E3:00:00:12 | Dynamic | fa11

1 | 00:14:78:3B:1E:E6 | Dynamic | gi1

Total number of entries: 2

Switch(config)# clear mac address-table dynamic interfaces gi1

switch#

show mac address-table dynamic

VID | MAC Address | Type | Ports

1 | 00:00:E3:00:00:12 | Dynamic | fa11

Total number of entries: 1

MAC Address-Table Aging-Time

Syntax

mac address-table aging-time <10-630>

Parameter

<10-630> Specify aging time value of second.

Default

Default aging out time is 300s.

Mode

Global Configuration

Usage

Use the MAC address-table aging-time Global configuration command to set the aging time of the address table. You can verify your settings by entering the show MAC address-table aging time Privileged EXEC command.

Example

The following example shows how to configure the dynamic mac entry aging outtime.

Switch(config)#

mac address-table aging-time 100

```
Switch#
  show mac address-table aging-time
Mac Address Table aging time: 100 sec
```

MAC Address-Table Static

Syntax

mac address-table static A:B:C:D:E:F vlan <1-4094> interfaces IF_PORTS

no mac address-table static A:B:C:D:E:F vlan <1-4094>

Parameter

A:B:C:D:E:F	Destination MAC address (unicast or multicast) to add to the address table. Packets with this destination address received in the specified VLAN are forwarded to the specified interface.
<1-4094>	Specify the VLAN for which the packet with the specified MAC address is received.
IF_PORTS	Interface to which the received packet is forwarded. Valid interfaces include physical ports and port channels.

Default

No static addresses are configured.

Mode

Global Configuration

Usage

Use the mac address-table static global configuration command to add static addresses to the MAC address table. Use the no form of this command to remove static entries from the table. You can verify your settings by entering the show mac address-table static Privileged EXEC command.

Example

The following example shows how to add static addresses to the MAC address table.

```
Switch(config)#
  mac address-table static 0:1:2:3:4:5 vlan 1 interfaces fa5
Switch(config)#
  mac address-table static 1:6:7:9:a:b vlan 100 interfaces fa1,fa5,gi1
Switch#
  show mac address-table static
VID | MAC Address | Type | Ports
1 | 00:01:02:03:04:05 | Static | fa5
100 | 01:06:07:09:0A:0B | Static | fa1,fa5,gi1
Total number of entries: 2
```

MAC Address-Table Drop

Syntax

mac address-table static A:B:C:D:E:F vlan <1-4094> drop

no mac address-table static A:B:C:D:E:F vlan <1-4094>

Parameter

A:B:C:D:E:F	Unicast source or destination MAC address. Packets with this MAC address are dropped.
<1-4094>	Specify the VLAN for which the packet with the specified MAC address is received.

Default

Unicast MAC address filtering is disabled. The switch does not drop traffic for specific source or destination MAC addresses.

Mode

Global Configuration

Usage

Use the mac address-table static drop global configuration command to enable unicast MAC address filtering and to configure the switch to drop traffic with a specific source or destination MAC address. Use the no form of this command to return to the default settings. You can verify your settings by entering the show mac address-table static Privileged EXEC command.

Example

The following example shows how to add filter mac addresses to the MAC address table.

```
Switch(config)#
  mac address-table static a:b:c:d:e:f vlan 20 drop
Switch#
  show mac address-table static
VID | MAC Address | Type | Ports
1 | 00:01:02:03:04:05 | Static | fa5
100 | 01:06:07:09:0A:0B | Static | fa1,fa5,gi1
20 | 0A:0B:0C:0D:0E:0F | Filtering | All
Total number of entries: 3
```

Show MAC Address-Table

Syntax

show mac address-table [(static|dynamic)] [interfaces IF_PORTS] [vlan <1-4094>]

show mac address-table A:B:C:D:E:F [vlan <1-4094>]

Parameter

static	Displays only dynamic MAC address table entries.
dynamic	Displays only static MAC address table entries.
IF_PORTS	Displays entries for a specific interface ID. The interface ID can be one of the following types: Ethernet port or portchannel.
<1-4094>	Displays entries for a specific VLAN.
A:B:C:D:E:F	Displays entries for a specific MAC address.

Default

None

Mode

Privileged EXEC

Usage

Use the show mac address-table command in EXEC mode to view entries in the MAC address table.

Example

The following example display all MAC address entries in mac address table

Switch#

show mac address-table

VID | MAC Address | Type | Ports

1 | DE:AD:BE:EF:01:02 | Management | CPU

1 | 00:00:E3:00:00:12 | Dynamic | fa11

1 | 00:01:02:03:04:05 | Static | fa5

1 | 00:14:78:3B:1E:E6 | Dynamic | gi1

100 | 01:06:07:09:0A:0B | Static | fa1,fa5,gi1

20 | 0A:0B:0C:0D:0E:0F | Static | All

Total number of entries: 6

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

switch#

show mac address-table 0:1:2:3:4:5

1 | 00:01:02:03:04:05 | Static | fa5

Total number of entries: 1

Show MAC Address-Table Counters

Syntax

show mac address-table counters

Parameter

None

Default

None

Mode

Privileged EXEC

Usage

Use the show mac address-table counters command in EXEC mode to display the number of addresses present in a MAC address-table.

Example

The following example shows how to display total the mac entry counters.

switch#

show mac address-table counters

Total number of entries: 5

Show MAC Address-Table Aging-Time

Syntax

show mac address-table aging-time

Parameter

None

Default

None

Mode

Privileged EXEC

Usage

Use the show mac address-table aging-time command in EXEC mode to display the aging time for dynamic mac entries.

Example

The following example shows how to display the aging time of dynamic MAC address entries.

Switch#

show mac address-table aging-time

Mac Address Table aging time: 300 sec

Chapter 15
Mirror

Mirror Session

Syntax

mirror session <1-4> source interfaces IF_PORTS (both | rx | tx)

no mirror session <1-4> source interfaces IF_PORTS (both|rx|tx)

mirror session <1-4> source vlan <1-4094>

no mirror session <1-4> source vlan

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

no mirror session <1-4> destination interface IF_NMLPORT

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

Parameter

<1-4>	Specify the mirror session to configure
IF_PORTS	Specify the source interface, Valid interfaces include physical ports and port channels.
both,rx,tx	Specify the traffic direction to mirror.
<1-4094>	Specify the mirrored VLAN ID
IF_NMLPORT	Specify the SPAN destination. A destination must be a physical port
allow-ingress	Enable ingress traffic forwarding.

Default

No monitor sessions are configured.

Mode

Global Configuration

Usage

Use the monitor session global configuration command to start a new Switched Port Analyzer (SPAN) source or destination session. Use the no form of this command to remove the SPAN session or to remove source or destination interfaces or filters from the SPAN session You can verify your settings by entering the show mirror Privileged EXEC command.

Example

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

Switch(config)#

mirror session 1 source interface fa2-5 both

Switch(config)#

mirror session 1 destination interface fa1

Switch(config)#

show mirror session 1

Session 1 Configuration

Source RX Port : fa2-5

Source TX Port : fa2-5

Destination port : fa1

Ingress State: disabled

Switch(config)#

mirror session 2 source vlan 100

Switch(config)#

mirror session 2 destination interface gi1 allow-ingress

Switch(config)#

show mirror session 2

Session 2 Configuration

Mirrored VLAN: 100

Destination port : gi1

Ingress State: enable

Show Mirror

Syntax

show mirror [session <1-4>]

Parameter

<1-4> Specify the mirror session to display

Default

None

Mode

Privileged EXEC

Usage

Use the show mirror command in EXEC mode to display mirror session configuration.

Example

This following example shows how to display mirror session configurations.

Switch(config)#

show mirror

Session 1 Configuration

Source RX Port : fa2-5

Source TX Port : fa2-5

Destination port : fa1

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

EnGenius®

Chapter 16
MLD Snooping

IPV6 MLD Snooping

Syntax

ipv6 mld snooping

no ipv6 mld snooping

show ipv6 mld snooping

Parameter

None

Default

no ipv6 mld snooping

Mode

Global Configuration

Usage

'no ipv6 mld snooping' will clear all ipv6 mld snooping dynamic groups and dynamic router ports, which makes the static ipv6 mld group invalid. They then will not learn the dynamic group and router port by a mld message. The configuration can use the 'show ipv6 mld snooping' command.

Example

The following example specifies the set ipv6 mld snooping test.

```
Switch(config)#
  ipv6 mld snooping
Switch#
  show ipv6 mld snooping
```

MLD Snooping Status

```
Snooping : Enabled
Report Suppression : Enabled
Operation Version : v1
Forward Method : mac
Unknown Multicast Action : Flood
Switch(config)#
  no ipv6 mld snooping
Switch#
   show ipv6 mld snooping
```

MLD Snooping Status

Snooping : Disabled

Report Suppression : Enabled

Operation Version : v1

Forward Method : mac

Unknown Multicast Action : Flood

IPv6 MLD Snooping Report-Suppression

Syntax

ipv6 mld snooping report-suppression

no ipv6 mld snooping report-suppression

Parameter

none

Default

ipv6 mld snooping report-suppression

Mode

Global Configuration

Usage

'no ipv6 mld snooping report-suppression' will disable the mld v1 igmp report suppression function. So when you receive a report, it will forward to the vlan router ports. The configuration can use 'show ipv6 mld snooping'.

Example

The following example specifies the disable ipv6 mld snooping reportsuppression test.

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

MLD Snooping Status

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

IPv6 MLD Snooping Version

Syntax

ipv6 mld snooping version (1|2)

Parameter

(1|2) Ipv6 mld snooping running version 1 or 2

Default

Ipv6 mld snooping version 2

Mode

Global Configuration

Usage

When the ipv6 mld snooping version is 1 ,the version 2 packet is not processed. The configuration can use 'show ipv6 mld snooping'.

Example

The following example specifies the set ipv6 mld snooping version 2 test.

Switch(config)#

ipv6 mld snooping version 2

Switch#

show ipv6 mld snooping

MLD Snooping Status

Snooping : Enabled

Report Suppression : Disabled

Operation Version : v2

Forward Method : mac

Unknown Multicast Action : Flood

IPv6 MLD Snooping VLAN

Syntax

ipv6 mld snooping vlan VLAN-LIST

no ipv6 mld snooping vlan VLAN-LIST

show ipv6 mld snooping vlan [VLAN-LIST]

Parameter

VLAN-LIST specifies VLAN ID list to set

Default

no ipv6 mld snooping vlan 1-4094

Mode

Global Configuration

Usage

'no ipv6 mld snooping vlan 1' will clear the vlan for all ipv6 mld snooping dynamic groups and dynamic router ports which makes the static ipv6 mld group invalid. The switch vlan ID is vlan 1. They then do not learn the dynamic group and router port by a mld message for vlan 1. The configuration can use 'show ipv6 mld snooping vlan 1'.

Example

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

test must be enable ipv6 mld snooping firstly.

```
Switch(config)#
  ipv6 mld snooping
Switch(config)#
  ipv6 mld snooping vlan 1
Switch#
  show ipv6 mld snooping vlan 1
MLD Snooping is globaly enabled
MLD Snooping VLAN 1 admin : enabled
MLD Snooping oper mode : enabled
MLD Snooping robustness: admin 2 oper 2
MLD Snooping query interval: admin 125 sec oper 125 sec
MLD Snooping query max response : admin 10 sec oper 10 sec
MLD Snooping last member query counter: admin 2 oper 2
MLD Snooping last member query interval: admin 1 sec oper 1 sec
MLD Snooping last immediate leave: disabled
```

MLD Snooping mrouter port learn by pim-dvmrp: enabled

Switch(config)#

no ipv6 mld snooping vlan 1

Switch#

show ipv6 mld snooping vlan 1

MLD Snooping is globaly enabled

MLD Snooping VLAN 1 admin : disabled

MLD Snooping oper mode : disabled

MLD Snooping robustness: admin 2 oper 2

MLD Snooping query interval: admin 125 sec oper 125 sec

MLD Snooping query max response : admin 10 sec oper 10 sec

MLD Snooping last member query counter: admin 2 oper 2

MLD Snooping last member query interval: admin 1 sec oper 1 sec

MLD Snooping last immediate leave: disabled

MLD Snooping mrouter port learn by pim-dvmrp: enabled

IPv6 MLD Snooping VLAN Parameters

Syntax

ipv6 mld snooping vlan <VLAN-LIST> last-member-query-count <1-7>

no ipv6 mld snooping vlan <VLAN-LIST> last-member-query-count

ipv6 mld snooping vlan <VLAN-LIST> last-member-query-interval <1-60>

no ipv6 mld snooping vlan <VLAN-LIST> last-member-query-interval

[no] ipv6 mld snooping vlan <VLAN-LIST> mrouter learn pim-dvmrp

[no] ipv6 mld snooping vlan <VLAN-LIST> fastleave

ipv6 mld snooping vlan <VLAN-LIST> query-interval <30-18000>

no ipv6 mld snooping vlan <VLAN-LIST> query-interval

ipv6 mld snooping vlan <VLAN-LIST> response-time <5-20>

no ipv6 mld snooping vlan <VLAN-LIST> response-time

ipv6 mld snooping vlan <VLAN-LIST> robustness-variable <1-7>

no ipv6 mld snooping vlan <VLAN-LIST> robustness-variable

Parameter

VLAN-LIST	Specifies VLAN ID list to set
last-member-query count <1-7>	specifies last member query count to set. Default is 2
last-member-query interval <1-60>	pecifies last member query interval to set. Default is 1
query-interval <30-18000>	specifies query interval to set. Default is 125
response-time <5-20>	specifies a response time to set. default is 10
robustness-variable <1-7>	specifies a robustness value to set, default is 2

Default

no ipv6 mld snooping vlan 1-4094 last-member-query-count

no ipv6 mld snooping vlan 1-4094 last-member-query-interval

ipv6 mld snooping vlan 1-4094 mrouter learn pim-dvmrp

no ipv6 mld snooping vlan 1-4094 fastleave

no ipv6 mld snooping vlan 1-4094 query-interval

no ipv6 mld snooping vlan 1-4094 response-time

no ipv6 mld snooping vlan 1-4094 robustness-variable

Mode

Global Configuration

Usage

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

Example

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

Switch(config)#

ipv6 mld snooping vlan 1 fastleave

Switch(config)#

ipv6 mld snooping vlan 1 last-member-query-count 5

Switch(config)#

ipv6 mld snooping vlan 1 last-member-query-interval 3

Switch(config)#

ipv6 mld snooping vlan 1 query-interval 100

Switch(config)#

ipv6 mld snooping vlan 1 response-time 12

Switch(config)#

ipv6 mld snooping vlan 1 robustness-variable 4

```
Switch#
  show ipv6 mld snooping vlan 1
MLD Snooping is globaly enabled
MLD Snooping VLAN 1 admin : disabled
MLD Snooping oper mode : disabled
MLD Snooping robustness: admin 4 oper 2
MLD Snooping query interval: admin 100 sec oper 125 sec
MLD Snooping query max response : admin 12 sec oper 10 sec
MLD Snooping last member query counter: admin 5 oper 2
MLD Snooping last member query interval: admin 3 sec oper 1 sec
MLD Snooping last immediate leave: enabled
MLD Snooping mrouter port learn by pim-dvmrp: enabled
```

IPv6 MLD Snooping Static Port

Syntax

[no] ipv6 mld snooping vlan <VLAN-LIST> static-port IF_PORTS

[no] ipv6 mld snooping vlan <VLAN-LIST> forbidden-port IF_PORTS

Parameter

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

Default

None static/forbidden ports

Mode

Global Configuration

Usage

'ipv6 mld snooping vlan 1 static-port fa1-2' will add the static port fa1-2 for vlan 1. The all known vlan 1 ipv6 group will add the static ports. 'ipv6 mld snooping vlan 1 forbidden-port fa3-4' will add the forbidden ports fa3-4 for vlan 1. The all known vlan 1 ipv6 group will remove the forbidden ports. The configuration can use 'show ipv6 mld snooping forward-all'.

Example

The following example specifies the set ipv6 mld snooping static/forbidden port test.

```
Switch(config)#
  ipv6 mld snooping vlan 1 static -port fa1-2
Switch(config)#
   ipv6 mld snooping vlan 1 forbidden -port fa3-4
Switch#
  show ipv6 mld snooping forward-all vlan 1
MLD Snooping VLAN : 1
MLD Snooping static port : fa1-2
MLD Snooping forbidden port : fa3-4
```

IPv6 MLD Snooping VLAN Static Router Port

Syntax

[no] ipv6 mld snooping vlan <VLAN-LIST> static-router-port IF_PORTS

[no] ipv6 mld snooping vlan <VLAN-LIST> forbidden-router-port IF_PORTS

Parameter

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

Default

None static/forbidden router ports

Mode

Global Configuration

Usage

'ipv6 mld snooping vlan 1 static-router-port fa1-2' will add the static router ports fa1-2 for vlan 1. 'ipv6 mld snooping vlan 1 forbidden-router-port fa2' will add the forbidden router to port fa2 for vlan 1. This will also remove fa2 from the static router port. therefor, the forbidden router port receive query will not forward. The configuration can use show ipv6 mld snooping router.

Example

The following example specifies that set ipv6 mld snooping static/forbidden test.

Switch(config)#

ipv6 mld snooping vlan 1 static-router-port fa1-2

Switch(config)#

ipv6 mld snooping vlan 1 forbidden-router-port fa2

Switch#

show ipv6 mld snooping router

Dynamic Router Table

VID | Port | Expiry Time(Sec)

Total Entry 0

Static Router Table

VID | Port Mask

1 | fa1

Total Entry 1

Forbidden Router Table

VID | Port Mask

1 | fa2

Total Entry 1

IPv6 MLD Snooping Static Group

Syntax

[no] ipv6 mld snooping vlan <VLAN-LIST> static-group <ip-addr> interface IF_PORT

[no] ipv6 mld snooping vlan <VLAN-LIST> group <ip-addr>

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

clear ipv6 mld snooping groups [(dynamic | static)]

Parameter

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

Default

None

Mode

Global Configuration

Usage

'ipv6 mld snooping vlan 1 static-group ff12::1 interface fa1' will be added to the static group. The static group will not learn from other dynamic ports. If the dynamic group exists, then the static group will overlap with the dynamic group. If you remove the last member of static group, the static group will be deleted. In order for the static group to be valid , it must let the mld snooping vlan be enabled and the ipv6 mld snooping be enabled. The configuration can use 'show ipv6 mld snooping group [(dynamic | static)]' to display it. It can use 'no ipv6 mld snooping vlan 1 group ff12::1' to delete the static group. It can also clear ipv6 mld snooping groups to delete the static group.

Example

The following example specifies that set ipv6 mld snooping static group test.

Switch(config)#

ipv6 mld snooping vlan 1 static-group ff12::1 interface fa1

Switch(config)#

ipv6 mld snooping vlan 1 static-group ff12::1 interface fa2

Switch#

show ipv6 mld snooping groups

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

1 | ff12::1 | Static| -- | fa1-2

Total Number of Entry = 1

Switch#

show ipv6 mld snooping groups

```
Switch#
  show ipv6 mld snooping groups
VLAN | Gourp IP Address | Type | Life(Sec) | Port
Total Number of Entry = 0
```

IPv6 MLD Profile

Syntax

ipv6 mld profile <1-128>

profile range ipv6 <ipv6-addr> [ipv6-addr] action (permit | deny)

show ipv6 mld profile [<1-128>]

Parameter

<1-128>	specifies profile ID
<ipv6-addr>	Start ipv6 multicast address
[ipv6-addr]	End ipv6 multicast address
(permit | deny)	Permit: allow Multicast address range ipv6 address learning deny: do not allow Multicast address range ipv6 address learning

Default

None

Mode

ipv6 mld profile <1-128>

Global Configuration

profile range ipv6 <ipv6-addr> [ipv6-addr] action (permit | deny)

mld profile config mode

Usage

Use ‘ipv6 mld profile 1’ entry to the mld profile config mode. Use ‘profile range ipv6 ff12::1 ff12::8 action permit’ to configure the profile entry. The profile entry is used by the port filter. The configuration can use ‘show ipv6 mld profile [<1-128>]’ to display

Example

The following example specifies that set ipv6 mld profile test.

Switch(config)#

ipv6 mld profile 1

Switch(config-mld-profile)#

profile range ipv6 ff13::1 ff13::10 action

permit

Switch(config-mld-profile)#

show ipv6 mld profile

IPv6 mld profile index: 1

IPv6 mld profile action: permit

Range low ip: ff13::1

Range high ip: ff13::10

Switch(config-mld-profile)#

exit

```
Switch(config)#
  ipv6 mld profile 5
Switch(config-mld-profile)#
   profile range ipv6 ff12::1 ff12::12 action deny
Switch(config-mld-profile)#
  show ipv6 mld profile
IPv6 mld profile index: 5
IPv6 mld profile action: deny
Range low ip: ff12::1
Range high ip: ff12::12
Switch(config-mld-profile)#
  exit
Switch(config)#
  exit
Switch#
  show ipv6 mld profile
IPv6 mld profile index: 1
IPv6 mld profile action: permit
```

Range low ip: ff13::1

Range high ip: ff13::10

IPv6 mld profile index: 5

IPv6 mld profile action: deny

Range low ip: ff12::1

Range high ip: ff12::12

IPv6 MLD Filter

Syntax

ipv6 mld filter <1-128>

[no] ipv6 mld filter

Show ipv6 mld filter [interfaces IF_PORTS]

Parameter

<1-128>	specifies profile ID
[interfaces IF_PORTS]	Specifies interfaces to display

Default

None

Mode

Interface mode

Usage

The following example specifies that set ipv6 mld filter test. The configure must create ipv6 mld profile firstly.

Switch(config)#

ipv6 mld profile 1

```
Switch(config-igmp-profile)#
  profile range ipv6 ff13::1 ff13::10 action
permit
Switch(config-igmp-profile)#
  exit
Switch(config)#
   interface fa1
Switch(config-if)#
   ipv6 mld filter 1
Switch(config-if)#
  exit
Switch(config)#
   exit
Switch#
   show ipv6 mld filter
Port ID | Profile ID
fa1 : 1
fa2 : None
```

fa3 : None

fa4 : None

fa5 : None

IPv6 MLD Max-Groups

Syntax

ipv6 mld max-groups <0-512>

no ipv6 mld max-groups

ipv6 mld max-groups action (deny | replace)

Show ipv6 mld max-group [interfaces IF_PORTS]

Show ipv6 mld max-group action [interfaces IF_PORTS]

Parameter

<1-128>	specifies profile ID
(deny | replace)	Deny: current port ipv4 group arrived max-groups, don't add group. Replace: current port ipv6 group arrived max-groups, remove port form rand group, and add port to group.

Default

no ipv6 mld max-groups

ipv6 mld max-groups action deny

Mode

Interface mode

Usage

use ‘ipv6 mld max-groups 10’ to limit port learning. The max group number is 10. When the port has learned more than 10 groups, then the extra groups will be removed from the port form group. static groups are excluded. The configuration can use ‘show ipv6 mld max-group & show ipv6 mld maxgroup action ’ to display.

Example

The following example specifies that set ipv6 mld max-groups and action is

replace test.

```
Switch(config)#
  interface fa1
Switch(config-if)#
  ipv6 mld max-groups 10
Switch(config-if)#
   ipv6 mld max-groups action replace
Switch(config-if)#
  exit
Switch(config)#
  exit
Switch#
  show ipv6 mld max-group
```

Port ID | Max Group

fa1 : 10

fa2 : 1024

fa3 : 1024

fa4 : 1024

fa5 : 1024

Switch#

show ipv6 mld max-group action

Port ID | Max-groups Action

fa1 : replace

fa2 : deny

fa3 : deny

fa4 : deny

fa5 : deny

Clear IPv6 MLD Snooping Groups

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

Default

Clear all ipv6 mld groups

Mode

privileged mode

Usage

This command will clear the ipv6 mld groups for dynamic or static or of all types. The configuration can use 'show ipv6 mld snooping groups' to check.

Example

The following example specifies that clear ipv6 mld snooping groups test.

Switch#

clear ipv6 mld snooping groups static

```
Switch#
  show ipv6 mld snooping groups
Switch#
  clear ipv6 mld snooping groups
Switch#
   show ipv6 mld snooping groups
```

Clear IPv6 MLD Snooping Statistics

Syntax

clear ipv6 mld snooping statistics

Parameter

None

Default

None

Mode

Privileged mode

Usage

This command will clear the mld statistics. The configuration can use show ipv6 mld snooping.

Example

The following example specifies the clear ipv6 mld snooping statistics test.

Switch#

lear ipv6 mld snooping statistics

Switch#

show ipv6 mld snooping

Show IPv6 MLD Snooping Counters

Syntax

show ipv6 mld snooping groups counters

Parameter

None

Default

None

Mode

Privileged mode

Usage

This command will display the ipv6 mld group counter, which includes the static group.

Example

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

Switch#

show ipv6 mld snooping counters

Show IPv6 MLD Snooping Groups

Syntax

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

Parameter

none	Show ipv6 mld groups include dynamic and static
(dynamic | static)	Display ipv6 mld group type is dynamic or static

Default

display all ipv6 mld groups

Mode

privileged mode

Usage

This command will display the ipv6 mld groups for dynamic or static or all of type.

Example

The following example specifies that show ipv6 mld snooping groups test.

Switch#

show ipv6 mld snooping groups

```
Switch#
  show ipv6 mld snooping groups dynamic
Switch#
  show ipv6 mld snooping groups static
```

Show IPv6 MLD Snooping Router

Syntax

show ipv6 mld snooping router [(dynamic | forbidden |static)]

Parameter

none	Show ipv6 mld router include dynamic and static and forbidden
(dynamic | static)	Display ipv6 mld router info for different type

Default

display all router info

Mode

privileged mode

Usage

This command will display the ipv6 mld router info.

Example

The following example specifies that show ipv6 mld snooping router test.

Switch#

show ipv6 mld snooping router

Switch# show ipv6 mld snooping router static

Switch# show ipv6 mld snooping router forbidden

Show IPv6 MLD Snooping

Syntax

show ipv6 mld snooping

Parameter

none Show ipv6 mld snooping global info.

Default

None

Mode

Privileged mode

Usage

This command will display the ipv6 mld snooping global info.

Example

The following example specifies that show ipv6 mld snooping test.

Switch#

show ipv6 mld snooping

MLD Snooping Status

Snooping : Disabled

Report Suppression : Enabled

Operation Version : v1

Forward Method : mac

Unknown Multicast Action : Flood

Packet Statistics

Total Rx : 0

Valid Rx : 0

Invalid Rx : 0

Other Rx : 0

General Query Rx : 0

General Query Tx : 0

GS Query Rx : 0

GS Query Tx : 0

GSS Query Rx : 0

GSS Query Tx : 0

Report Rx : 0

Show IPv6 MLD Snooping VLAN

Syntax

show ipv6 mld snooping vlan [VLAN-LIST]

Parameter

none	Show all ipv6 mld snooping vlan info
[VLAN-LIST]	Show specifies vlan ipv6 mld snooping info

Default

Show all ipv6 mld snooping vlan info.

Mode

Privileged mode

Usage

This command will display the ipv6 mld snooping vlan info.

Example

The following example specifies the show ipv6 mld snooping vlan test.

Switch#

show ipv6 mld snooping vlan

MLD Snooping is globaly disabled

MLD Snooping VLAN 1 admin : disabled

MLD Snooping oper mode : disabled

MLD Snooping robustness: admin 2 oper 2

MLD Snooping query interval: admin 125 sec oper 125 sec

MLD Snooping query max response : admin 10 sec oper 10 sec

MLD Snooping last member query counter: admin 2 oper 2

MLD Snooping last member query interval: admin 1 sec oper 1 sec

MLD Snooping last immediate leave: disabled

MLD Snooping mrouter port learn by pim-dvmrp: enabled

Show IPv6 MLD Snooping Forward-All

Syntax

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

Parameter

none	Show all ipv6 mld snooping vlan forward-all info
[vlan VLAN-LIST]	Show specifies vlan of ipv6 mld forward info.

Default

Show all vlan ipv6 mld forward all info.

Mode

Privileged mode

Usage

This command will display ipv6 mld snooping forward all info.

Example

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

```
Switch#
  show ipv6 mld snooping forward-all
MLD Snooping VLAN : 1
MLD Snooping static port : None
MLD Snooping forbidden port : None
```

Show IPv6 MLD Profile

Syntax

show ipv6 mld profile [<1-128>]

Parameter

none	Show all ipv6 mld snooping profile info.
[<1-128>]	Show specifies index profile info.

Default

Show all ipv6 mld profile info.

Mode

Privileged mode

Usage

This command will display the ipv6 mld profile info.

Example

The following example specifies the show ipv6 mld profile test.

Switch#

show ipv6 mld profile

IPv6 mld profile index: 1

Range high ip: ff13::10

Show IPv6 MLD Port Filter

Syntax

show ipv6 mld filter [interfaces IF_PORTS]

Parameter

none	Show all port filter
[interfaces IF_PORTS]	Show specifies ports filter

Default

Show all ports ipv6 mld filter.

Mode

Privileged mode

Usage

This command will display ipv6 mld port filter info.

Example

The following example specifies the show ipv6 mld filter test.

Switch#

show ipv6 mld filter

Port ID | Profile ID

fa1 : 1

fa2 : None

fa3 : None

fa4 : None

fa5 : None

Show IPv6 MLD Max-Group

Syntax

show ipv6 mld max-group [interfaces IF_PORTS]

Parameter

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

Default

Show all ports ipv6 mld max-group.

Mode

Privileged mode

Usage

This command will display the ipv6 mld port max-group.

Example

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

Switch(config)#

interface fa1

```
Switch(config-if)#
   ipv6 mld max-groups 50
Switch(config-if)#
  exit
Switch(config)#
  exit
Switch#
  show ipv6 mld max-group
Port ID | Max Group
fa1 : 50
fa2 : 1024
fa3 : 1024
fa4 : 1024
fa5 : 1024
```

Show IPv6 MLD Port Max-Group Action

Syntax

show ipv6 mld max-group action [interfaces IF_PORTS]

Parameter

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

Default

Show all ports ipv6 mld max-group action.

Mode

Privileged mode

Usage

This command will display the ipv6 mld port max-group action.

Example

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

Switch(config)#

interface fa1

```
Switch(config-if)#
  ipv6 mld max-groups action replace
Switch(config-if)#
  exit
Switch(config)#
  exit
Switch#
  show ipv6 mld max-group action
Port ID | Max-groups Action
fa1 : replace
fa2 : deny
fa3 : deny
fa4 : deny
fa5 : deny
```

EnGenius®

Chapter 17
Port Security

Port Security

Syntax

port-security

no port-security

Parameter

None

Default

Default is disabled.

Mode

Global Configuration

Usage

The “port-security” command enables the port security functionality on the port. Use the no form of this command to disable it.

Example

The following example shows how to enable port security on port 1 and set the learning limit number to 10.

switch(config)#

interface fa1

```
switch(config-if)#
  port-security address-limit 10 action discard
switch(config-if)#
  port-security
switch(config)#
  show port-security interfaces fa1
Port | Mode | Security | CurrentAddr | Action
fa1 | Dynamic | Enabled ( 10) | 0 | Discard
```

Port-Security Address-Limit

Syntax

port-security address-limit <1-256> action (forward|discard|shutdown)

no dot1x port-control 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 10 and the action is “discard”.

Mode

Interface Configuration

Usage

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.

Example

The following example shows how to enable port security on port 1 and set the learning limit number to 10.

```
switch(config)#
  interface fa1
switch(config-if)#
  port-security address-limit 10 action discard
switch(config-if)#
  port-security
switch(config)#
  show port-security interfaces fa1
Port | Mode | Security | CurrentAddr | Action
fa1 | Dynamic | Enabled ( 10) | 0 | Discard
```

Show Port-Security Interface

Syntax

show port-security interface IF_PORTS

Parameter

IF_PORTS Select port to show port-security configurations.

Default

No default value for this command.

Mode

Privileged EXEC

Usage

Use “show port-security interfaces” command to show port-security information of the specified port.

Example

This example shows how to show port-security configurations on interface fa1.

Switch#

show port-security interfaces fa1

Port | Mode | Security | CurrentAddr | Action

fa1 | Dynamic | Enabled (10) | 0 | Discard

EnGenius®

Chapter 18
Port Error Disable

Errdisable Recovery Cause

Syntax

errdisable recovery cause (all | acl | broadcast-flood | bpduguard | psecure-violation | unicast-flood | unknown-multicast-flood | selfloop)

no errdisable recovery cause (all | acl | broadcast-flood | bpduguard |psecure-violation | unicast-flood | unknown-multicast-flood | selfloop)

Parameter

all	Enable/Disable to auto recovery for port error disabled by all reasons.
acl	Enable/Disable to auto recovery for port error disabled by ACL shutdown port reason.
broadcast-flood	Enable/Disable to auto recovery for port error disabled by storm control broadcast flood reason.
bpduguard	Enable/Disable to auto recovery for port error disabled by STP BPDU Guard reason.
psecure-violation	Enable/Disable to auto recovery for port error disabled by violate port security rule reason.
unicast-flood	Enable/Disable to auto recovery for port error disabled by storm control unicast flood reason.
unknown-multicast-flood	Enable/Disable to auto recovery for port error disabled by storm control unknown multicast flood reason.
selfloop	Enable/Disable to auto recovery for port error disabled by self loop detect reason.

Default

Default auto recover state for all reasons are disabled.

Mode

Global Configuration

Usage

The port will be disabled by invalid actions detected by various protocols. The administrator can enable these error disabled ports manually by the “no shutdown” command in Interface Mode, or just turn on the auto recovery mechanism by this command to auto enable the error disabled port after an auto recovery interval.

Example

This example shows how to enable auto recovery with reason bpduguard and broadcast-flood.

Switch(config)#

errdisable recovery cause bpduguard

Switch(config)#

errdisable recovery cause broadcastflood

This example shows how to show current auto recovery state of each reason and port error disabled status.

Switch#

show errdisable recovery

ErrDisable Reason | Timer Status

bpduguard | enabled

selfloop | disabled

broadcast-flood | enabled

unknown-multicast-flood | disabled

unicast-flood | disabled

acl | disabled

psecure-violation | disabled

Timer Interval : 300 seconds

Interfaces that will be enabled at the next timeout:

Port | Error Disable Reason | Time Left

Errdisable Recovery Interval

Syntax

errdisable recovery interval <0-86400>

Parameter

<0-86400> Specify the auto recovery interval with unit second.

Default

Default auto recovery interval is 300 second.

Mode

Global Configuration

Usage

The port will be disabled by invalid actions detected by various protocols. The auto recovery mechanism will enable these error disabled ports after awhile. This command configures how long the port will be enabled after an error disables it.

Example

This example shows how to configure the auto recovery interval to 600 seconds.

Switch(config)#

errdisable recovery interval 600

This example shows how to show current auto recovery interval

```
Switch#
  show errdisable recovery
ErrDisable Reason | Timer Status
bpduguard | enabled
selfloop | disabled
broadcast-flood | enabled
unknown-multicast-flood | disabled
unicast-flood | disabled
acl | disabled
psecure-violation | disabled
Timer Interval : 600 seconds
Interfaces that will be enabled at the next timeout:
Port | Error Disable Reason | Time Left
```

Show Errdisable Recovery

Syntax

show errdisable recovery

Parameter

None

Default

No default value for this command.

Mode

Privileged EXEC

Usage

Use the “show errdisable recovery” command to show each error disable state, error disable recovery interval, and current error disabled port status.

Example

This example shows how to show current auto recovery interval

Switch#

show errdisable recovery

ErrDisable Reason | Timer Status

bpduguard | enabled

selfloop | disabled

broadcast-flood | enabled

unknown-multicast-flood | disabled

unicast-flood | disabled

acl | disabled

psecure-violation | disabled

Timer Interval : 600 seconds

Interfaces that will be enabled at the next timeout:

Port | Error Disable Reason | Time Left

Chapter 19
Port

Description

Syntax

description WORD<1-32>

no description

Parameter

WORD<1-32> Specifiy port description string.

Default

Default port description is empty.

Mode

Interface Configuration

Usage

Use the “description” command to give the port a name to identify it easily. If the description includes a space character, please use double quotes. Use the no form to restore descriptions to the empty string.

Example

This example shows how to modify port descriptions.

Switch(config)#

interface fa1

Switch(config-if)#

description userport

Switch(config-if)#

exit

Switch(config)#

interface fa2

Switch(config-if)#

description “uplink port”

This example shows how to show current port description on interface fa1 and fa2

Switch#

show interfaces fa1-2 status

Port Name Status Vlan Duplex

Speed Type

fa1 userport notconnect 1 auto

auto Copper

fa2 uplink port notconnect 1 auto

auto Copper

Speed

Syntax

speed (10 | 100 | 1000)

speed auto [(10 | 100 | 1000 | 10/100)]

Parameter

10	Specify port speed to force 10Mbits/s or auto with 10Mbits/s ability.
100	Specify port speed to force 100Mbits/s or auto with 100Mbits/s ability.
1000	Specify port speed to force 1000Mbits/s or auto with 1000Mbits/s ability.
10/100	Specify port speed to auto with 10Mbits/s and 100Mbits/s

Default

Default port speed is auto with all available abilities.

Mode

Interface Configuration

Usage

Use the "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.

Example

This example shows how to modify port speed configuration.

```
Switch(config)#
  interface fa1
Switch(config-if)#
  speed 100
Switch(config-if)#
  exit
Switch(config)#
   interface fa2
Switch(config-if)#
  speed auto 10/100
```

This example shows how to show current speed configuration

```
Switch#
  show running-config interfaces fa1-2
interface fa1
speed 100
interface fa2
```

speed auto 10/100

This example shows how to show current interface link speed

Switch#

show interfaces fa1-2 status

Port Name Status Vlan Duplex

Speed Type

fa1 connected 1 a-full

a-100M Copper

fa2 connected 1 a-full

a-100M Copper

Duplex

Syntax

duplex (auto | full | half)

Parameter

auto Specify port duplex to auto negotiation.

full Specify port duplex to force full duplex.

half Specify port duplex to force half duplex.

Default

Default port duplex is auto.

Mode

Interface Configuration

Usage

Use “duplex” command to change port duplex configuration.

Example

This example shows how to modify port duplex configuration.

```
Switch(config)#
   interface fa1
Switch(config-if)#
  duplex full
Switch(config-if)#
  exit
Switch(config)#
   interface fa2
Switch(config-if)#
  duplex half
```

This example shows how to show current speed configuration

```
Switch#
  show running-config interfaces fa1-2
interface fa1
duplex full
interface fa2
```

duplex half

This example shows how to show current interface link speed

Switch#

show interfaces fa1-2 status

Port Name Status Vlan Duplex

Speed Type

fa1 connected 1 full

a-100M Copper

fa2 connected 1 half

a-100M Copper

Flow-Control

Syntax

flow-control (off | on)

no flow-control

Parameter

Off	Disable port flow control.
On	Enable port flow control.

Default

Default port flow control is off.

Mode

Interface Configuration

Usage

Use the “flow-control” command to change port flow control configurations. Use no form to restore flow control to default (off) configurations.

Example

This example shows how to modify the port duplex configuration.

Switch(config)#

interface fa1

```
Switch(config-if)#
  flow-control on
This example shows how to show current flow control configuration
Switch#
  show interfaces fa1
Hardware is Fast Ethernet
Full-duplex, Auto-speed, media type is Copper
flow-control is on
0 packets input, 0 bytes, 0 throttles
Received 0 broadcasts (0 multicasts)
0 runts, 0 giants, 0 throttles
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
0 multicast, 0 pause input
0 input packets with dribble condition detected
379 packets output, 31981 bytes, 0 underrun
0 output errors, 0 collisions, 0 interface resets
0 babbles, 0 late collision, 0 deferred
0 PAUSE output
```

Shutdown

Syntax

shutdown

no shutdown

Parameter

None

Default

Default port admin state is no shutdown.

Mode

Interface Configuration

Usage

Use the “shutdown” command to disable the port and use “no shutdown” to enable the port. If port is disabled for some reason, use the “no shutdown” command to recover the port manually.

Example

This example shows how to modify port duplex configuration.

Switch(config)#

interface fa1

Switch(config-if)#

shutdown

This example shows how to show current admin state configuration

Switch#

show running-config interfaces fa1

interface fa1

shutdown

This example shows how to show current link status

Port Name Status Vlan Duplex

Speed Type

fa1 disable 1 full

auto Copper

Jumbo-Frame

Syntax

jumbo-frame <64-9216>

Parameter

<64-9216> Specify the maximum frame size.

Default

Default maximum frame size is 1522.

Mode

Interface Configuration

Usage

Use the “jumbo-frame” command to modify the maximum frame size. The only way to show this configuration is by using the “show running-config” command.

Example

This example shows how to modify maximum the frame size on fa1 to 9216 bytes.

Switch(config)#

interface fa1

Switch(config-if)#

jumbo-frame 9216

This example shows how to show current jumbo-frmae size

Switch#

show running-config interface fa1

interface fa1

jumbo-frame 9216

Protected

Syntax

protected

no protected

Parameter

<64-9216> Specify the maximum frame size.

Default

Default protected state is no protected.

Mode

Interface Configuration

Usage

Use the “protected” command to make the port protected. A protected port is only allowed to communicate with an unprotected port. In other words, a protected port is not allowed to communicate with another protected port. Use the no form to make a port unprotected.

Example

This example shows how to configure port fa1 and fa2 to be protected port.

```
Switch(config)#
  interface range fa1-2
Switch(config-if-range)#
  protected
```

This example shows how to show current protected port state.

```
Switch#
  show interfaces fa1-2 protected
Port | Protected State
fa1 |enabled
fa2 |enabled
```

EEE

Syntax

eee

no eee

Parameter

None

Default

Default eee state is disabled.

Mode

Interface Configuration

Usage

Use the “eee” command to make a port enabled for the energy efficient Ethernet feature and use “no eee” command to disable it. The only way to show this configuration is using “show running-config” command.

Example

This example shows how to configure port fa1 and fa2 to be protected port.

Switch(config)#

interface fa1

Switch(config-if)#

eee

This example shows how to show current jumbo-frmae size

Switch#

show running-config interface fa1

interface fa1

eee

Clear Interface

Syntax

clear interfaces IF_PORTS counters

Parameter

IF_PORTS Specifiy port to clear counters.

Default

No default value for this command.

Mode

Privileged EXEC

Usage

Use the “clear interface” command to clear counters on specific ports.

Example

This example shows how to clear counters on port fa1.

Switch(config)#

clear interfaces fa1 counters

This example shows how to show current counters

```
Switch#
  show interfaces fa1
Hardware is Fast Ethernet
Auto-duplex, Auto-speed, media type is Copper
flow-control is off
0 packets input, 0 bytes, 0 throttles
Received 0 broadcasts (0 multicasts)
0 runts, 0 giants, 0 throttles
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
0 multicast, 0 pause input
0 input packets with dribble condition detected
0 packets output, 0 bytes, 0 underrun
0 output errors, 0 collisions, 0 interface resets
0 babbles, 0 late collision, 0 deferred
0 PAUSE output
```

Show Interface

Syntax

show interfaces IF_PORTS

show interfaces IF_PORTS status

show interfaces IF_PORTS potected

Parameter

IF_PORTS Specifiy port to show.

Default

No default value for this command.

Mode

Privileged EXEC

Usage

Use “show interface” command to show port counters, parameters and status.

Example

This example shows how to show current counters

Switch#

show interfaces fa1

Hardware is Fast Ethernet

Auto-duplex, Auto-speed, media type is Copper

flow-control is off

0 packets input, 0 bytes, 0 throttles

Received 0 broadcasts (0 multicasts)

0 runts, 0 giants, 0 throttles

0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored

0 multicast, 0 pause input

0 input packets with dribble condition detected

0 packets output, 0 bytes, 0 underrun

0 output errors, 0 collisions, 0 interface resets

0 babbles, 0 late collision, 0 deferred

0 PAUSE output

This example shows how to show current protected port state.

Switch#

show interfaces fa1-2 protected

Port | Protected State

fa1 |enabled

fa2 |enabled

This example shows how to show current port status

Switch#

show interfaces fa1-2 status

Port Name Status Vlan Duplex

Speed Type

fa1 connected 1 full

a-100M Copper

EnGenius®

Chapter 20
QoS

QoS

Syntax

qos [(advanced | basic)]

no qos

Parameter

Advanced	Specify the device to qos advanced mode
Basic	Specify the device to qos basic mode

Default

Default qos mode is disabled.

Mode

Global Configuration

Usage

QoS havs the following 3 modes; use this command to switch between them.

Disable: QoS function is disabled and all packets will go through lowest priority

queue. It means first in will be first out, no QoS is guarantee.

Basic: According to basic trust type to assign queue for packets, and packets with higher priority are able to send first.

Advanced: Use ACL to classify packets to achieve flow-based QoS and do different kind of actions for different type of packets.

Example

This example shows how to change qos to basic mode.

Switch(config)#

qos basic

Switch(config)#

qos

This example shows how to change qos to advanced mode.

Switch(config)#

qos advanced

This example shows how to change qos to disabled mode.

Switch(config)#

no qos

This example shows how to check current qos mode.

Switch#

show qos

QoS Mode: basic

Basic trust: cos

QoS Trust (1)

Syntax

qos trust (cos | cos-dscp | dscp | precedence)

Parameter

cos	Specify the device to trust CoS
cos-dscp	Specify the device to trust DSCP for IP packets, and trust CoS for non-IP packets.
dscp	Specify the device to trust DSCP
precedence	Specify the device to trust IP Precedence

Default

Default qos basic mode trust type is cos

Mode

Global Configuration

Usage

In QoS basic mode, there are 4 trust types for device to judge the appropriate queue of the packets. This command is able to switch between these trust types.

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.

Example

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

Switch(config)#

qos trust cos

Switch(config)#

qos trust cos-dscp

Switch(config)#

qos trust dscp

Switch(config)#

qos trust precedence

This example shows how to check current qos trust type.

Switch#

show qos

QoS Mode: basic

Basic trust: cos

QoS Map

Syntax

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

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

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

Parameter

cos-queue	Configure or show CoS to queue map
dscp-queue	Configure or show DSCP to queue map
precedence-queue	Configure or show IP Precedence to queue map.
queue-cos	Configure or show queue to CoS map
queue-dscp	Configure or show queue to DSCP map
queue-precedence	Configure or show queue to IP Precedence map
SEQUENCE	Specify the cos, dscp, precedence or queue with one or multiple values.
<1-8>	Specify th queue id
<0-7>	Specify the cos or precedence values
<0-63>	Specify the dscp values

Default

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

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

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

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

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

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

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

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

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

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

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

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

Mode

Global Configuration

Usage

According to different trust types, packets will be assigned to different queues based on the specific qos map. For example, if the trust type is trust cos, the device will get the cos value in a packet and reference the cos-queue mapping to assign the correct queue. The queue to cos, dscp or precedence maps are used by a remarking feature. If the port remarking feature is enabled, the remarking function will reference these 3 tables to remark packets.

Example

This example shows how to map cos 6 and 7 to queue 1.

Switch(config)# qos map cos-queue 6 7 to 1

Switch(config)# 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

This example shows how to map queue 4 and 5 to cos 7.

Switch(config)#

qos map queue-cos 4 5 to 7

Switch(config)#

show qos map queue-cos

Queue to CoS mappings

Queue 1 2 3 4 5 6 7 8

Queue to CoS mappings

Queue 1 2 3 4 5 6 7 8

CoS 1 0 2 7 7 5 6 7

QoS Queue

Syntax

qos queue strict-priority-num <0-8>

qos queue weight SEQUENCE

show qos queueing

Parameter

strict-prioritynum <0-8>	Specify the strict priority queue number weight
SEQUENCE	Specify the non-strict priority queue weight value. The valid queue weight value is from 1 to 127.

Default

Default strict priority queue number is 8, it means all queues are strict priority queue.

The default queue weight for each queue is shown in following table.

Queue ID	Queue Weight
1	1
2	2
3	3
4	4
5	5
6	9
7	13
8	15

Mode

Global Configuration

Usage

The device support total 8 queues for QoS queueing. It is able to set the queue to be strict priority queue or weighted queue to prevent starvation. The queue with higher id value has higher priority. First, you need to decide how many strict priority queue you need. The strict priority queue will always occupy the higher priority queue. For example, if you specify the strict priority number to be 2, then the queue 7 and 8 will be the strict priority queues and the others are weighted queues. After you setup the number of strict priority queue, you need to setup the weight for the weighted queues by using "qos queue weight" command. And the bandwidth will shared by the weight you configured between these weighted queues.

Example

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

```
Switch(config)#
  qos queue strict-priority-num 3
Switch(config)#
  qos queue weight 5 10 15 20 25
Switch#
  show qos queueing
qid-weights Ef - Priority
1 - 5 dis- N/A
2 - 10 dis- N/A
3 - 15 dis- N/A
4 - 20 dis- N/A
5 - 25 dis- N/A
6 - N/A ena- 6
7 - N/A ena- 7
8 - N/A ena- 8
```

QoS CoS

Syntax

qos cos <0-7>

Parameter

cos <0-7> Specify the CoS value for the interface.

Default

Default CoS value for interface is 0.

Mode

Interface Configuration

Usage

Sometimes, there is no qos information in the packets, such as CoS, DSCP, IP Precedence. But you 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 the “qos cos” command to assign a port default cos value.

Example

This example shows how to configure default cos value 7 on interface fa1.

Switch(config)#

interface fa1

```
Switch(config-if)#
  qos cos 7
Switch(config-if)#
  end
Switch#
  show qos interfaces fa1
Port | CoS | Trust State | Remark Cos | Remark DSCP | Remark IP Prec
fa1 | 7 | enabled | disabled | disabled |
```

QoS Trust (2)

Syntax

qos trust

no qos trust

Parameter

None

Default

Default interface qos trust state is enabled.

Mode

Interface Configuration

Usage

After the QoS function is enabled in basic mode, the device also supports a per interface enable/disable qos function. If the trust state on the 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 be assigned to queue 1. Use “qos trust” to enable the trust state on the interface and use “no qos trust” to disable the trust state on the interface.

Example

This example shows how to disable qos trust state on interface fa1.

```
Switch(config)#
  interface fa1
Switch(config-if)#
  no qos trust
Switch(config-if)#
   end
Switch#
  show qos interfaces fa1
Port | CoS | Trust State | Remark Cos | Remark DSCP | Remark IP Prec
fa1 | 0 | disabled | disabled | disabled |
```

QoS Remark

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

Usage

the QoS remarking feature allows you to change priority information in packets based on an egress queue. For example, if 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 th e“qos remark” command to enable remarking feature on specific type.And use “no qow remark” command to disable it.

Example

This example shows how to enable remarking features on interface fa1.

```
Switch(config)#
   interface fa1
Switch(config-if)#
  qos remark cos
Switch(config-if)#
   qos remark dscp
Switch(config-if)#
   qos remark precedence
Switch(config-if)#
  end
Switch#
  show qos interfaces fa1
Port | CoS | Trust State | Remark Cos | Remark DSCP | Remark IP Prec
fa1 | 0 | enabled | enabled | enabled | enabled
```

Show QoS

Syntax

show qos

Parameter

None

Default

No default value for this command.

Mode

Privileged EXEC

Usage

Use “show qos” command to show qoe mode and trust type.

Example

This example shows how to check current qos mode.

Switch#

show qos

QoS Mode: basic

Basic trust: cos

Show QoS Map

Syntax

show qos map [(cos-queue | dscp-queue | precedence-queue | queue-cos |

queue-dscp | queue-precedence)]

Parameter

cos-queue	Show CoS to queue map.
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.

Default

No default value for this command.

Mode

Privileged EXEC

Usage

Use “show qos map” command to show all kinds of mapping for qos remapping and remarking features.

Example

Example

This example shows how to show all qos maps.

```
Switch(config)#
  show qos map
CoS to Queue mappings
COS 0 1 2 3 4 5 6 7
Queue 2 1 3 4 5 6 7 8
DSCP to Queue mappings
d1: d2 0 1 2 3 4 5 6 7 8 9
0: 1 1 1 1 1 1 1 1 2 2
1: 2 2 2 2 2 2 3 3 3 3
2: 3 3 3 3 4 4 4 4 4 4
3: 4 4 5 5 5 5 5 5 5 5
4: 6 6 6 6 6 6 6 6 7 7
5: 7 7 7 7 7 7 8 8 8 8
6: 8 8 8 8
IP Precedence to Queue mappings
IP Precedence 0 1 2 3 4 5 6 7
```

Queue 1 2 3 4 5 6 7 8

Queue to CoS mappings

Queue 1 2 3 4 5 6 7 8

CoS 1 0 2 3 4 5 6 7

Queue to DSCP mappings

Queue 1 2 3 4 5 6 7 8

DSCP 0 8 16 24 32 40 48 56

Show QoS Interface

Syntax

show qos interface IF_PORTS

Parameter

IF_PORTS Select port to show qos configurations.

Default

No default value for this command.

Mode

Privileged EXEC

Usage

Use the “show qos interfaces” command to show port default cos ,remarking state, and remarking type state informations.

Example

This example shows how to show qos configurations on interface fa1.

Switch#

show qos interfaces fa1

Port | CoS | Trust State | Remark Cos | Remark DSCP | Remark IP Prec

fa1 | 7 | enabled | disabled | disabled | disabled |

EnGenius®

Chapter 21
Rate Limit

Rate Limit

Syntax

rate-limit ingress <0-1000000>

no rate-limit ingress

rate-limit egress <0-1000000> [<128-56319>]

rate-limit egress queue <1-8> <0-1000000> [<1024-56319>]

no rate-limit egress [<1-8>]

Parameter

Cir	Specify the maximum number of kilobits per second of ingress traffic on a port. The range is 100 - max port speed.
Cbs	Specify the maximum permitted excess burst size (CBS) in bytes
<1-8>	Specify the egress shaper queue number

Default

Rate limiting is disabled.

Mode

Interface configuration

Usage

Use the rate-limit ingress Interface Configuration mode command to limit the incoming traffic rate on a port. Use the no form of this command to disable the rate limit Use the rate-limit egress Interface Configuration mode command to configure the egress port or queue shaper. Use the no form of this command to disable the shaper. You can verify your settings by entering the show running-config interfaces Privileged EXEC command.

Example

The following example shows how to configure ingress port rate limit and egress port & queue shaper.

Switch(config)#

interfaces fa7

Switch(config-if)#

rate-limit ingress 128

Switch(config-if)#

rate-limit egress 2048

Switch(config-if)#

rate-limit egress queue 1 512 1024

Switch#

show running-config interfaces fa7interface fa7

rate-limit ingress 128

rate-limit egress 2048 165

rate-limit egress queue 1 512 1024

VLAN Rate Limit

Syntax

rate-limit ingress <0-1000000> <9216-1000000> vlan <1-4094>

no rate-limit vlan <1-4094>

Parameter

<0-1000000>	Specify the average traffic rate (CIR) in 16 Kbps
<9216-1000000>	Specify the maximum burst size (CBS) in 128 bytes
<1-4094>	

Default

No vlan ratelimit are configured

Mode

Global Configuration or Interface Configuration

Usage

Use the rate-limit ingress vlan global configuration command or Interface Configuration to add Per VLAN RateLimit or Per VLAN Per Port RateLimit Settings. Use the no form of this command to delete the vlan ratelimit setting. You can verify your settings by entering the show rate-limit vlan Privileged EXEC command.

Example

Switch(config)#

rate-limit input 256 9216 vlan 2

Switch(config)#

interface fa1

Switch(config-if)#

rate-limit input 1024 9216 vlan 4

Switch(config)#

show rate-limit vlan

VLAN | Port | rate-limit [Kbps] | Burst [Bytes]

2 | ALL | 256 | 9216

4 | fa1 | 1024 | 9216

Show Rate Limit VLAN

Syntax

show rate-limit vlan [<1-4094>]

Parameter

<1-4094> Specify the rate-limit VLAN to display

Default

None

Mode

Privileged EXEC

Usage

Use the show rate-limit vlan command in EXEC mode to display VLAN RateLimit settings.

Example

This example shows how to display VLAN RateLimit setting

Switch(config)#

show rate-limit vlan

VLAN | Port | rate-limit [Kbps] | Burst [Bytes]

2 | ALL | 256 | 9216

4 | fa1 | 1024 | 9216

EnGenius®

Chapter 22
RMON

RMON Event

Syntax

rmon event <1-65535> [log] [trap COMMUNITY] [description

DESCRIPTION] [owner NAME]

no rmon event <1-65535>

Parameter

<1-65535>	Specify event index to create or modify.
[log]	(Optional)Specify to show syslog.
[trap COMMUNITY]	(Optional)Specify SNMP community to show SNMP trap.
[description DESCRIPTION]	(Optional)Specify description of event
[owner NAME]	(Optional)Specify owner of event.

Default

No default is defined.

Mode

Global Configuration

Usage

Use the rmon alarm command to add or modify a RMON alarm entry. Use the no form of this command to delete it.

Example

The example shows how to add a RMON event entry with log and trap action and then modify it action to log only. You can verify settings by the following show rmon event command.

```
switch(config)#
   rmon event 1 log trap public description test owner admin
switch(config)#
  show rmon event 1
Rmon Event Index : 1
Rmon Event Type : Log and Trap
Rmon Event Community : public
Rmon Event Description : test
Rmon Event Last Sent :
Rmon Event Owner : admin
switch(config)#
  rmon event 1 log description test owner admin
switch(config)#
  show rmon event 1
```

Rmon Event Index : 1

Rmon Event Type : Log

Rmon Event Community : public

Rmon Event Description : test

Rmon Event Last Sent :

Rmon Event Owner : admin

RMON Alarm

Syntax

rmon alarm <1-65535> interface IF_PORT (drop-events|octets|pkts|broadcast-pkts|multicast pkts|crc-align-errors|undersize-pkts|oversize-pkts|fragments|jabbers|collisions|pkts64octets|pkts65to127octets|pkts128to255octets|pkts256to511octets|pkts512to1023octets|pkts1024to1518octets) <1-2147483647> (absolute|delta) rising <0-2147483647> <0-65535>falling <0-2147483647> <0-65535> startup (rising|rising-falling|falling) [owner NAME]no rmon alarm <1-65535>

Parameter

<1-65535>	Specify alarm index to create or modify
IF_PORT	Specify the interface to sample
(variable)	Specify a mib object to sample
<1-2147483647>	Specify the time in seconds that the alarm monitors the MIB variable.
(absolute|delta)	Specify absolute to compare sample counter absolutely.Specify delta to compare delta counter between samples
<0-2147483647>	Specify a number which the alarm trigger risingevent
<0-65535>	Specify event index when the rising threshold exceeds.
<0-2147483647>	Specify a number which the alarm trigger falling event
<0-65535>	Specify event index when the falling threshold exceeds.
(rising|risingfalling| falling)	Specify only to how rising or falling startup event. Or show either rising or falling startup event.
[owner NAME]	(Optional) Specify owner of alarm.

Default

No default is defined.

Mode

Global Configuration

Usage

Use the rmon event command to add or modify a RMON event entry. Before you add an alarm entry, at least one event entry must be added. Use the no form of this command to delete it.

Example

The example shows how to add a RMON alarm entry that sample interface fa1 packets delta count every 300 seconds. A Trigger event of index 1 occurs if it is over rising a threshold of 10000, or a trigger event index of 2 if lit is ower than the falling threshold. You can verify settings by the following show rmon alarm command.

```
switch(config)#
  rmon event 1 log
switch(config)#
   rmon event 2 log
switch(config)#
  show rmon event all
Rmon Event Index : 1
Rmon Event Type : Log
```

Rmon Event Community :

Rmon Event Description :

Rmon Event Last Sent :

Rmon Event Owner :

Rmon Event Index : 2

Rmon Event Type : Log

Rmon Event Community :

Rmon Event Description :

Rmon Event Last Sent :

Rmon Event Owner :

Switch(config)#

rmon alarm 1 interface fa1 pkts 300 delta rising 10000 1falling 100 1 startup rising-falling owner admin

Rmon Alarm Index : 1

Rmon Alarm Sample Interval : 300

Rmon Alarm Sample Interface : fa1

Rmon Alarm Sample Variable : Pkts

Rmon Alarm Sample Type : delta

Rmon Alarm Type : Rising or Falling

Rmon Alarm Rising Threshold : 10000

Rmon Alarm Rising Event : 1

Rmon Alarm Falling Threshold : 100

Rmon Alarm Falling Event : 1

Rmon Alarm Owner : admin

RMON History

Syntax

rmon history <1-65535> interface IF_PORT [buckets <1-65535>]

[interval <1-3600>] [owner NAME]

no rmon history <1-65535>

Parameter

<1-65535>	Specify history index to create or modify.
IF_PORT	Specify the interface to sample
[bucket <1-65535>]	(Optional) Specify the maximum number of buckets.
[interval <>1-3600]	(Optional) Specify time interval for each sample
[owner NAME]	(Optional)Specify owner of history

Default

No default is defined.

Mode

Global Configuration

Usage

Use the rmon history command to add or modify a RMON history entry. Use the no form of this command to delete it.

Example

The example shows how to add a RMON history entry that monitors interface fa1 every 60 seconds and then modify it to monitor every 30 seconds. You can verify settings by the following show rmon history command.

```
switch(config)#
  rmon history 1 interface fa1 interval 60 owner admin
switch(config)#
  show rmon history 1
Rmon History Index : 1
Rmon Collection Interface: fa1
Rmon History Bucket : 50
Rmon history Interval : 60
Rmon History Owner : admin
switch(config)#
  rmon history 1 interface fa1 interval 30 owner admin
switch(config)#
   show rmon history 1
Rmon History Index : 1
Rmon Collection Interface: fa1
Rmon History Bucket : 50
```

Rmon history Interval : 30

Rmon History Owner : admin

Clear RMON Interfaces Statistics

Syntax

clear rmon interfaces IF_PORTS statistics

Parameter

IF_PORTS specifies ports to clear

Default

No default is defined

Mode

Global Configuration

Usage

Use the clear rmon interfaces statistics command to clear RMON etherStat statistics those are recorded on interface.

Example

The example shows how to clear RMON etherStat statistics on interface gi1. You can verify settings by the following show rmon interface statistics command.

switch#

clear rmon interfaces gi1 statistics

```
switch#
  show rmon interfaces gi1 statistics
Port gi1
etherStatsDropEvents : 0
etherStatsOctets : 0
etherStatsPkts : 0
etherStatsBroadcastPkts : 0
etherStatsMulticastPkts : 0
etherStatsCRCAlignErrors : 0
etherStatsUnderSizePkts : 0
etherStatsOverSizePkts : 0
etherStatsFragments : 0
etherStatsJabbers : 0
etherStatsCollisions : 0
etherStatsPkts64Octets : 0
etherStatsPkts65to127Octets : 0
etherStatsPkts128to255Octets : 0
etherStatsPkts256to511Octets : 0
```

etherStatsPkts512to1023Octets : 0

etherStatsPkts1024to1518Octets : 0

Show RMON Interfaces Statistics

Syntax

show rmon interfaces IF_PORTS statistics

Parameter

IF_PORTS specifies ports to show

Default

No default is defined

Mode

Global Configuration

Usage

Use the show rmon interfaces statistics command to show RMON etherStat statistics of the interface.

Example

The example shows how to show RMON etherStat statistics of interface gi1.

```
switch(config)#
  show rmon interfaces gi1 statistics
Port gi1
etherStatsDropEvents : 0
```

etherStatsOctets : 81882

etherStatsPkts : 578

etherStatsBroadcastPkts : 10

etherStatsMulticastPkts : 0

etherStatsCRCAlignErrors : 0

etherStatsUnderSizePkts : 0

etherStatsOverSizePkts : 0

etherStatsFragments : 0

etherStatsJabbers : 0

etherStatsCollisions : 0

etherStatsPkts64Octets : 355

etherStatsPkts65to127Octets : 126

etherStatsPkts128to255Octets : 0

etherStatsPkts256to511Octets : 42

etherStatsPkts512to1023Octets : 55

etherStatsPkts1024to1518Octets : 0

Show RMON Event

Syntax

show rmon event (<1-65535> | all)

Parameter

<1-65535> specifies event index to show

all Show all existed event

Default

No default is defined

Mode

Global Configuration

Usage

Use the show rmon event command to show an existing RMON event entry.

Example

The example shows how to show a rmon event entry.

switch(config)#

rmon event 1 log trap public description test owner admin

```
switch(config)#
  show rmon event 1
Rmon Event Index : 1
Rmon Event Type : Log and Trap
Rmon Event Community : public
Rmon Event Description : test
Rmon Event Last Sent :
Rmon Event Owner : admin
```

Show RMON Event Log

Syntax

show rmon event <1-65535> log

Parameter

<1-65535> specifies event index to show event log

Default

No default is defined

Mode

Global Configuration

Usage

Use the show rmon event log command to show a log triggered by a RMON alarm.

Example

The example shows how to show a rmon event log.

```
switch(config)#
  show rmon event 1 log
Index : 1
Alarm Index : 1
```

Action : Startup Falling

Time : (32918334) 3 days, 19:26:23.34

Description : fa1.Pkts=0 <= 100

Show RMON Alarm

Syntax

show rmon alarm (<1-65535> | all)

Parameter

<1-65535>	specifies alarm index to show
all	Show all existed alarm

Default

No default is defined

Mode

Global Configuration

Usage

Use the show rmon alarm command to show existing RMON alarm entries.

Example

The example shows how to show an rmon alarm entry.

Switch(config)#

rmon alarm 1 interface fa1 pkts 300 delta rising 10000 1

falling 100 1 startup rising-falling owner admin

Rmon Alarm Index : 1

Rmon Alarm Sample Interval : 300

Rmon Alarm Sample Interface : fa1

Rmon Alarm Sample Variable : Pkts

Rmon Alarm Sample Type : delta

Rmon Alarm Type : Rising or Falling

Rmon Alarm Rising Threshold : 10000

Rmon Alarm Rising Event : 1

Rmon Alarm Falling Threshold : 100

Rmon Alarm Falling Event : 1

Rmon Alarm Owner : admin

Show RMON History

Syntax

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

Parameter

<1-65535>	specifies history index to show
All	Show all existed history

Default

No default is defined

Mode

Global Configuration

Usage

Use the show rmon history command to show existing RMON history entries.

Example

The example shows how to show an RMON history entry.

switch(config)#

rmon history 1 interface fa1 interval 30 owner admin

```
switch(config)#
   show rmon history 1
Rmon History Index : 1
Rmon Collection Interface: fa1
Rmon History Bucket : 50
Rmon history Interval : 30
Rmon History Owner : admin
```

Show RMON History Statistics

Syntax

show rmon history <1-65535> statistic

Parameter

<1-65535> specifies history index to show history statistic

Default

No default is defined

Mode

Global Configuration

Usage

Use the show rmon history statistic command to show statistics that are recorded by RMON history.

Example

The example shows how to show RMON history statistics.

switch(config)#

show rmon history 1 statistics

Sample Index : 2

Interval Start : (32940466) 3 days, 19:30:04.66

DropEvents : 0

Octets : 117226

Pkts : 763

BroadcastPkts : 9

MulticastPkts : 0

CRCAlignErrors : 0

UnderSizePkts : 0

OverSizePkts : 0

Fragments : 0

Jabbers : 0

Collisions : 0

Utilization : 1

Sample Index : 1

Interval Start : (32939462) 3 days, 19:29:54.62

DropEvents : 0

Octets : 220

Pkts : 3

BroadcastPkts : 1

MulticastPkts : 0

CRCAlignErrors : 0

UnderSizePkts : 0

OverSizePkts : 0

Fragments : 0

Jabbers : 0

Collisions : 0

Utilization : 0

EnGenius®

Chapter 23
SNMP

SNMP

Syntax

snmp

no snmp

Parameter

None

Default

no snmp

Mode

Global Configuration

Usage

'no snmp' will disable snmp. 'snmp' will enable snmp. The configuration can use show snmp.

Example

The following example specifies the set global snmp test.

Switch(config)#

snmp

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

SNMP Trap

Syntax

[no] snmp trap (auth|linkUpDown|warm-start|cold-start|port-security)

Parameter

None

Default

snmp trap auth

snmp trap linkUpDown

snmp trap warm-start

snmp trap cold-start

snmp trap port-security

Mode

Global Configuration

Usage

'no snmp trap auth' snmp will not send auth failure trap. 'no snmp trap linkUpDown' snmp will not send linkup and link down trap. 'no snmp trap warm-start snmp will not send warm start trap. 'no snmp trap cold-start' snmp will not send cold start trap.'no snmp trap port-security' snmp will not send port-security trap. The configuration can use show snmp trap.

Example

The following example specifies the set trap auth disable test.

```
Switch(config)#
  no snmp auth
Switch#
  show snmp trap
SNMP auth failed trap : Disable
SNMP linkUpDown trap : Enable
SNMP warm-start trap : Enable
SNMP cold-start trap : Enable
SNMP port security trap: Enable
```

SNMP View

Syntax

snmp view NAME subtree OID oid-mask (all | MASK) viewtype

(included | excluded)

no snmp view NAME subtree (all |OID)

Parameter

Name	View Name
OID	View subtree OID
(all | MASK)	View subtree OID mask. All: all mask bit is '1'
(include | exclude)	View subtree is accessed or not allowed access.
(all | OID)	Delete the View name all subtree OID or specifies OID

Default

Default View is "all" and the subtree is 1. The type is included.

Mode

Global Configuration

Usage

The default view can't delete and be created by the user. The min view is sysUpTime. The configuration can use 'show snmp view' to check it.

Example

The following example specifies the set view systemView test.

```
Switch(config)#
  snmp view systemView subtree 1.3.6.1.2.1.1 oid-mask all viewtype included
Switch#
  show snmp view
View Name Subtree OID OID Mask View Type
all .1 all included
systemView .1.3.6.1.2.1.1 all included
```

SNMP Access Group

Syntax

snmp group NAME version (1 |2c |3) (noauth | auth | priv) read-view

NAME write-view NAME [notify-view NAME]

no snmp group NAME security-mode version (1 |2c | 3)

Parameter

Group Name	Access group name
1 | 2c | 3	Access model for snmp v1/v2/v3
noauth | auth | priv	Noauth for snmp v1/v2 Auth and priv group for snmp v3
Read-view	Name Access group specifies read view
Write-view	Name Access group specifies write view
Notify-view	Name Access group specifies notify view

Default

None

Mode

Global Configuration

Usage

The group version 1 and 2c are only for snmp community use. Version 3 is only for snmp user use. When the group version is 1 or 2c , You can only use noauth. The read/write/notify view must exist to proceed. The configuration can use 'show snmp group' to check.

Example

The following example specifies that set snmp group test.

Switch(config)#

snmp group group1 1 noauth read-view all write-viw ""

Switch(config)#

snmp group group2 2c noauth read-view all write-view all

Switch(config)#

snmp group group3 3 auth read-view all write-view all

Switch#

show snmp group

Group Name Model Level ReadView WriteView NotifyView

group1 v1 noauth all --- ---

group2 v2c noauth all all ---

group3 v3 auth all all ---

SNMP Community

Syntax

snmp community NAME [group NAME] [view NAME] (ro|rw)

no snmp community NAME

Parameter

Community Name	Snmp v1/v2 community name
[group Name]	Snmp community specifies access group name
[view Name]	Snmp community specifies view
(ro | rw)	Snmp community read or readwrite attribute

Default

None

Mode

Global Configuration

Usage

The community can't specify group and view at the same time. The community specifies the group which must exist and must match the security model. The community specifies the view which must exist as well. It will generate the no exist v1 or v2 access group for the community. The configuration can use 'show snmp community' to check.

Example

The following example specifies that configured community test.

Switch(config)#

snmp communit public ro

Switch(config)#

snmp communit private rw

Switch(config)#

snmp communit test1 view all

Switch#

show snmp comunity

Commnunity Name Group Name View Access

public public_group all ro

private private_group all rw

test1 test1_group all rw

SNMP User

Syntax

snmp user USERNAME GROUPNAME [auth (md5|sha)

AUTHPASSWD]

snmp user USERNAME GROUPNAME auth (md5|sha)

AUTHPASSWD priv PRIVPASSWD

no snmp user NAME

Parameter

USERNAME	Snmp user name
GROUPNAME	Snmp user specifies group.
[auth (md5 | sha)]	Snmp user auth protocol
AUTHPASSWD	Snmp user auth password
PRIVPASSWD	Snmp user priv password

Default

None

Mode

Global Configuration

Usage

The group version must be v3 and the security level must match the snmp user configuration. The AUTHPASSWD and PRIVPASSWD min length is 8. The configuration can use 'show snmp user' to check.

Example

The following example specifies the set auth snmp user test.

Switch(config)#

snmp group group3 3 auth read-view all write-view all

Switch(config)#

snmp user user1 group3 auth md5 12345678

Switch# show snmp user

Username: user1

Password: ********

Privilege Mode: rw

Access GroupName: group3

Authentication Protocol: md5

Encryption Protocol: none

Access SecLevel: auth

SNMP EngineID

Syntax

snmp engineid (default | ENGINEID)

snmp engineid remote (A.B.C.D|X:X::X:X) ENGINEID

no snmp engineid remote (A.B.C.D|X:X::X:X)

Parameter

(default |ENGINEID)	Default is MAC address. ENGINEID is 10~64 hex characters
(A.B.C.D|X:X::X:X)	Host ipv4/ipv6 address

Default

Snmp engineid default

Mode

Global Configuration

Usage

The default engineid is DUT MAC address. The configuration can use ‘show snmp engineid’.

Example

The following example specifies that set remote engine id test.

```
Switch(config)#
   snmp engineid remote 192.168.1.100 112233445566
Switch#
   show snmp engineid
Local SNMPV3 Engine id: DEADBEEF0114
IP address Remote SNMP engineID
192.168.1.100 112233445566
```

SNMP Host

Syntax

snmp host (A.B.C.D|X:X::X:X|HOSTNAME) [(traps | informs)] [version (1|2c)] NAME [udp-port <1-65535>] [timeout <1-300>] [retries <1-255>] snmp host (A.B.C.D|X:X::X:X|HOSTNAME) [(traps | informs)] version 3 [(auth | noauth | priv)] NAME [udp-port <1-65535>] [timeout <1-300>] [retries <1-255>]

no snmp host (A.B.C.D|X:X::X:X|HOSTNAME) [(traps | informs)] [version (1|2c|3)]

Parameter

(A.B.C.D|X:X::X:X|HOST NAME)	Snmp trap host ipv4/ipv6 address or host name
[(traps | informs)]	Snmp notification type is traps or informs
[version (1|2c|3)]	V1/v2c/v3 traps
[(auth | noauth | priv)]	V3 trap for auth/noauth/priv
NAME	Snmp community name or user name
[udp-port <1-65535>]	The manage receive trap udp port num
[timeout <1-300>]	The notify type is inform timeout value
[retries <1-255>]	The notify type is inform retries

Default

None

Mode

Global Configuration

Usage

This command can't configure version 1 inform. When using traps, this command can't configure the udp-port and retries. The host useer NAME which is a snmp community or user NAME must exist. The host user host security level must match the snmp user security level The configuration can use 'show snmp host' to check

Example

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

Switch(config)#

snmp community public ro

Switch(config)#

snmp community private rw

Switch(config)#

snmp group group3 3 auth read-view all write-view all

Switch(config)#

snmp user user1 group3 auth md5 12345678

Switch(config)#

snmp host 192.168.1.100 version 2c public

Switch(config)#

snmp host 192.168.1.100 informs version 2c private

```
Switch(config)#
  snmp host 192.168.1.100 version 3 auth user1
Switch#
  show snmp host
Server Community Name Notification Version Notification
Type UDP Port Retries Timeout
192.168.1.100 public v2c trap
192.168.1.100 private v2c inform 200 3 10
192.168.1.100 user1 v3 trap
```

Show SNMP

Syntax

show snmp

Parameter

None

Default

None

Mode

Privileged mode

Usage

This command will show the snmp status.

Example

The following example specifies that show snmp test.

Switch#

show snmp

Show SNMP Trap

Syntax

show snmp trap

Parameter

None

Default

None

Mode

Privileged mode

Usage

This command will display the snmp trap class auth/linkupdown/cold-start/warmstart/ port-security/ status.

Example

The following example specifies the display snmp trap test.

Switch#

show snmp trap

Show SNMP View

Syntax

show snmp view

Parameter

None

Default

None

Mode

Privileged mode

Usage

This command will display the snmp view entry.

Example

The following example specifies the display snmp view test.

Switch#

show snmp view

Show SNMP Group

Syntax

show snmp group

Parameter

None

Default

None

Mode

Privileged mode

Usage

This command will display the snmp group.

Example

The following example specifies the display snmp group test.

Switch#

show snmp group

Show SNMP Community

Syntax

show snmp community

Parameter

None

Default

None

Mode

Privileged mode

Usage

This command will display the snmp community entry.

Example

The following example specifies the display snmp community test.

Switch#

show snmp community

Show SNMP Host

Syntax

show snmp host

Parameter

None

Default

None

Mode

Privileged mode

Usage

This command will display the snmp host entry.

Example

The following example specifies that display snmp host test.

Switch#

show snmp host

Show SNMP User

Syntax

show snmp user

Parameter

None

Default

None

Mode

Privileged mode

Usage

This command will display the snmp user entry.

Example

The following example specifies that display snmp user test.

Switch#

show snmp user

Show SNMP EngineID

Syntax

show snmp engineid

Parameter

None

Default

None

Mode

Privileged mode

Usage

This command will display the snmp local/remote engine id.

Example

The following example specifies the display snmp local/remote engine id test.

Switch#

show snmp engineid

EnGenius®

Chapter 24
Storm Control

Storm-Control Unit

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

Usage

The Storm Control mechanism will try to calculate if ingress packets exceed the configured rate or not and enact the corresponding action. This command allows you to change the unit of the calculating method.

Example

This example shows how to configure the Storm Control rate unit as pps.

Switch(config)#

storm-control unit pps

This example shows how to show the storm control global configuration.

```
Switch#
  show storm-control
Storm control preamble and IFG: Excluded
Storm control unit: pps
```

Storm-Control IFG

Syntax

storm-control ifg (include | exclude)

Parameter

include	Include preamble & IFG (20 bytes) when count ingress storm control rate.
exclude	Exclude preamble & IFG (20 bytes) when count ingress storm control rate

Default

Default storm control inter frame gap is excluded.

Mode

Global Configuration

Usage

The Storm Control mechanism will try to calculate if ingress packets exceed the configured rate or not and do the corresponding action. This command allows you to decide to include/exclude the preamble and inter frame gap into the calculation.

Example

This example shows how to configure the Storm Control rate unit as pps.

Switch(config)#

storm-control ifg include

This example shows how to show Storm Control global configuration.

```
Switch#
  show storm-control
Storm control preamble and IFG: Included
Storm control unit: pps
```

Storm-Control

Syntax

storm-control

no storm-control

storm-control (broadcast | unknown-unicast | unknown-multicast) no storm-control (broadcast | unknown-unicast | unknown-multicast)

storm-control (broadcast | unknown-unicast | unknown-multicast) level <0-1000000>

no storm-control (broadcast | unknown-unicast | unknown-multicast) level

Parameter

broadcast	Select broadcast storm control type
unknown-unicast	Select unknown unicast storm control type
unknownmulticast	Select unknown multicast storm control type
level <0-1000000>	Specify the storm control rate for selected type

Default

Default broadcast storm control is disabled.

Default unknown multicast storm control is disabled

Default unknown unicast storm control is disabled

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

Usage

The Storm Control function is able to enable/disable on each single port. Use the “storm control” command to enable the storm control feature on the selected ports. Use the “no storm control” command to disable the Storm Control feature. Not every port is able to enable/disable on each 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. Each control type is allowed to have a different storm control rate. Use the “stormcontrol (broadcast | unknown-unicast | unknown-multicast) level” command to configure it and use no form to restore to its default value.

Example

This example shows how to enable Storm Control on interface fa1.

Switch(config)#

interface fa1

Switch(config-if)#

storm-control

This example shows how to enable broadcast Storm Control and configure the broadcast storm control rate to 200.

Switch(config)#

interface fa1

Switch(config-if)#

storm-control broadcast

Switch(config-if)#

storm-control broadcast level 200

This example shows how to show the current storm control configuration on interface fa1.

Switch#

show storm-control interfaces fa1

Port | State | Broadcast | Unkown-Multicast | Unknown-Unicast | Action|

| pps | pps | pps

fa1 enable 200 Off(10000) Off(10000)

Shutdown

Storm-Control Action

Syntax

storm-control action (drop | shutdown)

no storm-control action

Parameter

drop	Storm control rate calculates by octet-based
shutdown	

Default

Default storm control action is drop.

Mode

Interface Configuration

Usage

The storm control mechanism allows you to drop packets which exceed the Storm Control rate or just shutdown the port. Use no form to restore to default actions.

Example

This example shows how to configure Storm Control action to shutdown the port on interface fa1.

```
Switch(config)#
  interface fa1
Switch(config-if)#
  storm-control action shutdown
```

This example shows how to show the Storm Control action on interface fa1.

```
Switch#
  show storm-control interfaces fa1
Port | State | Broadcast | Unkown-Multicast | Unknown-Unicast | Action|
| pps | pps | pps
fa1 disable Off( 10000) Off( 10000) Off( 10000)
Shutdown
```

Show Storm-Control

Syntax

show storm-control

show storm-control interface IF_PORTS

Parameter

IF_PORTS Specify port to show.

Default

No default value for this command

Mode

Privileged EXEC

Usage

Use the “show storm-control” command to show all Storm Control related configurations including global configuration and per port configurations. Use the “show storm-control interface” command to show selected port Storm Control configurations.

Example

This example shows how to show storm control global configuration.

Switch#

show storm-control

Storm control preamble and IFG: Excluded

Storm control unit: pps

This example shows how to show current storm control configuration on interface fa1.

Switch#

show storm-control interfaces fa1

Port | State | Broadcast | Unkown-Multicast | Unknown-Unicast | Action

| | pps | pps | pps

fa1 enable 200 Off(10000) Off(10000)

Shutdown

EnGenius®

Chapter 25
Spanning Tree

Spanning-Tree

Syntax

spanning-tree

no spanning-tree

Default

spanning-tree

Mode

Global Configuration

Usage

Enables or Disables the Spanning-Tree Protocol. Use the `spanning-tree` command to enable STP or `no spanning-tree` command to disable STP.

Example

The following example sets the STP status to enabled/disabled.

```
Switch285500#
  configure
Switch285500(config)#
  spanning-tree
```

```
Switch285500(config)#
  exit
Switch285500#
  show spanning-tree
Spanning tree enabled mode STP
Default port cost method: long
Root ID Priority 32768
Address 00:05:83:28:55:00
This switch is the root
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
Number of topology changes 1 last change occurred 01:49:43 ago
Times: hold 0, topology change 0, notification 0
hello 2, max age 20, forward delay 15
Interfaces
Name State Prio.Nbr Cost Sts Role PortFast
Type
fa1 enabled 128.1 200000 Frw Desg No P2P
(STP)
```

Spanning-Tree BPDU

Syntax

spanning-tree bpdu (filtering | flooding)

Parameter

(filtering | flooding) Specify the forwarding action of BPDU to filtering or flooding.

Default

spanning-tree bpdu flooding

Mode

Global Configuration

Usage

Configure the BPDU forwarding action when STP is disabled.

Example

This example sets the BPDU forwarding action to filtering.

```
Switch285500#
  configure
Switch285500(config)#
  no spanning-tree
```

```
Switch285500(config)#
  spanning-tree bpdu filtering
Switch285500(config)#
   exit
Switch285500#
   show spanning-tree
Spanning tree disabled (BPDU filtering) mode STP
Default port cost method: long
Switch285500#
```

Spanning-Tree Mode

Syntax

spanning-tree mode (stp | rstp | mstp)

Parameter

stp	Specify the mode to Spanning Tree Protocol.
rstp	Specify the mode to Rapid Spanning Tree Protocol.
mstp	Specify the mode to Multiple Spanning Tree Protocol

Default

spanning-tree mode stp

Mode

Global Configuration

Usage

Configure the force-version of the Spanning-Tree Protocol. The configuration could be shown by the “show spanning-tree” command.

Example

This example sets STP mode to RSTP (Rapid Spanning Tree Protocol).

Switch285500#

configure

```
Switch285500(config)#
  spanning-tree mode rstp
Switch285500(config)#
  exit
Switch285500#
   show spanning-tree
Spanning tree enabled mode RSTP
Default port cost method: long
Root ID Priority 32768
Address 00:05:83:28:55:00
This switch is the root
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
Number of topology changes 1 last change occurred 00:05:13 ago
Times: hold 0, topology change 0, notification 0
hello 2, max age 20, forward delay 15
Interfaces
Name State Prio.Nbr Cost Sts Role PortFast
Type
```

fa1 enabled 128.1 200000 Dscd Desg No P2P

(RSTP)

Switch285500#

Spanning-Tree Priority

Syntax

spanning-tree priority <0-61440>

Parameter

<0-61440> Specify the bridge priority, it must multiples of 4096.

Default

spanning-tree priority 32768

Mode

Global Configuration

Usage

This command configures the bridge priority. The configuration could be shown by the “show spanning-tree” command.

Example

This example sets the bridge priority to 16384.

```
Switch285500#
  configure
Switch285500(config)#
  spanning-tree priority 16384
```

```
Switch285500(config)#
   exit
Switch285500#
  show spanning-tree
Spanning tree enabled mode RSTP
Default port cost method: long
Root ID Priority 16384
Address 00:05:83:28:55:00
This switch is the root
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
Number of topology changes 2 last change occurred 00:03:37 ago
Times: hold 0, topology change 0, notification 0
hello 2, max age 20, forward delay 15
Interfaces
Name State Prio.Nbr Cost Sts Role PortFast Type
fa1 enabled 128.1 200000 Frw Desg No P2P
(RSTP)
Switch285500#
```

Spanning-Tree Hello-Time

Syntax

spanning-tree hello-time <1-10>

Parameter

<1-10> Specify the hello-time interval (second).

Default

spanning-tree hello-time 2

Mode

Global Configuration

Usage

This command configures the BPDU hello-time interval (in second). The configuration could be shown by the “show spanning-tree” command.

Example

This example sets the BPDU hello-time to 5 sec.

Switch285500#

configure

```
Switch285500(config)#
  spanning-tree hello-time 5
Switch285500(config)#
  exit
Switch285500#
   show spanning-tree
Spanning tree enabled mode RSTP
Default port cost method: long
Root ID Priority 16384
Address 00:05:83:28:55:00
This switch is the root
Hello Time 5 sec Max Age 20 sec Forward Delay 15 sec
Number of topology changes 2 last change occurred 00:00:01 ago
Times: hold 0, topology change 0, notification 0
hello 5, max age 20, forward delay 15
Interfaces
Name State Prio.Nbr Cost Sts Role PortFast
Type
```

fa1 enabled 128.1 200000 Frw Desg No P2P

(RSTP)

Switch285500#

Spanning-Tree Max-Hops

Syntax

spanning-tree max-hops <1-40>

Parameter

<1-40> Specify the max-hops value.

Default

spanning-tree max-hops 20

Mode

Global Configuration

Usage

This command configures the maximum hops value for MSTP. The configuration could be shown by “show spanning-tree” command.

Example

This example sets the max-hops to 15.

Switch285500#

configure

```
Switch285500(config)#
  spanning-tree max-hops 15
Switch285500(config)#
  exit
Switch285500#
  show spanning-tree
Spanning tree enabled mode MSTP
Default port cost method: long
Gathering information
###### MST 0 Vlans Mapped: 1-4094
CST Root ID Priority 16384
Address 00:05:83:28:55:00
This switch is root for CST and IST master
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
Max hops 15
Name State Prio.Nbr Cost Sts Role PortFast Type
fa1 enabled 128.1 200000 Frw Desg No P2P Intr
Switch285500#
```

Spanning-Tree Forward-Delay

Syntax

spanning-tree forward-delay <4-30>

Parameter

<4-30> Specify the forward-delay interval (second).

Default

spanning-tree forward-delay 15

Mode

Global Configuration

Usage

This command configures the BPDU forward-delay interval (in seconds). The configuration could be shown by the “show spanning-tree” command.

Example

This example sets the BPDU forward-delay to 30 sec.

Switch285500#

configure

```
Switch285500(config)#
  spanning-tree forward-delay 30
Switch285500(config)#
  exit
Switch285500#
  show spanning-tree
Spanning tree enabled mode STP
Default port cost method: long
Root ID Priority 16384
Address 00:05:83:28:55:00
This switch is the root
Hello Time 2 sec Max Age 20 sec Forward Delay 30 sec
Number of topology changes 6 last change occurred 00:00:30 ago
Times: hold 0, topology change 0, notification 0
hello 2, max age 20, forward delay 30
Interfaces
Name State Prio.Nbr Cost Sts Role PortFast Type
fa1 enabled 128.1 200000 Frw Desg No P2P
```

(STP)

Switch285500#

Spanning-Tree Maximum-Age

Syntax

spanning-tree maximum-age <6-40>

Parameter

<6-40> Specify the maximum-age time (second).

Default

spanning-tree maximum-age 20

Mode

Global Configuration

Usage

This command configures the BPDU maximum-age interval (in seconds). The configuration could be shown by the “show spanning-tree” command.

Example

This example sets the BPDU maximum-age to 10 sec.

Switch285500#

configure

```
Switch285500(config)#
  spanning-tree maximum-age 10
Switch285500(config)#
  exit
Switch285500#
  show spanning-tree
Spanning tree enabled mode STP
Default port cost method: long
Root ID Priority 16384
Address 00:05:83:28:55:00
This switch is the root
Hello Time 2 sec Max Age 10 sec Forward Delay 15 sec
Number of topology changes 7 last change occurred 00:00:02 ago
Times: hold 0, topology change 0, notification 0
hello 2, max age 10, forward delay 15
Interfaces
Name State Prio.Nbr Cost Sts Role PortFast Type
fa1 enabled 128.1 200000 Frw Desg No P2P
```

(STP)

Switch285500#

Spanning-Tree TX-Hold-Count

Syntax

spanning-tree tx-hold-count <1-10>

Parameter

<1-10> Specify the tx-hold-count value.

Default

spanning-tree tx-hold-count 6

Mode

Global Configuration

Usage

This command configures the BPDU tx-hold-count.

Example

This example sets the BPDU hello-time to 5 sec.

Switch285500#

configure

Switch285500(config)#

spanning-tree tx-hold-count 10

```
Switch285500(config)#
  exit
```

Spanning-Tree Pathcost Method

Syntax

spanning-tree pathcost method (long | short)

Parameter

long Specify the type of pathcost value to 32 bits (long).

short Specify the type of pathcost value to 16 bits (short).

Default

spanning-tree pathcost method long

Mode

Global Configuration

Usage

This command configures the BPDU pathcost value type to 16bits (short) or 32 bits (long). The configuration could be shown by the “show spanning-tree” command.

Example

This example sets the type of pathcost value to short.

Switch285500#

configure

```
Switch285500(config)#
   spanning-tree pathcost method short
Switch285500(config)#
  exit
Switch285500#
  show spanning-tree
Spanning tree enabled mode STP
Default port cost method: short
Root ID Priority 32768
Address 00:05:83:28:55:00
This switch is the root
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
Number of topology changes 11 last change occurred 00:00:17 ago
Times: hold 0, topology change 0, notification 0
hello 2, max age 20, forward delay 15
Interfaces
Name State Prio.Nbr Cost Sts Role PortFast Type
fa1 enabled 128.1 19 Frw Desg No P2P
```

(STP)

Switch285500#

Spanning-Tree Port-Priority

Syntax

spanning-tree port-priority <0-240>

Parameter

<0-240> Specify the STP port priority. It must multiples of 16.

Default

spanning-tree port-priority 128

Mode

Port Configuration

Usage

This command per port configures the STP port priority. The configuration could be shown by th e“show spanning-tree interface” command.

Example

This example sets port fa1 STP port priority to 64.

Switch285500#

configure

```
Switch285500(config)#
   interface fa1
Switch285500(config-if)#
   spanning-tree port-priority 64
Switch285500(config-if)#
  exit
Switch285500(config)#
   exit
Switch285500#
  show spanning-tree interfaces fa1
Port fa1 enabled
State: forwarding Role: designated
Port id: 64.1 Port cost: 200000
Type: P2P (STP) Port Fast: No
Designated bridge Priority : 32768 Address: 00:05:83:28:55:00
Designated port id: 64.1 Designated path cost: 0
BPDU Filter: Disabled BPDU guard: Disabled
BPDU: sent 1794, received 0
```

```
Switch285500#
```

Spanning-Tree Cost

Syntax

spanning-tree cost <0-200000000>

Parameter

<0-200000000> Specify the STP port cost. In short pathcost method, the range is from 0 to 65535. (0 = Auto)

Default

spanning-tree cost 0

Mode

Port Configuration

Usage

This command per port configures the STP port cost. The configuration could be shown by the “show spanning-tree interface” command.

Example

This example sets port fa1 STP port cost to 100.

Switch285500#

configure

```
Switch285500(config)#
  interface fa1
Switch285500(config-if)#
  spanning-tree cost 100
Switch285500(config-if)#
   exit
Switch285500(config)#
  exit
Switch285500#
   show spanning-tree interfaces fa1
Port fa1 enabled
State: forwarding Role:
designated
Port id: 128.1 Port cost: 100
Type: P2P (STP) Port Fast: No
Designated bridge Priority : 32768 Address:
00:05:83:28:55:00
Designated port id: 128.1 Designated path
```

cost: 0

BPDU Filter: Disabled BPDU guard:

Disabled

BPDU: sent 2158, received 0

Switch285500#

Spanning-Tree Edge

Syntax

spanning-tree edge

no spanning-tree edge

Default

no spanning-tree edge

Mode

Port Configuration

Usage

This command per port configures the STP edge port function. The configuration could be shown by the “show spanning-tree interface” command.

Example

This example sets port fa1 STP edge port to enable.

```
Switch285500#
  configure
Switch285500(config)#
  interface fa1
```

```
Switch285500(config-if)#
   spanning-tree edge
Switch285500(config-if)#
  exit
Switch285500(config)#
  exit
Switch285500#
   show spanning-tree interfaces fa1
Port fa1 enabled
State: forwarding Role:
designated
Port id: 128.1 Port cost:
200000
Type: P2P (STP) Port Fast: Yes
Designated bridge Priority : 32768 Address:
00:05:83:28:55:00
Designated port id: 128.1 Designated path
cost: 0
```

Disabled

BPDU: sent 2257, received 0

Switch285500#

Spanning-Tree BPDU-Filter

Syntax

spanning-tree bpdu-filter

no spanning-tree bpdu-filter

Default

no spanning-tree bpdu-filter

Mode

Port Configuration

Usage

This command per port configures the STP BPDU Filter status. The configuration could be shown by the “show spanning-tree interface” command.

Example

This example sets port fa1 STP BPDU Filter status to be enabled.

Switch285500#

  configure

Switch285500(config)#

  interface fa1

```
Switch285500(config-if)#
  spanning-tree bpdu-filter
Switch285500(config-if)#
   exit
Switch285500(config)#
   exit
Switch285500#
   show spanning-tree interfaces fa1
Port fa1 enabled
State: forwarding Role:
designated
Port id: 128.1 Port cost: 200000
Type: P2P (STP) Port Fast: No
Designated bridge Priority : 32768 Address: 00:05:83:28:55:00
Designated port id: 128.1 Designated path
cost: 0
BPDU Filter: Enabled BPDU guard:
Disabled
```

BPDU: sent 2386, received 0

Switch285500#

Spanning-Tree BPDU-Guard

Syntax

spanning-tree bpdu-guard

no spanning-tree bpdu-guard

Default

no spanning-tree bpdu-guard

Mode

Port Configuration

Usage

This command per port configures the STP BPDU Guard status. The configuration could be shown by the “show spanning-tree interface” command.

Example

This example sets port fa1 STP BPDU Guard status to enabled.

```
Switch285500#
  configure
Switch285500(config)#
  interface fa1
```

```
Switch285500(config-if)#
   spanning-tree bpdu-guard
Switch285500(config-if)#
  exit
Switch285500(config)#
  exit
Switch285500#
  show spanning-tree interfaces fa1
Port fa1 enabled
State: forwarding Role:
designated
Port id: 128.1 Port cost: 200000
Type: P2P (STP) Port Fast: No
Designated bridge Priority : 32768 Address:
00:05:83:28:55:00
Designated port id: 128.1 Designated path
cost: 0
BPDU Filter: Disabled BPDU guard:
```

Enabled

BPDU: sent 2327, received 0

Switch285500#

Spanning-Tree Link-Type

Syntax

(point-to-point | shared) Specify the STP port link-type to Point-to-Point or Shared medium.

Default

no spanning-tree link-type

Mode

Port Configuration

Usage

This command per port configures the STP port link-type. The configuration could be shown by “show spanning-tree interface” command.

Example

This example sets port fa1 STP port link-type to be Shared.

Switch285500#

configure

Switch285500(config)#

interface fa1

```
Switch285500(config-if)#
   spanning-tree link-type shared
Switch285500(config-if)#
  exit
Switch285500(config)#
  exit
Switch285500#
  show spanning-tree interfaces fa1
Port fa1 enabled
State: forwarding Role:
designated
Port id: 128.1 Port cost: 200000
Type: Shared (STP) Port Fast: No
Designated bridge Priority : 32768 Address:
00:05:83:28:55:00
Designated port id: 128.1 Designated path
cost: 0
BPDU Filter: Disabled BPDU guard:
```

Disabled

BPDU: sent 2393, received 0

Switch285500#

Spanning-Tree MST Configuration

Syntax

spanning-tree mst configuration

name NAME

revision <0-65535>

instance <0-15> vlan [VLAN-LIST]

Parameter

NAME	Specify the MSTP bridge name of MST Configuration ID. (Max. 32 chars)
<0-65535>	Specify the MSTP revision number of MST Configuration ID.
<0-15>	Specify the MST instance ID.
VLAN-LIST	Specify the VLAN list to be mapped to this specified instance.

Default

name (Switch's MAC address)

revision 0

instance 0 vlan all

Mode

Global Configuration

Usage

This command configures the MSTP Configuration ID. The configuration could be shown by the “show spanning-tree mst configuration” command.

Example

This example sets MSTP Configuration ID, name to `Region1`, revision to

`123` and VLAN 100 mapped to instance 1.

```
Switch285500#
  configure
Switch285500(config)#
  spanning-tree mst configuration
Switch285500(config-mst)#
  name Region1
Switch285500(config-mst)#
   revision 123
Switch285500(config-mst)#
   instance 1 vlan 100
Switch285500(config-mst)#
   exit
```

```
Switch285500(config)#
   exit
Switch285500#
   show spanning-tree mst configuration
Name [Region1]
Revision 123 Instances configured 2
Instance Vlans mapped
0 1-99,101-4094
1 100
Switch285500#
```

Spanning-Tree MST Priority

Syntax

spanning-tree mst <0-15> priority <0-61440>

Parameter

<0-15> Specify the MST instance ID to configure.

<0-61440> Specify the bridge priority, it must multiples of 4096.

Default

spanning-tree mst 0 priority 32768

Mode

Global Configuration

Usage

This command configures the MST instance priority. The configuration could be shown by the “show spanning-tree mst” command.

Example

This example sets the priority of MST instance 1 to 4096.

Switch285500#

configure

```
Switch285500(config)#
  spanning-tree mode mstp
Switch285500(config)#
  spanning-tree mst 1 priority 4096
Switch285500(config)#
  exit
Switch285500#
  show spanning-tree mst 1
MST Instance Information
Instance Type : MSTI (1)
Bridge Identifier : 4096/ 1/00:05:83:28:55:00
Regional Root Bridge : 4096/ 1/00:05:83:28:55:00
Internal Root Path Cost : 0
Remaining Hops : 20
Topology changes : 2
Last Topology Change : 100
VLANs mapped: 100
Interface Role Sts Cost Prio.Nbr Type
```

fa1 Desg FWD 200000 128.1 P2P Intr

Spanning-Tree MST Cost

Syntax

spanning-tree mst <0-15> cost <0-200000000>

Parameter

<0-15>	Specify the MST instance ID to configure.
<0-200000000>	Specify the STP port cost. In short pathcost method, the range is from 0 to 65535. (0 = Auto)

Default

spanning-tree mst 0 cost 0

Mode

Port Configuration

Usage

This command configures the MSTP port cost for this MST instance. The configuration could be shown by the “show spanning-tree mst interface” command.

Example

This example sets the port fa1 STP pathcost of the MST instance 1 to 100.

Switch285500#

configure

```
Switch285500(config)#
  interface fa1
Switch285500(config-if)#
  spanning-tree mst 1 cost 100
Switch285500(config-if)#
   exit
Switch285500(config)#
  exit
Switch285500#
  show spanning-tree mst 1 interfaces fa1
MST Port Information
Instance Type : MSTI (1)
Port Identifier : 128/1
Internal Path-Cost : 100 /100
Regional Root Bridge : 4097/00:05:83:28:55:00
Internal Root Cost : 0
Designated Bridge : 4097/00:05:83:28:55:00
Internal Port Path Cost : 100
```

Port Role : Designated

Port State : Forwarding

Switch285500#

Spanning-Tree MST Port-Priority

Syntax

spanning-tree mst <0-15> priority <0-240>

Parameter

<0-15>	Specify the MST instance ID to configure.
<0-240>	Specify the STP port priority. It must multiples of 16.

Default

spanning-tree mst 0 port-priority 128

Mode

Port Configuration

Usage

This command configures the MST port priority. The configuration could be shown by the “show spanning-tree mst interface” command.

Example

This example sets port fa1 MST port priority of MST instance 1 to 32.

Switch285500#

configure

```
Switch285500(config)#
   interface fa1
Switch285500(config-if)#
  spanning-tree mst 1 cost 0
Switch285500(config-if)#
  exit
Switch285500(config)#
   exit
Switch285500#
Switch285500#
Switch285500#
Switch285500#
  configure
Switch285500(config)#
  interface fa1
Switch285500(config-if)#
  spanning-tree mst 1 port-priority 32
```

```
Switch285500(config-if)#
  exit
Switch285500(config)#
   exit
Switch285500#
  show spanning-tree mst 1 interfaces fa1
MST Port Information
Instance Type : MSTI (1)
Port Identifier : 32/1
Internal Path-Cost : 0 /200000
Regional Root Bridge : 32769/00:05:83:28:55:00
Internal Root Cost : 0
Designated Bridge : 32769/00:05:83:28:55:00
Internal Port Path Cost : 200000
Port Role : Designated
Port State : Forwarding
Switch285500#
```

EnGenius®

Chapter 26
System File

Boot System

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

Usage

Dual image allows a user to have a backup image in the flash partition. Use the “boot system” command to select the active firmware image and another firmware image will become a new backup.

Example

This example shows how to select image1 as the active image.

Switch(config)#

boot system image1

Select “image1” Success

This example shows how to show active image partition.

Switch#

show flash

File Name File Size Modified

startup-config 1191 2000-01-01 00:00:23

rsa1 974 2000-01-01 00:00:18

rsa2 1675 2000-01-01 00:00:18

dsa2 668 2000-01-01 00:00:18

ssl_cert 993 2000-01-01 00:00:18

image0 (backup) 4372401 2012-09-24 01:57:29

image1 (active) 5555970 2012-06-12 12:17:46

Save

Syntax

Save

Parameter

Default

No default value for this command.

Mode

Privileged EXEC

Usage

Use the “save” command to save the running configuration to the startup configuration file. This command is equal to “copy running-config startup-config”.

Example

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

Switch#

save

Success

This example shows how to show startup configuration

```
Switch#
    show startup-config
! System Description:
! System Version: v2.5.0-beta.32811
! System Name:
! System Up Time: 0 days, 4 hours, 31 mins, 43 secs
!
!
!
!
username “” privilege user secret “dnXencJRwfIV6”
username “admin” secret “FzjrGO6vfbERY”
voice-vlan vpt 0
voice-vlan dscp 0
```

Copy

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

Default

No default value for this command.

Mode

Privileged EXEC

Usage

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

Firmware Image

Configuration Files

Syslog Files

Language Files

Security Certificate

Example

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

Switch#

copy running-config startupst-config

This example shows how to backup running configuration to remote tftp

server 192.168.111 with file name test1.cfg.

Switch#

copy running-config

tftp://192.168.1.111/test1.cfg

Uploading file...Please Wait...

Uploading Done

This example shows how to upgrade startup configuration from remote tftp server 192.168.1.111 with file name test2.cfg.

```
Switch#
  copy tftp://192.168.1.111/test2.cfg startupconfig
Downloading file...Please Wait...
Downloading Done
Upgrade config success. Do you want to reboot now?
(y/n)n
```

This example shows how to backup security file dsa2 to remote tftp server 192.168.1.111 with file name dsa2.

```
Switch#
  copy flash://dsa2 tftp://192.168.1.111/dsa2
Uploading file...Please Wait...
Uploading Done
```

Delete

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

Default

No default value for this command.

Mode

Privileged EXEC

Usage

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

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

This example shows how to show file status in flash.

Switch#

show flash

File Name File Size Modified

startup-config 1191 2000-01-01 00:00:23

rsa1 974 2000-01-01 00:00:18

rsa2 1675 2000-01-01 00:00:18

dsa2 668 2000-01-01 00:00:18

ssl_cert 993 2000-01-01 00:00:18

image0 (active) 4372401 2012-09-24 01:57:29

image1 (backup) 0

Restore-Defaults

Syntax

restore-defaults

Parameter

None

Default

No default value for this command.

Mode

Privileged EXEC

Usage

Use the “restore-defaults” command to restore factory default settings of the system. The command is equal to “delete startup-config”,

Example

This example shows how to restore factory defaults.

Switch#

restore-defaults

Restore Default Success. Do you want to reboot now? (y/n)n

Show Config

Syntax

show (running-config | startrup-config | backup-config)

Parameter

running-config Show running configuration on terminal

startup-config Show startup configuration on terminal

backup-config Show backup configuration on terminal

Default

No default value for this command.

Mode

Privileged EXEC

Usage

The configuration file is text based. Therefore, the configuration on the terminal can be shown and read by this command.

Example

This example shows how to show the startup configuration.

Switch#

show startup-config

```
! System Description:
! System Version: v2.5.0-beta.32811
! System Name: switch
! System Up Time: 0 days, 4 hours, 31 mins, 43 secs
!
!
!
!
username “” privilege user secret “dnXencJRwfIV6”
username “admin” secret “FzjrGO6vfbERY”
voice-vlan vpt 0
voice-vlan dscp 0
```

This example shows how to show running configuration

```
Switch#
  show running-config
! System Description:
! System Version: v2.5.0-beta.32811
! System Name:
```

! System Up Time: 0 days, 5 hours, 23 mins, 42 secs

!

!

!

!

username “” privilege user secret “dnXencJRwfIV6”

username “admin” secret “FzjrGO6vfbERY”

voice-vlan vpt 0

voice-vlan dscp 0

Show Flash

Syntax

show flash

Parameter

None

Default

No default value for this command.

Mode

Privileged EXEC

Usage

Use “show flash” command to show all files’ status which stored in flash.

Example

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

Switch#

show flash

File Name File Size Modified

startup-config 1191 2000-01-01 00:00:23

rsa1 974 2000-01-01 00:00:18

rsa2 1675 2000-01-01 00:00:18

dsa2 668 2000-01-01 00:00:18

ssl_cert 993 2000-01-01 00:00:18

image0 (active) 4372401 2012-09-24 01:57:29

image1 (backup) 0

EnGenius®

Chapter 27
Time

Clock Set

Syntax

clock set HH:MM:SS (jan|feb|mar|apr|may|jun|jul|aug|sep|oct|nov|dec) <1-31> <2000-2037>

Parameter

HH:MM:SS Specify static time of year month day hour minute second

(jan|feb|mar|apr

|may|jun|jul|aug|

sep|oct|nov|dec) <1-31>

<2000-2037>

Default

No default is defined.

Mode

Global Configuration

Usage

Use the clock set command to set the static time. The static time won't save to configuration file.

Example

The example shows how to set static time of switch. You can verify settings by the following show show clock command.

```
switch#
  clock set 11:03:00 sep 21 2012
11:03:00 DFL(UTC+8) Sep 21 2012
switch#
  show clock
11:03:21 DFL(UTC+8) Sep 21 2012
No time source
```

Clock Timezone

Syntax

clock timezone ACRONYM HOUR-OFFSET [minutes <0-59>]

no clock timezone

Parameter

ACRONYM	Specify acronym name of time zone
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

Usage

Use the clock timezone command to set the timezone settings. Use the no form of this command to apply the default settings.

Example

The example shows how to set time zone of switch and then restore to default time zone. You can verify settings by the following show show clock command.

```
switch(config)#
   clock timezone test +5
switch(config)#
   show clock detail
10:13:27 test(UTC+5) Sep 21 2012
No time source
Time zone:
Acronym is test
Offset is UTC+5
switch(config)#
  no clock timezone
switch(config)#
  show clock detail
13:14:50 DFL(UTC+8) Sep 21 2012
No time source
Time zone:
```

Acronym is DFL

Offset is UTC+8

Clock Source

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

Usage

Use the clock source command to set the source of time. “local” means that you use the static setting by the user manual set. The “sntp” means that you use the remote SNTP server. Use the no form of this command to reset to default settings.

Example

The example shows how to set clock source of switch. You can verify settings by the following show show clock command.

switch(config)#

clock source sntp

```
switch(config)#
   show clock detail
08:32:12 test(UTC+5) Sep 21 2012
No time source
```

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

Parameter

ACRONYM	Specify acronym name of time zone
(jan|feb|mar|apr|may|jun |jul|aug|sep|oct|nov|dec) <1-31> <2000-2037> HH:MM (jan|feb|mar|apr| may|jun|jul|aug|sep|oct|nov|dec) <1-31> <2000- 2037> HH:MM	Specify non-recurring daylight saving time duration.
<1-1440>	Specify adjust offset of daylight saving time
usa	Using daylight saving time in the United States that starts on the second Sunday of March and ends on the first Sunday of November.
eu	Using daylight saving time in the Europe that starts on the last Sunday in March and ending on the last Sunday in October.
(<1-5>|first|last) (sun|mon| tue|wed|thu|fri|sat) (jan |feb|mar|apr|may|jun| jul|aug|sep|oct|nov|dec) HH:MM (<1-5>|first|last) (sun|mon|tue|wed|thu|fri|sat) (jan|feb|mar|apr|may| jun|jul|aug|sep|oct|nov|dec) HH:MM	Specify ecurring daylight saving time duration

Default

No default daylight saving time is defined.

Mode

Global Configuration

Usage

Use the clock summer-time command to set daylight saving time for the system time. The “usa” or “eu” settings means that the global daylight saving policy which is defined by international organizations is in use. In both the “date”and “recurring” settings, 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” setting means that time is adjusted every year within the month . Use the no form of this command to apply the default settings.

Example

The example shows how to set clock source for the switch. You can verify settings by the following show clock command.

```
switch(config)#
   clock source sntp
switch(config)#
  show clock detail
08:32:12 test(UTC+5) Sep 21 2012
No time source
```

Show Clock

Syntax

show clock [detail]

Parameter

detail Show more detail information of clock

Default

No default is defined

Mode

Global Configuration

Usage

Use the show clock command to show the clock on the switch. The “detail” means that show more information of clock such as time zone and daylight saving time.

Example

The example shows how to show clock of switch and detail information.

Switch334455(config)#

clock source sntp

```
Switch334455(config)#
  clock summer-time DLS recurring usa
Switch334455(config)#
  sntp host 192.168.1.100
Switch334455(config)#
  show clock
14:34:43 DLS(UTC+9) Sep 25 2012
Time source is sntp
Switch334455(config)#
  show clock detail
14:35:39 DLS(UTC+9) Sep 25 2012
Time source is sntp
Time zone:
Acronym is DFL
Offset is UTC+8
Summertime:
Acronym is DLS
Recurring every year.
```

Begins at 2 0 3 2:0

Ends at 1 0 11 2:0

Offset is 60 minutes.

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.

Mode

Global Configuration

Usage

Use the sntp command to set a remote SNTP server. The default server port is 123. Use the no form of this command to set the default settings.

Example

The example shows how to set the remote SNTP server of switch. You can verify settings by the following show sntp command.

```
switch(config)#
  clock source sntp
switch(config)#
  sntp host 192.168.1.100
switch(config)#
  show sntp
SNTP is Enabled
SNTP Server address: 192.168.1.100
SNTP Server port: 123
```

Show SNTP

Syntax

show sntp

Parameter

None

Default

No default is defined

Mode

Global Configuration

Usage

Use the show sntp command to remote SNTP server information.

Example

The example shows how to show the remote SNTP server.

Switch334455(config)#

show sntp

SNTP is Enabled

SNTP Server address: 192.168.1.100

SNTP Server port: 123

Chapter 28
VLAN

VLAN

Syntax

vlan

no vlan

Default

vlan 1

Mode

Global Configuration

Usage

Create or remove a VLAN entry. Using the `vlan` command to enter the VLAN configuration mode.

Example

The following example creates and removes a VLAN entry (100).

```
SwitchEF0101#
  configure
SwitchEF0101(config)#
   vlan 100
```

```
SwitchEF0101(config-vlan)#
  exit
SwitchEF0101(config)#
   no vlan 100
SwitchEF0101(config)#
  exit
SwitchEF0101#
```

VLAN Name

Syntax

vlan name NAME

Parameter

NAME Specify the name of the VLAN (Max. 32 chars).

Default

vlan name VLANxxxx

Mode

VLAN Configuration

Usage

Configure the name of a VLAN entry.

Example

This example sets the VLAN name of VLAN 100 to be `VLAN-onehundred`.

```
SwitchEF0101#
   configure
SwitchEF0101(config)#
  vlan 100
```

```
SwitchEF0101(config-vlan)#
  name VLAN-one-hundred
SwitchEF0101(config-vlan)#
  exit
SwitchEF0101(config)#
```

Switchport Mode

Syntax

switchport mode (access | hybrid | trunk [uplink] | tunnel)

Parameter

access	Specify the VLAN mode to Access port.
hybrid	Specify the VLAN mode to Hybrid port.
trunk	Specify the VLAN mode to Trunk port.
uplink	Specify the Uplink property on this Trunk port.
tunnel	Specify the VLAN mode to Dot1Q Tunnel port.

Default

Switchport mode trunk

Mode

Port Configuration

Usage

The VLAN mode is used to configure the port for different port roles.

Access port

Accepts only untagged frames and join an untagged VLAN.

Hybrid port

Supports all functions as defined in IEEE 802.1Q specifications.

Trunk port

An untagged member of one VLAN at most, it 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. The configuration could be shown by the “show interface switchport” command.

Example

This example sets VLAN mode to Access port.

```
SwitchEF0101(config)#
   interface fa12
SwitchEF0101(config-if)#
  switchport mode access
SwitchEF0101(config-if)#
   exit
SwitchEF0101(config)#
  exit
```

```
SwitchEF0101#
   show interfaces switchport fa12
Port : fa12
Port Mode : Access
Ingress Filtering : enabled
Acceptable Frame Type : untagged-only
Ingress UnTagged VLAN ( NATIVE ) : 1
Trunking VLANs Enabled:
Port is member in:
Vlan Name Egress rule
1 default Untagged
Forbidden VLANs:
Vlan Name
SwitchEF0101#
```

Switchport Hybrid PVID

Syntax

switchport hybrid pvid <1-4094>

Parameter

<1-4094> Specify the port-based VLAN ID on the Hybrid port.

Default

switchport hybrid pvid 1

Mode

Port Configuration

Usage

This command configures the hybrid port's PVID. The configuration could be shown by the "show interface switchport" command.

Example

This example sets PVID to 100.

SwitchEF0101#

configure

```
SwitchEF0101(config)#
  interface fa10
SwitchEF0101(config-if)#
  switchport mode hybrid
SwitchEF0101(config-if)#
  switchport hybrid pvid 100
SwitchEF0101(config-if)#
   exit
SwitchEF0101(config)#
  exit
SwitchEF0101#
  show interfaces switchport fa10
Port : fa10
Port Mode : General
Ingress Filtering : enabled
Acceptable Frame Type : all
Ingress UnTagged VLAN ( NATIVE ) : 100
Trunking VLANs Enabled:
```

Port is member in:

Vlan Name Egress rule

1 default Untagged

Forbidden VLANs:

Vlan Name

SwitchEF0101#

Switchport Hybrid Ingress-Filtering Disable

Syntax

switchport bybrid ingress-filtering disable

no switchport hybrid ingress-filtering disable

Default

no switchport hybrid ingress-filtering disable

Mode

Port Configuration

Usage

This command per port configures the ingress-filtering status. This filtering is used to filter the frames coming from the non-member ingress port. The configuration could be shown by the “show interface switchport” command.

Example

This example sets ingress-filtering to disable.

SwitchEF0101#

configure

SwitchEF0101(config)#

interface fa10

```
SwitchEF0101(config-if)#
  switchport mode hybrid
SwitchEF0101(config-if)#
  switchport hybrid ingress-filtering disable
SwitchEF0101(config-if)#
  exit
SwitchEF0101(config)#
   exit
SwitchEF0101#
  show interfaces switchport fa10
Port : fa10
Port Mode : General
Ingress Filtering : disabled
Acceptable Frame Type : all
Ingress UnTagged VLAN ( NATIVE ) : 100
Trunking VLANs Enabled:
Port is member in:
Vlan Name Egress rule
```

1 default Untagged

Forbidden VLANs:

Vlan Name

SwitchEF0101#

Switchport Hybrid Acceptable-Frame-Type

Syntax

switchport hybrid acceptable-frame-type (all | tagged-only | untaggedonly)

Parameter

all	Specify to accept all frames.
tagged-only	Specify to only accept tagged frames.
untagged-only	Specify to only accept untagged frames.

Default

switchport hybrid acceptable-frame-type all

Mode

Port Configuration

Usage

This command per port configures the acceptable-frame-type. The configuration could be shown by the “show interface switchport” command.

Example

This example sets acceptable-frame-type to tagged-only.

SwitchEF0101#

configure

```
SwitchEF0101(config)#
  interface fa10
SwitchEF0101(config-if)#
  switchport mode hybrid
SwitchEF0101(config-if)#
   switchport hybrid acceptable-frame-type taggedonly
SwitchEF0101(config-if)#
   exit
SwitchEF0101(config)#
   exit
SwitchEF0101# show interfaces switchport fa10
Port : fa10
Port Mode : General
Ingress Filtering : disabled
Acceptable Frame Type : tagged-only
Ingress UnTagged VLAN ( NATIVE ) : 100
Trunking VLANs Enabled:
Port is member in:
```

Vlan Name Egress rule

1 default Untagged

Forbidden VLANs:

Vlan Name

SwitchEF0101#

Switchport Hybrid Allowed VLAN Add

Syntax

switchport hybrid allowed vlan add VLAN-LIST [(tagged | untagged)]

Parameter

VLAN-LIST	Specifies the VLAN list to be added.
(tagged | untagged)	Specifies the member type to tagged or untagged.

Mode

Port Configuration

Usage

This command per hybrid port configures the allowed VLAN list. The configuration could be shown by the “show interface switchport” command.

Example

This example sets port fa10 VLAN to join the VLAN 100 as a tagged member.

SwitchEF0101#

  configure

SwitchEF0101(config)#

  interface fa10

SwitchEF0101(config-if)# switchport hybrid allowed vlan add 100

```
SwitchEF0101(config-if)#
  switchport hybrid allowed vlan add 100
SwitchEF0101(config-if)#
   exit
SwitchEF0101(config)#
   exit
SwitchEF0101#
  show interfaces switchport fa10
Port : fa10
Port Mode : General
Ingress Filtering : disabled
Acceptable Frame Type : tagged-only
Ingress UnTagged VLAN ( NATIVE ) : 100
Trunking VLANs Enabled:
Port is member in:
Vlan Name Egress rule
1 default Untagged
100 VLAN-one-hundred Tagged
```

Forbidden VLANs:

Vlan Name

SwitchEF0101#

Switchport Hybrid Allowed VLAN Remove

Syntax

switchport hybrid allowed vlan remove VLAN-LIST

Parameter

VLAN-LIST Specifies the VLAN list to be removed.

Mode

Port Configuration

Usage

This command per hybrid port configures to remove the allowed VLAN list. The configuration could be shown by the “show interface switchport” command.

Example

This example sets port fa10 VLAN to leave the VLAN 100.

```
SwitchEF0101#
   configure
SwitchEF0101(config)#
  interface fa10
SwitchEF0101(config-if)# switchport hybrid allowed vlan remove 100
```

```
SwitchEF0101(config-if)#
  switchport hybrid allowed vlan remove 100
SwitchEF0101(config-if)#
   exit
SwitchEF0101(config)#
   exit
SwitchEF0101#
  show interfaces switchport fa10
Port : fa10
Port Mode : General
Ingress Filtering : disabled
Acceptable Frame Type : tagged-only
Ingress UnTagged VLAN ( NATIVE ) : 100
Trunking VLANs Enabled:
Port is member in:
Vlan Name Egress rule
1 default Untagged
Forbidden VLANs:
```

Vlan Name

SwitchEF0101#

Switchport Access VLAN

Syntax

switchport access vlan <1-4094>

Parameter

<1-4094> Specifies the access VLAN ID.

Mode

Port Configuration

Usage

This command per Access port configures the native VLAN ID. The configuration could be shown by the “show interface switchport” command.

Example

This example sets the Access port fa10 native VLAN ID to 100.

SwitchEF0101#

configure

SwitchEF0101(config)#

interface fa10

```
SwitchEF0101(config-if)#
  switchport mode access
SwitchEF0101(config-if)#
  switchport access vlan 100
SwitchEF0101(config-if)#
  exit
SwitchEF0101(config)#
   exit
SwitchEF0101#
  show interfaces switchport fa10
Port : fa10
Port Mode : Access
Ingress Filtering : enabled
Acceptable Frame Type : untagged-only
Ingress UnTagged VLAN ( NATIVE ) : 100
Trunking VLANs Enabled:
Port is member in:
Vlan Name Egress rule
```

100 VLAN-one-hundred Untagged

Forbidden VLANs:

Vlan Name

SwitchEF0101#

Switchport Tunnel VLAN

Syntax

switchport tunnel vlan <1-4094>

Mode

Port Configuration

Usage

The command per Tunnel port configures the native VLAN. The configuration could be shown by the “show interface switchport” command.

Example

This example sets Tunnel port fa10 native VLAN to 100.

SwitchEF0101#

configure

SwitchEF0101(config)#

interface fa10

SwitchEF0101(config-if)#

switchport mode tunnel

```
SwitchEF0101(config-if)#
  switchport tunnel vlan 100
SwitchEF0101(config-if)#
   exit
SwitchEF0101(config)#
   exit
SwitchEF0101#
   show interfaces switchport fa10
Port : fa10
Port Mode : Dot1qtunnel
Ingress Filtering : enabled
Acceptable Frame Type : all
Ingress UnTagged VLAN ( NATIVE ) : 100
Trunking VLANs Enabled:
Port is member in:
Vlan Name Egress rule
100 VLAN-one-hundred Untagged
Forbidden VLANs:
```

Vlan Name

SwitchEF0101#

Switchport Trunk Native VLAN

Syntax

switchport trunk native vlan <1-4094>

Mode

Port Configuration

Usage

The command per Trunk port configures the native VLAN. The configuration could be shown by the “show interface switchport” command.

Example

This example sets Trunk port fa10 native VLAN to 100.

SwitchEF0101#

configure

SwitchEF0101(config)#

interface fa10

SwitchEF0101(config-if)#

switchport mode trunk

```
SwitchEF0101(config-if)#
  switchport trunk native vlan 100
SwitchEF0101(config-if)#
   exit
SwitchEF0101(config)#
  exit
SwitchEF0101#
  show interfaces switchport fa10
Port : fa10
Port Mode : Trunk
Ingress Filtering : enabled
Acceptable Frame Type : all
Ingress UnTagged VLAN ( NATIVE ) : 100
Trunking VLANs Enabled:
Port is member in:
Vlan Name Egress rule
100 VLAN-one-hundred Untagged
Forbidden VLANs:
```

Vlan Name

SwitchEF0101#

Switchport Trunk Allowed VLAN

Syntax

switchport trunk allowed vlan (add | remove) (VLAN-LIST | all)

Parameter

(add | remove)	Specify the action to add or remove the allowed VLAN list.
(VLAN-LIST | all)	Specify the VLAN list or all VLANs to be added or removed.

Mode

Port Configuration

Usage

The command per Trunk port configures the allowed VLAN list. The configuration could be shown by the “show interface switchport” command.

Example

This example sets Trunk port fa10 to add the allowed VLAN 100.

SwitchEF0101#

  configure

SwitchEF0101(config)#

  interface fa10

```
SwitchEF0101(config-if)#
  switchport trunk allowed vlan add 100
SwitchEF0101(config-if)#
  exit
SwitchEF0101(config)#
  exit
SwitchEF0101#
  show interfaces switchport fa10
Port : fa10
Port Mode : Trunk
Ingress Filtering : enabled
Acceptable Frame Type : all
Ingress UnTagged VLAN ( NATIVE ) : 1
Trunking VLANs Enabled: 100
Port is member in:
Vlan Name Egress rule
1 default Untagged
100 VLAN-one-hundred Tagged
```

Forbidden VLANs:

Vlan Name

SwitchEF0101#

Switchport Default-VLAN Tagged

Syntax

switchport default-vlan tagged

no switchport default-vlan tagged

Mode

Port Configuration

Usage

The command per port configures the membership of the default VLAN to be tagged. The configuration could be shown by the “show interface switchport” command.

Example

This example sets the Trunk port fa10 membership with the default VLAN to tagged.

SwitchEF0101#

configure

SwitchEF0101(config)#

interface fa10

SwitchEF0101(config-if)#

witchport default-vlan tagged

```
SwitchEF0101(config-if)#
  exit
SwitchEF0101(config)#
   exit
SwitchEF0101#
  show interfaces switchport fa10
Port : fa10
Port Mode : Trunk
Ingress Filtering : enabled
Acceptable Frame Type : all
Ingress UnTagged VLAN ( NATIVE ) : 4095
Trunking VLANs Enabled: 100
Port is member in:
Vlan Name Egress rule
1 default Tagged
100 VLAN-one-hundred Tagged
Forbidden VLANs:
Vlan Name
```

SwitchEF0101#

Switchport Forbidden Default-VLAN

Syntax

switchport forbidden default-vlan

no switchport forbidden default-vlan

Mode

Port Configuration

Usage

The command per port configures the membership of the default VLAN to forbidden. The configuration could be shown by the “show interface switchport” command.

Example

This example sets the membership of the default VLAN with port fa10 to forbidden.

```
SwitchEF0101#
   configure
SwitchEF0101(config)#
  interface fa10
SwitchEF0101(config-if)#
  switchport forbidden default-vlan
```

```
SwitchEF0101(config-if)#
  exit
SwitchEF0101(config)#
  exit
SwitchEF0101#
  show interfaces switchport fa10
Port : fa10
Port Mode : Trunk
Ingress Filtering : enabled
Acceptable Frame Type : all
Ingress UnTagged VLAN ( NATIVE ) : 4095
Trunking VLANs Enabled: 100
Port is member in:
Vlan Name Egress rule
100 VLAN-one-hundred Tagged
Forbidden VLANs:
Vlan Name
1 default
```

SwitchEF0101#

Switchport Forbidden VLAN

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

Usage

The command per port configures the membership of the specfied VLANs to the forbidden setting. The configuration could be shown by the “show interface switchport” command.

Example

This example sets the membership of the VLAN 100 with port fa10 to

forbidden.

SwitchEF0101#

configure

SwitchEF0101(config)#

interface fa10

```
SwitchEF0101(config-if)#
   switchport forbidden vlan add 100
SwitchEF0101(config-if)#
  exit
SwitchEF0101(config)#
  exit
SwitchEF0101#
   show interfaces switchport fa10
Port : fa10
Port Mode : Trunk
Ingress Filtering : enabled
Acceptable Frame Type : all
Ingress UnTagged VLAN ( NATIVE ) : 1
Trunking VLANs Enabled: 100
Port is member in:
Vlan Name Egress rule
1 default Untagged
Forbidden VLANs:
```

Vlan Name

100 VLAN-one-hundred

SwitchEF0101#

Management-VLAN

Syntax

management-vlan vlan <1-4094>

no management-vlan

Parameter

<1-4094> Specify the VLAN ID of management-vlan.

Default

In default, management VLAN 1 is created

Mode

Global Configuration

Usage

(1) Set <1-4094> as management VLAN id; suggest to create the VLAN and make the port to be member of it firstly.

(2) When use no command, restore management vlan to be default VLAN.

(3) If want to see management vlan created ,use “show management-vlan”

Example

(1) The following example specifies that management vlan 2 is created

Switch(config)#

management-vlan vlan 2

(2) The following example specifies that management-vlan is restored to be the default VLAN.

Switch(config)#

no management-vlan

Show Management-VLAN

Syntax

show management-vlan

Parameter

None

Default

None

Mode

Global /Enable Configuration

Usage

Display information about the management vlan.

Example

The following example specifies the show management vlan.

Switch(config)#

show management-vlan

MAC VLAN MAC

Syntax

vlan mac-vlan mac A:B:C:D:E:F vlan <1-4094>

no vlan mac-vlan mac A:B:C:D:E:F

Parameter

A:B:C:D:E:F specifies mac address to configure

<1-4094> Specifies the MAC VLAN ID to configure.

Default

no mac vlan entries are configured

Mode

Global Configuration

Usage

Use the vlan mac-vlan mac Global Configuration mode command to add a mac vlan entry with a spefied mac address. Use the no form of this command to remove the mac vlan entries. You can verify your settings by entering the show vlan mac vlan Privileged EXEC command.

Example

The following example shows how to add a mac vlan entry

```
Switch(config)#
  vlan mac-vlan mac 0:0:0:0:0:1 vlan 100
Switch(config)#
  show vlan mac-vlan
MAC Address | VID
00:00:00:00:00:01 | 100
MAC VLAN Total Entry : 1
MAC VLAN Maximum Entry: 128
```

MAC VLAN Enable

Syntax

vlan mac-vlan

no vlan mac-vlan

Parameter

None

Default

MAC VLAN disabled on all interfaces

Mode

Interface configuration

Usage

Use the vlan mac-vlan Interface Configuration mode command to enable the MAC VLAN function on specified interfaces. Use the no form of this command to disable the MAC VLAN function. You can verify your settings by entering the show vlan mac-vlan interfaces IF_PORTS Privileged EXEC command.

Example

The following example shows how to the enable the MAC VLAN function on specified interfaces.

```
Switch(config)#
  interface range fa1,fa5
Switch(config-if-range)#
  vlan mac-vlan
Switch#
  show vlan mac-vlan interfaces fa1-6
Port | status
fa1 | Enabled
fa2 | Disabled
fa3 | Disabled
fa4 | Disabled
fa5 | Enabled
fa6 | Disabled
```

Show VLAN MAC-VLAN

Syntax

show vlan mac-vlan

Parameter

None

Default

None

Mode

Privileged EXEC

Usage

Use the show vlan mac-vlan command in EXEC mode to display a specific MAC VLAN entry or All MAC VLAN entries.

Example

The following example shows how to display MAC VLAN entry configurations.

Switch(config)#

show vlan mac-vlan

MAC Address | VID

00:00:00:00:00:01 | 100

MAC VLAN Total Entry : 1

MAC VLAN Maximum Entry: 128

Show MAC-VLAN Interfaces

Syntax

show vlan mac-vlan interfaces IF_PORTS

Parameter

IF_PORTS Specify interface mac vlan status to display

Default

None

Mode

Privileged EXEC

Usage

Use the show vlan mac-vlan interface command in EXEC mode to display a specificed interace or the all interfaces MAC VLAN status.

Example

The following example shows how to display the MAC VLAN interfaces settings.

Switch#

show vlan mac-vlan interfaces fa1-6

Port | status

fa1 | Enabled

fa2 | Disabled

fa3 | Disabled

fa4 | Disabled

fa5 | Enabled

fa6 | Disabled

Protocol-VLAN Group

Syntax

vlan protocol-vlan group <1-8> frame-type

(ethernet_ii|llc_other|snap_1042) protocol-value VALUE

no vlan protocol-vlan group <1-8>

Parameter

<1-8>	Specify protocol vlan group to configure
(ethernet_ii|llc_other|snap_1042)	Specify protocol based frame type
VALUE	Specify protocol value to configure

Default

no protocol vlan group are configured.

Mode

Global Configuration

Usage

Use the vlan protocol-vlan group Global Configuration mode command to add a protocol vlan group with specified proto type and value. Use the no form of this command to remove the protocol vlan group settings. You can verify your settings by entering the show vlan proto-vlan Privileged EXEC command.

Example

The following example show how to configure protocol vlan group:

Switch(config)#

vlan protocol-vlan group 1 frame-type ethernet_ii

protocol-value 0x806

Switch(config)#

vlan protocol-vlan group 2 frame-type llc_other protocolvalue 0x800

Switch#

show vlan protocol-vlan

Group ID | Status | Type | value

1 | Enabled | Ethernet | 0x0806

2 | Enabled | LLC other | 0x0800

3 | Disabled | -- | --

4 | Disabled | -- | --

5 | Disabled | -- | --

6 | Disabled | -- | --

7 | Disabled | -- | --

8 | Disabled | -- | --

Protocol VLAN Binding

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.

Default

In default all group are not binding to any interface.

Mode

Interface configuration

Usage

Use the vlan protocol-vlan binding Interface Configuration mode command to bind a protocol VLAN Group on specified interfaces. Use the no form of this command to cancel protocol VLAN Group Binding. You can verify your settings by entering the show vlan protocol-vlan interfaces IF_PORTS Privileged EXEC command.

Example

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

```
Switch(config)#
  interface fa1
Switch(config-if)#
  vlan protocol-vlan group 1 vlan 2
Switch(config-if)#
   vlan protocol-vlan group 2 vlan 3
Switch#
  show vlan protocol-vlan interfaces fa1
Port fa1 :
Group 1
Status : Enabled
VLAN ID : 2
Group 2
Status : Enabled
VLAN ID : 3
Group 3
```

Group 3

Status : Disabled

Group 4

Status : Disabled

Group 5

Status : Disabled

Group 6

Status : Disabled

Group 7

Status : Disabled

Group 8

Status : Disabled

Show Protocol VLAN Group

Syntax

show vlan protocol-vlan [group <1-8>]

Parameter

<1-8> Specify protocol vlan group to display

Default

None

Mode

Privileged EXEC

Usage

Use the show vlan proto-vlan command in EXEC mode to display the Proto VLAN group configuration.

Example

The following example shows how to display a Proto VLAN group configuration.

Switch#

show vlan protocol-vlan

Group ID | Status | Type | value

1 | Enabled | Ethernet | 0x0806

2 | Enabled | LLC other | 0x0800

3 | Disabled | -- | --

4 | Disabled | -- | --

5 | Disabled | -- | --

6 | Disabled | -- | --

7 | Disabled | -- | --

8 | Disabled | -- | --

Show Protocol VLAN Interfaces

Syntax

show vlan protocol-vlan interfaces IF_PORTS

Parameter

IF_PORTS Specify interfaces protocol vlan to display

Default

None

Mode

Privileged EXEC

Usage

Use the show vlan mac-vlan interface command in EXEC mode to display the Protocol VLAN interfaces settings.

Example

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

Switch#

show vlan protocol-vlan interfaces fa1

Port fa1 :

Group 1

Group 1

Status : Enabled

VLAN ID : 2

Group 2

Status : Enabled

VLAN ID : 3

Group 3

Status : Disabled

Group 4

Status : Disabled

Group 5

Status : Disabled

Group 6

Status : Disabled

Group 7

Status : Disabled

Group 8

Status : Disabled

Chapter 29
Voice VLAN

Voice VLAN State

Syntax

voice-vlan mode (auto | oui)

no voice-vlan

Parameter

auto	Specify Auto voice vlan is enabled
Oui	Specify voice vlan enabled in oui mode

Default

Auto voice vlan is enabled

Mode

Global Configuration

Usage

Use the voice vlan state global configuration command to set the type of voice VLAN that is functional on the device or disable voice VLAN entirely. Use the no form of this command to disable the voice vlan function. You can verify your settings by entering the show voice vlan Privileged EXEC command. To change voice vlan mode from auto to oui or oui to auto, you must first disable the voice vlan function.

Example

The following example shows how to change the voice vlan state from auto to oui mode and vice versa.

```
Switch(config)#
  no voice-vlan
Switch(config)#
   voice-vlan mode oui
Switch# show voice-vlan
Administrate Voice VLAN state : oui-enabled
Voice VLAN ID : 100
Voice VLAN VPT : 5
Voice VLAN DSCP : 46
Voice VLAN Aging : 1440 minutes
Voice VLAN CoS : 6
Voice VLAN 1p Remark: disabled
```

Voice VLAN ID

Syntax

voice-vlan vlan <1-4094>

Parameter

<1-4094> Specify the voice VLAN ID

Default

The default Voice VLAN ID is DFLT VLAN ID.

Mode

Global Configuration

Usage

Use the voice vlan id global configuration command to configure the VLAN identifier of the voice VLAN. Statically, you can verify your settings by entering the show voice vlan Privileged EXEC command.

Example

The following example shows how to set the Voice VLAN ID. Before proceeding, please make sure that VLAN EXIST is enabled.

Switch(config)#

voice-vlan vlan 128

```
Switch#
  show voice-vlan
Administrate Voice VLAN state : oui-enabled
Voice VLAN ID : 128
Voice VLAN VPT : 5
Voice VLAN DSCP : 46
Voice VLAN Aging : 1440 minutes
Voice VLAN CoS : 6
Voice VLAN 1p Remark: disabled
```

Voice VLAN VPT

Syntax

voice-vlan vpt <0-7>

Parameter

<0-7> Specify the vpt value to be advertised by LLDP

Default

The default vpt value is 5.

Mode

Global Configuration

Usage

Use the voice vlan vpt global configuration command to configure the voice VLAN vpt value You can verify your settings by entering the show voice vlan Privileged EXEC command.

Example

The following example show how to set the vpt value.

Switch(config)#

voice-vlan vpt 3

```
Switch#
  show voice-vlan
Administrate Voice VLAN state : oui-enabled
Voice VLAN ID : 128
Voice VLAN VPT : 3
Voice VLAN DSCP : 46
Voice VLAN Aging : 1440 minutes
Voice VLAN CoS : 6
Voice VLAN 1p Remark: disabled
```

Voice VLAN DSCP

Syntax

voice-vlan dscp <0-63>

Parameter

<0-63> specify a value of DSCP that will be advertised by LLDP

Default

The default dscp value is 46.

Mode

Global Configuration

Usage

Use the voice vlan dscp global configuration command to configure the voice VLAN dscp value. You can verify your settings by entering the show voice vlan Privileged EXEC command.

Example

The following example show how to set dscp value.

Switch(config)#

voice-vlan dscp 55

```
Switch#
    show voice-vlan
Administrate Voice VLAN state : oui-enabled
Voice VLAN ID : 128
Voice VLAN VPT : 3
Voice VLAN DSCP : 55
Voice VLAN Aging : 1440 minutes
Voice VLAN CoS : 6
Voice VLAN 1p Remark: disabled
```

Voice VLAN OUI Table

Syntax

voice-vlan oui-table A:B:C DESCRIPTION

no voice-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 voice VLAN OUI table.

Default

The default system has 8 oui addresses.

Mode

Global Configuration

Usage

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

Example

This following example shows how to add OUI Mac.

Switch(config)#

voice-vlan oui-table add 00:01:02 “Test”

Switch#

show voice-vlan mode oui

Voice VLAN Aging : 1440 minutes

Voice VLAN CoS : 7

Voice VLAN 1p Remark: enabled

OUI table

OUI MAC | Description

00:E0:BB | 3COM

00:03:6B | Cisco

00:E0:75 | Veritel

00:D0:1E | Pingtel

00:01:E3 | Siemens

00:60:B9 | NEC/Philips

00:0F:E2 | H3C

Port | State | Cos Mode

fa1 | Disabled | Src

fa2 | Disabled | Src

fa3 | Disabled | Src

lag6 | Disabled | Src

lag7 | Disabled | Src

lag8 | Disabled | Src

Voice VLAN CoS

Syntax

voice-vlan cos <0-7> [remark]

no voice-vlan

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

Usage

Use the voice vlan cos global configuration command to configure the voice VLAN cos value and 1p remark function. You can verify your settings by entering the show voice vlan Privileged EXEC command.

Example

The following example shows how to set cos value and enable the 1p remark function.

Switch(config)#

voice-vlan cos 7 remark

```
Switch#
  show voice-vlan
Administrate Voice VLAN state : oui-enabled
Voice VLAN ID : 128
Voice VLAN VPT : 3
Voice VLAN DSCP : 55
Voice VLAN Aging : 1440 minutes
Voice VLAN CoS : 7
Voice VLAN 1p Remark: enable
```

Voice VLAN Aging-Time

Syntax

voice-vlan aing-time <30-1440>

Parameter

<30-1440> Specify the voice VLAN aging timeout interval in minutes

Default

The default aging-timeout value is 1440 minutes.

Mode

Global Configuration

Usage

Use the voice vlan aging-time global configuration command to configure the voice VLAN aging timeout. You can verify your settings by entering the show voice vlan Privileged EXEC command.

Example

The following example shows how to set the aging time.

Switch(config)#

voice-vlan aging-time 720

```
Switch#
  show voice-vlan
Administrate Voice VLAN state : oui-enabled
Voice VLAN ID : 128
Voice VLAN VPT : 3
Voice VLAN DSCP : 55
Voice VLAN Aging : 720 minutes
Voice VLAN CoS : 7
Voice VLAN 1p Remark: enable
```

Voice VLAN CoS Mode

Syntax

voice-vlan cos (src | all)

no voice-vlan

Parameter

src	Specify QoS attributes are applied to packets with OUIs in the source MAC address.
All	Specify QoS attributes are applied to packets that are classified to the Voice VLAN.

Default

The default all port in Src mode.

Mode

Interface configuration

Usage

Use the voice vlan cos mode Interface configuration command to configure the OUI voice VLAN cos mode. You can verify your settings by entering the show voice vlan Privileged EXEC command.

Example

The following example shows how to configure voice packet QoS attributes on an interface.

```
Switch(config)#
  interface range fa1-3
Switch(config-if)#
  voice-vlan cos all
Switch#
  show voice-vlan mode oui interfaces fa1-8
Voice VLAN Aging : 1440 minutes
Voice VLAN CoS : 7
Voice VLAN 1p Remark: enabled
```

OUI table

OUI MAC | Description

00:E0:BB | 3COM

00:03:6B | Cisco

00:E0:75 | Veritel

00:D0:1E | Pingtel

00:01:E3 | Siemens

00:60:B9 | NEC/Philips

00:0F:E2 | H3C

00:09:6E | Avaya

Port | State | Cos Mode

fa1 | Disabled | All

fa2 | Disabled | All

fa3 | Disabled | All

fa4 | Disabled | Src

fa5 | Disabled | Src

fa6 | Disabled | Src

fa7 | Disabled | Src

fa8 | Disabled | Src

Voice VLAN Enable

Syntax

voice-vlan mode

no voice-vlan

Parameter

None

Default

The default all port admin-staus is disabled.

Mode

Interface Configuration

Usage

Use the voice vlan enable Interface configuration command to enable the OUI voice VLAN settings on an interface. Use the no form of this command to disable voice vlan on an interface. You can verify your settings by entering the show voice vlan mode oui Privileged EXEC command.

Example

The following example shows how to enable the voice VLAN function in oui mode on an interface.

Switch(config)#

interface range fa1-3

Switch(config-if)#

voice-vlan

Switch#

show voice-vlan mode oui interfaces fa1-8

Voice VLAN Aging : 1440 minutes

Voice VLAN CoS : 7

Voice VLAN 1p Remark: enabled

OUI table

OUI MAC | Description

00:E0:BB | 3COM

00:03:6B | Cisco

00:E0:75 | Veritel

00:D0:1E | Pingtel

00:01:E3 | Siemens

00:60:B9 | NEC/Philips

00:0F:E2 | H3C

00:09:6E | Avaya

Port | State | Cos Mode

fa1 | Enabled | All

fa2 | Enabled | All

fa3 | Enabled | All

fa4 | Disabled | Src

fa5 | Disabled | Src

fa6 | Disabled | Src

fa7 | Disabled | Src

fa8 | Disabled | Src

Show Voice VLAN

Syntax

show voice-vlan

show voice-vlan mode auto

show voice-vlan mode oui [interfaces IF_PORTS]

Parameter

IF_PORTS Specifies intefaces to display voice VLAN settings in oui mode

Default

None

Mode

Privileged EXEC

Usage

Use the show voice vlan command in EXEC mode to display the voice VLAN status for all interfaces or for a specific interface if the voice VLAN type is an OUI.

Example

The following example shows how to display the voice vlan auto mode and oui mode settings.

Switch#

show voice-vlan mode auto

Voice VLAN ID : 128

Voice VLAN VPT : 3

Voice VLAN DSCP : 55

switch#

show voice-vlan mode oui interface fa1-5

Voice VLAN Aging : 1440 minutes

Voice VLAN CoS : 7

Voice VLAN 1p Remark: enabled

OUI table

OUI MAC | Description

00:E0:BB | 3COM

00:03:6B | Cisco

00:E0:75 | Veritel

00:D0:1E | Pingtel

00:01:E3 | Siemens

00:60:B9 | NEC/Philips

00:0F:E2 | H3C

00:09:6E | Avaya

Port | State | Cos Mode

fa1 | Disabled | Src

fa2 | Disabled | Src

fa3 | Disabled | Src

fa4 | Disabled | Src

fa5 | Disabled | Src