S3900 SERIES CLI REFERENCE GUIDE

Models:S3900-48T4S/S3900-24F4S/S3900-24T4S

USER MANUAL

Contents

1. User Interface Commands

The general commands are some basic functions.

Login

User can access switch through console or telnet.

The default administrator name/password is admin/admin.

The default guest name/password is guest/guest.

hostname

This command customizes the CLI prompt. Use the no form to restore the default prompt.

Syntax

hostname *string*

no hastname

string - Any alphanumeric string to use for the CLI prompt. (Maximum length: 255 characters)

Default Configuration

Console

Command Mode

Global Configuration

Example

Console(config)#hostname RD2

RD2(config)#

enable

This command activates EXEC mode. In privileged mode, additional commands are available, and certain commands display additional information.

Syntax

enable [*level*]

level - Privilege level to log into the device.

The device has two predefined privilege levels: 0: Normal Exec, 15: EXEC. Enter level 15 to access EXEC mode.

Default Configuration

Level 15

Command Mode

Normal Exec

User Guidelines

- "super" is the default password required to change the command mode from Normal Exec to EXEC. (To set this password, see the enable password command.)
- The "#" character is appended to the end of the prompt to indicate that the system is in privileged access mode.

Example

Console>enable

Password: [privileged level password]

Console#

disable

This command returns to Normal Exec mode from privileged mode. In normal access mode, you can only display basic information on the switch's configuration or Ethernet statistics. To gain access to all commands, you must use the privileged mode.

Default Configuration

None

Command Mode

EXEC

User Guidelines

The ">" character is appended to the end of the prompt to indicate that the system is in normal access mode.

Example

Console#disable

Console>

quit

This command exits the configuration program.

Default Configuration

None

Command Mode

Normal Exec, EXEC

User Guidelines

The quit and exit commands can both exit the configuration program.

Example

This example shows how to quit a CLI session:

Console#quit

Press ENTER to start session

User Access Verification

Username:

show history

This command shows the contents of the command history buffer.

Default Configuration

None

Command Mode

Normal Exec, EXEC

User Guidelines

The history buffer size is fixed at 10 Execution commands and 10 Configuration commands.

Example

In this example, the show history command lists the contents of the command history buffer:

Console#show history

Execution command history:

2 config

1 show history

Configuration command history:

4 interface vlan 1

3 exit
2 interface vlan 1
1 end
Console#

The ! command repeats commands from the Execution command history buffer when you are in Normal Exec or EXEC Mode, and commands from the Configuration command history buffer when you are in any of the configuration modes. In this example, the !2 command repeats the second command in the Execution history buffer (config).

Console#!2
Console#config
Console(config)#

configure terminal

This command activates Global Configuration mode. You must enter this mode to modify any settings on the switch. You must also enter Global Configuration mode prior to enabling some of the other configuration modes, such as Interface Configuration, Line Configuration, and VLAN Database Configuration.

Default Configuration

None

Command Mode

EXEC

Example

Console#configure terminal
Console(config)#

restart

This command restarts the system.

NOTE: When the system is restarted, it will always run the Power-On SelfTest. It will also retain all configuration information stored in non-volatile memory by the copy running-config startup-config command.

Default Configuration

None

Command Mode

EXEC

User Guidelines

This command resets the entire system.

Example

This example shows how to reset the switch:

Console#relstart
System will be restarted, continue <y/n>? y

end

This command returns to EXEC mode.

Default Configuration

None

Command Mode

Global Configuration, Interface Configuration, Line Configuration, VLAN Database Configuration, and Multiple Spanning Tree Configuration.

Example

This example shows how to return to the EXEC mode from the Interface Configuration mode:

Console(config-if)#end

Console#

exit

This command returns to the previous configuration mode or exits the configuration program.

Default Configuration

None

Command Mode

Any

Example

This example shows how to return to the EXEC mode from the Global Configuration mode, and then quit the CLI session:

Console(config)#exit

Console#exit

Press ENTER to start session

User Access Verification

Username:

2. Line Commands

You can access the onboard configuration program by attaching a VT100 compatible device to the server's serial port. These commands are used to set communication parameters for the serial port or Telnet (i.e., a virtual terminal).

line

This command identifies a specific line for configuration, and to process subsequent line configuration commands.

Syntax

line {console | vty}

console - Console terminal line.

vty - Virtual terminal for remote console access (i.e., Telnet).

Default Configuration

There is no default line.

Command Mode

Global Configuration

User Guidelines

Telnet is considered a virtual terminal connection and will be shown as "VTY" in screen displays such as show users. However, the serial communication parameters (e.g., databits) do not affect Telnet connections.

Example

To enter console line mode, enter the following command:

Console(config)#line console

Console(config-line)#

databits

This command sets the number of data bits per character that are interpreted and generated by the console port. Use the no form to restore the default value.

Syntax

databits {7 | 8}

no databits

7 - Seven data bits per character

8 - Eight data bits per character.

Default Configuration

8 data bits per character

Command Mode

Line Configuration

User Guidelines

The databits command can be used to mask the high bit on input from devices that generate 7 data bits with parity. If parity is being generated, specify 7 data bits per character. If no parity is required, specify 8 data bits per character.

Example

To specify 7 data bits, enter this command:

Console(config-line)#databits 7

Console(config-line)#

exec-timeout

This command sets the interval that the system waits until user input is detected.

Use the no form to restore the default.

Syntax

exec-timeout [*seconds*]

no exec-timeout

seconds - Integer that specifies the timeout interval. (Range: 60 - 65535 seconds; 0: no timeout)

Default Configuration

10 minutes

Command Mode

Line Configuration

User Guidelines

- If user input is detected within the timeout interval, the session is kept open; otherwise the session is terminated.
- This command applies to both the local console and Telnet connections.
- The timeout for Telnet cannot be disabled.
- Using the command without specifying a timeout restores the default setting.

Example

To set the timeout to two minutes, enter this command:

Console(config-line)#exec-timeout 120

Console(config-line)#

login

This command enables password checking at login. Use the no form to disable password checking and allow connections without a password.

Syntax

login [local]

no login

local - Selects local password checking. Authentication is based on the user name specified with the username command.

Default Configuration

login local

Command Mode

Line Configuration

User Guidelines

- There are three authentication modes provided by the switch itself at login:

a. login selects authentication by a single global password as specified by the password line configuration command. When using this method, the management interface starts in Normal Exec (NE) mode.

b. login local selects authentication via the user name and password specified by the username command (i.e., default setting). When using this method, the management interface starts in Normal Exec (NE) or EXEC (PE) mode, depending on the user's privilege level (0 or 15 respectively).

c. no login selects no authentication. When using this method, the management interface starts in Normal Exec (NE) mode.

- This command controls login authentication via the switch itself. To configure user names and passwords for remote authentication servers, you must use the RADIUS or TACACS software installed on those servers.
- Example

Console(config-line)#login local

Console(config-line)#

parity

This command defines the generation of a parity bit. Use the no form to restore the default setting.

Syntax

parity {none | even | odd}

no parity

none - No parity

even - Even parity

odd - Odd parity

Default Configuration

No parity

Command Mode

Line Configuration

User Guidelines

Communication protocols provided by devices such as terminals and modems often require a specific parity bit setting.

Example

To specify no parity, enter this command:

Console(config-line)#parity none

Console(config-line)#

password

This command specifies the password for a line. Use the no form to remove the password.

Syntax

password {0 | 7} *password*

no password

{0 | 7} - 0 means plain password, 7 means encrypted password

password - Character string that specifies the line password. (Maximum length: 32 characters plain text or encrypted, case sensitive)

Default Configuration

No password is specified.

Command Mode

Line Configuration

User Guidelines

- When a connection is started on a line with password protection, the system prompts for the password. If you enter the correct password, the system shows a prompt. You can use the password-thresh command to set the number of times a user can enter an incorrect password before the system terminates the line connection and returns the terminal to the idle state.
- The encrypted password is required for compatibility with legacy password settings (i.e., plain text or encrypted) when reading the configuration file during system bootup or when downloading the configuration file from an FTP server. There is no need for you to manually configure encrypted passwords.
- Example

To specify no parity, enter this command:

Console(config-line)# password 0 secret

Console(config-line)#

password-thresh

This command sets the password intrusion threshold which limits the number of failed logon attempts. Use the no form to remove the threshold value.

Syntax

password-thresh [*threshold*]

no password-thresh

threshold - The number of allowed password attempts. (Range: 1-120; 0: no threshold)

Default Configuration

The default value is three attempts.

Command Mode

Line Configuration

User Guidelines

When the logon attempt threshold is reached, the system interface becomes silent for a specified amount of time before allowing the next logon attempt. (Use the silent-time command to set this interval.) When this threshold is reached for Telnet, the Telnet logon interface shuts down.

Example

To set the password threshold to five attempts, enter this command:

Console(config-line)#password-thresh 5

Console(config-line)#

silent-time

This command sets the amount of time the management console is inaccessible after the number of unsuccessful logon attempts exceeds the threshold set by the password-thresh command. Use the no form to remove the silent time value.

Syntax

silent-time [*seconds*]

no silent-time

seconds - The number of seconds to disable console response. (Range: 0-65535; where 0 means disabled)

Default Configuration

Disabled

Command Mode

Line Configuration

Example

To set the silent time to 60 seconds, enter this command:

Console(config-line)# silent-time 60

Console(config-line)#

speed

This command sets the terminal line's baud rate. This command sets both the transmit (to terminal) and receive (from terminal) speeds. Use the no form to restore the default setting.

Syntax

speed *bps*

no speed

bps - Baud rate in bits per second. (Options: 9600, 19200, 38400, 57600, 115200 bps)

Default Configuration

115200 bps

Command Mode

Line Configuration

User Guidelines

Set the speed to match the baud rate of the device connected to the serial port. Some baud rates available on devices connected to the port might not be supported. The system indicates if the speed you selected is not supported.

Example

To specify 57600 bps, enter this command:

Console(config-line)#speed 57600

Console(config-line)#

stopbits

This command sets the number of the stop bits transmitted per byte. Use the no form to restore the default setting.

Syntax

stopbits {1 | 2}

no stopbits

1 - One stop bit

2 - Two stop bits

Default Configuration

1 stop bit

Command Mode

Line Configuration

Example

To specify 2 stop bits, enter this command:

Console(config-line)#stopbits 2

Console(config-line)#

timeout login response

This command sets the interval that the system waits for a user to log into the CLI. Use the no form to restore the default setting.

Syntax

timeout login response [*seconds*]

no timeout login response

seconds - Integer that specifies the timeout interval. (Range: 10 - 300 seconds)

Default Configuration

300 seconds

Command Mode

Line Configuration

User Guidelines

- If a login attempt is not detected within the timeout interval, the connection is
- terminated for the session.
- This command applies to both the local console and Telnet connections.
- The timeout for Telnet cannot be disabled.
- Using the command without specifying a timeout restores the default setting.
- Example

To set the timeout to two minutes, enter this command:

Console(config-line)#timeout login response 120

Console(config-line)#

disconnect

This command terminates an SSH, Telnet, or console connection.

Syntax

disconnect *session-id*

session-id – The session identifier for an SSH, Telnet or console connection.

(Range: 0-8)

Command Mode

EXEC

User Guidelines

Specifying session identifier "0" will disconnect the console connection. Specifying any other identifiers for an active session will disconnect an SSH or Telnet connection.

Example

Console#disconnect 1

Console#

show line

This command displays the terminal line's parameters.

Syntax

show line [console | vty]

console - Console terminal line.

vty - Virtual terminal for remote console access (i.e., Telnet).

Default Configuration

Shows all lines

Command Mode

Normal Exec, EXEC

User Guidelines

- If a login attempt is not detected within the timeout interval, the connection is
- terminated for the session.
- This command applies to both the local console and Telnet connections.
- The timeout for Telnet cannot be disabled.
- Using the command without specifying a timeout restores the default setting.

Example

To show all lines, enter this command:

Console#show line

Terminal Configuration for this session:

Length : 24

Width : 80

History Size : 10

Escape Character(ASCII-number) : 27

Terminal Type : VT100

Console Configuration:

Password Threshold: 3 times

EXEC Timeout: 600 seconds

Login Timeout: 300 seconds

Silent Time: Disabled

Baud Rate: 115200

Data Bits: 8

Parity: None

Stop Bits: 1

VTY Configuration:

Password Threshold: 3 times

EXEC Timeout: 600 seconds

Login Timeout: 300 sec.

Silent Time: Disabled

Console#

3. Log Commands

This section describes commands used to configure event logging on the switch.

logging level

This command limits syslog messages saved to switch memory based on severity. The no form returns the logging of syslog messages to the default level.

Syntax

logging level {flash | ram} *level*

no logging level {flash | ram}

flash - Event history stored in flash memory (i.e., permanent memory).

ram - Event history stored in temporary RAM (i.e., memory flushed on power reset).

level - One of the levels listed below. Messages sent include the selected level down to level 0. (Range: 0-7)

Level	Severity Name	Description
7	debugging	Debug information
6	messages	normal messages
5	notifications	notification of system.
4	warnings	Warning conditions
3	minor	minor alarm
2	normal	normal alarm
1	Critical	Critical alarm
0	emergencies	System unusable

Default Configuration

Flash: errors (level 3 - 0)

RAM: debugging (level 7 - 0)

Command Mode

Global Configuration

User Guidelines

The message level specified for flash memory must be a higher priority

(i.e., numerically lower) than that specified for RAM.

Example

Console(config)#logging level ram 0

Console(config)#

logging host

This command adds a syslog server host IP address that will receive logging messages. Use the no form to remove a syslog server host.

Syntax

[no] logging host *host-ip-address*

host-ip-address - The IP address of a syslog server.

Default Configuration

None

Command Mode

Global Configuration

User Guidelines

- Use this command more than once to build up a list of host IP addresses.
- The maximum number of host IP addresses allowed is five.

Example

Console(config)#logging host 10.1.0.3

Console(config)#

logging on

This command controls logging of error messages, sending debug or error messages to a logging process. The no form disables the logging process.

Syntax

[no] logging on

Default Configuration

None

Command Mode

Global Configuration

User Guidelines

The logging process controls error messages saved to switch memory or sent to remote syslog servers. You can use the logging level command to control the type of error messages that are stored in memory. You can use the logging trap command to control the type of error messages that are sent to specified syslog servers.

Example

Console(config)#logging on

Console(config)

clear logging

This command clears messages from the log buffer.

Syntax

clear logging [flash | ram]

flash - Event history stored in flash memory (i.e., permanent

memory).

ram - Event history stored in temporary RAM (i.e., memory flushed

on power reset).

Default Configuration

Flash and RAM

Command Mode

EXEC

Example

Console#clear logging

Console#

show log

This command displays the log messages stored in local memory.

Syntax

show log {flash | ram}

flash - Event history stored in flash memory (i.e., permanent memory).

ram - Event history stored in temporary RAM (i.e., memory flushed on power reset).

Default Configuration

None

Command Mode

EXEC

User Guidelines

- All log messages are retained in RAM and Flash after a warm restart (i.e., power is reset through the command interface).
- All log messages are retained in Flash and purged from RAM after a cold restart (i.e., power is turned off and then on through the power source).

Example

The following example shows the event message stored in RAM.

Console#show log ram

[1] 00:01:30 2001-01-01

"VLAN 1 link-up notification."

level: 6, module: 5, function: 1, and event no.: 1

[0] 00:01:30 2001-01-01

"Unit 1, Port 1 link-up notification."

level: 6, module: 5, function: 1, and event no.: 1

Console#

show logging

This command displays the configuration settings for logging messages to local switch memory, to an SMTP event handler, or to a remote syslog server.

Syntax

show logging {flash | ram | mail}

flash - Displays settings for storing event messages in flash memory (i.e., permanent memory).

ram - Displays settings for storing event messages in temporary RAM (i.e., memory flushed on power reset).

mail - Displays settings for the SMTP event handler

Default Configuration

None

Command Mode

EXEC

Example

The following example shows that system logging is enabled, the message level for flash memory is “errors” (i.e., default level 3 - 0), and the message level for RAM is “debugging” (i.e., default level 7 - 0).

Console#show logging flash

Syslog logging: Enabled

History logging in FLASH: level errors

Console#show logging ram

Syslog logging: Enabled

History logging in RAM: level debugging

Console#

These commands configure SMTP event handling, and forwarding of alert messages to the specified SMTP servers and email recipients.

logging mail

This command enables SMTP event handling. Use the no form to disable this function.

Syntax

[no] logging mail

Default Configuration

Enabled

Command Mode

Global Configuration

Example

Console(config)#logging mail

Console(config)#

logging mail host

This command specifies SMTP servers that will be sent alert messages. Use the no form to remove an SMTP server.

Syntax

[no] logging mail host *ip-address*

ip-address - IPv4 or IPv6 address of an SMTP server that will be sent alert messages for event handling.

Default Configuration

None

Command Mode

Global Configuration

User Guidelines

- You can specify up to three SMTP servers for event handing. However, you must enter a separate command to specify each server.
- To send email alerts, the switch first opens a connection, sends all the email alerts waiting in the queue one by one, and finally closes the connection.
- To open a connection, the switch first selects the server that successfully sent mail during the last connection, or the first server configured by this command. If it fails to send mail, the switch selects the next server in the list and tries to send mail again. If it still fails, the system will repeat the process at a periodic interval. (A trap will be triggered if the switch cannot successfully open a connection.)

Example

Console(config)#logging mail host 192.168.1.19

Console(config)#

logging mail level

This command sets the severity threshold used to trigger alert messages. Use the no form to restore the default setting.

Syntax

logging mail level *level*

no logging mail level

level - One of the system message levels. Messages

sent include the selected level down to level 0. (Range: 0-7; Default: 7)

Default Configuration

Level 7

Command Mode

Global Configuration

User Guidelines

The specified level indicates an event threshold. All events at this level or higher will be sent to the configured email recipients. (For example, using Level 7 will report all events from level 7 to level 0.)

Example

This example will send email alerts for system errors from level 3 through 0.

Console(config)#logging mail level 3

Console(config)#

logging mail destination

This command specifies the email recipients of alert messages. Use the no form to remove a recipient.

Syntax

[no] logging mail destination *email-address*

email-address - The destination email address used in alert messages. (Range: 1-41 characters)

Default Configuration

None

Command Mode

Global Configuration

User Guidelines

You can specify up to five recipients for alert messages. However, you must enter a separate command to specify each recipient.

Example

Console(config)#logging mail destination ted@this-company.com

Console(config)#

logging mail source

This command sets the email address used for the "From" field in alert messages. Use the no form to restore the default value.

Syntax

logging mail source *email-address*

no logging mail source

email-address - The source email address used in alert messages. (Range: 1-41 characters)

Default Configuration

None

Command Mode

Global Configuration

User Guidelines

You may use an symbolic email address that identifies the switch, or the address of an administrator responsible for the switch.

Example

Console(config)#logging mail source bill@this-company.com

Console(config)#

show logging mail

This command displays the settings for the SMTP event handler.

Command Mode

Normal Exec, EXEC

Example

Console#show logging mail

SMTP servers

192.168.1.19

SMTP Minimum Severity Level: 7

SMTP destination email addresses

---

ted@this-company.com

SMTP Source Email Address: bill@this-company.com

SMTP Status: Enabled

Console#

3.1 Clock Commands

sntp client

This command enables SNTP client requests for time synchronization from NTP or SNTP time servers specified with the sntp server command. Use the no form to disable SNTP client requests.

Syntax

[no] sntp client

Default Configuration

Disabled

Command Mode

Global Configuration

User Guidelines

- The time acquired from time servers is used to record accurate dates and times for log events. Without SNTP, the switch only records the time starting from the factory default set at the last bootup (i.e., 00:00:00, Jan. 1, 2001).
- This command enables client time requests to time servers specified via the sntp server command. It issues time synchronization requests based on the interval set via the sntp poll command.

Example

Console(config)#sntp server 10.1.0.19

Console(config)#sntp poll 60

Console(config)#sntp client

Console(config)#end

Console#show sntp

Current Time: Dec 23 02:52:44 2002

Poll Interval: 60

Current Mode: unicast

SNTP Status: Enabled

SNTP Server 137.92.140.80 0.0.0.0 0.0.0.0

Current Server: 137.92.140.80

Console#

sntp poll

This command sets the interval between sending time requests when the switch is set to SNTP client mode. Use the no form to restore to the default.

Syntax

sntp poll *seconds*

no sntp poll

seconds - Interval between time requests.

(Range: 16-16384 seconds)

Default Configuration

16 seconds

Command Mode

Global Configuration

Example

Console(config)#sntp poll 60

Console#

sntp server

This command sets the IP address of the servers to which SNTP time requests are issued. Use the this command with no arguments to clear all time servers from the current list. Use the no form to clear all time servers from the current list, or to clear a specific server.

Syntax

sntp server [*ip1* [*ip2* [*ip3*]]]

no sntp server [*ip1* [*ip2* [*ip3*]]]

ip - IP address of a time server (NTP or SNTP). (Range: 1 - 3 addresses)

Default Configuration

None

Command Mode

Global Configuration

User Guidelines

This command specifies time servers from which the switch will poll for time updates when set to SNTP client mode. The client will poll the time servers in the order specified until a response is received. It issues time synchronization requests based on the interval set via the sntp poll command.

Example

Console(config)#sntp server 10.1.0.19

Console#

show sntp

This command displays the current time and configuration settings for the SNTP client, and indicates whether or not the local time has been properly updated.

Command Mode

Normal Exec, EXEC

User Guidelines

This command displays the current time, the poll interval used for sending time synchronization requests, and the current SNTP mode (i.e., unicast).

Example

Console#show sntp

Current Time : Nov 5 18:51:22 2006

Poll Interval : 16 seconds

Current Mode : Unicast

SNTP Status : Enabled

SNTP Server : 137.92.140.80 0.0.0.0 0.0.0.0

Current Server : 137.92.140.80

Console#

ntp authenticate

This command enables authentication for NTP client-server communications. Use the no form to disable authentication.

Syntax

[no] ntp authenticate

Default Configuration

Disabled

Command Mode

Global Configuration

User Guidelines

You can enable NTP authentication to ensure that reliable updates are received from only authorized NTP servers. The authentication keys and their associated key number must be centrally managed and manually distributed to NTP servers and clients. The key numbers and key values must match on both the server and client.

Example

Console(config)#ntp authenticate

Console(config)#

ntp authentication-key

This command configures authentication keys and key numbers to use when NTP authentication is enabled. Use the no form of the command to clear a specific authentication key or all keys from the current list.

Syntax

ntp authentication-key *number* md5 *key*

no ntp authentication-key [*number*]

number - The NTP authentication key ID number. (Range: 1-65535)

md5 - Specifies that authentication is provided by using the message digest algorithm 5.

key - An MD5 authentication key string. The key string can be up to 32 case-sensitive printable ASCII characters (no spaces).

Default Configuration

None

Command Mode

Global Configuration

User Guidelines

- The key number specifies a key value in the NTP authentication key list. Up to 255 keys can be configured on the switch. Re-enter this command for each server you want to configure.
- Note that NTP authentication key numbers and values must match on both the server and client.
- NTP authentication is optional. When enabled with the ntp authenticate command, you must also configure at least one key number using this command.
- Use the no form of this command without an argument to clear all authentication keys in the list.

Example

Console(config)#ntp authentication-key 45 md5 thisiskey45

Console(config)#

ntp client

This command enables NTP client requests for time synchronization from NTP time servers specified with the ntp servers command. Use the no form to disable NTP client requests.

Syntax

[no] ntp client

Default Configuration

Disabled

Command Mode

Global Configuration

User Guidelines

- The SNTP and NTP clients cannot be enabled at the same time. First disable the SNTP client before using this command.
- The time acquired from time servers is used to record accurate dates and times for log events. Without NTP, the switch only records the time starting from the factory default set at the last bootup (i.e., 00:00:00, Jan. 1, 2001).
- This command enables client time requests to time servers specified via the ntp servers command. It issues time synchronization requests based on the interval set via the ntp poll command.

Example

Console(config)#ntp client

Console(config)#

ntp server

This command sets the IP addresses of the servers to which NTP time requests are issued. Use the no form of the command to clear a specific time server or all servers from the current list.

Syntax

ntp server *ip-address* [key *key-number*]

no ntp server [*ip-address*]

ip-address - IP address of an NTP time server.

key-number - The number of an authentication key to use in communications with the server. (Range: 1-65535)

Default Configuration

Version number: 3

Command Mode

Global Configuration

User Guidelines

- This command specifies time servers that the switch will poll for time updates when set to NTP client mode. It issues time synchronization requests based on the interval set with the ntp poll command. The client will poll all the time servers configured, the responses received are filtered and compared to determine the most reliable and accurate time update for the switch.
- You can configure up to 50 NTP servers on the switch. Re-enter this command for each server you want to configure.
- NTP authentication is optional. If enabled with the ntp authenticate command, you must also configure at least one key number using the ntp authentication-key command.
- Use the no form of this command without an argument to clear all configured servers in the list.

Example

Console(config)#ntp server 192.168.10.20

Console(config)#ntp server 192.168.10.11

Console(config)#ntp server 192.168.5.25 key 21

Console(config)#

show ntp

This command displays the current time and configuration settings for the NTP client, and indicates whether or not the local time has been properly updated.

Command Mode

Normal Exec, EXEC

User Guidelines

This command displays the current time, the poll interval used for sending time synchronization requests, and the current NTP mode (i.e., unicast).

Example

Console#show ntp

Current Time: Apr 20 18:37:34 2015

Polling: 1024 seconds

Current Mode: unicast

NTP Status: Disabled

NTP Authenticate Status: Enabled

Last Update NTP Server: 0.0.0.0 Port: 0

Last Update Time: Jan 1 00:00:00 1970 UTC

NTP Server 192.168.10.20 version 3

NTP Server 192.168.10.21 version 3

NTP Server 192.168.3.22 version 3 key 3

NTP Authentication Key 19 md5 42V68751663T6K11P2J307210R885

Console#

clock timezone

This command sets the time zone for the switch's internal clock.

Syntax

clock timezone *name* hour *hours* minute *minutes* {before-utc | after-utc}

name - Name of timezone, usually an acronym. (Range: 1-30 characters)

hours - Number of hours before/after UTC. (Range: 0-12 hours before UTC, 0-13 hours after UTC)

minutes - Number of minutes before/after UTC. (Range: 0-59 minutes)

before-utc - Sets the local time zone before (east) of UTC.

after-utc - Sets the local time zone after (west) of UTC.

Default Configuration

None

Command Mode

Global Configuration

User Guidelines

This command sets the local time zone relative to the Coordinated Universal Time (UTC, formerly Greenwich Mean Time or GMT), based on the earth's prime meridian, zero degrees longitude. To display a time corresponding to your local time, you must indicate the number of hours and minutes your time zone is east (before) or west (after) of UTC.

Example

Console(config)#clock timezone Japan hours 8 minute 0 after-UTC

Console(config)#

calendar set

This command sets the system clock. It may be used if there is no time server on your network, or if you have not configured the switch to receive signals from a time server.

Syntax

calendar set *hour min sec* {*day month year* | *month day year*}

hour - Hour in 24-hour format. (Range: 0 - 23)

min - Minute. (Range: 0 - 59)

sec - Second. (Range: 0 - 59)

day - Day of month. (Range: 1 - 31)

month - january | february | march | april | may | june | july | august | september | october | november | december

year - Year (4-digit). (Range: 1970 - 2037)

Default Configuration

None

Command Mode

EXEC

User Guidelines

Note that when SNTP is enabled, the system clock cannot be manually configured.

Example

This example shows how to set the system clock to 16:17:35, February 1st, 2016.

Console#calendar set 16:17:35 1 February 2016

Console#

show calendar

This command displays the system clock.

Default Configuration

None

Command Mode

Normal Exec, EXEC

Example

Console#show calendar

16:17:35 1 February 2016

Console#

time-range

This command specifies the name of a time range, and enters time range configuration mode. Use the no form to remove a previously specified time range.

Syntax

[no] time-range *name*

name - Name of the time range. (Range: 1-16 characters)

Default Configuration

None

Command Mode

Global Configuration

User Guidelines

This command sets a time range for use by other functions, such as Access Control Lists.

Example

Console(config)#time-range r&d

Console(config-time-range)#

absolute

This command sets the time range for the execution of a command. Use the no form to remove a previously specified time.

Syntax

absolute start *hour minute day month year* [end *hour minutes day month year*]

absolute end *hour minutes day month year*

no absolute

hour - Hour in 24-hour format. (Range: 0-23)

minute - Minute. (Range: 0-59)

day - Day of month. (Range: 1-31)

month - january | february | march | april | may | june | july | august | september | october | november | december

year - Year (4-digit). (Range: 2009-2109)

Default Configuration

None

Command Mode

Time Range Configuration

User Guidelines

- If a time range is already configured, you must use the no form of this command to remove the current entry prior to configuring a new time range.
- If both an absolute rule and one or more periodic rules are configured for the same time range (i.e., named entry), that entry will only take effect if the current time is within the absolute time range and one of the periodic time ranges.

Example

This example configures the time for the single occurrence of an event.

Console(config)#time-range r&d

Console(config-time-range)#absolute start 1 2 3 april 2014 end 2 3 1 april

2014

Console(config-time-range)#

periodic

This command sets the time range for the periodic execution of a command. Use the no form to remove a previously specified time range.

Syntax

[no] periodic {daily | friday | monday | saturday | sunday | thursday | tuesday | wednesday | weekdays | weekend} *hour minute* to {daily | friday | monday | saturday | sunday | thursday | tuesday | wednesday | weekdays | weekend | *hour minute*}

daily - Daily

friday - Friday

monday - Monday

saturday - Saturday

sunday - Sunday

thursday - Thursday

tuesday - Tuesday

wednesday - Wednesday

weekdays - Weekdays

weekend - Weekends

hour - Hour in 24-hour format. (Range: 0-23)

minute - Minute. (Range: 0-59)

Default Configuration

None

Command Mode

Time Range Configuration

User Guidelines

- If a time range is already configured, you must use the no form of this command to remove the current entry prior to configuring a new time range.
- If both an absolute rule and one or more periodic rules are configured for the same time range (i.e., named entry), that entry will only take effect if the current time is within the absolute time range and one of the periodic time ranges.

Example

This example configures a time range for the periodic occurrence of an event.

Console(config)#time-range sales

Console(config-time-range)#periodic daily 2 1 to 3 1

Console(config-time-range)#

show time-range

This command shows configured time ranges.

Syntax

show time-range [*name*]

name - Name of the time range. (Range: 1-30 characters)

Default Configuration

None

Command Mode

EXEC

Example

Console#show time-range r&d

Time-range r&d:

absolute start 01:01 01 April 2009

periodic Daily 01:01 to Daily 02:01

periodic Daily 02:01 to Daily 03:01

Console#

4. Clustering Commands

Switch Clustering is a method of grouping switches together to enable centralized management through a single unit. Switches that support clustering can be grouped together regardless of physical location or switch type, as long as they are connected to the same local network.

Using Switch Clustering

- A switch cluster has a primary unit called the "Commander" which is used to manage all other "Member" switches in the cluster. The management station can use either Telnet or the web interface to communicate directly with the Commander through its IP address, and then use the Commander to manage the Member switches through the cluster's "internal" IP addresses.
- Clustered switches must be in the same Ethernet broadcast domain. In other words, clustering only functions for switches which can pass information between the Commander and potential Candidates or active Members through VLAN 4094.
- Once a switch has been configured to be a cluster Commander, it automatically discovers other cluster-enabled switches in the network.

These "Candidate" switches only become cluster Members when manually selected by the administrator through the management station.

Note:

Cluster Member switches can be managed either through a Telnet connection to the Commander, or through a web management connection to the Commander. When using a console connection, from the Commander CLI prompt, use the rcommand to connect to the Member switch.

cluster

This command enables clustering on the switch. Use the no form to disable clustering.

Syntax

[no] cluster

Default Configuration

Disabled

Command Mode

Global Configuration

User Guidelines

- To create a switch cluster, first be sure that clustering is enabled on the switch (the default is enabled), then set the switch as a Cluster Commander. Set a Cluster IP Pool that does not conflict with any other IP subnets in the network. Cluster IP addresses are assigned to switches when they become Members and are used for communication between Member switches and the Commander.
- Switch clusters are limited to the same Ethernet broadcast domain.
- There can be up to 100 candidates and 36 member switches in one cluster.
- A switch can only be a Member of one cluster.
- Configured switch clusters are maintained across power resets and network changes.

Example

Console(config)#cluster

Console(config)#

cluster commander

This command enables the switch as a cluster Commander. Use the no form to disable the switch as cluster Commander.

Syntax

[no] cluster commander

Default Configuration

Disabled

Command Mode

Global Configuration

User Guidelines

- Once a switch has been configured to be a cluster Commander, it automatically discovers other cluster-enabled switches in the network. These "Candidate" switches only become cluster Members when manually selected by the administrator through the management station.
- Cluster Member switches can be managed through a Telnet connection to the Commander. From the Commander CLI prompt, use the rcommand id command to connect to the Member switch.

Example

Console(config)#cluster commander

Console(config)#

cluster ip-pool

This command sets the cluster IP address pool. Use the no form to reset to the default address.

Syntax

cluster ip-pool *ip-address*

no cluster ip-pool

ip-address - The base IP address for IP addresses assigned to cluster Members. The IP address must start 10.x.x.x.

Default Configuration

10.254.254.1

Command Mode

Global Configuration

User Guidelines

- An "internal" IP address pool is used to assign IP addresses to Member switches in the cluster. Internal cluster IP addresses are in the form 10.*x.x.member-ID*. Only the base IP address of the pool needs to be set since Member IDs can only be between 1 and 36.
- Set a Cluster IP Pool that does not conflict with addresses in the network IP subnet. Cluster IP addresses are assigned to switches when they become Members and are used for communication between Member switches and the Commander.
- You cannot change the cluster IP pool when the switch is currently in Commander mode. Commander mode must first be disabled.

Example

Console(config)#cluster ip-pool 10.4.3.2

Console(config)#

cluster member

This command configures a Candidate switch as a cluster Member. Use the no form to remove a Member switch from the cluster.

Syntax

cluster member mac-address *mac-address* id *member-id*

no cluster member id *member-id*

mac-address - The MAC address of the Candidate switch.

member-id - The ID number to assign to the Member switch. (Range: 1-36)

Default Configuration

No Members

Command Mode

Global Configuration

User Guidelines

- The maximum number of cluster Members is 36.
- The maximum number of cluster Candidates is 100.

Example

Console(config)#cluster member mac-address 00-32-34-66-76-6a id 4

Console(config)#

rcommand

This command provides access to a cluster Member CLI for configuration.

Syntax

rcommand id *member-id*

member-id - The ID number of the Member switch. (Range: 1-36)

Command Mode

EXEC

User Guidelines

- This command only operates through a Telnet connection to the Commander switch. Managing cluster Members using the local console CLI on the Commander is not supported.
- There is no need to enter the username and password for access to the Member switch CLI.

Example

Console#rcommand id 1

CLI session with the S3900 is opened.

To end the CLI session, enter [Exit].

Vty-0#

show cluster

This command shows the switch clustering configuration.

Command Mode

EXEC

Example

Console#show cluster

Role : commander

Interval Heartbeat : 30

Heartbeat Loss Count : 3 seconds

Number of Members : 1

Number of Candidates : 2

Console#

show cluster candidates

This command shows the discovered Candidate switches in the network.

Command Mode

EXEC

Example

Console#show cluster candidates

Cluster Candidates:

Role MAC Address Description

---------- ---------- ----------

Active member 64-9D-99-00-00-FE S3900

CANDIDATE 64-9D-99-0B-47-A0 S3900

Console#

show cluster members

This command shows the current switch cluster members.

Command Mode

EXEC

Example

Console#show cluster members

Cluster Members:

ID: 1

Role: Active member

IP Address: 10.254.254.2

MAC Address: 64-9D-99-00-00-FE

Description: S3900

Console#

5. SNMP Commands

SNMP commands control access to this switch from management stations using the Simple Network Management Protocol (SNMP), as well as the error types sent to trap managers.

SNMP Version 3 also provides security features that cover message

integrity, authentication, and encryption; as well as controlling user access to specific areas of the MIB tree. To use SNMPv3, first set an SNMP engine ID (or accept the default), specify read and write access views for the MIB tree, configure SNMP user groups with the required security model (i.e., SNMP v1, v2c or v3) and security level (i.e., authentication and privacy), and then assign SNMP users to these groups, along with their specific authentication and privacy passwords.

5.1General SNMP Commands

snmp-server server

This command enables the SNMPv3 engine and services for all management clients (i.e., versions 1, 2c, 3). Use the no form to disable the server.

Syntax

[no] snmp-server server

Default Configuration

Enabled

Command Mode

Global Configuration

Example

Console(config)#snmp-server server

Console(config)#

snmp-server community

This command defines community access strings used to authorize management access by clients using SNMP v1 or v2c. Use the no form to remove the specified community string.

Syntax

snmp-server community *string* [ro | rw]

no snmp-server community *string*

string - Community string that acts like a password and permits access to the SNMP protocol. (Maximum length: 32 characters, case sensitive; Maximum number of strings: 5)

ro - Specifies read-only access. Authorized management stations are only able to retrieve MIB objects.

rw - Specifies read/write access. Authorized management stations are able to both retrieve and modify MIB objects.

Default Configuration

- public - read-only access. Authorized management stations are only able to retrieve MIB objects.
- private - read/write access. Authorized management stations are able to both retrieve and modify MIB objects.

Command Mode

Global Configuration

Example

Console(config)#snmp-server community alpha rw

Console(config)#

snmp-server contact

This command sets the system contact string. Use the no form to remove the system contact information.

Syntax

snmp-server contact *string*

no snmp-server contact

string - String that describes the system contact information. (Maximum length: 255 characters)

Default Configuration

None

Command Mode

Global Configuration

Example

Console(config)#snmp-server contact Paul

Console(config)#

snmp-server location

This command sets the system location string. Use the no form to remove the location string.

Syntax

snmp-server location *text*

no snmp-server location

text - String that describes the system location. (Maximum length: 255 characters)

Default Configuration

None

Command Mode

Global Configuration

Example

Console(config)#snmp-server location WC-19

Console(config)#

show snmp

This command can be used to check the status of SNMP communications.

Default Configuration

None

Command Mode

Normal Exec, EXEC

User Guidelines

This command provides information on the community access strings, counters for SNMP input and output protocol data units, and whether or not SNMP logging has been enabled with the snmp-server enable traps command.

Example

Console#show snmp

SNMP Agent: Enabled

SNMP Traps:

Authentication: Enabled

Link-up-down: Enabled

SNMP Communities:

1. public, and the access level is read-only

2. private, and the access level is read/write

0 SNMP packets input
0 Bad SNMP version errors
0 Unknown community name
0 Illegal operation for community name supplied
0 Encoding errors
0 Number of requested variables
0 Number of altered variables
0 Get-request PDUs
0 Get-next PDUs
0 Set-request PDUs
0 SNMP packets output
0 Too big errors
0 No such name errors
0 Bad values errors
0 General errors
0 Response PDUs
0 Trap PDUs
SNMP Logging: Disabled
Console#

5.2 SNMP Target Host Commands

snmp-server enable traps

This command enables this device to send Simple Network Management Protocol traps or informs (i.e., SNMP notifications). Use the no form to disable SNMP notifications.

Syntax

[no] snmp-server enable traps [authentication | link-up-down | ethernet cfm]

authentication - Keyword to issue authentication failure notifications.

link-up-down - Keyword to issue link-up or link-down notifications.

ethernet cfm - Connectivity Fault Management traps.

Default Configuration

Issue authentication and link-up-down traps.

Command Mode

Global Configuration

User Guidelines

- If you do not enter a snmp-server enable traps command, no notifications controlled by this command are sent. In order to configure this device to send SNMP notifications, you must enter at least one snmp-server enable traps command. If you enter the command with no keywords, both authentication and link-up-down notifications are enabled. If you enter the command with a keyword, only the notification type related to that keyword is enabled.
- The snmp-server enable traps command is used in conjunction with the snmp-server host command. Use the snmp-server host command to specify which host or hosts receive SNMP notifications. In order to send notifications, you must configure at least one snmp-server host command.

- The authentication, link-up, and link-down traps are legacy notifications, and therefore when used for SNMP Version 3 hosts, they must be enabled in conjunction with the corresponding entries in the Notify View assigned by the snmp-server group command.

Example

Console(config)#snmp-server enable traps link-up-down

Console(config)#

snmp-server host

This command specifies the recipient of a Simple Network Management Protocol notification operation. Use the no form to remove the specified

host.

Syntax

snmp-server host *host-addr* [inform [retry *retries* | timeout *seconds*]] *community-string* [version {1 | 2c | 3 {auth | noauth | priv} [udp-port *port*]}

no snmp-server host *host-addr*

host-addr - Internet address of the host (the targeted recipient). (Maximum host addresses: 5 trap destination IP address entries)

inform - Notifications are sent as inform messages. Note that this option is only available for version 2c and 3 hosts. (Default: traps are used)

retries - The maximum number of times to resend an inform message if the recipient does not acknowledge receipt. (Range: 0-255; Default: 3)

seconds - The number of seconds to wait for an acknowledgment before resending an inform message. (Range: 0-2147483647 centiseconds; Default: 1500 centiseconds)

community-string - Password-like community string sent with the notification operation to SNMP V1 and V2c hosts. Although you can set this string using the snmp-server host command by itself, we recommend defining it with the snmp-server community command prior to using the snmp-server host command. (Maximum length: 32 characters)

version - Specifies whether to send notifications as SNMP Version 1, 2c or 3 traps. (Range: 1, 2c, 3; Default: 1)

auth | noauth | priv - This group uses SNMPv3 with authentication, no authentication, or with authentication and privacy.

port - Host UDP port to use. (Range: 1-65535; Default: 162)

Default Configuration

Host Address: None

Notification Type: Traps

SNMP Version: 1

UDP Port: 162

Command Mode

Global Configuration

User Guidelines

- If you do not enter a snmp-server host command, no notifications are sent. In order to configure the switch to send SNMP notifications, you must enter at least one snmp-server host command. In order to enable multiple hosts, you must issue a separate snmp-server host command for each host.
- The snmp-server host command is used in conjunction with the snmp-server enable traps command. Use the snmp-server enable traps command to enable the sending of traps or informs and to specify which SNMP notifications are sent globally. For a host to receive notifications, at least one snmp-server enable traps command and the snmp-server host command for that host must be enabled.

- Some notification types cannot be controlled with the snmp-server enable traps command. For example, some notification types are always enabled.
- Notifications are issued by the switch as trap messages by default. The recipient of a trap message does not send a response to the switch. Traps are therefore not as reliable as inform messages, which include a request for acknowledgement of receipt. Informs can be used to ensure that critical information is received by the host. However, note that informs consume more system resources because they must be kept in memory until a response is received. Informs also add to network traffic. You should consider these effects when deciding whether to issue notifications as traps or informs.

To send an inform to a SNMPv2c host, complete these steps:

1. Enable the SNMP agent.
2. Create a view with the required notification messages.
3. Create a group that includes the required notify view.
4. Allow the switch to send SNMP traps; i.e., notifications.
5. Specify the target host that will receive inform messages with the snmp-server host command as described in this section.

To send an inform to a SNMPv3 host, complete these steps:

1. Enable the SNMP agent.
2. Create a local SNMPv3 user to use in the message exchange process.
3. Create a view with the required notification messages.
4. Create a group that includes the required notify view.
5. Allow the switch to send SNMP traps; i.e., notifications.
6. Specify the target host that will receive inform messages with the snmp-server host command as described in this section.

- The switch can send SNMP Version 1, 2c or 3 notifications to a host IP address, depending on the SNMP version that the management station supports. If the snmp-server host command does not specify the SNMP version, the default is to send SNMP version 1 notifications.
- If you specify an SNMP Version 3 host, then the community string is interpreted as an SNMP user name. The user name must first be defined with the snmp-server user command. Otherwise, an SNMPv3 group will be automatically created by the snmp-server host command using the name of the specified community string, and default settings for the read, write, and notify view.

Example

Console(config)#snmp-server host 10.1.19.23 batman

Console(config)#

5.3 SNMPv3 Commands

snmp-server engine-id

This command configures an identification string for the SNMPv3 engine. Use the no form to restore the default.

Syntax

snmp-server engine-id {local | remote {*ip-address*}} *engineid-string*

no snmp-server engine-id {local | remote {*ip-address*}}

local - Specifies the SNMP engine on this switch.

remote - Specifies an SNMP engine on a remote device.

ip-address - The Internet address of the remote device.

engineid-string - String identifying the engine ID. (Range: 1-26 hexadecimal characters)

Default Configuration

A unique engine ID is automatically generated by the switch based on its MAC address.

Command Mode

Global Configuration

User Guidelines

- An SNMP engine is an independent SNMP agent that resides either on this switch or on a remote device. This engine protects against message replay, delay, and redirection. The engine ID is also used in combination with user passwords to generate the security keys for authenticating and encrypting SNMPv3 packets.
- A remote engine ID is required when using SNMPv3 informs. (See the snmp-server host command.) The remote engine ID is used to compute the security digest for authentication and encryption of packets passed between the switch and a user on the remote host. SNMP passwords are localized using the engine ID of the authoritative agent. For informs, the authoritative SNMP agent is the remote agent. You therefore need to configure the remote agent's SNMP engine ID before you can send proxy requests or informs to it.
- Trailing zeroes need not be entered to uniquely specify a engine ID. In other words, the value "0123456789" is equivalent to "0123456789" followed by 16 zeroes for a local engine ID.
- A local engine ID is automatically generated that is unique to the switch. This is referred to as the default engine ID. If the local engine ID is deleted or changed, all SNMP users will be cleared. You will need to reconfigure all existing users.

Example

Console(config)#snmp-server engine-id local 1234567890

Console(config)#snmp-server engineID remote 9876543210 192.168.1.19

Console(config)#

snmp-server group

This command adds an SNMP group, mapping SNMP users to SNMP views. Use the no form to remove an SNMP group.

Syntax

snmp-server group *groupname* {v1 | v2c | v3 {auth | noauth | priv}}

[read *readview*] [write *writeview*] [notify *notifyview*]

no snmp-server group *groupname*

groupname - Name of an SNMP group. (Range: 1-32 characters)

v1 | v2c | v3 - Use SNMP version 1, 2c or 3.

auth | noauth | priv - This group uses SNMPv3 with authentication, no authentication, or with authentication and privacy.

readview - Defines the view for read access. (1-32 characters)

writeview - Defines the view for write access. (1-32 characters)

notifyview - Defines the view for notifications. (1-32 characters)

Default Configuration

Default groups: public15 (read only), private16 (read/write)

readview - Every object belonging to the Internet OID space (1).

writeview - Nothing is defined.

notifyview - Nothing is defined.

Command Mode

Global Configuration

User Guidelines

- A group sets the access policy for the assigned users.
- When authentication is selected, the MD5 or SHA algorithm is used as specified in the snmp-server user command.
- When privacy is selected, the DES 56-bit algorithm is used for data encryption.

Example

Console(config)#snmp-server group r&d v3 auth write daily

Console(config)#

snmp-server user

This command adds a user to an SNMP group, restricting the user to a specific SNMP Read, Write, or Notify View. Use the no form to remove a user from an SNMP group.

Syntax

snmp-server user *username groupname* [remote *ip-address*] {v1 | v2c | v3 [encrypted] [auth {md5 | sha} *auth-password* [priv des56 *priv-password*]]

no snmp-server user *username* {v1 | v2c | v3 | remote}

username - Name of user connecting to the SNMP agent. (Range: 1-32 characters)

groupname - Name of an SNMP group to which the user is assigned. (Range: 1-32 characters)

remote - Specifies an SNMP engine on a remote device.

ip-address - The Internet address of the remote device.

v1 | v2c | v3 - Use SNMP version 1, 2c or 3.

encrypted - Accepts the password as encrypted input.

auth - Uses SNMPv3 with authentication.

md5 | sha - Uses MD5 or SHA authentication.

auth-password - Authentication password. Enter as plain text if the encrypted option is not used. Otherwise, enter an encrypted password. (A minimum of eight characters is required.)

priv des56 - Uses SNMPv3 with privacy with DES56 encryption.

priv-password - Privacy password. Enter as plain text if the encrypted option is not used. Otherwise, enter an encrypted password.

Default Configuration

None

Command Mode

Global Configuration

User Guidelines

- Local users (i.e., the command does not specify a remote engine identifier) must be configured to authorize management access for SNMPv3 clients, or to identify the source of SNMPv3 trap messages sent from the local switch.
- Remote users (i.e., the command specifies a remote engine identifier) must be configured to identify the source of SNMPv3 inform messages sent from the local switch.
- The SNMP engine ID is used to compute the authentication/privacy digests from the password. You should therefore configure the engine ID with the snmp-server engine-id command before using this configuration command.
- Before you configure a remote user, use the snmp-server engine-id command to specify the engine ID for the remote device where the user resides. Then use the snmp-server user command to specify the user and the IP address for the remote device where the user resides. The remote agent's SNMP engine ID is used to compute

authentication/privacy digests from the user's password. If the remote engine ID is not first configured, the snmp-server user command specifying a remote user will fail.

- SNMP passwords are localized using the engine ID of the authoritative agent. For informs, the authoritative SNMP agent is the remote agent. You therefore need to configure the remote agent's SNMP engine ID before you can send proxy requests or informs to it.

Example

Console(config)#snmp-server user steve group r&d v3 auth md5 greenpeace priv
des56 einstien

Console(config)#snmp-server user mark group r&d remote 192.168.1.19 v3 auth
md5 greenpeace priv des56 einstien

Console(config)#

snmp-server view

This command adds an SNMP view which controls user access to the MIB. Use the no form to remove an SNMP view.

Syntax

snmp-server view *view-name oid-tree* {included | excluded}

no snmp-server view *view-name*

view-name - Name of an SNMP view. (Range: 1-32 characters)

oid-tree - Object identifier of a branch within the MIB tree. Wild cards can be used to mask a specific portion of the OID string. (Refer to the examples.)

included - Defines an included view.

excluded - Defines an excluded view.

Default Configuration

defaultview (includes access to the entire MIB tree)

Command Mode

Global Configuration

User Guidelines

- Views are used in the snmp-server group command to restrict user access to specified portions of the MIB tree.
- The predefined view "defaultview" includes access to the entire MIB tree.

EXAMPLES

This view includes MIB-2.

Console(config)#snmp-server view mib-2 1.3.6.1.2.1 included

Console(config)#

This view includes the MIB-2 interfaces table, ifDescr. The wild card is used to select all the index values in this table.

Console(config)#snmp-server view ifEntry.2 1.3.6.1.2.1.2.2.1.*.2 included

Console(config)#

This view includes the MIB-2 interfaces table, and the mask selects all index entries.

Console(config)#snmp-server view ifEntry.a 1.3.6.1.2.1.2.2.1.1.* included

Console(config)#

show snmp engine-id

This command shows the SNMP engine ID.

Command Mode

EXEC

Example

This example shows the default engine ID.

Console#show snmp engine-id
Local SNMP EngineID: 8000002a8000000000e8666672
Local SNMP EngineBoots: 1
Remote SNMP EngineID IP address
80000000030004e2b316c54321 192.168.1.19
Console#

show snmp group

Four default groups are provided – SNMPv1 read-only access and read/write access, and SNMPv2c read-only access and read/write access.

Command Mode

EXEC

Example

Console#show snmp group
Group Name: r&d
Security Model: v3
Read View: defaultview
Write View: daily
Notify View: none
Storage Type: permanent
Row Status: active
Group Name: public
Security Model: v1
Read View: defaultview
Write View: none
Notify View: none
Storage Type: volatile
Row Status: active
Group Name: public
Security Model: v2c
Read View: defaultview
Write View: none
Notify View: none
Storage Type: volatile
Row Status: active
Group Name: private
Security Model: v1
Read View: defaultview
Write View: defaultview
Notify View: none
Storage Type: volatile
Row Status: active
Group Name: private
Security Model: v2c
Read View: defaultview

Write View: defaultview
Notify View: none
Storage Type: volatile
Row Status: active
Console#
show snmp user
This command shows information on SNMP users.
Command Mode
EXEC
Example
Console#show snmp user
EngineId: 800000ca030030f1df9ca00000
User Name: steve
Authentication Protocol: md5
Privacy Protocol: des56
Storage Type: nonvolatile
Row Status: active
show snmp view
This command shows information on the SNMP views.
Command Mode
EXEC
Example
Console#show snmp view
View Name: mib-2
Subtree OID: 1.2.2.3.6.2.52642
View Type: included
Storage Type: permanent
Row Status: active
View Name: defaultview
Subtree OID: 52642
View Type: included
Storage Type: volatile
Row Status: active
Console#

5.4 Additional Trap Commands

memory
This command sets an SNMP trap based on configured thresholds for memory utilization. Use the no form to restore the default setting.
Syntax
memory {rising *rising-threshold* | falling *falling-threshold*}
no memory {rising | falling}
rising-threshold - Rising threshold for memory utilization alarm expressed in percentage. (Range: 1-100)

falling-threshold - Falling threshold for memory utilization alarm expressed in percentage. (Range: 1-100)

Default Configuration

Rising Threshold: 90%

Falling Threshold: 70%

Command Mode

Global Configuration

User Guidelines

Once the rising alarm threshold is exceeded, utilization must drop beneath the falling threshold before the alarm is terminated, and then exceed the rising threshold again before another alarm is triggered.

Example

Console(config)#memory rising 80

Console(config)#memory falling 60

Console#

cpu

This command sets an SNMP trap based on configured thresholds for CPU utilization. Use the no form to restore the default setting.

Syntax

cpu {rising *rising-threshold* | falling *falling-threshold*}

no cpu {rising | falling}

rising-threshold - Rising threshold for CPU utilization alarm expressed in percentage. (Range: 1-100)

falling-threshold - Falling threshold for CPU utilization alarm expressed in percentage. (Range: 1-100)

Default Configuration

Rising Threshold: 90%

Falling Threshold: 70%

Command Mode

Global Configuration

User Guidelines

Once the rising alarm threshold is exceeded, utilization must drop beneath the falling threshold before the alarm is terminated, and then exceed the rising threshold again before another alarm is triggered.

Example

Console(config)#cpu rising 80

Console(config)#cpu falling 60

Console#

6. Rmon Commands

Remote Monitoring allows a remote device to collect information or respond to specified events on an independent basis. This switch is an

RMON-capable device which can independently perform a wide range of tasks, significantly reducing network management traffic. It can continuously run diagnostics and log information on network performance. If an event is triggered, it can automatically notify the network administrator of a failure and provide historical information about the event. If it cannot connect to the management agent, it will continue to perform any specified tasks and pass data back to the management station the next time it is contacted.

This switch supports mini-RMON, which consists of the Statistics, History, Event and Alarm groups. When RMON is enabled, the system gradually builds up information about its physical interfaces, storing this information in the relevant RMON database group. A management agent then periodically communicates with the switch using the SNMP protocol. However, if the switch encounters a critical event, it can automatically send a trap message to the management agent which can then respond to the event if so configured.

rmon alarm

This command sets threshold bounds for a monitored variable. Use the no form to remove an alarm.

Syntax

rmon alarm *index variable interval* {absolute | delta} rising-threshold *threshold* [*event-index*] falling-threshold *threshold* [*event-index*] [owner *name*]

no rmon alarm *index*

index – Index to this entry. (Range: 1-65535)

variable – The object identifier of the MIB variable to be sampled. Only variables of the type etherStatsEntry.n.n may be sampled. Note that etherStatsEntry.n uniquely defines the MIB variable, and etherStatsEntry.n.n defines the MIB variable, plus the etherStatsIndex. For example, 1.3.6.1.2.1.16.1.1.1.6.1 denotes etherStatsBroadcastPkts, plus the etherStatsIndex of 1.

interval – The polling interval. (Range: 1-31622400 seconds)

absolute – The variable is compared directly to the thresholds at the end of the sampling period.

delta – The last sample is subtracted from the current value and the difference is then compared to the thresholds.

threshold – An alarm threshold for the sampled variable. (Range: 0-2147483647)

event-index – The index of the event to use if an alarm is triggered. If there is no corresponding entry in the event control table, then no event will be generated. (Range: 0-65535)

name – Name of the person who created this entry. (Range: 1-127 characters)

Default Configuration

1.3.6.1.2.1.16.1.1.1.6.1 - 1.3.6.1.2.1.16.1.1.1.6.28

Taking delta samples every 30 seconds,

Rising threshold is 892800, assigned to event 0

Falling threshold is 446400, assigned to event 0

Command Mode

Global Configuration

User Guidelines

- If an event is already defined for an index, the entry must be deleted before any changes can be made with this command.

- If the current value is greater than or equal to the rising threshold, and the last sample value was less than this threshold, then an alarm will be generated. After a rising event has been generated, another such event will not be generated until the sampled value has fallen below the rising threshold, reaches the falling threshold, and again moves back up to the rising threshold.
- If the current value is less than or equal to the falling threshold, and the last sample value was greater than this threshold, then an alarm will be generated. After a falling event has been generated, another such event will not be generated until the sampled value has risen above the falling threshold, reaches the rising threshold, and again moves back down to the failing threshold.

Example

Console(config)#rmon alarm 1 1.3.6.1.2.1.16.1.1.1.6.1 15 delta

rising-threshold 100 1 falling-threshold 30 1 owner mike

Console(config)#

rmon event

This command creates a response event for an alarm. Use the no form to remove an event.

Syntax

rmon event *index* [log] | [trap *community*] | [description *string*] | [owner *name*]

no rmon event *index*

index – Index to this entry. (Range: 1-65535)

log – Generates an RMON log entry when the event is triggered. Log messages are processed based on the current configuration settings for event logging.

trap – Sends a trap message to all configured trap managers.

community – A password-like community string sent with the trap operation to SNMP v1 and v2c hosts. Although this string can be set using the rmon event command by itself, it is recommended that the string be defined using the snmp-server community command prior to using the rmon event command. (Range: 1-32 characters)

string – A comment that describes this event. (Range: 1-127 characters)

name – Name of the person who created this entry. (Range: 1-127 characters)

Default Configuration

None

Command Mode

Global Configuration

- User Guidelines
- If an event is already defined for an index, the entry must be deleted before any changes can be made with this command.
- The specified events determine the action to take when an alarm triggers this event. The response to an alarm can include logging the alarm or sending a message to a trap manager.

Example

Console(config)#rmon event 2 log description urgent owner mike

Console(config)#

rmon collection history

This command periodically samples statistics on a physical interface. Use the no form to disable periodic sampling.

Syntax

rmon collection history controlEntry *index* [[owner *name*] [buckets *number*] [interval *seconds*]] | [buckets *number*] [interval *seconds*] | interval *seconds*

no rmon collection history controlEntry *index*

index – Index to this entry. (Range: 1-65535)

number – The number of buckets requested for this entry. (Range: 1-65536)

seconds – The polling interval. (Range: 1-3600 seconds)

name – Name of the person who created this entry. (Range: 1-127 characters)

Default Configuration

1.3.6.1.2.1.16.1.1.1.6.1 - 1.3.6.1.2.1.16.1.1.1.6.28

Buckets: 50

Interval: 30 seconds for even numbered entries,

1800 seconds for odd numbered entries

Command Mode

Interface Configuration (Ethernet)

User Guidelines

- By default, each index number equates to a port on the switch, but can be changed to any number not currently in use.
- If periodic sampling is already enabled on an interface, the entry must be deleted before any changes can be made with this command.
- The information collected for each sample includes: input octets, packets, broadcast packets, multicast packets, undersize packets, oversize packets, fragments, jabbers, CRC alignment errors, collisions, drop events, and network utilization.
- The switch reserves two controlEntry index entries for each port. If a default index entry is re-assigned to another port by this command, the show running-config command will display a message indicating that this index is not available for the port to which is normally assigned. For example, if control entry 15 is assigned to port 5 as shown below, the show running-config command will indicate that this entry is not available for port 8.

Console(config)#interface ethernet 1/5

Console(config-if)#rmon collection history controlEntry 15

Console(config-if)#end

Console#show running-config

!

interface ethernet 1/5

rmon collection history controlEntry 15 buckets 50 interval 1800

...

interface ethernet 1/8

no rmon collection history controlEntry 15

Example

Console(config)#interface ethernet 1/1

Console(config-if)#rmon collection history controlentry 21 owner mike buckets

24 interval 60

Console(config-if)#

rmon collection stats

This command enables the collection of statistics on a physical interface. Use the no form to disable statistics collection.

Syntax

rmon collection stats controlEntry *index* [owner *name*]

no rmon collection stats controlEntry *index*

index – Index to this entry. (Range: 1-65535)

name – Name of the person who created this entry. (Range: 1-127 characters)

Default Configuration

Enabled

Command Mode

Interface Configuration (Ethernet)

User Guidelines

- By default, each index number equates to a port on the switch, but can be changed to any number not currently in use.
- If statistics collection is already enabled on an interface, the entry must be deleted before any changes can be made with this command.
- The information collected for each entry includes: input octets, packets, broadcast packets, multicast packets, undersize packets, oversize packets, fragments, jabbers, CRC alignment errors, collisions, drop events, and packets of specified lengths.

Example

Console(config)#interface ethernet 1/1

Console(config-if)#rmon collection stats controlEntry 1 owner mike

Console(config-if)#

show rmon alarms

This command shows the settings for all configured alarms.

Command Mode

EXEC

Example

Console#show rmon alarms

Alarm 1 is valid, owned by

Monitors 1.3.6.1.2.1.16.1.1.1.6.1 every 30 seconds

Taking delta samples, last value was 0

Rising threshold is 892800, assigned to event 0

Falling threshold is 446400, assigned to event 0

..

show rmon events

This command shows the settings for all configured events.

Command Mode

EXEC

Example

Console#show rmon events

Event 2 is valid, owned by mike

Description is urgent

Event firing causes log and trap to community , last fired 00:00:00

Console#

show rmon history

This command shows the sampling parameters configured for each entry in the history group.

Command Mode

EXEC

Example

Console#show rmon history

Entry 1 is valid, and owned by

Monitors 1.3.6.1.2.1.2.2.1.1.1 every 1800 seconds

Requested # of time intervals, ie buckets, is 8

Granted # of time intervals, ie buckets, is 8

Sample # 1 began measuring at 00:00:01

Received 77671 octets, 1077 packets,

61 broadcast and 978 multicast packets,

0 undersized and 0 oversized packets,

0 fragments and 0 jabbers packets,

0 CRC alignment errors and 0 collisions.

# of dropped packet events is 0

Network utilization is estimated at 0

...

show rmon statistics

This command shows the information collected for all configured entries in the statistics group.

Command Mode

EXEC

Example

Console#show rmon statistics

Interface 1 is valid, and owned by

Monitors 1.3.6.1.2.1.2.2.1.1.1 which has

Received 164289 octets, 2372 packets,

120 broadcast and 2211 multicast packets,

0 undersized and 0 oversized packets,

0 fragments and 0 jabbers,

0 CRC alignment errors and 0 collisions.

# of dropped packet events (due to lack of resources): 0

# of packets received of length (in octets):

64: 2245, 65-127: 87, 128-255: 31,

256-511: 5, 512-1023: 2, 1024-1518: 2

..

7. SFLOW

Flow sampling (sFlow) can be used with a remote sFlow Collector to provide an accurate, detailed and real-time overview of the types and

levels of traffic present on the network. The sFlow Agent samples 1 out of n packets from all data traversing the switch, re-encapsulates the samples as sFlow datagrams and transmits them to the sFlow Collector. This sampling occurs at the internal hardware level where all traffic is seen, whereas traditional probes only have a partial view of traffic as it is sampled at the monitored interface. Moreover, the processor and memory load imposed by the sFlow agent is minimal since local analysis does not take place.

sflow owner

This command creates an sFlow collector on the switch. Use the no form to remove

the sFlow receiver.

Syntax

sflow owner *owner-name* timeout *timeout-value*

[destination *{ipv4-address | ipv6-address}*] [port *destination-udp-port*]

[max-datagram-size *max-datagram-size*] [version {v4 | v5}]

no sflow owner *owner-name*

name - Name of the collector. (Range: 1-30 alphanumeric characters)

timeout-value - The length of time the sFlow interface is available to send samples to a receiver, after which the owner and associated polling and sampling data source instances are removed from the configuration. (Range: 30-10000000 seconds)

ipv4-address - IPv4 address of the sFlow collector. Valid IPv4 addresses consist of four decimal numbers, 0 to 255, separated by periods.

ipv6-address - IPv6 address of the sFlow collector. A full IPv6 address including the network prefix and host address bits. An IPv6 address consists of 8 colon-separated 16-bit hexadecimal values. One double colon may be used to indicate the appropriate number of zeros required to fill the undefined fields.

destination-udp-port - The UDP port on which the collector is listening for sFlow streams. (Range: 1-65535)

max-datagram-size - The maximum size of the sFlow datagram payload. (Range: 200-1500 bytes)

version {v4 | v5} - Sends either v4 or v5 sFlow datagrams to the receiver.

Default Configuration

No owner is configured

UDP Port: 6343

Version: v4

Maximum Datagram Size: 1400 bytes

Command Mode

Global Configuration

User Guidelines

- Use the sflow owner command to create an owner instance of an sFlow collector. If the socket port, maximum datagram size, and datagram version are not specified, then the default values are used.
- Once an owner is created, the sflow owner command can again be used to modify the owner's port number. All other parameter values for the owner will be retained if the port is modified.
- Use the no sflow owner command to remove the collector.

- When the sflow owner command is issued, it's associated timeout value will immediately begin to count down. Once the timeout value has reached zero seconds, the sFlow owner and it's associated sampling sources will be deleted from the configuration.

Example

This example shows an sflow collector being created on the switch.

Console(config)#sflow owner stat_server1 timeout 100 destination 192.168.220.225 port 22500 max-datagram-size 512 version v5

Console(config)#

sflow polling

This command enables an sFlow polling data source, for a specified interface, that polls periodically based on a specified time interval. Use the no form to remove the polling data source instance from the switch's sFlow configuration.

Syntax

sflow polling {interface *interface*} instance *instance-id* receiver *owner-name* polling-interval *seconds*

no sflow polling {interface *interface*} instance *instance-id*

interface - The source from which the samples will be taken at specified intervals and sent to a collector.

ethernet *unit/port*

unit - Unit identifier. (Range: 1-6)

port - Port number. (Range: 1-28/52)

instance-id - An instance ID used to identify the sampling source. (Range: 1)

owner-name - The associated receiver, to which the samples will be sent. (Range: 1-30 alphanumeric characters)

polling-interval - The time interval at which the sFlow process adds counter values to the sample datagram. (Range: 0-10000000 seconds, 0 disables this feature)

Default Configuration

No sFlow polling instance is configured.

Command Mode

Global Configuration

User Guidelines

This command enables a polling data source and configures the interval at which counter values are added to the sample datagram.

Example

This example sets the polling interval to 10 seconds.

Console(config)# sflow polling interface ethernet 1/1 instance 1 receiver test polling-interval 10

sflow sampling

This command enables an sFlow data source instance for a specific interface that takes samples periodically based on the number of packets processed. Use the no form to remove the sampling data source instance from the switch's sFlow configuration.

Syntax

sflow sampling {interface *interface*} instance *instance-id* receiver *owner-name* sampling-rate *sample-rate* [max-header-size *max-header-size*]

no sflow sample {interface *interface*} instance *instance-id*

interface - The source from which the samples will be taken and sent to a collector.

ethernet unit/port

unit - Unit identifier. (Range: 1-6)

port - Port number. (Range: 1-28/52)

instance-id - An instance ID used to identify the sampling source. (Range: 1)

owner-name - The associated receiver, to which the samples will be sent. (Range: 1-30 alphanumeric characters)

sample-rate - The packet sampling rate, or the number of packets out of which one sample will be taken. (Range: 256-16777215 packets)

max-header-size - The maximum size of the sFlow datagram header. (Range: 64-256 bytes)

Default Configuration

No sFlow sampling instance id configured.

Maximum Header Size: 128 bytes

Command Mode

Global Configuration

Example

This example enables a sampling data source on Ethernet interface 1/1, an associated receiver named "owner1", and a sampling rate of one out of 100. The maximum header size is also set to 200 bytes.

Console(config)# sflow sampling interface ethernet 1/1 instance 1 receiver owner1 sampling-rate 100 max-header-size 200

show sflow

This command shows the global and interface settings for the sFlow process.

Syntax

show sflow [owner *owner-name* | interface *interface*]

owner-name - The associated receiver, to which the samples are sent. (Range: 1-30 alphanumeric characters)

interface

ethernet *unit*/*port*

unit - Stack unit. (Range: 1)

port - Port number. (Range: 1-28)

Command Mode

EXEC

Example

Console#show sflow interface ethernet 1/2

Receiver Owner Name : stat1

Receiver Timeout : 99633 sec

Receiver Destination : 192.168.32.32

Receiver Socket Port : 6343

Maximum Datagram Size : 1400 bytes

Datagram Version : 4

Data Source : Eth 1/2

Sampling Instance ID : 1

Sampling Rate : 512

Maximum Header Size : 128 bytes

Console#

8. User Accounts

The basic commands required for management access and assigning command privilege levels are listed in this section.

enable password

After initially logging onto the system, you should set the EXEC password. Remember to record it in a safe place. This command controls access to the EXEC level from the Normal Exec level. Use the no form to reset the default password.

Syntax

enable password [level *level*] {0 | 7} *password*

no enable password [level *level*]

level *level* - Level 15 for EXEC. (Levels 0-14 are not used.)

{0 | 7} - 0 means plain password, 7 means encrypted password.

password - Password for this privilege level. (Maximum length: 32 characters plain text or encrypted, case sensitive)

Default Configuration

The default is level 15.

The default password is "super"

Command Mode

Global Configuration

User Guidelines

- You cannot set a null password. You will have to enter a password to change the command mode from Normal Exec to EXEC with the enable command.
- The encrypted password is required for compatibility with legacy password settings (i.e., plain text or encrypted) when reading the configuration file during system bootup or when downloading the configuration file from a TFTP server. There is no need for you to manually configure encrypted passwords.

Example

Console(config)#enable password level 15 0 admin

Console(config)#

username

This command adds named users, requires authentication at login, specifies or changes a user's password (or specify that no password is required), or specifies or changes a user's access level. Use the no form to remove a user name.

Syntax

username *name* { privilege *level* | nopassword | password {0 | 7} *password*}

no username *name*

name - The name of the user. (Maximum length: 32 characters, case sensitive. Maximum users: 16)

privilege *level* - Specifies the user level. The device has two predefined privilege levels:

0: Normal Exec, 15: EXEC.

nopassword - No password is required for this user to log in. {0 | 7} - 0 means plain password, 7 means encrypted password.

password *password* - The authentication password for the user. (Maximum length: 32 characters plain text or encrypted, case sensitive)

Default Configuration

The default privilege is Normal Exec.

The factory defaults for the user names and passwords are:

username	privilege	password
guest	0	guest
admin	15	admin

Command Mode

Global Configuration

User Guidelines

The encrypted password is required for compatibility with legacy password settings (i.e., plain text or encrypted) when reading the configuration file during system bootup or when downloading the configuration file from an FTP/TFTP server. There is no need for you to manually configure encrypted passwords.

Example

This example shows how the set the access level and password for a user.

Console(config)#username bob privilege 15

Console(config)#username bob password 0 smith

Console(config)#

privilege

This command assigns a privilege level to specified command groups or individual commands. Use the no form to restore the default setting.

Syntax

privilege *mode* [all] level *level command*

no privilege *mode* [all] *command*

mode - The configuration mode containing the specified *command*.

all - Modifies the privilege level for all subcommands under the specified *command*.

level *level* - Specifies the privilege level for the specified *command*. This device has three predefined privilege levels: 0: Normal Exec, 8: Manager, 15: EXEC. (Range: 0-15)

command - Specifies any command contained within the specified

mode.

Default Configuration

Privilege level 0 provides access to a limited number of the commands which display the current status of the switch, as well as several database clear and reset functions. Level 8 provides access to all display status and configuration commands, except for those controlling various authentication and security features. Level 15 provides full access to all commands.

Command Mode

Global Configuration

Example

This example sets the privilege level for the ping command to EXEC.

Console(config)#privilege exec level 15 ping

Console(config)#

show privilege

This command shows the privilege level for the current user, or the privilege level for commands modified by the privilege command.

Syntax

show privilege [command]

command - Displays the privilege level for all commands modified by the privilege command.

Command Mode

EXEC

Example

This example shows the privilege level for any command modified by the privilege command.

```
Console#show privilege command
privilege line all level 0 accounting
privilege exec level 15 ping
Console(config)#
```

9. Authentication

Three authentication methods can be specified to authenticate users logging into the system for management access. The commands in this section can be used to define the authentication method and sequence.

authentication enable

This command defines the authentication method and precedence to use when changing from Exec command mode to EXEC command mode with the enable command. Use the no form to restore the default.

Syntax

authentication enable {[local] [radius] [tacacs]}

no authentication enable

local - Use local password only.

radius - Use RADIUS server password only.

tacacs - Use TACACS server password.

Default Configuration

Local

Command Mode

Global Configuration

User Guidelines

- RADIUS uses UDP while TACACS+ uses TCP. UDP only offers best effort delivery, while TCP offers a connection-oriented transport. Also, note that RADIUS encrypts only the password in the access-request packet from the client to the server, while TACACS+ encrypts the entire body of the packet.
- RADIUS and TACACS+ logon authentication assigns a specific privilege level for each user name and password pair. The user name, password, and privilege level must be configured on the authentication server.
- You can specify three authentication methods in a single command to indicate the authentication sequence. For example, if you enter "authentication enable radius tacacs local" the user name and password on the RADIUS server is verified first. If the RADIUS server is not available, then authentication is attempted on the TACACS+ server. If the TACACS+ server is not available, the local user name and password is checked.

Example

Console(config)#authentication enable radius

Console(config)#

authentication login

This command defines the login authentication method and precedence. Use the no form to restore the default.

Syntax

authentication login {[local] [radius] [tacacs]}

no authentication login

local - Use local password.

radius - Use RADIUS server password.

tacacs - Use TACACS server password.

Default Configuration

Local

Command Mode

Global Configuration

User Guidelines

- RADIUS uses UDP while TACACS+ uses TCP. UDP only offers best effort delivery, while TCP offers a connection-oriented transport. Also, note that RADIUS encrypts only the password in the access-request packet from the client to the server, while TACACS+ encrypts the entire body of the packet.
- RADIUS and TACACS+ logon authentication assign a specific privilege level for each user name and password pair. The user name, password, and privilege level must be configured on the authentication server.
- You can specify three authentication methods in a single command to indicate the authentication sequence. For example, if you enter "authentication login radius tacacs local" the user name and password on the RADIUS server is verified first. If the RADIUS server is not available, then authentication is attempted on the TACACS+ server. If the TACACS+ server is not available, the local user name and password is checked.

Example

Console(config)#authentication login radius

Console(config)#

10. RADIUS Client

Remote Authentication Dial-in User Service (RADIUS) is a logon authentication protocol that uses software running on a central server to control access to RADIUS-aware devices on the network. An authentication server contains a database of multiple user name/password pairs with associated privilege levels for each user or group that require management access to a switch.

radius-server acct-port

This command sets the RADIUS server network port for accounting messages. Use the no form to restore the default.

Syntax

radius-server acct-port *port-number*

no radius-server acct-port

port-number - RADIUS server UDP port used for accounting messages. (Range: 1-65535)

Default Configuration

1813

Command Mode

Global Configuration

Example

Console(config)#radius-server acct-port 181

Console(config)#

radius-server auth-port

This command sets the RADIUS server network port. Use the no form to restore the default.

Syntax

radius-server auth-port *port-number*

no radius-server auth-port

port-number - RADIUS server UDP port used for authentication messages. (Range: 1-65535)

Default Configuration

1812

Command Mode

Global Configuration

Example

Console(config)#radius-server auth-port 181

Console(config)#

radius-server host

This command specifies primary and backup RADIUS servers, and authentication and accounting parameters that apply to each server. Use the no form to remove a specified server, or to restore the default values.

Syntax

[no] radius-server *index* host *host-ip-address* [acct-port *acct-port*] [auth-port *auth-port*] [key *key*] [retransmit *retransmit*] [timeout *timeout*]

index - Allows you to specify up to five servers. These servers are queried in sequence until a server responds or the retransmit period expires.

host-ip-address - IP address of server.

acct-port - RADIUS server UDP port used for accounting messages. (Range: 1-65535)

auth-port - RADIUS server UDP port used for authentication messages. (Range: 1-65535)

key - Encryption key used to authenticate logon access for client. Do not use blank spaces in the string. (Maximum length: 48 characters)

retransmit - Number of times the switch will try to authenticate logon access via the RADIUS server. (Range: 1-30)

timeout - Number of seconds the switch waits for a reply before resending a request. (Range: 1-65535)

Default Configuration

auth-port - 1812

acct-port - 1813

timeout - 5 seconds

retransmit - 2

Command Mode

Global Configuration

Example

Console(config)#radius-server 1 host 192.168.1.20 port 181 timeout 10

retransmit 5 key green

Console(config)#

radius-server key

This command sets the RADIUS encryption key. Use the no form to restore the default.

Syntax

radius-server key *key-string*

no radius-server key

key-string - Encryption key used to authenticate logon access for client. Do not use blank spaces in the string. (Maximum length: 48 characters)

Default Configuration

None

Command Mode

Global Configuration

Example

Console(config)#radius-server key green

Console(config)#

radius-server retransmit

This command sets the number of retries. Use the no form to restore the default.

Syntax

radius-server retransmit *number-of-retries*

no radius-server retransmit

number-of-retries - Number of times the switch will try to authenticate logon access via the RADIUS server. (Range: 1 - 30)

Default Configuration

2

Command Mode

Global Configuration

Example

Console(config)#radius-server retransmit 5

Console(config)#

radius-server timeout

This command sets the interval between transmitting authentication requests to the RADIUS server. Use the no form to restore the default.

Syntax

radius-server timeout *number-of-seconds*

no radius-server timeout

number-of-seconds - Number of seconds the switch waits for a reply before resending a request. (Range: 1-65535)

Default Configuration

5

Command Mode

Global Configuration

Example

Console(config)#radius-server timeout 10

Console(config)#

show radius-server

This command displays the current settings for the RADIUS server.

Default Configuration

None

Command Mode

EXEC

Example

Console#show radius-server

Remote RADIUS Server Configuration:

Global Settings:

Authentication Port Number: 1812

Accounting Port Number: 1813

Retransmit Times: 2

Request Timeout: 5

Server 1:

Server IP Address: 192.168.1.1

Authentication Port Number: 1812

Accounting Port Number: 1813

Retransmit Times: 2

Request Timeout: 5

RADIUS Server Group:

Group Name Member Index

------------------------ ----------

radius 1

Console#

11. TACACS + Client

Terminal Access Controller Access Control System (TACACS+) is a logon authentication protocol that uses software running on a central server to control access to TACACS-aware devices on the network. An authentication server contains a database of multiple user name/password pairs with associated privilege levels for each user or group that require management access to a switch.

tacacs-server host

This command specifies the TACACS+ server and other optional parameters. Use the no form to remove the server, or to restore the default values.

Syntax

tacacs-server *index* host *host-ip-address* [key *key*] [port *port-number*] [retransmit *retransmit*] [timeout *timeout*]

no tacacs-server *index*

index - The index for this server. (Range: 1)

host-ip-address - IP address of a TACACS+ server.

key - Encryption key used to authenticate logon access for the client. Do not use blank spaces in the string. (Maximum length: 48 characters)

port-number - TACACS+ server TCP port used for authentication messages. (Range: 1-65535)

retransmit - Number of times the switch will try to authenticate logon access via the TACACS+ server. (Range: 1-30)

timeout - Number of seconds the switch waits for a reply before resending a request. (Range: 1-540)

Default Configuration

authentication port - 49

timeout - 5 seconds

retransmit - 2

Command Mode

Global Configuration

Example

Console(config)#tacacs-server 1 host 192.168.1.25 port 181 timeout 10

retransmit 5 key green

Console(config)#

tacacs-server key

This command sets the TACACS+ encryption key. Use the no form to restore the default.

Syntax

tacacs-server key *key-string*

no tacacs-server key

key-string - Encryption key used to authenticate logon access for the client. Do not use blank spaces in the string. (Maximum length: 48 characters)

Default Configuration

None

Command Mode

Global Configuration

Example

Console(config)#tacacs-server key green

Console(config)#

tacacs-server port

This command specifies the TACACS+ server network port. Use the no form to restore the default.

Syntax

tacacs-server port *port-number*

no tacacs-server port

port-number - TACACS+ server TCP port used for authentication messages. (Range: 1-65535)

Default Configuration

49

Command Mode

Global Configuration

Example

Console(config)#tacacs-server port 181

Console(config)#

tacacs-server retransmit

This command sets the number of retries. Use the no form to restore the default.

Syntax

tacacs-server retransmit *number-of-retries*

no tacacs-server retransmit

number-of-retries - Number of times the switch will try to authenticate logon access via the TACACS+ server. (Range: 1 - 30)

Default Configuration

2

Command Mode

Global Configuration

Example

Console(config)#tacacs-server retransmit 5

Console(config)#

tacacs-server timeout

This command sets the interval between transmitting authentication requests to the TACACS+ server. Use the no form to restore the default.

Syntax

tacacs-server timeout *number-of-seconds*

no tacacs-server timeout

number-of-seconds - Number of seconds the switch waits for a reply before resending a request. (Range: 1-540)

Default Configuration

5

Command Mode

Global Configuration

Example

Console(config)#tacacs-server timeout 10

Console(config)#

show tacacs-server

This command displays the current settings for the TACACS+ server.

Default Configuration

None

Command Mode

EXEC

Example

```
Console#show tacacs-server
Remote TACACS+ Server Configuration:
Global Settings:
Server Port Number: 49
Retransmit Times: 2
Timeout: 5
Server 1:
Server IP Address: 10.11.12.13
Server Port Number: 49
Retransmit Times: 2
Timeout: 4
TACACS+ Server Group:
Group Name Member Index
------------------------ -------------
tacacs+                  1
Console#
```

12. AAA

The Authentication, Authorization, and Accounting (AAA) feature provides the main framework for configuring access control on the switch. The AAA functions require the use of configured RADIUS or TACACS+ servers in the network.

aaa accounting dot1x

This command enables the accounting of requested 802.1X services for network access. Use the no form to disable the accounting service.

Syntax

aaa accounting dot1x {default | *method-name*} start-stop list {radius | tacacs+ |*server-group*}

no aaa accounting dot1x {default | *method-name*}

default - Specifies the default accounting method for service requests.

method-name - Specifies an accounting method for service requests. (Range: 1-64 characters)

start-stop - Records accounting from starting point and stopping point.

list - Specifies the server group to use.

radius - Specifies all RADIUS hosts configure with the radiusserver host command.

tacacs+ - Specifies all TACACS+ hosts configure with the tacacs-server host command.

server-group - Specifies the name of a server group configured with the aaa group server command. (Range: 1-64 characters)

Default Configuration

Accounting is not enabled

No servers are specified

Command Mode

Global Configuration

User Guidelines

Note that the default and *method-name* fields are only used to describe the accounting method(s) configured on the specified RADIUS or TACACS+ servers, and do not actually send any information to the servers about the methods to use.

Example

Console(config)#aaa accounting dot1x default start-stop list radius

Console(config)#

aaa accounting login

This command enables the accounting of requested Exec services for network access. Use the no form to disable the accounting service.

Syntax

aaa accounting login {default | *method-name*} start-stop list {radius | tacacs+ |*server-group*}

no aaa accounting login {default | *method-name*}

default - Specifies the default accounting method for service requests.

method-name - Specifies an accounting method for service requests. (Range: 1-64 characters)

start-stop - Records accounting from starting point and stopping point.

list - Specifies the server group to use.

radius - Specifies all RADIUS hosts configure with the radiusserver host command.

tacacs+ - Specifies all TACACS+ hosts configure with the tacacs-server host command.

server-group - Specifies the name of a server group configured with the aaa group server command. (Range: 1-64 characters)

Default Configuration

Accounting is not enabled

No servers are specified

Command Mode

Global Configuration

User Guidelines

- This command runs accounting for Exec service requests for the local console and Telnet connections.
- Note that the default and *method-name* fields are only used to describe the accounting method(s) configured on the specified RADIUS or TACACS+ servers, and do not actually send any information to the servers about the methods to use.

Example

Console(config)#aaa accounting login default start-stop list tacacs+

Console(config)#

aaa accounting update

This command enables the sending of periodic updates to the accounting server. Use the no form to disable accounting updates.

Syntax

aaa accounting update [periodic *interval*]

no aaa accounting update

interval - Sends an interim accounting record to the server at this interval. (Range: 1-2147483647 minutes)

Default Configuration

1 minute

Command Mode

Global Configuration

User Guidelines

- When accounting updates are enabled, the switch issues periodic interim accounting records for all users on the system.
- Using the command without specifying an interim interval enables updates, but does not change the current interval setting.

Example

Console(config)#aaa accounting update periodic 30

Console(config)#

aaa authorization login

This command enables the authorization for Exec access. Use the no form to disable the authorization service.

Syntax

aaa authorization login {default | *method-name*} list {tacacs+ | *server-group*}

no aaa authorization login {default | *method-name*}

default - Specifies the default authorization method for Exec access.

method-name - Specifies an authorization method for Exec access. (Range: 1-64 characters)

list - Specifies the server group to use.

tacacs+ - Specifies all TACACS+ hosts configured with the tacacs-server host command.

server-group - Specifies the name of a server group configured with the aaa group server command. (Range: 1-64 characters)

Default Configuration

Authorization is not enabled

No servers are specified

Command Mode

Global Configuration

User Guidelines

- This command performs authorization to determine if a user is allowed to run an Exec shell.
- AAA authentication must be enabled before authorization is enabled.
- If this command is issued without a specified named method, the default method list is applied to all interfaces or lines (where this authorization type applies), except those that have a named method explicitly defined.

Example

Console(config)#aaa authorization login default list tacacs+

Console(config)#

aaa list server

Use this command to name a group of security server hosts. To remove a server group from the configuration list, enter the no form of this command.

Syntax

[no] aaa list server {radius | tacacs+} *group-name*

radius - Defines a RADIUS server group.

tacacs+ - Defines a TACACS+ server group.

group-name - A text string that names a security server group. (Range: 1-64 characters)

Default Configuration

None

Command Mode

Global Configuration

Example

Console(config)#aaa list server radius tps

Console(config-sg-radius)#

server

This command adds a security server to an AAA server group. Use the no form to remove the associated server from the group.

Syntax

[no] server {*index* | *ip-address*}

index - Specifies the server index. (Range: RADIUS 1-5, TACACS+ 1)

ip-address - Specifies the host IP address of a server.

Default Configuration

None

Command Mode

Server Group Configuration

User Guidelines

- When specifying the index for a RADIUS server, that server index must already be defined by the radius-server host command.

- When specifying the index for a TACACS+ server, that server index must already be defined by the tacacs-server host command.

Example

Console(config)#aaa group server radius tps

Console(config-sg-radius)#server 10.2.68.120

Console(config-sg-radius)#

accounting dot1x

This command applies an accounting method for 802.1X service requests on an interface. Use the no form to disable accounting on the interface.

Syntax

accounting dot1x {default | *list-name*}

no accounting dot1x

default - Specifies the default method list created with the aaa accounting dot1x command.

list-name - Specifies a method list created with the aaa accounting dot1x command.

Default Configuration

None

Command Mode

Interface Configuration

Example

Console(config)#interface ethernet 1/2

Console(config-if)#accounting dot1x tps

Console(config-if)#

show accounting

This command displays the current accounting settings per function and per port.

Syntax

show accounting [[[dot1x [statistics [username *user-name* | interface *interface*]] | login [statistics] | statistics]

dot1x - Displays dot1x accounting information.

exec - Displays Exec accounting records.

statistics - Displays accounting records.

user-name - Displays accounting records for a specifiable username.

interface

ethernet *unit*/*port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-28)

Default Configuration

None

Command Mode

EXEC

Example

Console#show accounting

Accounting Type: dot1x

Method List: default

Group List: radius

Interface: Eth 1/1

Method List: tps

Group List: radius

Interface: Eth 1/2

Console#

13. Web Server

This section describes commands used to configure web browser management access to the switch.

server http port

This command specifies the TCP port number used by the web browser interface. Use the no form to use the default port.

Syntax

server http port *port-number*

no server http port

port-number - The TCP port to be used by the browser interface. (Range: 1-65535)

Default Configuration

80

Command Mode

Global Configuration

Example

Console(config)#server http port 769

Console(config)#

server http enable

This command allows this device to be monitored or configured from a browser. Use the no form to disable this function.

Syntax

[no] server http enable

Default Configuration

Enabled

Command Mode

Global Configuration

Example

Console(config)#server http enable

Console(config)#

server https secure-port

This command specifies the UDP port number used for HTTPS connection to the switch's web interface. Use the no form to restore the default port.

Syntax

server https secure-port *port_number*

no server https secure-port

port_number – The UDP port used for HTTPS. (Range: 1-65535)

Default Configuration

443

Command Mode

Global Configuration

User Guidelines

◆ You cannot configure the HTTP and HTTPS servers to use the same port.

◆ If you change the HTTPS port number, clients attempting to connect to the HTTPS server must specify the port number in the URL, in this format: https://*device:port_number*

Example

Console(config)#server https secure-port 1000

Console(config)#

server https enable

This command enables the secure hypertext transfer protocol (HTTPS) over the Secure Socket Layer (SSL), providing secure access (i.e., an encrypted connection) to the switch's web interface. Use the no form to disable this function.

Syntax

[no] server https enable

Default Configuration

Enabled

Command Mode

Global Configuration

User Guidelines

- Both HTTP and HTTPS service can be enabled independently on the switch. However, you cannot configure the HTTP and HTTPS servers to use the same UDP port.
- If you enable HTTPS, you must indicate this in the URL that you specify in your browser: https://*device*[:*port_number*]

Example

Console(config)#server https enble

Console(config)#

14. Telnet Server

This section describes commands used to configure Telnet management access to the switch. This switch also supports a Telnet client function. A Telnet connection can be made from this switch to another device by entering the telnet command at the EXEC configuration level.

server telnet max-sessions

This command specifies the maximum number of Telnet sessions that can simultaneously connect to this system. Use the no from to restore the default setting.

Syntax

server telnet max-sessions *session-count*

no server telnet max-sessions

session-count - The maximum number of allowed Telnet session. (Range: 0-8)

Default Configuration

4 sessions

Command Mode

Global Configuration

User Guidelines

A maximum of eight sessions can be concurrently opened for Telnet and Secure Shell (i.e., both Telnet and SSH share a maximum number or eight sessions).

Example

Console(config)#server telnet max-sessions 1

Console(config)#

server telnet port

This command specifies the TCP port number used by the Telnet interface. Use the no form to use the default port.

Syntax

server telnet port *port-number*

no server telnet port

port-number - The TCP port number to be used by the browser interface. (Range: 1-65535)

Default Configuration

23

Command Mode

Global Configuration

Example

Console(config)#server telnet port 123

Console(config)#

server telnet enable

This command allows this device to be monitored or configured from Telnet. Use the no form to disable this function.

Syntax

[no] server telnet enable

Default Configuration

Enabled

Command Mode

Global Configuration

Example

Console(config)#server telnet enable

Console(config)#

show line telnet

This command displays the configuration settings for the Telnet server.

Command Mode

Normal Exec, EXEC

Example

Console#show line telnet

IP Telnet Configuration:

Telnet Status: Enabled

Telnet Service Port: 23

Telnet Max Session: 4

Console#

15. SSH

This section describes the commands used to configure the SSH server. Note that you also need to install a SSH client on the management station when using this protocol to configure the switch. The switch supports both SSH Version 1.5 and 2.0 clients.

Configuration Guidelines

The SSH server on this switch supports both password and public key authentication. If password authentication is specified by the SSH client, then the password can be authenticated either locally or via a RADIUS or TACACS+ remote authentication server, as specified by the authentication login command. If public key authentication is specified by the client, then you must configure authentication keys on both the client and the switch as described in the following section. Note that regardless of whether you use public key or password authentication, you still have to generate authentication keys on the switch and enable the SSH server.

To use the SSH server, complete these steps:

1. Generate a Host Key Pair – Use the ip ssh crypto host-key generate command to create a host public/private key pair.

2. Provide Host Public Key to Clients – Many SSH client programs automatically import the host public key during the initial connection setup with the switch. Otherwise, you need to manually create a known hosts file on the management station and place the host public key in it. An entry for a public key in the known hosts file would appear similar to the following example:

10.1.0.54 1024 35

15684995401867669259333946775054617325313674890836547254

15020245593199868544358361651999923329781766065830956

10825913212890233765468017262725714134287629413011961955667825

95664104869574278881462065194174677298486546861571773939016477

93559423035774130980227370877945452408397175264635805817671670

9574804776117

3. Import Client's Public Key to the Switch – Use the copy tftp public-key command to copy a file containing the public key for all the SSH client's granted management access to the switch. (Note that these clients must be configured locally on the switch with the username command.) The clients are subsequently authenticated using these keys. The current firmware only accepts public key files based on standard UNIX format as shown in the following example for an RSA key:

1024 36

13410816856098939210409449201554253476316419218729589211431738

80055536161631051775940838686311092912322268285192543746031009

37187721199696317813662774141689851320491172048303392543241016

37997592371449011938006090253948408482717819437228840253311595

21348610229029789827213532671316294325328189150453063939166 43

4. Set the Optional Parameters – Set other optional parameters, including the authentication timeout, the number of retries, and the server key size.

5. Enable SSH Service – Use the ip ssh server enable command to enable the SSH server on the switch.

6. Authentication – One of the following authentication methods is employed:

Password Authentication (for SSH v1.5 or V2 Clients)

a. The client sends its password to the server.

b. The switch compares the client's password to those stored in memory.

c. If a match is found, the connection is allowed.

NOTE: To use SSH with only password authentication, the host public key must still be given to the client, either during initial connection or manually entered into the known host file. However, you do not need to configure the client's keys.

Public Key Authentication – When an SSH client attempts to contact the switch, the SSH server uses the host key pair to negotiate a session key and encryption method. Only clients that have a private key corresponding to the public keys stored on the switch can access it. The following exchanges take place during this process:

Authenticating SSH v1.5 Clients

a. The client sends its RSA public key to the switch.

b. The switch compares the client's public key to those stored in memory.

c. If a match is found, the switch uses its secret key to generate a random 256-bit string as a challenge, encrypts this string with the user's public key, and sends it to the client.

d. The client uses its private key to decrypt the challenge string, computes the MD5 checksum, and sends the checksum back to the switch.

e. The switch compares the checksum sent from the client against that computed for the original string it sent. If the two check sums match, this means that the client's private key corresponds to an authorized public key, and the client is authenticated.

Authenticating SSH v2 Clients

a. The client first queries the switch to determine if DSA public key authentication using a preferred algorithm is acceptable.

b. If the specified algorithm is supported by the switch, it notifies the client to proceed with the authentication process. Otherwise, it rejects the request.

c. The client sends a signature generated using the private key to the switch.

d. When the server receives this message, it checks whether the supplied key is acceptable for authentication, and if so, it then checks whether the signature is correct. If both checks succeed, the client is authenticated.

NOTE: The SSH server supports up to four client sessions. The maximum number of client sessions includes both current Telnet sessions and SSH sessions.

NOTE: The SSH server can be accessed using any configured IPv4 or IPv6 interface address on the switch.

ip ssh authentication-retries

This command configures the number of times the SSH server attempts to reauthenticate a user. Use the no form to restore the default setting.

Syntax

ip ssh authentication-retries *count*

no ip ssh authentication-retries

count – The number of authentication attempts permitted after which the interface is reset. (Range: 1-5)

Default Configuration

3

Command Mode

Global Configuration

Example

Console(config)#ip ssh authentication-retires 2

Console(config)#

ip ssh server enable

This command enables the Secure Shell (SSH) server on this switch. Use the no form to disable this service.

Syntax

[no] ip ssh server enable

Default Configuration

Disabled

Command Mode

Global Configuration

User Guidelines

- The SSH server supports up to four client sessions. The maximum number of client sessions includes both current Telnet sessions and SSH sessions.
- The SSH server uses DSA or RSA for key exchange when the client first establishes a connection with the switch, and then negotiates with the client to select either DES (56-bit) or 3DES (168-bit) for data encryption.
- You must generate DSA and RSA host keys before enabling the SSH server.

Example

Console#ip ssh crypto host-key generate dsa

Console#configure

Console(config)#ip ssh server enable

Console(config)#

ip ssh timeout

This command configures the timeout for the SSH server. Use the no form to restore the default setting.

Syntax

ip ssh timeout *seconds*

no ip ssh timeout

seconds – The timeout for client response during SSH negotiation. (Range: 1-120)

Default Configuration

10 seconds

Command Mode

Global Configuration

User Guidelines

The timeout specifies the interval the switch will wait for a response from the client during the SSH negotiation phase. Once an SSH session has been established, the timeout for user input is controlled by the exec-timeout command for vty sessions.

Example

Console(config)#ip ssh timeout 60

Console(config)#

delete public-key

This command deletes the specified user's public key.

Syntax

delete public-key *username* [dsa | rsa]

username – Name of an SSH user. (Range: 1-8 characters)

dsa – DSA public key type.

rsa – RSA public key type.

Default Configuration

Deletes both the DSA and RSA key.

Command Mode

EXEC

Example

Console#delete public-key admin dsa

Console#

ip ssh crypto host-key generate

This command generates the host key pair (i.e., public and private).

Syntax

ip ssh crypto host-key generate [dsa | rsa]

dsa – DSA (Version 2) key type.

rsa – RSA (Version 1) key type.

Default Configuration

Generates both the DSA and RSA key pairs.

Command Mode

EXEC

User Guidelines

- The switch uses only RSA Version 1 for SSHv1.5 clients and DSA Version 2 for SSHv2 clients.
- This command stores the host key pair in memory (i.e., RAM). Use the ip ssh save host-key command to save the host key pair to flash memory.
- Some SSH client programs automatically add the public key to the known hosts file as part of the configuration process. Otherwise, you must manually create a known hosts file and place the host public key in it.
- The SSH server uses this host key to negotiate a session key and encryption method with the client trying to connect to it.

Example

Console#ip ssh crypto host-key generate dsa

Console#

ip ssh crypto zeroize

This command clears the host key from memory (i.e. RAM).

Syntax

ip ssh crypto zeroize [dsa | rsa]

dsa – DSA key type.

rsa – RSA key type.

Default Configuration

Clears both the DSA and RSA key.

Command Mode

EXEC

User Guidelines

- This command clears the host key from volatile memory (RAM). Use the no ip ssh save host-key command to clear the host key from flash memory.
- The SSH server must be disabled before you can execute this command.

Example

Console#ip ssh crypto zeroize dsa

Console#

ip ssh save host-key

This command saves the host key from RAM to flash memory.

Syntax

ip ssh save host-key

Default Configuration

Saves both the DSA and RSA key.

Command Mode

EXEC

Example

Console#ip ssh save host-key dsa

Console#

show ip ssh

This command displays the connection settings used when authenticating client access to the SSH server.

Command Mode

EXEC

Example

Console#show ip ssh

SSH Enabled - Version 2.0

Negotiation Timeout : 120 seconds; Authentication Retries : 3

Server Key Size : 768 bits

Console#

show public-key

This command shows the public key for the specified user or for the host.

Syntax

show public-key [user [*username*]| host]

username – Name of an SSH user. (Range: 1-8 characters)

Default Configuration

Shows all public keys.

Command Mode

EXEC

User Guidelines

- If no parameters are entered, all keys are displayed. If the user keyword is entered, but no user name is specified, then the public keys for all users are displayed.
- When an RSA key is displayed, the first field indicates the size of the host key (e.g., 1024), the second field is the encoded public exponent (e.g., 35), and the last string is the encoded modulus. When a DSA key is displayed, the first field indicates that the encryption method used by SSH is based on the Digital Signature Standard (DSS), and the last string is the encoded modulus.

Example

Console#show public-key host

Host:

RSA:

1024 65537 13236940658254764031382795526536375927835525327972629521130241

07194210616557594245909392360969540503627752575562510038661309893938345231 0

33280214988866192159556859887989191950588394018138744046890877916030583776 8

185490002831341625008348718449522087429212255691665655296328163516964040831
5547660664151657116381
DSA:
ssh-dss AAAB3NzaC1kc3MAAACBAPWKZTPbsRIB8ydEXcxM3dyV/yrDbKStIlnzD/Dg0h2Hxc
YV44sXZ2JXhamLK6P8bvuiyacWbUW/a4PAtp1KMSdqsKeh3hKoA3vRRSy1N2XFfAKxl5fwFfv
JlPdOkFgzLGMinvSNYQwiQXbKTBH0Z4mUZpE85PWxDZMaCNBPjBrRAAAAFQChb4vsdfQGNIjwbv
wrNLaQ77isiwAAAIEAsy5YWDC99ebYHNRj5kh47wY4i8cZvH+/p9cnrfwFTMU01VFDly3IR
2G395NLy5Qd7ZDxfA9mCOfT/yyEfbobMJZi8oGCstSNOxrZZVnMqWrTYfdrKX7YKBw/Kjw6Bm
iFq7O+jAhf1Dg45loAc27s6TLdtny1wRq/ow2eTCD5nekAAACBAJ8rMccXTxHLFAczWS7EjOy
DbsloBfPuSAb4oAsyjKXKVYNLQkTLZfcFRu41bS2KV5LAwecsigF/+DjKGWtPNlQqabKgYCw2
o/dVzX4Gg+yqdTlYmGA7fHGm8ARGeiG4ssFKy4Z6DmYPXFum1Yg0fhLwuHpOSKdxT3kk475S7
w0W
Console#
show ssh
This command displays the current SSH server connections.
Command Mode
EXEC
Example
Console#show ssh
Connection Version State Username Encryption
0 2.0 Session-Started admin ctos aes128-cbc-hmac-md5
stoc aes128-cbc-hmac-md5
Console#

16. 802.1X

The switch supports IEEE 802.1X (dot1x) port-based access control that prevents unauthorized access to the network by requiring users to first submit credentials for authentication. Client authentication is controlled centrally by a RADIUS server using EAP (Extensible Authentication Protocol).

dot1x default

This command sets all configurable dot1x global and port settings to their default values.

Command Mode

Global Configuration

Example

Console(config)#dot1x default

Console(config)#

dot1x eapol-pass-through

This command passes EAPOL frames through to all ports in STP forwarding state when dot1x is globally disabled. Use the no form to restore the default.

Syntax

[no] dot1x eapol-pass-through

Default Configuration

Discards all EAPOL frames when dot1x is globally disabled

Command Mode

Global Configuration

User Guidelines

- When this device is functioning as intermediate node in the network and does not need to perform dot1x authentication, the dot1x eapol pass-through command can be used to forward EAPOL frames from other switches on to the authentication servers, thereby allowing the authentication process to still be carried out by switches located on the edge of the network.
- When this device is functioning as an edge switch but does not require any attached clients to be authenticated, the no dot1x eapol-passthrough command can be used to discard unnecessary EAPOL traffic.

Example

This example instructs the switch to pass all EAPOL frame through to any ports in STP forwarding state.

Console(config)#dot1x eapol-pass-through

Console(config)#

dot1x system-auth-control

This command enables IEEE 802.1X port authentication globally on the switch. Use the no form to restore the default.

Syntax

[no] dot1x system-auth-control

Default Configuration

Disabled

Command Mode

Global Configuration

Example

Console(config)#dot1x system-auth-control

Console(config)#

dot1x intrusion-action

This command sets the port's response to a failed authentication, either to block all traffic, or to assign all traffic for the port to a guest VLAN. Use the no form to reset the default.

Syntax

dot1x intrusion-action {block-traffic | guest-vlan}

no dot1x intrusion-action

block-traffic - Blocks traffic on this port.

guest-vlan - Assigns the user to the Guest VLAN.

DEFAULT

block-traffic

Command Mode

Interface Configuration

User Guidelines

For guest VLAN assignment to be successful, the VLAN must be configured and set as active (see the vlan database command) and assigned as the guest VLAN for the port (see the network-access guest-vlan command).

Example

Console(config)#interface eth 1/2

Console(config-if)#dot1x intrusion-action guest-vlan

Console(config-if)#

dot1x max-reauth-req

This command sets the maximum number of times that the switch sends an EAP-request/identity frame to the client before restarting the authentication process. Use the no form to restore the default.

Syntax

dot1x max-reauth-req *count*

no dot1x max-reauth-req

count – The maximum number of requests (Range: 1-10)

DEFAULT

2

Command Mode

Interface Configuration

Example

Console(config)#interface eth 1/2

Console(config-if)#dot1x max-reauth-req 2

Console(config-if)#

dot1x max-req

This command sets the maximum number of times the switch port will retransmit an EAP request/identity packet to the client before it times out the authentication session. Use the no form to restore the default.

Syntax

dot1x max-req *count*

no dot1x max-req

count – The maximum number of requests (Range: 1-10)

DEFAULT

2

Command Mode

Interface Configuration

Example

Console(config)#interface eth 1/2

Console(config-if)#dot1x max-req 2

Console(config-if)#

dot1x operation-mode

This command allows hosts (clients) to connect to an 802.1X-authorized port. Use the no form with no keywords to restore the default to single host. Use the no form with the multi-host max-count keywords to restore the default maximum count.

Syntax

dot1x operation-mode {single-host | multi-host [max-count *count*] | mac-based-auth}

no dot1x operation-mode [multi-host max-count]

single-host – Allows only a single host to connect to this port.

multi-host – Allows multiple host to connect to this port.

max-count – Keyword for the maximum number of hosts.

count – The maximum number of hosts that can connect to a port. (Range: 1-1024; Default: 5)

mac-based – Allows multiple hosts to connect to this port, with each host needing to be authenticated.

DEFAULT

Single-host

Command Mode

Interface Configuration

User Guidelines

- The "max-count" parameter specified by this command is only effective if the dot1x mode is set to "auto" by the dot1x port-control command.
- In "multi-host" mode, only one host connected to a port needs to pass authentication for all other hosts to be granted network access. Similarly, a port can become unauthorized for all hosts if one attached host fails re-authentication or sends an EAPOL logoff message.
- In "mac-based-auth" mode, each host connected to a port needs to pass authentication. The number of hosts allowed access to a port operating in this mode is limited only by the available space in the secure address table (i.e., up to 1024 addresses).

Example

Console(config)#interface eth 1/2

Console(config-if)#dot1x operation-mode multi-host max-count 10

Console(config-if)#

dot1x port-control

This command sets the dot1x mode on a port interface. Use the no form to restore the default.

Syntax

dot1x port-control {auto | force-authorized | force-unauthorized}

no dot1x port-control

auto – Requires a dot1x-aware connected client to be authorized by the RADIUS server. Clients that are not dot1x-aware will be denied access.

force-authorized – Configures the port to grant access to all clients, either dot1x-aware or otherwise.

force-unauthorized – Configures the port to deny access to all clients, either dot1x-aware or otherwise.

DEFAULT

force-authorized

Command Mode

Interface Configuration

Example

Console(config)#interface eth 1/2

Console(config-if)#dot1x port-control auto

Console(config-if)#

dot1x re-authentication

This command enables periodic re-authentication for a specified port. Use the no form to disable re-authentication.

Syntax

[no] dot1x re-authentication

Command Mode

Interface Configuration

User Guidelines

- The re-authentication process verifies the connected client's user ID and password on the RADIUS server. During re-authentication, the client remains connected the network and the process is handled transparently by the dot1x client software. Only if re-authentication fails is the port blocked.
- The connected client is re-authenticated after the interval specified by the dot1x timeout re-authperiod command. The default is 3600 seconds.

Example

Console(config)#interface eth 1/2

Console(config-if)#dot1x re-authentication

Console(config-if)#

dot1x timeout quiet-period

This command sets the time that a switch port waits after the maximum request count has been exceeded before attempting to acquire a new client. Use the no form to reset the default.

Syntax

dot1x timeout quiet-period *seconds*

no dot1x timeout quiet-period

seconds - The number of seconds. (Range: 1-65535)

DEFAULT

60 seconds

Command Mode

Interface Configuration

Example

Console(config)#interface eth 1/2

Console(config-if)#dot1x timeout quiet-period 350

Console(config-if)#

dot1x timeout re-authperiod

This command sets the time period after which a connected client must be re-authenticated. Use the no form of this command to reset the default.

Syntax

dot1x timeout re-authperiod *seconds*

no dot1x timeout re-authperiod

seconds - The number of seconds. (Range: 1-65535)

DEFAULT

3600 seconds

Command Mode

Interface Configuration

Example

Console(config)#interface eth 1/2

Console(config-if)#dot1x timeout re-authperiod 300

Console(config-if)#

dot1x timeout supp-timeout

This command sets the time that an interface on the switch waits for a response to an EAP request from a client before re-transmitting an EAP packet. Use the no form to reset to the default value.

Syntax

dot1x timeout supp-timeout *seconds*

no dot1x timeout supp-timeout

seconds - The number of seconds. (Range: 1-65535)

DEFAULT

30 seconds

Command Mode

Interface Configuration

User Guidelines

This command sets the timeout for EAP-request frames other than EAP-request/identity frames. If dot1x authentication is enabled on a port, the switch will initiate authentication when the port link state comes up. It will send an EAP-request/identity frame to the client to request its identity, followed by one or more requests for authentication information. It may also send other EAP-request frames to the client during an active connection as required for reauthentication.

Example

Console(config)#interface eth 1/2

Console(config-if)#dot1x timeout supp-timeout 300

Console(config-if)#

dot1x timeout tx-period

This command sets the time that an interface on the switch waits during an authentication session before re-transmitting an EAP packet. Use the no form to reset to the default value.

Syntax

dot1x timeout tx-period *seconds*

no dot1x timeout tx-period

seconds - The number of seconds. (Range: 1-65535)

DEFAULT

30 seconds

Command Mode

Interface Configuration

Example

Console(config)#interface eth 1/2

Console(config-if)#dot1x timeout tx-period 300

Console(config-if)#

dot1x re-authenticate

This command forces re-authentication on all ports or a specific interface.

Syntax

dot1x re-authenticate [*interface*]

interface

ethernet *unit*/*port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-28)

Command Mode

EXEC

User Guidelines

The re-authentication process verifies the connected client's user ID and password on the RADIUS server. During re-authentication, the client remains connected the network and the process is handled transparently by the dot1x client software. Only if re-authentication fails is the port blocked.

Example

Console#dot1x re-authenticate

Console#

dot1x identity profile

This command sets the dot1x supplicant user name and password. Use the no form to delete the identity settings.

Syntax

dot1x identity profile {username *username* | password *password*}

no dot1x identity profile {username | password}

username - Specifies the supplicant user name. (Range: 1-8 characters)

password - Specifies the supplicant password. (Range: 1-8 characters)

DEFAULT

No user name or password

Command Mode

Global Configuration

User Guidelines

The global supplicant user name and password are used to identify this switch as a supplicant when responding to an MD5 challenge from the authenticator. These parameters must be set when this switch passes client authentication requests to another authenticator on the network.

Example

Console(config)#dot1x identity profile username steve

Console(config)#dot1x identity profile password excess

Console(config)#

dot1x max-start

This command sets the maximum number of times that a port supplicant will send an EAP start frame to the client before assuming that the client is 802.1X unaware. Use the no form to restore the default value.

Syntax

dot1x max-start *count*

no dot1x max-start

count - Specifies the maximum number of EAP start frames.

(Range: 1-65535)

DEFAULT

3

Command Mode

Interface Configuration

Example

Console(config)#interface eth 1/2

Console(config-if)#dot1x max-start 10

Console(config-if)#

dot1x pae supplicant

This command enables dot1x supplicant mode on a port. Use the no form to disable dot1x supplicant mode on a port.

Syntax

[no] dot1x pae supplicant

DEFAULT

Disabled

Command Mode

Interface Configuration

User Guidelines

- When devices attached to a port must submit requests to another authenticator on the network, configure the identity profile parameters which identify this switch as a supplicant, and enable dot1x supplicant mode for those ports which must authenticate clients through a remote authenticator using this command. In this mode the port will not respond to dot1x messages meant for an authenticator.
- This switch can be configured to serve as the authenticator on selected ports by setting the control mode to "auto", and as a supplicant on other ports by the setting the control mode to "force-authorized" and enabling dot1x supplicant mode with this command.
- A port cannot be configured as a dot1x supplicant if it is a member of a trunk or LACP is enabled on the port.

Example

Console(config)#interface ethernet 1/2

Console(config-if)#dot1x pae supplicant

Console(config-if)#

dot1x timeout auth-period

This command sets the time that a supplicant port waits for a response from the authenticator. Use the no form to restore the default setting.

Syntax

dot1x timeout auth-period *seconds*

no dot1x timeout auth-period

seconds - The number of seconds. (Range: 1-65535)

DEFAULT

30 seconds

Command Mode

Interface Configuration

User Guidelines

This command sets the time that the supplicant waits for a response from the authenticator for packets other than EAPOL-Start.

Example

Console(config)#interface eth 1/2

Console(config-if)#dot1x timeout auth-period 60

Console(config-if)#

dot1x timeout held-period

This command sets the time that a supplicant port waits before resending its credentials to find a new an authenticator. Use the no form to reset the default.

Syntax

dot1x timeout held-period *seconds*

no dot1x timeout held-period

seconds - The number of seconds. (Range: 1-65535)

DEFAULT

60 seconds

Command Mode

Interface Configuration

Example

Console(config)#interface eth 1/2

Console(config-if)#dot1x timeout held-period 120

Console(config-if)#

dot1x timeout start-period

This command sets the time that a supplicant port waits before resending an EAPOL start frame to the authenticator. Use the no form to restore the default setting.

Syntax

dot1x timeout start-period *seconds*

no dot1x timeout start-period

seconds - The number of seconds. (Range: 1-65535)

DEFAULT

30 seconds

Command Mode

Interface Configuration

Example

Console(config)#interface eth 1/2

Console(config-if)#dot1x timeout start-period 60

Console(config-if)#

show dot1x

This command shows general port authentication related settings on the switch or a specific interface.

Syntax

show dot1x [statistics] [interface *interface*]

statistics - Displays dot1x status for each port.

interface

ethernet *unit*/*port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-28)

Command Mode

EXEC

User Guidelines

This command displays dot1x information.

Example

Console#show dot1x

Global 802.1X Parameters

System Auth Control : Enabled

Authenticator Parameters:

EAPOL Pass Through : Disabled

Supplicant Parameters:

Identity Profile Username : steve

802.1X Port Summary

Port Type Operation Mode Control Mode Authorized

-------- ------------ -------------- ------------------ ----------

Eth 1/ 1 Disabled Single-Host Force-Authorized Yes

Eth 1/ 2 Disabled Single-Host Force-Authorized Yes

...

Eth 1/27 Disabled Single-Host Force-Authorized Yes

Eth 1/28 Enabled Single-Host Auto Yes

802.1X Port Details

802.1X Authenticator is enabled on port 1/1

802.1X Supplicant is disabled on port 1/1

...

802.1X Authenticator is enabled on port 28

Reauthentication : Enabled

Reauth Period : 3600

Quiet Period : 60

TX Period : 30

Supplicant Timeout : 30

Server Timeout : 10

Reauth Max Retries : 2

Max Request : 2

Operation Mode : Multi-host

Port Control : Auto

Intrusion Action : Block traffic

Supplicant : 00-e0-29-94-34-65

Authenticator PAE State Machine

State : Authenticated

Reauth Count : 0

Current Identifier : 3

Backend State Machine

State : Idle

Request Count : 0

Identifier(Server) : 2

Reauthentication State Machine

State : Initialize

Console#

17. Management IP Filter

This section describes commands used to configure IP management access to the switch.

management

This command specifies the client IP addresses that are allowed management access to the switch through various protocols. Use the no form to restore the default setting.

Syntax

[no] management {all-client | http-client | snmp-client | telnet-client} *start-address* [*end-address*]

all-client - Adds IP address(es) to all groups.

http-client - Adds IP address(es) to the web group.

snmp-client - Adds IP address(es) to the SNMP group.

telnet-client - Adds IP address(es) to the Telnet group.

start-address - A single IP address, or the starting address of a range.

end-address - The end address of a range.

Default Configuration

All addresses

Command Mode

Global Configuration

User Guidelines

- If anyone tries to access a management interface on the switch from an invalid address, the switch will reject the connection, enter an event message in the system log, and send a trap message to the trap manager.
- IP address can be configured for SNMP, web, and Telnet access respectively. Each of these groups can include up to five different sets of addresses, either individual addresses or address ranges.
- When entering addresses for the same group (i.e., SNMP, web, or Telnet), the switch will not accept overlapping address ranges. When entering addresses for different groups, the switch will accept overlapping address ranges.
- You cannot delete an individual address from a specified range. You must delete the entire range, and reenter the addresses.
- You can delete an address range just by specifying the start address, or by specifying both the start address and end address.

Example

This example restricts management access to the indicated addresses.

```
Console(config)#management all-client 192.168.1.19
Console(config)#management all-client 192.168.1.25 192.168.1.30
Console#
```

show management

This command displays the client IP addresses that are allowed management access to the switch through various protocols.

Syntax

show management {all-client | http-client | snmp-client | telnet-client}

all-client - Displays IP addresses for all groups.

http-client - Displays IP addresses for the web group.

snmp-client - Displays IP addresses for the SNMP group.

telnet-client - Displays IP addresses for the Telnet group.

Command Mode

EXEC

Example

Console#show management all-client

Management Ip Filter

HTTP-Client:

Start IP address End IP address

---

1. 192.168.1.19 192.168.1.19

2. 192.168.1.25 192.168.1.30

SNMP-Client:

Start IP address End IP address

---

1. 192.168.1.19 192.168.1.19

2. 192.168.1.25 192.168.1.30

TELNET-Client:

Start IP address End IP address

---

1. 192.168.1.19 192.168.1.19

2. 192.168.1.25 192.168.1.30

Console#

18. PPPoE Intermediate Agent

This section describes commands used to configure the PPoE Intermediate Agent (PPPoE IA) relay parameters required for passing authentication messages between a client and broadband remote access servers.

pppoe intermediate-agent

This command enables the PPPoE Intermediate Agent globally on the switch. Use the no form to disable this feature.

Syntax

[no] pppoe intermediate-agent

Default Configuration

Disabled

Command Mode

Global Configuration

User Guidelines

- The switch inserts a tag identifying itself as a PPPoE Intermediate Agent residing between the attached client requesting network access and the ports connected to broadband remote access servers (BRAS). The switch extracts access-loop information from the client's PPPoE Active Discovery Request, and forwards this information to all trusted ports designated by the pppoe intermediate-agent trust command. The BRAS detects the presence of the subscriber's circuit-Id tag inserted by the switch during the PPPoE discovery phase, and sends this tag as a NASport-Id attribute in PPP authentication and AAA accounting requests to a RADIUS server.
- PPPoE IA must be enabled globally by this command before this feature can be enabled on an interface using the pppoe intermediate-agent port-enable command.

Example

Console(config)#pppoe intermediate-agent

Console(config)#

pppoe intermediate-agent format-type

This command sets the access node identifier and generic error message for the switch. Use the no form to restore the default settings.

Syntax

pppoe intermediate-agent format-type {access-node-identifier *id-string* | generic-error-message *error-message*}

no pppoe intermediate-agent format-type {access-nodeidentifier | generic-error-message}

id-string - String identifying this switch as an PPPoE IA to the PPPoE server. (Range: 1-48 ASCII characters)

error-message - An error message notifying the sender that the PPPoE Discovery packet was too large.

Default Configuration

- Access Node Identifier: IP address of the management interface
- Generic Error Message: PPPoE Discover packet too large to process. Try reducing the number of tags added.

Command Mode

Global Configuration

User Guidelines

- The switch uses the access-node-identifier to generate the circuit-id for PPPoE discovery stage packets sent to the BRAS, but does not modify the source or destination MAC address of these PPPoE discovery packets.
- These messages are forwarded to all trusted ports designated by the pppoe intermediate-agent trust command.

Example

Console(config)#pppoe intermediate-agent format-type access-node-identifier billibong

Console(config)#

pppoe intermediate-agent port-enable

This command enables the PPPoE IA on an interface. Use the no form to disable this feature.

Syntax

[no] pppoe intermediate-agent port-enable

Default Configuration

Disabled

Command Mode

Interface Configuration (Ethernet, Port Channel)

User Guidelines

PPPoE IA must also be enabled globally on the switch for this command to tack effect.

Example

Console(config)#int ethernet 1/5

Console(config-if)#pppoe intermediate-agent port-enable

Console(config-if)#

pppoe intermediate-agent port-format-type

This command sets the circuit-id or remote-id for an interface. Use the no form to restore the default settings.

Syntax

pppoe intermediate-agent port-format-type {circuit-id | remote-id} *id-string*

circuit-id - String identifying the circuit identifier (or interface) on this switch to which the user is connected. (Range: 1-10 ASCII characters)

remote-id - String identifying the remote identifier (or interface) on this switch to which the user is connected. (Range: 1-63 ASCII characters)

Default Configuration

circuit-id: unit/port:vlan-id or 0/trunk-id:vlan-id

remote-id: port MAC address

Command Mode

Interface Configuration (Ethernet, Port Channel)

User Guidelines

- The PPPoE server extracts the Line-Id tag from PPPoE discovery stage messages, and uses the Circuit-Id field of that tag as a NAS-Port-Id attribute in AAA access and accounting requests.
- The switch intercepts PPPoE discovery frames from the client and inserts a unique line identifier using the PPPoE Vendor-Specific tag (0x0105) to PPPoE Active Discovery Initiation (PADI) and Request (PADR) packets. The switch then forwards these packets to the PPPoE server. The tag contains the Line-Id of the customer line over which the discovery packet was received, entering the switch (or access node) where the intermediate agent resides.
- Outgoing PAD Offer (PADO) and Session-confirmation (PADS) packets sent from the PPPoE Server include the Circuit-Id tag inserted by the switch, and should be stripped out of PADO and PADS packets which are to be passed directly to end-node clients using the pppoe intermediate-agent vendor-tag strip command.

Example

Console(config)#int ethernet 1/5

Console(config-if)#pppoe intermediate-agent port-format-type circuit-id

ECS4500-28

Console(config-if)#

pppoe intermediate-agent trust

This command sets an interface to trusted mode to indicate that it is connected to a PPPoE server. Use the no form to set an interface to untrusted mode.

Syntax

[no] pppoe intermediate-agent trust

Default Configuration

Untrusted

Command Mode

Interface Configuration (Ethernet, Port Channel)

User Guidelines

- Set any interfaces connecting the switch to a PPPoE Server as trusted. Interfaces that connect the switch to users (PPPoE clients) should be set as untrusted.
- At least one trusted interface must be configured on the switch for the PPPoE IA to function.

Example

Console(config)#int ethernet 1/5

Console(config-if)#pppoe intermediate-agent trust

Console(config-if)#

pppoe intermediate-agent vendor-tag strip

This command enables the stripping of vendor tags from PPPoE Discovery packets sent from a PPPoE server. Use the no form to disable this feature.

Syntax

[no] pppoe intermediate-agent vendor-tag strip

Default Configuration

Disabled

Command Mode

Interface Configuration (Ethernet, Port Channel)

User Guidelines

This command only applies to trusted interfaces. It is used to strip off vendor-specific tags (which carry subscriber and line identification information) in PPPoE Discovery packets received from an upstream PPPoE server before forwarding them to a user.

Example

Console(config)#int ethernet 1/5

Console(config-if)#pppoe intermediate-agent vendor-tag strip

Console(config-if)#

clear pppoe intermediate-agent statistics

This command clears statistical counters for the PPPoE Intermediate Agent.

Syntax

clear pppoe intermediate-agent statistics [interface [*interface*]]

interface

ethernet *unit*/*port*

unit - Stack unit. (Range: 1)

port - Port number. (Range: 1-28)

port-channel *channel-id* (Range: 1-12)

Command Mode

EXEC

Example

Console#clear pppoe intermediate-agent statistics

Console#

show pppoe intermediate-agent info

This command displays configuration settings for the PPPoE Intermediate Agent.

Syntax

show pppoe intermediate-agent info [interface [*interface*]]

interface

ethernet *unit*/*port*

unit - Stack unit. (Range: 1)

port - Port number. (Range: 1-28)

port-channel *channel-id* (Range: 1-12)

Command Mode

EXEC

Example

Console#show pppoe intermediate-agent info

PPPoE Intermediate Agent Global Status : Enabled

PPPoE Intermediate Agent Admin Access Node Identifier : 192.168.0.2

PPPoE Intermediate Agent Oper Access Node Identifier : 192.168.0.2

PPPoE Intermediate Agent Admin Generic Error Message :

PPPoE Discover packet too large to process. Try reducing the number of tags

added.

PPPoE Intermediate Agent Oper Generic Error Message :

PPPoE Discover packet too large to process. Try reducing the number of tags

added.

Consoleshow pppoe intermediate-agent info interface ethernet 1/1

Interface PPPoE IA Trusted Vendor-Tag Strip Admin Circuit-ID Admin Remote-ID

Oper Circuit-ID Oper Remote-ID

--------- -------- ------- ---------- ---------- ----------

Eth 1/2 Yes No Yes ECS4510-28T ECS4510-28T

ECS4510-28T ECS4510-28T

Console#

show pppoe intermediate-agent statistics

This command displays statistics for the PPPoE Intermediate Agent.

Syntax

show pppoe intermediate-agent statistics interface [*interface*]

interface

ethernet *unit*/*port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-28)

port-channel *channel-id* (Range: 1-12)

Command Mode

EXEC

Example

Console#show pppoe intermediate-agent statistics interface ethernet 1/1

Eth 1/1 statistics

Received: All PADI PADO PADR PADS PADT

---

3 0 0 0 0 3

Dropped: Response from untrusted Request towards untrusted Malformed

---

0 0 0

Console#

19. Port Security

These commands can be used to enable port security on a port. When using port security, the switch stops learning new MAC addresses on
the specified port when it has reached a configured maximum number.
Only incoming traffic with source addresses already stored in the dynamic or static address table for this port will be authorized to access the network. The port will drop any incoming frames with a source MAC address that is unknown or has been previously learned from another port. If a device with an unauthorized MAC address attempts to use the switch port, the intrusion will be detected and the switch can automatically take action by disabling the port and sending a trap message.
port security
This command enables or configures port security. Use the no form without any keywords to disable port security. Use the no form with the appropriate keyword to restore the default settings for a response to security violation or for the maximum number of allowed addresses.
Syntax
port security [action {shutdown | trap | trap-and-shutdown} | max-mac-count *address-count*]
no port security [action | max-mac-count]
action - Response to take when port security is violated.
shutdown - Disable port only.
trap - Issue SNMP trap message only.
trap-and-shutdown - Issue SNMP trap message and disable port.
max-mac-count
address-count - The maximum number of MAC addresses that can be learned on a port. (Range: 0 - 1024, where 0 means disabled)
Default Configuration
Status: Disabled
Action: None
Maximum Addresses: 0
Command Mode
Interface Configuration (Ethernet)
User Guidelines

- The default maximum number of MAC addresses allowed on a secure port is zero (that is, port security is disabled). To use port security, you must configure the maximum number of addresses allowed on a port using the port security max-mac-count command.
- When port security is enabled using the port security command, or the maximum number or allowed addresses is set to value lower than the current limit after port security has been enabled, the switch first clears all dynamically learned entries from the address table. It then starts learning new MAC addresses on the specified port, and stops learning addresses when it reaches a configured maximum number. Only incoming traffic with source addresses already stored in the dynamic or static address table will be accepted.
- To configure the maximum number of address entries which can be learned on a port, specify the maximum number of dynamic addresses allowed. The switch will learn up to the maximum number of allowed address pairs <source MAC address, VLAN> for frames received on the port. (The specified maximum address count is effective when port security is enabled or disabled.) Note that you can manually add additional secure

addresses to a port using the mac-address-table static command. When the port has reached the maximum number of MAC addresses, the port will stop learning new addresses. The MAC addresses already in the address table will be retained and will not be aged out.

- If port security is enabled, and the maximum number of allowed addresses are set to a non-zero value, any device not in the address table that attempts to use the port will be prevented from accessing the switch.
- If a port is disabled due to a security violation, it must be manually reenabled using the no shutdown command.

A secure port has the following restrictions:

a. Cannot be connected to a network interconnection device.

b. Cannot be a trunk port.

Example

The following example enables port security for port 5, and sets the response to a security violation to issue a trap message:

Console(config)#interface ethernet 1/5

Console(config-if)#port security action trap

show port security

This command displays port security status and the secure address count.

Syntax

show port security [interface *interface*]

interface - Specifies a port interface.

ethernet *unit*/*port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-28)

Command Mode

EXEC

Example

This example shows the port security settings and number of secure

addresses for all ports.

Console#show port security

Global Port Security Parameters

Secure MAC Aging Mode: Disabled

Port Security Port Summary

Port Port Security Port Status Intrusion Action MaxMacCnt CurrMacCnt

---

Eth 1/ 1 Disabled Secure/Down None 0 2

Eth 1/ 2 Enabled Secure/Up None 10 0

Eth 1/ 3 Disabled Secure/Down None 0 0

Eth 1/ 4 Disabled Secure/Down None 0 0

Eth 1/ 5 Disabled Secure/Down None 0 0

20. Network Access

Network Access authentication controls access to the network by authenticating the MAC address of each host that attempts to connect to a switch port. Traffic received from a specific MAC address is forwarded by the switch only if the source MAC address is successfully authenticated by a central RADIUS server. While authentication for a MAC address is in progress, all traffic is blocked until authentication is completed. Once successfully authenticated, the RADIUS server may optionally assign VLAN and QoS settings for the switch port.

network-access aging

Use this command to enable aging for authenticated MAC addresses stored in the secure MAC address table. Use the no form of this command to disable address aging.

Syntax

[no] network-access aging

Default Configuration

Disabled

Command Mode

Global Configuration

User Guidelines

- Authenticated MAC addresses are stored as dynamic entries in the switch's secure MAC address table and are removed when the aging time expires. The address aging time is determined by the macaddress-table aging-time command.
- This parameter applies to authenticated MAC addresses configured by the MAC Address Authentication process described in this section, as well as to any secure MAC addresses authenticated by 802.1X, regardless of the 802.1X Operation Mode (Single-Host, Multi-Host, or MAC-Based authentication).
- The maximum number of secure MAC addresses supported for the switch system is 1024.

Example

Console(config-if)#network-access aging

Console(config-if)#

network-access mac-filter

Use this command to add a MAC address into a filter table. Use the no form of this command to remove the specified MAC address.

Syntax

[no] network-access mac-filter *filter-id* mac-address *mac-address* [mask *mask-address*]

filter-id - Specifies a MAC address filter table. (Range: 1-64)

mac-address - Specifies a MAC address entry. (Format: xx-xx-xx-xx-xx-xx)

mask - Specifies a MAC address bit mask for a range of addresses.

Default Configuration

Disabled

Command Mode

Global Configuration

User Guidelines

- Specified addresses are exempt from network access authentication.

- This command is different from configuring static addresses with the mac-address-table static command in that it allows you configure a range of addresses when using a mask, and then to assign these addresses to one or more ports with the network-access port-mac-filter command.
- Up to 64 filter tables can be defined.
- There is no limitation on the number of entries that can entered in a filter table.

Example

Console(config)#network-access mac-filter 1 mac-address 11-22-33-44-55-66

Console(config)#

mac-authentication reauth-time

Use this command to set the time period after which a connected MAC address must be re-authenticated. Use the no form of this command to restore the default value.

Syntax

mac-authentication reauth-time *seconds*

no mac-authentication reauth-time

seconds - The re-authentication time period. (Range: 120-1000000 seconds)

Default Configuration

1800

Command Mode

Global Configuration

User Guidelines

- The re-authentication time is a global setting and applies to all ports.
- When the re-authentication time expires for a secure MAC address it is re-authenticated with the RADIUS server. During the re-authentication process traffic through the port remains unaffected.

Example

Console(config)#mac-authentication reauth-time 300

Console(config)#

network-access dynamic-qos

Use this command to enable the dynamic QoS feature for an authenticated port. Use the no form to restore the default.

Syntax

[no] network-access dynamic-qos

Default Configuration

Disabled

Command Mode

Interface Configuration

User Guidelines

- The RADIUS server may optionally return dynamic QoS assignments to be applied to a switch port for an authenticated user.
- When the last user logs off of a port with a dynamic QoS assignment, the switch restores the original QoS configuration for the port.
- When a user attempts to log into the network with a returned dynamic QoS profile that is different from users already logged on to the same port, the user is denied access.
- While a port has an assigned dynamic QoS profile, any manual QoS configuration changes only take effect after all users have logged off of the port.

Note:

Any configuration changes for dynamic QoS are not saved to the switch configuration file.

Example

The following example enables the dynamic QoS feature on port 1.

Console(config)#interface ethernet 1/1

Console(config-if)#network-access dynamic-qos

Console(config-if)#

network-access dynamic-vlan

Use this command to enable dynamic VLAN assignment for an authenticated port. Use the no form to disable dynamic VLAN assignment.

Syntax

[no] network-access dynamic-vlan

Default Configuration

Enabled

Command Mode

Interface Configuration

User Guidelines

- When enabled, the VLAN identifiers returned by the RADIUS server through the 802.1X authentication process will be applied to the port, providing the VLANs have already been created on the switch. GVRP is not used to create the VLANs.
- The VLAN settings specified by the first authenticated MAC address are implemented for a port. Other authenticated MAC addresses on the port must have same VLAN configuration, or they are treated as an authentication failure.
- If dynamic VLAN assignment is enabled on a port and the RADIUS server returns no VLAN configuration, the authentication is still treated as a success, and the host assigned to the default untagged VLAN.
- When the dynamic VLAN assignment status is changed on a port, all authenticated addresses are cleared from the secure MAC address table.

Example

The following example enables dynamic VLAN assignment on port 1.

Console(config)#interface ethernet 1/1

Console(config-if)#network-access dynamic-vlan

Console(config-if)#

network-access guest-vlan

Use this command to assign all traffic on a port to a guest VLAN when 802.1x authentication is rejected. Use the no form of this command to disable guest VLAN assignment.

Syntax

network-access guest-vlan *vlan-id*

no network-access guest-vlan

vlan-id - VLAN ID (Range: 1-4094)

Default Configuration

Disabled

Command Mode

Interface Configuration

User Guidelines

- The VLAN to be used as the guest VLAN must be defined and set as active (See the vlan database command).
- When used with 802.1X authentication, the intrusion-action must be set for "guest-vlan" to be effective (see the dot1x intrusion-action command).

Example

Console(config)#interface ethernet 1/1

Console(config-if)#network-access guest-vlan 25

Console(config-if)#

network-access link-detection

Use this command to enable link detection for the selected port. Use the no form of this command to restore the default.

Syntax

[no] network-access link-detection

Default Configuration

Disabled

Command Mode

Interface Configuration

Example

Console(config)#interface ethernet 1/1

Console(config-if)#network-access link-detection

Console(config-if)#

network-access link-detection link-down

Use this command to detect link-down events. When detected, the switch can shut down the port, send an SNMP trap, or both. Use the no form of this command to disable this feature.

Syntax

network-access link-detection link-down action [shutdown | trap | trap-and-shutdown]

no network-access link-detection

action - Response to take when port security is violated.

shutdown - Disable port only.

trap - Issue SNMP trap message only.

trap-and-shutdown - Issue SNMP trap message and disable the port.

Default Configuration

Disabled

Command Mode

Interface Configuration

Example

Console(config)#interface ethernet 1/1

Console(config-if)#network-access link-detection link-down action trap

Console(config-if)#

network-access link-detection link-up

Use this command to detect link-up events. When detected, the switch can shut down the port, send an SNMP trap, or both. Use the no form of this command to disable this feature.

Syntax

network-access link-detection link-up action [shutdown | trap | trap-and-shutdown]

no network-access link-detection

action - Response to take when port security is violated.

shutdown - Disable port only.

trap - Issue SNMP trap message only.

trap-and-shutdown - Issue SNMP trap message and disable the port.

Default Configuration

Disabled

Command Mode

Interface Configuration

Console(config)#interface ethernet 1/1

Console(config-if)#network-access link-detection link-up action trap

Console(config-if)#

network-access link-detection link-up-down

Use this command to detect link-up and link-down events. When either event is detected, the switch can shut down the port, send an SNMP trap, or both. Use the no form of this command to disable this feature.

Syntax

network-access link-detection link-up-down action [shutdown | trap | trap-and-shutdown]

no network-access link-detection

action - Response to take when port security is violated.

shutdown - Disable port only.

trap - Issue SNMP trap message only.

trap-and-shutdown - Issue SNMP trap message and disable the port.

Default Configuration

Disabled

Command Mode

Interface Configuration

Example

Console(config)#interface ethernet 1/1

Console(config-if)#network-access link-detection link-up-down action trap

Console(config-if)#

network-access max-mac-count

Use this command to set the maximum number of MAC addresses that can be authenticated on a port interface via all forms of authentication. Use the no form of this command to restore the default.

Syntax

network-access max-mac-count *count*

no network-access max-mac-count

count - The maximum number of authenticated IEEE 802.1X and MAC addresses allowed. (Range: 0-2048; 0 for unlimited)

Default Configuration

1024

Command Mode

Interface Configuration

User Guidelines

The maximum number of MAC addresses per port is 1024, and the maximum number of secure MAC addresses supported for the switch system is 1024. When the limit is reached, all new MAC addresses are treated as authentication failures.

Example

Console(config-if)#network-access max-mac-count 5

Console(config-if)#

network-access mode mac-authentication

Use this command to enable network access authentication on a port. Use the no form of this command to disable network access authentication.

Syntax

[no] network-access mode mac-authentication

Default Configuration

Disabled

Command Mode

Interface Configuration

User Guidelines

- When enabled on a port, the authentication process sends a Password Authentication Protocol (PAP) request to a configured RADIUS server. The user name and password are both equal to the MAC address being authenticated.
- On the RADIUS server, PAP user name and passwords must be configured in the MAC address format XX-XX-XX-XX-XX-XX (all in upper case).
- Authenticated MAC addresses are stored as dynamic entries in the switch secure MAC address table and are removed when the aging time expires. The maximum number of secure MAC addresses supported for the switch system is 1024.
- Configured static MAC addresses are added to the secure address table when seen on a switch port. Static addresses are treated as authenticated without sending a request to a RADIUS server.
- MAC authentication, 802.1X, and port security cannot be configured together on the same port. Only one security mechanism can be applied.
- MAC authentication cannot be configured on trunk ports.
- When port status changes to down, all MAC addresses are cleared from the secure MAC address table. Static VLAN assignments are not restored.
- The RADIUS server may optionally return a VLAN identifier list. VLAN identifier list is carried in the "Tunnel-Private-Group-ID" attribute. The VLAN list can contain multiple VLAN identifiers in the format "1u,2t," where "u" indicates untagged VLAN and "t" tagged VLAN. The "Tunnel-Type" attribute should be set to "VLAN," and the "Tunnel-Medium-Type" attribute set to "802."

Example

Console(config-if)#network-access mode mac-authentication

Console(config-if)#

network-access port-mac-filter

Use this command to enable the specified MAC address filter. Use the no form of this command to disable the specified MAC address filter.

Syntax

network-access port-mac-filter *filter-id*

no network-access port-mac-filter

filter-id - Specifies a MAC address filter table. (Range: 1-64)

Default Configuration

None

Command Mode

Interface Configuration

Command Mode

- Entries in the MAC address filter table can be configured with the network-access mac-filter command.
- Only one filter table can be assigned to a port.

Example

Console(config)#interface ethernet 1/1

Console(config-if)#network-access port-mac-filter 1

Console(config-if)#

mac-authentication intrusion-action

Use this command to configure the port response to a host MAC authentication failure. Use the no form of this command to restore the default.

Syntax

mac-authentication intrusion-action {block traffic | pass traffic}

no mac-authentication intrusion-action

Default Configuration

Block Traffic

Command Mode

Interface Con figuration

Example

Console(config-if)#mac-authentication intrusion-action block-traffic

Console(config-if)#

mac-authentication max-mac-count

Use this command to set the maximum number of MAC addresses that can be authenticated on a port via MAC authentication. Use the no form of this command to restore the default.

Syntax

mac-authentication max-mac-count *count*

no mac-authentication max-mac-count

count - The maximum number of MAC-authenticated MAC addresses allowed. (Range: 1-1024)

Default Configuration

1024

Command Mode

Interface Configuration

Example

Console(config-if)#mac-authentication max-mac-count 32

Console(config-if)#

clear network-access

Use this command to clear entries from the secure MAC addresses table.

Syntax

clear network-access mac-address-table [static | dynamic] [address *mac-address*] [interface *interface*]

static - Specifies static address entries.

dynamic - Specifies dynamic address entries.

mac-address - Specifies a MAC address entry. (Format: xx-xx-xxxx-xx-xx)

interface - Specifies a port interface.

ethernet *unit*/*port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-28)

Default Configuration

None

Command Mode

EXEC

Example

Console#clear network-access mac-address-table interface ethernet 1/1

Console#

show network-access

Use this command to display the MAC authentication settings for port interfaces.

Syntax

show network-access [interface *interface*]

interface - Specifies a port interface.

ethernet *unit*/*port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-28)

Default Configuration

Displays the settings for all interfaces.

Command Mode

EXEC

Example

Console#show network-access interface ethernet 1/1

Global secure port information

Reauthentication Time : 1800

MAC Address Aging : Disabled

Port : 1/1

MAC Authentication : Disabled

MAC Authentication Intrusion Action : Block traffic

MAC Authentication Maximum MAC Counts : 1024

Maximum MAC Counts : 1024

Dynamic VLAN Assignment : Enabled

Dynamic QoS Assignment : Disabled

MAC Filter ID : Disabled

Guest VLAN : Disabled

Link Detection : Disabled

Detection Mode : Link-down

Detection Action : Trap

Console#

show network-access mac-address-table

Use this command to display secure MAC address table entries.

Syntax

show network-access mac-address-table [static | dynamic] [address *mac-address* [*mask*]] [interface *interface*] [sort {address | interface}]

static - Specifies static address entries.

dynamic - Specifies dynamic address entries.

mac-address - Specifies a MAC address entry. (Format: xx-xx-xx-xx-xx-xx)

mask - Specifies a MAC address bit mask for filtering displayed addresses.

interface - Specifies a port interface.

ethernet *unit*/*port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-28)

sort - Sorts displayed entries by either MAC address or interface.

Default Configuration

Displays all filters.

Command Mode

EXEC

User Guidelines

When using a bit mask to filter displayed MAC addresses, a 1 means "care" and a 0 means "don't care". For example, a MAC of 00-00-01-02-03-04 and mask FF-FF-FF-00-00-00 would result in all MACs in the range 00-00-01-00-00-00 to 00-00-01-FF-FF-FF to be displayed. All other MACs would be filtered out.

Example

Console#show network-access mac-address-table

---- ----------------- --------------- --------- --------------------------

Port MAC-Address RADIUS-Server Attribute Time

---- ----------------- --------------- --------- --------------------------

1/1 00-00-01-02-03-04 172.155.120.17 Static 00d06h32m50s

1/1 00-00-01-02-03-05 172.155.120.17 Dynamic 00d06h33m20s

1/1 00-00-01-02-03-06 172.155.120.17 Static 00d06h35m10s

1/3 00-00-01-02-03-07 172.155.120.17 Dynamic 00d06h34m20s

Console#

show network-access mac-filter

Use this command to display information for entries in the MAC filter tables.

Syntax

show network-access mac-filter [*filter-id*]

filter-id - Specifies a MAC address filter table. (Range: 1-64)

Default Configuration

Displays all filters.

Command Mode

EXEC

Example

Console#show network-access mac-filter

Filter ID MAC Address MAC Mask

--------- ---------- ----------

1 64-9D-99-02-03-08 FF-FF-FF-FF-FF-FF

Console#

21. Web Authentication

Web authentication allows stations to authenticate and access the network in situations where 802.1X or Network Access authentication are infeasible or impractical. The web authentication feature allows unauthenticated hosts to request and receive a DHCP assigned IP address and perform DNS queries. All other traffic, except for HTTP protocol traffic, is blocked. The switch intercepts HTTP protocol traffic and redirects it to a switch-generated web page that facilitates user name and password authentication via RADIUS. Once authentication is successful, the web browser is forwarded on to the originally requested web page. Successful authentication is valid for all hosts connected to the port.

NOTE: RADIUS authentication must be activated and configured for the web authentication feature to work properly.

NOTE: Web authentication cannot be configured on trunk ports.

web-auth login-attempts

This command defines the limit for failed web authentication login attempts. After the limit is reached, the switch refuses further login attempts until the quiet time expires. Use the no form to restore the default.

Syntax

web-auth login-attempts *count*

no web-auth login-attempts

count - The limit of allowed failed login attempts. (Range: 1-3)

Default Configuration

3 login attempts

Command Mode

Global Configuration

Example

Console(config)#web-auth login-attempts 2

Console(config)#

web-auth quiet-period

This command defines the amount of time a host must wait after exceeding the limit for failed login attempts, before it may attempt web authentication again. Use the no form to restore the default.

Syntax

web-auth quiet-period *time*

no web-auth quiet period

time - The amount of time the host must wait before attempting authentication again. (Range: 1-180 seconds)

Default Configuration

60 seconds

Command Mode

Global Configuration

Example

Console(config)#web-auth quiet-period 120

Console(config)#

web-auth session-timeout

This command defines the amount of time a web-authentication session remains valid. When the session timeout has been reached, the host is logged off and must re-authenticate itself the next time data transmission takes place. Use the no form to restore the default.

Syntax

web-auth session-timeout *timeout*

no web-auth session timeout

timeout - The amount of time that an authenticated session remains valid. (Range: 300-3600 seconds)

Default Configuration

3600 seconds

Command Mode

Global Configuration

Example

Console(config)#web-auth session-timeout 1800

Console(config)#

web-auth system-auth-control

This command globally enables web authentication for the switch. Use the no form to restore the default.

Syntax

[no] web-auth system-auth-control

Default Configuration

Disabled

Command Mode

Global Configuration

User Guidelines

Both web-auth system-auth-control for the switch and web-auth for an interface must be enabled for the web authentication feature to be active.

Example

Console(config)#web-auth system-auth-control

Console(config)#

web-auth

This command enables web authentication for an interface. Use the no form to restore the default.

Syntax

[no] web-auth

Default Configuration

Disabled

Command Mode

Interface Configuration

User Guidelines

Both web-auth system-auth-control for the switch and web-auth for a port must be enabled for the web authentication feature to be active.

Example

Console(config-if)#web-auth

Console(config-if)#

show web-auth

This command displays global web authentication parameters.

Command Mode

EXEC

Example

Console#show web-auth
Global Web-Auth Parameters
System Auth Control : Enabled
Session Timeout : 3600
Quiet Period : 60
Max Login Attempts : 3
Console#

show web-auth interface

This command displays interface-specific web authentication parameters and statistics.

Syntax

show web-auth interface *interface*

interface - Specifies a port interface.

ethernet *unit*/*port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-28)

Command Mode

EXEC

Example

Console#show web-auth interface ethernet 1/2
Web Auth Status: Enabled
Host Summary
IP address Web-Auth-State Remaining-Session-Time
--- --- ---
1.1.1.1 Authenticated 295
1.1.1.2 Authenticated 111
Console#

show web-auth summary

This command displays a summary of web authentication port parameters and statistics.

Command Mode

EXEC

Example

Console#show web-auth summary
Global Web-Auth Parameters
System Auth Control: Enabled
Port Status Authenticated Host Count
---- --- ---
1/ 1 Disabled 0
1/ 2 Enabled 8
1/ 3 Disabled 0
1/ 4 Disabled 0
1/ 5 Disabled 0
..

22. DHCPV4 Snooping

DHCPv4 snooping allows a switch to protect a network from rogue DHCPv4 servers or other devices which send port-related information to a DHCPv4 server. This information can be useful in tracking an IP address back to a physical port. This section describes commands used to configure DHCPv4 snooping.

ip dhcp snooping

This command enables DHCP snooping globally. Use the no form to restore the default setting.

Syntax

[no] ip dhcp snooping

Default Configuration

Disabled

Command Mode

Global Configuration

User Guidelines

- Network traffic may be disrupted when malicious DHCP messages are received from an outside source. DHCP snooping is used to filter DHCP messages received on an unsecure interface from outside the network or fire wall. When DHCP snooping is enabled globally by this command, and enabled on a VLAN interface by the ip dhcp snooping vlan command, DHCP messages received on an untrusted interface (as specified by the no ip dhcp snooping trust command) from a device not listed in the DHCP snooping table will be dropped.
- When enabled, DHCP messages entering an untrusted interface are filtered based upon dynamic entries learned via DHCP snooping.
- Table entries are only learned for trusted interfaces. Each entry includes a MAC address, IP address, lease time, VLAN identifier, and port identifier.
- When DHCP snooping is enabled, the rate limit for the number of DHCP messages that can be processed by the switch is 100 packets per second. Any DHCP packets in excess of this limit are dropped.
- Filtering rules are implemented as follows:

a. If global DHCP snooping is disabled, all DHCP packets are forwarded.

b. If DHCP snooping is enabled globally, and also enabled on the VLAN where the DHCP packet is received, all DHCP packets are forwarded for a *trusted* port. If the received packet is a DHCP ACK message, a dynamic DHCP snooping entry is also added to the binding table.

c. If DHCP snooping is enabled globally, and also enabled on the VLAN where the DHCP packet is received, but the port is *not trusted*, it is processed as follows:

i. If the DHCP packet is a reply packet from a DHCP server (including OFFER, ACK or NAK messages), the packet is dropped.

ii. If the DHCP packet is from a client, such as a DECLINE or RELEASE message, the switch forwards the packet only if the corresponding entry is found in the binding table.

iii. If the DHCP packet is from client, such as a DISCOVER, REQUEST, INFORM, DECLINE or RELEASE message, the packet is forwarded if MAC address verification is disabled (as specified by the ip dhcp snooping verify mac-address command). However, if MAC address verification is enabled, then the packet will only be forwarded if the client's hardware address stored in the DHCP packet is the same as the source MAC address in the Ethernet header.

iv. If the DHCP packet is not a recognizable type, it is dropped.

- If a DHCP packet from a client passes the filtering criteria above, it will only be forwarded to trusted ports in the same VLAN.
- If a DHCP packet is from server is received on a trusted port, it will be forwarded to both trusted and untrusted ports in the same VLAN.

a. If DHCP snooping is globally disabled, all dynamic bindings are removed from the binding table.

b. *Additional considerations when the switch itself is a DHCP client* – The port(s) through which the switch submits a client request to the DHCP server must be configured as trusted (using the ip dhcp snooping trust command). Note that the switch will not add a dynamic entry for itself to the binding table when it receives an ACK message from a DHCP server. Also, when the switch sends out DHCP client packets for itself, no filtering takes place. However, when the switch receives any messages from a DHCP server, any packets received from untrusted ports are dropped.

Example

This example enables DHCP snooping globally for the switch.

Console(config)#ip dhcp snooping

Console(config)#

ip dhcp snooping information option

This command enables the use of DHCP Option 82 information for the switch, and specifies the frame format to use for the remote-id when Option 82 information is generated by the switch. Use the no form without any keywords to disable this function, the no form with the encode no-subtype keyword to enable use of sub-type and sub-length in CID/RID fields, or the no form with the remote-id keyword to set the remote ID to the switch's MAC address encoded in hexadecimal.

Syntax

ip dhcp snooping information option [encode no-subtype] [remote-id {ip-address [encode {ascii | hex}] | mac-address [encode {ascii | hex}] |

string *string*}]

no ip dhcp snooping information option [encode no-subtype] [remote-id [ip-address encode] | [mac-address encode]]

encode no-subtype - Disables use of sub-type and sub-length fields in circuit-ID (CID) and remote-ID (RID) in Option 82 information.

mac-address - Inserts a MAC address in the remote ID sub-option for the DHCP snooping agent (that is, the MAC address of the switch's CPU).

ip-address - Inserts an IP address in the remote ID sub-option for the DHCP snooping agent (that is, the IP address of the management interface).

encode - Indicates encoding in ASCII or hexadecimal.

string - An arbitrary string inserted into the remote identifier field. (Range: 1-32 characters)

Default Configuration

Option 82: Disabled

CID/RID sub-type: Enabled

Remote ID: MAC address (hexadecimal)

Command Mode

Global Configuration

User Guidelines

- DHCP provides a relay mechanism for sending information about the switch and its DHCP clients to the DHCP server. Known as DHCP Option 82, it allows compatible DHCP servers to use the information when assigning IP addresses, or to set other services or policies for clients.
- When the DHCP Snooping Information Option 82 is enabled, the requesting client (or an intermediate relay agent that has used the information fields to describe itself) can be identified in the DHCP request packets forwarded by the switch and in reply packets sent back from the DHCP server.
- When the DHCP Snooping Information Option is enabled, clients can be identified by the switch port to which they are connected rather than just their MAC address. DHCP client-server exchange messages are then forwarded directly between the server and client without having to flood them to the entire VLAN.
- DHCP snooping must be enabled for the DHCP Option 82 information to be inserted into packets. When enabled, the switch will only add/ remove option 82 information in incoming DCHP packets but not relay them. Packets are processed as follows:

a. If an incoming packet is a DHCP request packet with option 82 information, it will modify the option 82 information according to settings specified with ip dhcp snooping information policy command.

b. If an incoming packet is a DHCP request packet without option 82 information, enabling the DHCP snooping information option will add option 82 information to the packet.

c. If an incoming packet is a DHCP reply packet with option 82 information, enabling the DHCP snooping information option will remove option 82 information from the packet.

- DHCP Snooping Information Option 82 and DHCP Relay Information Option 82 cannot both be enabled at the same time.

Example

This example enables the DHCP Snooping Information Option.

Console(config)#ip dhcp snooping information option

Console(config)#

ip dhcp snooping information policy

This command sets the DHCP snooping information option policy for DHCP client packets that include Option 82 information.

Syntax

ip dhcp snooping information policy {drop | keep | replace}

drop - Drops the client's request packet instead of relaying it.

keep - Retains the Option 82 information in the client request, and forwards the packets to trusted ports.

replace - Replaces the Option 82 information circuit-id and remote-id fields in the client's request with information about the relay agent itself, inserts the relay agent's address (when DHCP snooping is enabled), and forwards the packets to trusted ports.

Default Configuration

replace

Command Mode

Global Configuration

User Guidelines

When the switch receives DHCP packets from clients that already include DHCP Option 82 information, the switch can be configured to set the action policy for these packets. The switch can either drop the DHCP packets, keep the existing information, or replace it with the switch's relay information.

Example

Console(config)#ip dhcp snooping information policy drop

Console(config)#

ip dhcp snooping verify mac-address

This command verifies the client's hardware address stored in the DHCP packet against the source MAC address in the Ethernet header. Use the no form to disable this function.

Syntax

[no] ip dhcp binding verify mac-address

Default Configuration

Enabled

Command Mode

Global Configuration

User Guidelines

If MAC address verification is enabled, and the source MAC address in the Ethernet header of the packet is not same as the client's hardware address in the DHCP packet, the packet is dropped.

Example

This example enables MAC address verification.

Console(config)#ip dhcp snooping verify mac-address

Console(config)#

ip dhcp snooping vlan

This command enables DHCP snooping on the specified VLAN. Use the no form to restore the default setting.

Syntax

[no] ip dhcp snooping vlan *vlan-id*

vlan-id - ID of a configured VLAN (Range: 1-4094)

Default Configuration

Disabled

Command Mode

Global Configuration

User Guidelines

- When DHCP snooping enabled globally using the ip dhcp snooping command, and enabled on a VLAN with this command, DHCP packet filtering will be performed on any untrusted ports within the VLAN as specified by the ip dhcp snooping trust command.
- When the DHCP snooping is globally disabled, DHCP snooping can still be configured for specific VLANs, but the changes will not take effect until DHCP snooping is globally re-enabled.
- When DHCP snooping is globally enabled, and then disabled on a VLAN, all dynamic bindings learned for this VLAN are removed from the binding table.

Example

This example enables DHCP snooping for VLAN 1.

Console(config)#ip dhcp snooping vlan 1

Console(config)#

ip dhcp snooping information option circuit-id

This command specifies DHCP Option 82 circuit-id suboption information. Use the no form to use the default settings.

Syntax

ip dhcp snooping information option circuit-id string *string*

no dhcp snooping information option circuit-id

string - An arbitrary string inserted into the circuit identifier field. (Range: 1-32 characters)

Default Configuration

VLAN-Unit-Port

Command Mode

Interface Configuration (Ethernet, Port Channel)

User Guidelines

DHCP provides a relay mechanism for sending information about the switch and its DHCP clients to the DHCP server. DHCP Option 82 allows compatible DHCP servers to use the information when assigning IP addresses, to set other services or policies for clients. For more information of this process, refer to the Command Usage section under the ip dhcp snooping information option command.

Example

This example sets the DHCP Snooping Information circuit-id suboption

string.

Console(config)#interface ethernet 1/1

Console(config-if)#ip dhcp snooping information option circuit-id string mv2

Console(config-if)#

ip dhcp snooping trust

This command configures the specified interface as trusted. Use the no form to restore the default setting.

Syntax

[no] ip dhcp snooping trust

Default Configuration

All interfaces are untrusted

Command Mode

Interface Configuration (Ethernet, Port Channel)

User Guidelines

- A trusted interface is an interface that is configured to receive only messages from within the network. An untrusted interface is an interface that is configured to receive messages from outside the network or fire wall.
- Set all ports connected to DHCP servers within the local network or fire wall to trusted, and all other ports outside the local network or fire wall to untrusted.
- When DHCP snooping is enabled globally using the ip dhcp snooping command, and enabled on a VLAN with ip dhcp snooping vlan command, DHCP packet filtering will be performed on any untrusted ports within the VLAN according to the default status, or as specifically configured for an interface with the no ip dhcp snooping trust command.
- When an untrusted port is changed to a trusted port, all the dynamic DHCP snooping bindings associated with this port are removed.
- *Additional considerations when the switch itself is a DHCP client* – The port(s) through which it submits a client request to the DHCP server must be configured as trusted.

Example

This example sets port 5 to untrusted.

Console(config)#interface ethernet 1/5

Console(config-if)#no ip dhcp snooping trust

Console(config-if)#

clear ip dhcp snooping binding

This command clears DHCP snooping binding table entries from RAM. Use this command without any optional keywords to clear all entries from the binding table.

Syntax

clear ip dhcp snooping binding [*mac-address* vlan *vlan-id*]

mac-address - Specifies a MAC address entry. (Format: xx-xx-xx-xx-xx-xx)

vlan-id - ID of a configured VLAN (Range: 1-4094)

Command Mode

EXEC

Example

Console(config)#clear ip dhcp snooping binding 11-22-33-44-55-66 vlan 1

Console(config)#

clear ip dhcp snooping database flash

This command removes all dynamically learned snooping entries from flash memory.

Command Mode

EXEC

Example

Console(config)#clear ip dhcp snooping database flash

Console(config)#

ip dhcp snooping database flash

This command writes all dynamically learned snooping entries to flash memory.

Command Mode

EXEC

User Guidelines

This command can be used to store the currently learned dynamic DHCP snooping entries to flash memory. These entries will be restored to the snooping table when the switch is reset. However, note that the lease time shown for a dynamic entry that has been restored from flash memory will no longer be valid.

Example

Console(config)#ip dhcp snooping database flash

Console(config)#

show ip dhcp snooping

This command shows the DHCP snooping configuration settings.

Command Mode

EXEC

Example

Console#show ip dhcp snooping

Global DHCP Snooping status: disable

DHCP Snooping Information Option Status: disable

DHCP Snooping Information Policy: replace

DHCP Snooping is configured on the following VLANs:

1

Verify Source Mac-Address: enable

Interface Trusted

---------- ----------

Eth 1/1 No

Eth 1/2 No

Eth 1/3 No

Eth 1/4 No

Eth 1/5 Yes

...

show ip dhcp snooping binding

This command shows the DHCP snooping binding table entries.

Command Mode

EXEC

Example

Console#show ip dhcp snooping binding

MAC Address IP Address Lease(sec) Type VLAN Interface

------------------ --------------- ---------- -------------------- ---- ------

64-9D-99-44-55-66 192.168.0.99 0 Dynamic-DHCPSNP 1 Eth 1/5

Console#

23. DHCPV6 Snooping

DHCPv6 snooping allows a switch to protect a network from rogue DHCPv6 servers or other devices which send port-related information to a DHCPv6 server. This information can be useful in tracking an IP address back to a physical port. This section describes commands used to configure DHCPv6 snooping.

ipv6 dhcp snooping

This command enables DHCPv6 snooping globally. Use the no form to restore the default setting.

Syntax

[no] ipv6 dhcp snooping

Default Configuration

Disabled

Command Mode

Global Configuration

User Guidelines

- Network traffic may be disrupted when malicious DHCPv6 messages are received from an outside source. DHCPv6 snooping is used to filter DHCPv6 messages received on an unsecure interface from outside the network or fire wall. When DHCPv6 snooping is enabled globally by this command, and enabled on a VLAN interface by the ipv6 dhcp snooping vlan command, DHCP messages received on an untrusted interface (as specified by the no ipv6 dhcp snooping trust command) from a device not listed in the DHCPv6 snooping table will be dropped.
- When enabled, DHCPv6 messages entering an untrusted interface are filtered based upon dynamic entries learned via DHCPv6 snooping.
- Table entries are only learned for trusted interfaces. Each entry includes a MAC address, IPv6 address, lease time, binding type, VLAN identifier, and port identifier.
- When DHCPv6 snooping is enabled, the rate limit for the number of DHCPv6 messages that can be processed by the switch is 100 packets per second. Any DHCPv6 packets in excess of this limit are dropped.
- Filtering rules are implemented as follows:

a. If global DHCPv6 snooping is disabled, all DHCPv6 packets are forwarded.

b. If DHCPv6 snooping is enabled globally, and also enabled on the VLAN where the DHCPv6 packet is received, DHCPv6 packets are forwarded for a *trusted* port as described below.

c. If DHCPv6 snooping is enabled globally, and also enabled on the VLAN where the DHCP packet is received, but the port is *not trusted*, DHCP packets are processed according to message type as follows:

DHCP Client Packet

i. Request: Update entry in binding cache, recording client's DHCPv6 Unique Identifier (DUID), server's DUID, Identity Association (IA) type, IA Identifier, and address (4 message exchanges to get IPv6 address), and forward to trusted port.

ii. Solicit: Add new entry in binding cache, recording client's DUID, IA type, IA ID (2 message exchanges to get IPv6 address with rapid commit option, otherwise 4 message exchanges), and forward to trusted port.

iii. Decline: If no matching entry is found in binding cache, drop this packet.

iv. Renew, Rebind, Release, Confirm: If no matching entry is found in binding cache, drop this packet.

v. If the DHCPv6 packet is not a recognizable type, it is dropped.

If a DHCPv6 packet from a client passes the filtering criteria above, it will only be forwarded to trusted ports in the same VLAN.

24. DHCP Server Packet

If a DHCP server packet is received on an *untrusted* port, drop this packet and add a log entry in the system.

If a DHCPv6 Reply packet is received from a server on a *trusted* port, it will be processed in the following manner:

A. Check if IPv6 address in IA option is found in binding table:

If yes, continue to C.

If not, continue to B.

B. Check if IPv6 address in IA option is found in binding cache:

If yes, continue to C.

If not, check failed, and forward packet to trusted port.

C. Check status code in IA option:

If successful, and entry is in binding table, update lease time and forward to original destination.

If successful, and entry is in binding cache, move entry from binding cache to binding table, update lease time and forward to original destination.

Otherwise, remove binding entry. and check failed.

- If a DHCPv6 Relay packet is received, check the relay message option in Relay-Forward or Relay-Reply packet, and process client and server packets as described above.
- If DHCPv6 snooping is globally disabled, all dynamic bindings are removed from the binding table.

Additional considerations when the switch itself is a DHCPv6 client – The port(s) through which the switch submits a client request to the DHCPv6 server must be configured as trusted (using the ipv6 dhcp snooping trust command). Note that the switch will not add a dynamic entry for itself to the binding table when it receives an ACK message from a DHCPv6 server. Also, when the switch sends out DHCPv6 client packets for itself, no filtering takes place. However, when the switch receives any messages from a DHCPv6 server, any packets received from untrusted ports are dropped.

Example

This example enables DHCPv6 snooping globally for the switch.

Console(config)#ipv6 dhcp snooping

Console(config)#

ipv6 dhcp snooping vlan

This command enables DHCPv6 snooping on the specified VLAN. Use the no form to restore the default setting.

Syntax

[no] ipv6 dhcp snooping vlan {*vlan-id* | *vlan-range*}

vlan-id - ID of a configured VLAN (Range: 1-4094)

vlan-range - A consecutive range of VLANs indicated by the use a hyphen, or a random group of VLANs with each entry separated by a comma.

Default Configuration

Disabled

Command Mode

Global Configuration

User Guidelines

- When DHCPv6 snooping enabled globally using the ipv6 dhcp snooping command, and enabled on a VLAN with this command, DHCPv6 packet filtering will be performed on any untrusted ports within the VLAN as specified by the ipv6 dhcp snooping trust command.

- When the DHCPv6 snooping is globally disabled, DHCPv6 snooping can still be configured for specific VLANs, but the changes will not take effect until DHCPv6 snooping is globally re-enabled.
- When DHCPv6 snooping is enabled globally, and then disabled on a VLAN, all dynamic bindings learned for this VLAN are removed from the binding table.

Example

This example enables DHCP6 snooping for VLAN 1.

Console(config)#ipv6 dhcp snooping vlan 1

Console(config)#

ipv6 dhcp snooping max-binding

This command sets the maximum number of entries which can be stored in the binding database for an interface. Use the no form to restore the default setting.

Syntax

ipv6 dhcp snooping max-binding *count*

no ipv6 dhcp snooping max-binding

count - Maximum number of entries. (Range: 1-5)

Default Configuration

5

Command Mode

Interface Configuration (Ethernet, Port Channel)

Example

This example sets the maximum number of binding entries to 1.

Console(config)#interface ethernet 1/1

Console(config-if)#ipv6 dhcp snooping max-binding 1

Console(config-if)#

ipv6 dhcp snooping trust

This command configures the specified interface as trusted. Use the no form to restore the default setting.

Syntax

[no] ipv6 dhcp snooping trust

Default Configuration

All interfaces are untrusted

Command Mode

Interface Configuration (Ethernet, Port Channel)

User Guidelines

- A trusted interface is an interface that is configured to receive only messages from within the network. An untrusted interface is an interface that is configured to receive messages from outside the network or fire wall.
- Set all ports connected to DHCv6 servers within the local network or fire wall to trusted, and all other ports outside the local network or fire wall to untrusted.
- When DHCPv6 snooping is enabled globally using the ipv6 dhcp snooping command, and enabled on a VLAN with ipv6 dhcp snooping vlan command, DHCPv6 packet filtering will be performed on any untrusted ports within the VLAN according to the default status, or as specifically configured for an interface with the no ipv6 dhcp snooping trust command.
- When an untrusted port is changed to a trusted port, all the dynamic DHCPv6 snooping bindings associated with this port are removed.

- *Additional considerations when the switch itself is a DHCPv6 client* – The port(s) through which it submits a client request to the DHCPv6 server must be configured as trusted.

Example

This example sets port 5 to untrusted.

Console(config)#interface ethernet 1/5

Console(config-if)#no ipv6 dhcp snooping trust

Console(config-if)#

clear ipv6 dhcp snooping binding

This command clears DHCPv6 snooping binding table entries from RAM. Use this command without any optional keywords to clear all entries from the binding table.

Syntax

clear ipv6 dhcp snooping binding [*mac-address ipv6-address*]

mac-address - Specifies a MAC address entry. (Format: xx-xx-xx-xx-xx-xx)

ipv6-address - Corresponding IPv6 address. This address must be entered according to RFC 2373 "IPv6 Addressing Architecture", using 8 colon-separated 16-bit hexadecimal values. One double

colon may be used in the address to indicate the appropriate

number of zeros required to fill the undefined fields.

Command Mode

EXEC

Example

Console(config)#clear ipv6 dhcp snooping binding 00-12-cf-01-02-03 2001::1

Console(config)#

clear ipv6 dhcp snooping database flash

This command removes all dynamically learned snooping entries from flash memory.

Command Mode

EXEC

Example

Console(config)#clear ipv6 dhcp snooping database flash

Console(config)#

show ipv6 dhcp snooping

This command shows the DHCPv6 snooping configuration settings.

Command Mode

EXEC

Example

Console#show ipv6 dhcp snooping

Global DHCPv6 Snooping status: disabled

DHCPv6 Snooping is configured on the following VLANs:

1,

Interface Trusted Max-binding Current-binding

--------- --------- ----------- ---------------

Eth 1/1 No 5 0

Eth 1/2 No 5 0

Eth 1/3 No 5 0

Eth 1/4 No 5 0

Eth 1/5 Yes 5 0

...

show ipv6 dhcp snooping binding

This command shows the DHCPv6 snooping binding table entries.

Command Mode

EXEC

Example

Console#show ipv6 dhcp snooping binding

NA - Non-temporary address

TA - Temporary address

---------- ---------- ---- ------- ----

Link-layer Address: 00-13-49-aa-39-26

IPv6 Address Lifetime VLAN Port Type

---------- ---------- ---- ------- ----

2001:b021:1435:5612:ab3c:6792:a452:6712 2591998 1 Eth 1/5 NA

---------- ---------- ---- ------- ----

Link-layer Address: 00-12-cf-01-02-03

IPv6 Address Lifetime VLAN Port Type

---------- ---------- ---- ------- ----

2001:b000::1 2591912 1 Eth 1/3 NA

Console#

show ipv6 dhcp snooping statistics

This command shows statistics for DHCPv6 snooping client, server and relay packets.

Command Mode

EXEC

Example

Console#show ipv6 dhcp snooping statistics

DHCPv6 Snooping Statistics:

Client Packet: Solicit, Request, Confirm, Renew, Rebind,

Decline, Release, Information-request

Server Packet: Advertise, Reply, Reconfigure

Relay Packet: Relay-forward, Relay-reply

State Client Server Relay Total

-------- -------- -------- -------- --------

Received 10 9 0 19

Sent 9 9 0 18

Droped 1 0 0 1

Console#

25. IPv4 Source Guard

IPv4 Source Guard is a security feature that filters IP traffic on network interfaces based on manually configured entries in the IP Source Guard table, or dynamic entries in the DHCP Snooping table when enabled (see "DHCPv4 Snooping"). IP source guard can be used to prevent traffic attacks caused when a host tries to use the IP address of a neighbor to access the network. This section describes commands used to configure IP Source Guard.

ip source-guard binding

This command adds a static address to the source-guard binding table. Use the no form to remove a static entry.

Syntax

ip source-guard binding *mac-address* vlan *vlan-id ip-address* interface ethernet *unit/port*

no ip source-guard binding *mac-address* vlan *vlan-id*

mac-address - A valid unicast MAC address.

vlan-id - ID of a configured VLAN (Range: 1-4094)

ip-address - A valid unicast IP address, including classful types A, B or C.

unit - Unit identifier. (Range: 1-6)

port - Port number. (Range: 1-28/52)

Default Configuration

No configured entries

Command Mode

Global Configuration

User Guidelines

- Table entries include a MAC address, IP address, lease time, entry type (Static-IP-SG-Binding, Dynamic-DHCP-Binding), VLAN identifier, and port identifier.
- All static entries are configured with an infinite lease time, which is indicated with a value of zero by the show ip source-guard command.
- When source guard is enabled, traffic is filtered based upon dynamic entries learned via DHCP snooping, or static addresses configured in the source guard binding table with this command.
- Static bindings are processed as follows:

a. If there is no entry with same VLAN ID and MAC address, a new entry is added to binding table using the type of static IP source guard binding.

b. If there is an entry with same VLAN ID and MAC address, and the type of entry is static IP source guard binding, then the new entry will replace the old one.

c. If there is an entry with same VLAN ID and MAC address, and the type of the entry is dynamic DHCP snooping binding, then the new entry will replace the old one and the entry type will be changed to static IP source guard binding.

Example

This example configures a static source-guard binding on port 5.

Console(config)#ip source-guard binding 11-22-33-44-55-66 vlan 1 192.168.0.99 interface ethernet 1/5

Console(config-if)#

ip source-guard

This command configures the switch to filter inbound traffic based source IP address, or source IP address and corresponding MAC address. Use the no form to disable this function.

Syntax

ip source-guard {sip | sip-mac}

no ip source-guard

sip - Filters traffic based on IP addresses stored in the binding table.

sip-mac - Filters traffic based on IP addresses and corresponding MAC addresses stored in the binding table.

Default Configuration

Disabled

Command Mode

Interface Configuration (Ethernet)

User Guidelines

- Source guard is used to filter traffic on an insecure port which receives messages from outside the network or fire wall, and therefore may be subject to traffic attacks caused by a host trying to use the IP address of a neighbor.
- Setting source guard mode to "sip" or "sip-mac" enables this function on the selected port. Use the "sip" option to check the VLAN ID, source IP address, and port number against all entries in the binding table. Use the "sip-mac" option to check these same parameters, plus the source MAC address. Use the no ip source guard command to disable this function on the selected port.
- When enabled, traffic is filtered based upon dynamic entries learned via DHCP snooping, or static addresses configured in the source guard binding table.
- Table entries include a MAC address, IP address, lease time, entry type (Static-IP-SG-Binding, Dynamic-DHCP-Binding, VLAN identifier, and port identifier.
- Static addresses entered in the source guard binding table with the ip source-guard binding command are automatically configured with an infinite lease time. Dynamic entries learned via DHCP snooping are configured by the DHCP server itself.
- If the IP source guard is enabled, an inbound packet's IP address (sip option) or both its IP address and corresponding MAC address (sip-mac option) will be checked against the binding table. If no matching entry is found, the packet will be dropped.
- Filtering rules are implemented as follows:

a. If DHCP snooping is disabled, IP source guard will check the VLAN ID, source IP address, port number, and source MAC address (for the sip-mac option). If a matching entry is found in the binding table and the entry type is static IP source guard binding, the packet will be forwarded.

b. If the DHCP snooping is enabled, IP source guard will check the VLAN ID, source IP address, port number, and source MAC address (for the sip-mac option). If a matching entry is found in the binding table and the entry type is static IP source guard binding, or dynamic DHCP snooping binding, the packet will be forwarded.

c. If IP source guard if enabled on an interface for which IP source bindings (dynamically learned via DHCP snooping or manually configured) are not yet configured, the switch will drop all IP traffic on that port, except for DHCP packets.

d. Only unicast addresses are accepted for static bindings.

Example

This example enables IP source guard on port 5.

```
Console(config)#interface ethernet 1/5
Console(config-if)#ip source-guard sip
Console(config-if)#
```

ip source-guard max-binding

This command sets the maximum number of entries that can be bound to an interface. Use the no form to restore the default setting.

Syntax

ip source-guard max-binding *number*

no ip source-guard max-binding

number - The maximum number of IP addresses that can be mapped to an interface in the binding table. (Range: 1-5)

Default Configuration

5

Command Mode

Interface Configuration (Ethernet)

User Guidelines

- This command sets the maximum number of address entries that can be mapped to an interface in the binding table, including both dynamic entries discovered by DHCP snooping and static entries set by the ip source-guard command.

Example

This example sets the maximum number of allowed entries in the binding table for port 5 to one entry.

Console(config)#interface ethernet 1/5

Console(config-if)#ip source-guard max-binding 1

Console(config-if)#

ip source-guard mode

This command sets the source-guard learning mode to search for addresses in the

ACL binding table or the MAC address binding table. Use the no form to restore the

default setting.

Syntax

ip source-guard mode {acl | mac}

no ip source-guard mode

mode - Specifies the learning mode.

acl - Searches for addresses in the ACL binding table.

mac - Searches for addresses in the MAC address binding table.

Default Configuration

ACL

Command Mode

Interface Configuration (Ethernet)

User Guidelines

There are two modes for the filtering table:

- ACL - IP traffic will be forwarded if it passes the checking process in the ACL mode binding table.
- MAC - A MAC entry will be added in MAC address table if IP traffic passes the checking process in MAC mode binding table.

Example

This command sets the binding table mode for the specified interface to MAC mode:

Console(config)#interface ethernet 1/5

Console(config-if)#ip source-guard mode mac

Console(config-if)#

clear ip source-guard binding blocked

This command clears source-guard binding table entries from RAM.

Syntax

clear ip source-guard binding blocked

Command Mode

EXEC

User Guidelines

When IP Source-Guard detects an invalid packet it creates a blocked record. These records can be viewed using the show ip source-guard binding blocked command. A maximum of 512 blocked records can be stored before the switch overwrites the oldest record with new blocked records. Use the clear ip source-guard binding blocked command tob clear this table.

Example

This command clears the blocked record table.

Console(config)#clear ip source-guard binding blocked

Console(config)#

show ip source-guard

This command shows whether source guard is enabled or disabled on each interface.

Command Mode

EXEC

Example

Console#show ip source-guard

Interface Filter-type Max-binding

--------- ----------- -----------

Eth 1/1 DISABLED 5

Eth 1/2 DISABLED 5

Eth 1/3 DISABLED 5

Eth 1/4 DISABLED 5

Eth 1/5 SIP 1

Eth 1/6 DISABLED 5

.

show ip source-guard binding

This command shows the source guard binding table.

Syntax

show ip source-guard binding [dhcp-snooping | static]

dhcp-snooping - Shows dynamic entries configured with DHCP Snooping commands.

static - Shows static entries configured with the ip source-guard binding command.

Command Mode

EXEC

Example

Console#show ip source-guard binding

MacAddress IpAddress Lease(sec) Type VLAN Interface

----------------- --------------- ---------- -------------------- ---- --------

11-22-33-44-55-66 192.168.0.99 0 Static 1 Eth 1/5

Console#

26. IPv6 Source Guard

IPv6 Source Guard is a security feature that filters IPv6 traffic on non-routed, Layer 2 network interfaces based on manually configured entries in the IPv6 Source Guard table, or dynamic entries in the Neighbor Discovery Snooping table or DHCPv6 Snooping table when either snooping protocol is enabled. IPv6 source guard can be used to prevent traffic attacks caused when a host tries to use the IPv6 address of a neighbor to access the network. This section describes commands used to configure IPv6 Source Guard.

ipv6 source-guard binding

This command adds a static address to the source-guard binding table. Use the no

form to remove a static entry.

Syntax

ipv6 source-guard binding *mac-address* vlan *vlan-id ipv6-address* interface ethernet *unit/port*

no ipv6 source-guard binding *mac-address* vlan *vlan-id*

mac-address - A valid unicast MAC address.

vlan-id - ID of a configured VLAN (Range: 1-4094)

ipv6-address - Corresponding IPv6 address. This address must be entered according to RFC 2373 "IPv6 Addressing Architecture," using 8 colon-separated

16-bit hexadecimal values. One double colon may be used in the address to indicate the appropriate number of zeros required to fill the undefined fields.

unit - Unit identifier. (Range: 1-6)

port - Port number. (Range: 1-28/52)

Default Configuration

No configured entries

Command Mode

Global Configuration

User Guidelines

- Table entries include an associated MAC address, IPv6 global unicast address, entry type (Static-IPv6-SG-Binding, Dynamic-ND-Snooping, Dynamic-DHCPv6- Snooping), VLAN identifier, and port identifier.
- Traffic filtering is based only on the source IPv6 address, VLAN ID, and port number.
- All static entries are configured with an infinite lease time, which is indicated with a value of zero by the show ipv6 source-guard command.
- When source guard is enabled, traffic is filtered based upon dynamic entries learned via ND snooping, DHCPv6 snooping, or static addresses configured in the source guard binding table with this command.
- Static bindings are processed as follows:

a. If there is no entry with same and MAC address and IPv6 address, a new entry is added to binding table using static IPv6 source guard binding.

b. If there is an entry with same MAC address and IPv6 address, and the type of entry is static IPv6 source guard binding, then the new entry will replace the old one.

c. If there is an entry with same MAC address and IPv6 address, and the type of the entry is either a dynamic ND snooping binding or DHCPv6 snooping binding, then the new entry will replace the old one and the entry type will be changed to static IPv6 source guard binding.

d. Only unicast addresses are accepted for static bindings.

Example

This example configures a static source-guard binding on port 5.

Console(config)#ipv6 source-guard binding 00-ab-11-cd-23-45 vlan 1 2001::1 interface ethernet 1/5

Console(config-if)#

ipv6 source-guard

This command configures the switch to filter inbound traffic based on the source IP address stored in the binding table. Use the no form to disable this function.

Syntax

ipv6 source-guard sip

no ipv6 source-guard

sip - Filters traffic based on IP addresses stored in the binding table.

Default Configuration

Disabled

Command Mode

Interface Configuration (Ethernet)

User Guidelines

- Source guard is used to filter traffic on an insecure port which receives messages from outside the network or fire wall, and therefore may be subject to traffic attacks caused by a host trying to use the IP address of a neighbor.
- This command checks the VLAN ID, IPv6 global unicast source IP address, and port number against all entries in the binding table. Use the no ipv6 source guard command to disable this function on the selected port.
- After IPv6 source guard is enabled on an interface, the switch initially blocks all IPv6 traffic received on that interface, except for ND packets allowed by ND snooping and DHCPv6 packets allowed by DHCPv6 snooping. A port access control list (ACL) is applied to the interface. Traffic is then filtered based upon dynamic entries learned via ND snooping or DHCPv6 snooping, or static addresses configured in the source guard binding table. The port allows only IPv6 traffic with a matching entry in the binding table and denies all other IPv6 traffic.
- Table entries include a MAC address, IPv6 global unicast address, entry type
- (Static-IPv6-SG-Binding, Dynamic-ND-Snooping, Dynamic-DHCPv6-Snooping), VLAN identifier, and port identifier.
- Static addresses entered in the source guard binding table with the ipv6 source-guard binding command are automatically configured with an infinite lease time. Dynamic entries learned via DHCPv6 snooping are configured by the DHCPv6 server itself.
- If IPv6 source guard is enabled, an inbound packet's source IPv6 address will be checked against the binding table. If no matching entry is found, the packet will be dropped.
- Filtering rules are implemented as follows:

a. If ND snooping and DHCPv6 snooping are disabled, IPv6 source guard will check the VLAN ID, source IPv6 address, and port number. If a matching entry is found in the binding table and the entry type is static IPv6 source guard binding, the packet will be forwarded.

b. If ND snooping or DHCPv6 snooping is enabled, IPv6 source guard will check the VLAN ID, source IP address, and port number. If a matching entry is found in the binding table and the entry type is static IPv6 source guard binding, dynamic ND snooping binding, or dynamic DHCPv6 snooping binding, the packet will be forwarded.

c. If IPv6 source guard if enabled on an interface for which IPv6 source bindings (dynamically learned via ND snooping or DHCPv6 snooping, or manually configured) are not yet configured, the switch will drop all IPv6 traffic on that port, except for ND packets and DHCPv6 packets.

d. Only IPv6 global unicast addresses are accepted for static bindings.

Example

This example enables IP source guard on port 5.

Console(config)#interface ethernet 1/5

Console(config-if)#ipv6 source-guard sip

Console(config-if)#

ipv6 source-guard max-binding

This command sets the maximum number of entries that can be bound to an interface. Use the no form to restore the default setting.

Syntax

ipv6 source-guard max-binding *number*

no ipv6 source-guard max-binding

number - The maximum number of IPv6 addresses that can be mapped to an interface in the binding table. (Range: 1-5)

Default Configuration

5

Command Mode

Interface Configuration (Ethernet)

User Guidelines

- This command sets the maximum number of address entries that can be mapped to an interface in the binding table, including both dynamic entries discovered by ND snooping, DHCPv6 snooping, and static entries set by the ipv6 source-guard command.
- IPv6 source guard maximum bindings must be set to a value higher than DHCPv6 snooping maximum bindings and ND snooping maximum bindings.
- If IPv6 source guard, ND snooping, and DHCPv6 snooping are enabled on a port, the dynamic bindings used by ND snooping, DHCPv6 snooping, and IPv6 source guard static bindings cannot exceed the maximum allowed bindings set by the ipv6 source-guard max-binding command. In other words, no new entries will be added to the IPv6 source guard binding table.
- If IPv6 source guard is enabled on a port, and the maximum number of allowed bindings is changed to a lower value, precedence is given to deleting entries learned through DHCPv6 snooping, ND snooping, and then manually configured IPv6 source guard static bindings, until the number of entries in the binding table reaches the newly configured maximum number of allowed bindings.

Example

This example sets the maximum number of allowed entries in the binding table for port 5 to one entry.

Console(config)#interface ethernet 1/5

Console(config-if)#ipv6 source-guard max-binding 1

Console(config-if)#

show ipv6 source-guard

This command shows whether IPv6 source guard is enabled or disabled on each interface.

Command Mode

EXEC

Example

Console#show ipv6 source-guard

Interface Filter-type Max-binding

--------- ----------- -----------

Eth 1/1 DISABLED 5

Eth 1/2 DISABLED 5

Eth 1/3 DISABLED 5

Eth 1/4 DISABLED 5

Eth 1/5 SIP 1

Eth 1/6 DISABLED 5

show ipv6 source-guard binding

This command shows the IPv6 source guard binding table.

Syntax

show ipv6 source-guard binding [dynamic | static]

dynamic - Shows dynamic entries configured with ND Snooping or DHCPv6 Snooping commands

static - Shows static entries configured with the ipv6 source-guard binding command.

Command Mode

EXEC

Example

Console#show ipv6 source-guard binding

MAC Address IPv6 Address VLAN Interface Type

---------- ---------- ---- --------- ----

649D-99CD-2345 2001::1 1 Eth 1/5 STA

Console#

27. ARP Inspection

ARP Inspection validates the MAC-to-IP address bindings in Address Resolution Protocol (ARP) packets. It protects against ARP traffic with invalid address bindings, which forms the basis for certain "man-in-the-middle" attacks. This is accomplished by intercepting all ARP requests and responses and verifying each of these packets before the local ARP cache is updated or the packet is forwarded to the appropriate destination, dropping any invalid ARP packets.

ARP Inspection determines the validity of an ARP packet based on valid IP-to-MAC address bindings stored in a trusted database – the DHCP snooping binding database. ARP Inspection can also validate ARP packets against user-configured ARP access control lists (ACLs) for hosts with statically configured IP addresses.

This section describes commands used to configure ARP Inspection.

ip arp inspection

This command enables ARP Inspection globally on the switch. Use the no form to disable this function.

Syntax

[no] ip arp inspection

Default Configuration

Disabled

Command Mode

Global Configuration

User Guidelines

- When ARP Inspection is enabled globally with this command, it becomes active only on those VLANs where it has been enabled with the ip arp inspection vlan command.
- When ARP Inspection is enabled globally and enabled on selected VLANs, all ARP request and reply packets on those VLANs are redirected to the CPU and their switching is handled by the ARP Inspection engine.
- When ARP Inspection is disabled globally, it becomes inactive for all VLANs, including those where ARP Inspection is enabled.
- When ARP Inspection is disabled, all ARP request and reply packets bypass the ARP Inspection engine and their manner of switching matches that of all other packets.
- Disabling and then re-enabling global ARP Inspection will not affect the ARP Inspection configuration for any VLANs.
- When ARP Inspection is disabled globally, it is still possible to configure ARP Inspection for individual VLANs. These configuration changes will only become active after ARP Inspection is globally enabled again.

Example

Console(config)#ip arp inspection

Console(config)#

ip arp inspection filter

This command specifies an ARP ACL to apply to one or more VLANs. Use the no form to remove an ACL binding.

Syntax

ip arp inspection filter *arp-acl-name* vlan {*vlan-id* | *vlan-range*} [static]

arp-acl-name - Name of an ARP ACL. (Maximum length: 16 characters)

vlan-id - VLAN ID. (Range: 1-4094)

vlan-range - A consecutive range of VLANs indicated by the use a hyphen, or a random group of VLANs with each entry separated by a comma.

static - ARP packets are only validated against the specified ACL, address bindings in the DHCP snooping database is not checked.

Default Configuration

ARP ACLs are not bound to any VLAN

Static mode is not enabled

Command Mode

Global Configuration

User Guidelines

- ARP ACLs are configured with commands.
- If static mode is enabled, the switch compares ARP packets to the specified ARP ACLs. Packets matching an IP-to-MAC address binding in a permit or deny rule are processed accordingly. Packets not matching any of the ACL rules are dropped. Address bindings in the DHCP snooping database are not checked.
- If static mode is not enabled, packets are first validated against the specified ARP ACL. Packets matching a deny rule are dropped. All remaining packets are validated against the address bindings in the DHCP snooping database.

Example

Console(config)#ip arp inspection filter sales vlan 1

Console(config)#

ip arp inspection log-buffer logs

This command sets the maximum number of entries saved in a log message, and the rate at which these messages are sent. Use the no form to restore the default settings.

Syntax

ip arp inspection log-buffer logs *message-number* interval *seconds*

no ip arp inspection log-buffer logs

message-number - The maximum number of entries saved in a log message. (Range: 0-256, where 0 means no events are saved)

seconds - The interval at which log messages are sent. (Range: 0-86400)

Default Configuration

Message Number: 5

Interval: 1 second

Command Mode

Global Configuration

User Guidelines

- ARP Inspection must be enabled with the ip arp inspection command before this command will be accepted by the switch.
- By default, logging is active for ARP Inspection, and cannot be disabled.
- When the switch drops a packet, it places an entry in the log buffer. Each entry contains flow information, such as the receiving VLAN, the port number, the source and destination IP addresses, and the source and destination MAC addresses.
- If multiple, identical invalid ARP packets are received consecutively on the same VLAN, then the logging facility will only generate one entry in the log buffer and one corresponding system message.
- The maximum number of entries that can be stored in the log buffer is determined by the *message-number* parameter. If the log buffer fills up before a message is sent, the oldest entry will be replaced with the newest one.

- The switch generates a system message on a rate-controlled basis determined by the *seconds* values. After the system message is generated, all entries are cleared from the log buffer.

Example

Console(config)#ip arp inspection log-buffer logs 1 interval 10

Console(config)#

ip arp inspection validate

This command specifies additional validation of address components in an ARP packet. Use the no form to restore the default setting.

Syntax

ip arp inspection validate {dst-mac [ip] [src-mac] | ip [src-mac] | src-mac}

no ip arp inspection validate

dst-mac - Checks the destination MAC address in the Ethernet header against the target MAC address in the ARP body. This check is performed for ARP responses. When enabled, packets with different MAC addresses are classified as invalid and are dropped.

ip - Checks the ARP body for invalid and unexpected IP addresses. Addresses include 0.0.0.0, 255.255.255.255, and all IP multicast addresses. Sender IP addresses are checked in all ARP requests and responses, while target IP addresses are checked only in ARP responses.

src-mac - Checks the source MAC address in the Ethernet header against the sender MAC address in the ARP body. This check is performed on both ARP requests and responses. When enabled, packets with different MAC addresses are classified as invalid and are dropped.

Default Configuration

No additional validation is performed

Command Mode

Global Configuration

User Guidelines

By default, ARP Inspection only checks the IP-to-MAC address bindings specified in an ARP ACL or in the DHCP Snooping database.

Example

Console(config)#ip arp inspection validate dst-mac

Console(config)#

ip arp inspection vlan

This command enables ARP Inspection for a specified VLAN or range of VLANs. Use the no form to disable this function.

Syntax

[no] ip arp inspection vlan {*vlan-id* | *vlan-range*}

vlan-id - VLAN ID. (Range: 1-4094)

vlan-range - A consecutive range of VLANs indicated by the use a hyphen, or a random group of VLANs with each entry separated by a comma.

Default Configuration

Disabled on all VLANs

Command Mode

Global Configuration

User Guidelines

- When ARP Inspection is enabled globally with the ip arp inspection command, it becomes active only on those VLANs where it has been enabled with this command.
- When ARP Inspection is enabled globally and enabled on selected VLANs, all ARP request and reply packets on those VLANs are redirected to the CPU and their switching is handled by the ARP Inspection engine.
- When ARP Inspection is disabled globally, it becomes inactive for all VLANs, including those where ARP Inspection is enabled.
- When ARP Inspection is disabled, all ARP request and reply packets bypass the ARP Inspection engine and their manner of switching matches that of all other packets.
- Disabling and then re-enabling global ARP Inspection will not affect the ARP Inspection configuration for any VLANs.
- When ARP Inspection is disabled globally, it is still possible to configure ARP Inspection for individual VLANs. These configuration changes will only become active after ARP Inspection is globally enabled again.

Example

Console(config)#ip arp inspection vlan 1,2

Console(config)#

ip arp inspection limit

This command sets a rate limit for the ARP packets received on a port. Use the no form to restore the default setting.

Syntax

ip arp inspection limit {rate *pps* | none}

no ip arp inspection limit

pps - The maximum number of ARP packets that can be processed by the CPU per second. (Range: 0-2048, where 0 means that no ARP packets can be forwarded)

none - There is no limit on the number of ARP packets that can be processed by the CPU.

Default Configuration

15

Command Mode

Interface Configuration (Port, Static Aggregation)

User Guidelines

- This command applies to both trusted and untrusted ports.
- When the rate of incoming ARP packets exceeds the configured limit, the switch drops all ARP packets in excess of the limit.

Example

Console(config)#interface ethernet 1/1

Console(config-if)#ip arp inspection limit rate 150

Console(config-if)#

ip arp inspection trust

This command sets a port as trusted, and thus exempted from ARP Inspection. Use the no form to restore the default setting.

Syntax

[no] ip arp inspection trust

Default Configuration

Untrusted

Command Mode

Interface Configuration (Port, Static Aggregation)

User Guidelines

Packets arriving on untrusted ports are subject to any configured ARP Inspection and additional validation checks. Packets arriving on trusted ports bypass all of these checks, and are forwarded according to normal switching rules.

Example

Console(config)#interface ethernet 1/1

Console(config-if)#ip arp inspection trust

Console(config-if)#

show ip arp inspection configuration

This command displays the global configuration settings for ARP Inspection.

Command Mode

EXEC

Example

Console#show ip arp inspection configuration

ARP inspection global information:

Global IP ARP Inspection status : disabled

Log Message Interval : 10 s

Log Message Number : 1

Need Additional Validation(s) : Yes

Additional Validation Type : Destination MAC address

Console#

show ip arp inspection interface

This command shows the trust status and ARP Inspection rate limit for ports.

Syntax

show ip arp inspection interface [*interface*]

interface

ethernet *unit*/*port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-28)

Command Mode

EXEC

Example

Console#show ip arp inspection interface ethernet 1/1

Port Number Trust Status Rate Limit (pps)

------------ ---------- ----------

Eth 1/1 Trusted 150

Console#

show ip arp inspection log

This command shows information about entries stored in the log, including the associated VLAN, port, and address components.

Command Mode

EXEC

Example

Console#show ip arp inspection log

Total log entries number is 1

Num VLAN Port Src IP Address Dst IP Address Src MAC Address Dst MAC Address

--- ---- ---- --------------- --------------- ----------------- ---------------

1 1 11 192.168.2.2 192.168.2.1 64-9D-99-A0-E2-7C FF-FF-FF-FF-FF-FF

Console#

show ip arp inspection statistics

This command shows statistics about the number of ARP packets processed, or dropped for various reasons.

Command Mode

EXEC

Example

Console#Console#show ip arp inspection statistics

ARP packets received before rate limit : 150

ARP packets dropped due to rate limt : 5

Total ARP packets processed by ARP Inspection : 150

ARP packets dropped by additional validation (source MAC address) : 0

ARP packets dropped by additional validation (destination MAC address): 0

ARP packets dropped by additional validation (IP address) : 0

ARP packets dropped by ARP ACLs : 0

ARP packets dropped by DHCP snooping : 0

Console#

show ip arp inspection vlan

This command shows the configuration settings for VLANs, including ARP Inspection status, the ARP ACL name, and if the DHCP Snooping database is used after ARP ACL validation is completed.

Syntax

show ip arp inspection vlan [*vlan-id* | *vlan-range*]

vlan-id - VLAN ID. (Range: 1-4094)

vlan-range - A consecutive range of VLANs indicated by the use a hyphen, or a random group of VLANs with each entry separated by a comma.

Command Mode

EXEC

Example

Console#show ip arp inspection vlan 1

VLAN ID DAI Status ACL Name ACL Status

-------- --------------- -------------------- --------------------

1 disabled sales static

Console#

28. DoS Protection

A denial-of-service attack (DoS attack) is an attempt to block the services provided by a computer or network resource. This kind of attack tries to prevent an Internet site or service from functioning efficiently or at all. In general, DoS attacks are implemented by either forcing the target to reset, to consume most of its resources so that it can no longer provide its intended service, or to obstruct the communication media between the intended users and the target so that they can no long communicate adequately.

This section describes commands used to protect against DoS attacks.

dos-protection echo-chargen

This command protects against DoS echo/chargen attacks in which the echo service repeats anything sent to it, and the chargen (character generator) service generates a continuous stream of data. When used together, they create an infinite loop and result in a denial-of-service. Use the no form to disable this feature.

Syntax

dos-protection echo-chargen [bit-rate-in-kilo *rate*]

no dos-protection echo-chargen

rate – Maximum allowed rate. (Range: 64-2000 kbits/second)

Default Configuration

Disabled, 1000 kbits/second

Command Mode

Global Configuration

Example

Console(config)#dos-protection echo-chargen 65

Console(config)#

dos-protection smurf

This command protects against DoS smurf attacks in which a perpetrator generates a large amount of spoofed ICMP Echo Request traffic to the broadcast destination IP address (255.255.255.255), all of which uses a spoofed source address of the intended victim. The victim should crash due to the many interrupts required to send ICMP Echo response packets. Use the no form to disable this feature.

Syntax

[no] dos-protection smurf

Default Configuration

Enabled

Command Mode

Global Configuration

Example

Console(config)#dos-protection smurf

Console(config)#

dos-protection tcp-flooding

This command protects against DoS TCP-flooding attacks in which a perpetrator sends a succession of TCP SYN requests (with or without a spoofed-Source IP) to a target and never returns ACK packets. These half-open connections will bind resources on the target, and no new connections can be made, resulting in a denial of service. Use the no form to disable this feature.

Syntax

dos-protection tcp-flooding [bit-rate-in-kilo *rate*]

no dos-protection tcp-flooding

rate – Maximum allowed rate. (Range: 64-2000 kbits/second)

Default Configuration

Disabled, 1000 kbits/second

Command Mode

Global Configuration

Example

Console(config)#dos-protection tcp-flooding 65

Console(config)#

dos-protection tcp-null-scan

This command protects against DoS TCP-null-scan attacks in which a TCP NULL scan message is used to identify listening TCP ports. The scan uses a series of strangely configured TCP packets which contain a sequence number of 0 and no flags. If the target's TCP port is closed, the target replies with a TCP RST (reset) packet. If the target TCP port is open, it simply discards the TCP NULL scan. Use the no form to disable this feature.

Syntax

[no] dos-protection tcp-null-scan

Default Configuration

Enabled

Command Mode

Global Configuration

Example

Console(config)#dos-protection tcp-null-scan

Console(config)#

dos-protection tcp-syn-fin-scan

This command protects against DoS TCP-SYN/FIN-scan attacks in which a TCP SYN/FIN scan message is used to identify listening TCP ports. The scan uses a series of strangely configured TCP packets which contain SYN (synchronize) and FIN (finish) flags. If the target's TCP port is closed, the target replies with a TCP RST (reset) packet. If the target TCP port is open, it simply discards the TCP SYN FIN scan. Use the no form to disable this feature.

Syntax

[no] dos-protection syn-fin-scan

Default Configuration

Enabled

Command Mode

Global Configuration

Example

Console(config)#dos-protection syn-fin-scan

Console(config)#

dos-protection tcp-xmas-scan

This command protects against DoS TCP-xmas-scan in which a so-called TCP XMAS scan message is used to identify listening TCP ports. This scan uses a series of strangely configured TCP packets which contain a sequence number of 0 and the URG, PSH and FIN flags. If the target's TCP port is closed, the target replies with a TCP RST packet. If the target TCP port is open, it simply discards the TCP XMAS scan. Use the no form to disable this feature.

Syntax

[no] dos-protection tcp-xmas-scan

Default Configuration

Enabled

Command Mode

Global Configuration

Example

Console(config)#dos-protection tcp-xmas-scan

Console(config)#

dos-protection udp-flooding

This command protects against DoS UDP-flooding attacks in which a perpetrator sends a large number of UDP packets (with or without a spoofed-Source IP) to random ports on a remote host. The target will determine that application is listening at that port, and reply with an ICMP Destination Unreachable packet. It will be forced to send many ICMP packets, eventually leading it to be unreachable by other clients. Use the no form to disable this feature.

Syntax

dos-protection udp-flooding [bit-rate-in-kilo *rate*]

no dos-protection udp-flooding

rate – Maximum allowed rate. (Range: 64-2000 kbits/second)

Default Configuration

Disabled, 1000 kbits/second

Command Mode

Global Configuration

Example

Console(config)#dos-protection udp-flooding 65

Console(config)#

dos-protection win-nuke

This command protects against DoS WinNuke attacks in which affected the Microsoft Windows 3.1x/95/NT operating systems. In this type of attack, the perpetrator sends the string of OOB out-of-band (OOB) packets contained a TCP URG flag to the target computer on TCP port 139 (NetBIOS), casing it to lock up and display a "Blue Screen of Death." This did not cause any damage to, or change data on, the computer's hard disk, but any unsaved data would be lost. Microsoft made patches to prevent the WinNuke attack, but the OOB packets still put the service in a tight loop that consumed all available CPU time. Use the no form to disable this feature.

Syntax

dos-protection win-nuke [bit-rate-in-kilo *rate*]

no dos-protection udp-flooding

rate – Maximum allowed rate. (Range: 64-2000 kbits/second)

Default Configuration

Disabled, 1000 kbits/second

Command Mode

Global Configuration

Example

Console(config)#dos-protection win-nuke 65

Console(config)#

show dos-protection

This command shows the configuration settings for the DoS protection commands.

Command Mode

EXEC

Example

Console#show dos-protection

Global DoS Protection:

Echo-Chargen Attack : Disabled, 1000 kilobits per second

Smurf Attack : Enabled

TCP Flooding Attack : Disabled, 1000 kilobits per second

TCP Null Scan : Enabled

TCP SYN/FIN Scan : Enabled

TCP XMAS Scan : Enabled

UDP Flooding Attack : Disabled, 1000 kilobits per second

WinNuke Attack : Disabled, 1000 kilobits per second

Console#

29. ACL Command

Access Control Lists (ACL) provide packet filtering for IPv4 frames (based on address, protocol, Layer 4 protocol port number or TCP control code), IPv6 frames (based on address, DSCP traffic class, or next header type), or any frames (based on MAC address or Ethernet type). To filter packets, first create an access list, add the required rules, and then bind the list to a specific port. This section describes the Access Control List commands.

29.1 IPV4 ACLs

The commands in this section configure ACLs based on IPv4 addresses, TCP/UDP port number, protocol type, and TCP control code. To configure IPv4 ACLs, first create an access list containing the required permit or deny rules, and then bind the access list to one or more ports.

ip access-list

This command adds an IP access list and enters configuration mode for standard or extended IPv4 ACLs. Use the no form to remove the specified

ACL.

Syntax

[no] ip access-list [extended] *acl-name*

extended – Specifies an ACL that filters packets based on the source or destination IP address, and other more specific criteria.

acl-name – Name of the ACL. (Maximum length: 32 characters, no spaces or other special characters)

Default Configuration

None

Command Mode

Global Configuration

User Guidelines

The command without "extended" parameter specifies a standard acl.

- An ACL can contain up to 64 rules.

Example

Console(config)# ip access-list david

Console(config-std-acl)#

permit, deny (Standard)

This command adds a rule to a Standard IPv4 ACL. The rule sets a filter condition for packets emanating from the specified source. Use the no form to remove a rule.

Syntax

{permit | deny} {any | *source bitmask* | host *source*} [time-range *time-range-name*]

no {permit | deny} {any | *source bitmask* | host *source*}

any – Any source IP address.

source – Source IP address.

bitmask – Dotted decimal number representing the address bits to match.

host – Keyword followed by a specific IP address.

time-range-name - Name of the time range. (Range: 1-30 characters)

Default Configuration

None

Command Mode

Standard IPv4 ACL

User Guidelines

- New rules are appended to the end of the list.
- Address bit masks are similar to a subnet mask, containing four integers from 0 to 255, each separated by a period. The binary mask uses 1 bits to indicate "match" and 0 bits to indicate "ignore." The bitmask is bitwise ANDed with the specified source IP address, and then compared with the address for each IP packet entering the port(s) to which this ACL has been assigned.

Example

This example configures one permit rule for the specific address 10.1.1.21 and another rule for the address range 168.92.16.x – 168.92.31.x using a bitmask.

Console(config-std-acl)#permit host 10.1.1.21

Console(config-std-acl)#permit 168.92.16.0 255.255.240.0

Console(config-std-acl)#

permit, deny (Extended)

This command adds a rule to an Extended IPv4 ACL. The rule sets a filter condition for packets with specific source or destination IP addresses, protocol types, source or destination protocol ports, or TCP control codes. Use the no form to remove a rule.

Syntax

{permit | deny} [*protocol-number* | udp] {any | *source address-bitmask* | host *source*} {any | *destination address-bitmask* | host *destination*} [precedence *precedence*] [dscp *dscp*] [source-port *sport* [*bitmask*]] [destination-port *dport* [*port-bitmask*]] [time-range *time-range-name*]

no {permit | deny} [*protocol-number* | udp] {any | *source address-bitmask* | host *source*} {any | *destination address-bitmask* | host *destination*} [precedence *precedence*] dscp *dscp*] [source-port *sport* [*bitmask*]] [destination-port *dport* [*port-bitmask*]]

{permit | deny} tcp {any | *source address-bitmask* | host *source*} {any | *destination address-bitmask* | host *destination*} [precedence *precedence*] [dscp *dscp*] [source-port *sport* [*bitmask*]] [destination-port *dport* [*port-bitmask*]] [control-flag *control-flags flag-bitmask*] [time-range *time-range-name*]

no {permit | deny} tcp {any | *source address-bitmask* | host *source*} {any | *destination address-bitmask* | host *destination*} [precedence *precedence*] [dscp *dscp*] [source-port *sport* [*bitmask*]] [destination-port *dport* [*port-bitmask*]] [control-flag *control-flags flag-bitmask*]

protocol-number – A specific protocol number. (Range: 0-255)

source – Source IP address.

destination – Destination IP address.

address-bitmask – Decimal number representing the address bits to match.

host – Keyword followed by a specific IP address.

precedence – IP precedence level. (Range: 0-7)

dscp – DSCP priority level. (Range: 0-63)

sport – Protocol18 source port number. (Range: 0-65535)

dport – Protocol18 destination port number. (Range: 0-65535)

port-bitmask – Decimal number representing the port bits to match. (Range: 0-65535)

control-flags – Decimal number (representing a bit string) that specifies flag bits in byte 14 of the TCP header. (Range: 0-63)

flag-bitmask – Decimal number representing the code bits to match.

time-range-name - Name of the time range. (Range: 1-30 characters)

Default Configuration

None

Command Mode

Extended IPv4 ACL

User Guidelines

- All new rules are appended to the end of the list.
- Address bit masks are similar to a subnet mask, containing four integers from 0 to 255, each separated by a period. The binary mask uses 1 bit to indicate "match" and 0 bits to indicate "ignore." The bit mask is bitwise ANDed with the specified source IP address, and then compared with the address for each IP packet entering the port(s) to which this ACL has been assigned.
- You can specify both Precedence and ToS in the same rule. However, if DSCP is used, then neither Precedence nor ToS can be specified.
- The control-code bitmask is a decimal number (representing an equivalent bit mask) that is applied to the control code. Enter a decimal number, where the equivalent binary bit "1" means to match a bit and "0" means to ignore a bit. The following bits may be specified:

a. 1 (fin) – Finish

b. 2 (syn) – Synchronize

c. 4 (rst) – Reset

d. 8 (psh) – Push

e. 16 (ack) – Acknowledgement

f. 32 (urg) – Urgent pointer

For example, use the code value and mask below to catch packets with the following flags set:

a. SYN flag valid, use "control-code 2 2"

b. Both SYN and ACK valid, use "control-code 18 18"

c. SYN valid and ACK invalid, use "control-code 2 18"

Example

This example accepts any incoming packets if the source address is within subnet 10.7.1.x. For example, if the rule is matched; i.e., the rule (10.7.1.0 & 255.255.255.0) equals the masked address (10.7.1.2 & 255.255.255.0), the packet passes through.

Console(config-ext-acl)#permit 10.7.1.1 255.255.255.0 any

Console(config-ext-acl)#

This allows TCP packets from class C addresses 192.168.1.0 to any destination address when set for destination TCP port 80 (i.e., HTTP).

Console(config-ext-acl)#permit 192.168.1.0 255.255.255.0 any destination-port

80

Console(config-ext-acl)#

This permits all TCP packets from class C addresses 192.168.1.0 with the TCP control code set to "SYN."

Console(config-ext-acl)#permit tcp 192.168.1.0 255.255.255.0 any controlflag 2 2

Console(config-ext-acl)#

ip service-acl

This command binds an IPv4 ACL to a port. Use the no form to remove the port.

Syntax

ip service-acl *acl-name* {in | out} [time-range *time-range-name*] [counter]

no ip service-acl *acl-name* in

acl-name – Name of the ACL. (Maximum length: 16 characters)

in – Indicates that this list applies to ingress packets.

out – Indicates that this list applies to egress packets.

time-range-name - Name of the time range. (Range: 1-30 characters)

counter – Enables counter for ACL statistics.

Default Configuration

None

Command Mode

Interface Configuration (Ethernet)

- If an ACL is already bound to a port and you bind a different ACL to it, the switch will replace the old binding with the new one.

Example

Console(config)#int eth 1/2

Console(config-if)#ip service-acl david in

Console(config-if)#

show interfaces ip access-lists

This command shows the ports assigned to IP ACLs.

Command Mode

EXEC

Example

Console#show interfaces ip access-lists

Interface ethernet 1/2

IP access-list david in

Console#

show ip access-list

This command displays the rules for configured IPv4 ACLs.

Syntax

show ip access-list {standard | extended} [*acl-name*]

standard – Specifies a standard IP ACL.

extended – Specifies an extended IP ACL.

acl-name – Name of the ACL. (Maximum length: 16 characters)

Command Mode

EXEC

Example

Console#show ip access-list standard

IP standard access-list david:

permit host 10.1.1.21

permit 168.92.0.0 255.255.15.0

Console#

29.2 IPV6 ACLs

The commands in this section configure ACLs based on IPv6 addresses, DSCP traffic class, or next header type. To configure IPv6 ACLs, first create an access list containing the required permit or deny rules, and then bind the access list to one or more ports.

ipv6 access-list

This command adds an IP access list and enters configuration mode for standard or extended IPv6 ACLs. Use the no form to remove the specified ACL.

Syntax

[no] ipv6 access-list [extended] *acl-name*

standard – Specifies an ACL that filters packets based on the source IP address.

extended – Specifies an ACL that filters packets based on the destination IP address, and other more specific criteria.

acl-name – Name of the ACL. (Maximum length: 32 characters)

Default Configuration

None

Command Mode

Global Configuration

User Guidelines

The command without "extended" parameter specifies a standard acl

Example

Console(config)#ipv6 access-list david

Console(config-std-ipv6-acl)#

permit, deny (Standard)

This command adds a rule to a Standard IPv6 ACL. The rule sets a filter condition for packets emanating from the specified source. Use the no form to remove a rule.

Syntax

{permit | deny} {any | host *source-ipv6-address* |

source-ipv6-address[*/prefix-length*]} [time-range *time-range-name*]

no {permit | deny} {any | host *source-ipv6-address* |

source-ipv6-address[*/prefix-length*]}

any – Any source IP address.

host – Keyword followed by a specific IP address.

source-ipv6-address - An IPv6 source address or network class. The address must be formatted according to RFC 2373 "IPv6 Addressing Architecture", using 8 colon-separated 16-bit hexadecimal values. One double colon may be used in the address to indicate the appropriate number of zeros required to fill the undefined fields.

prefix-length - A decimal value indicating how many contiguous bits (from the left) of the address comprise the prefix; i.e., the network portion of the address. (Range: 0-128)

time-range-name - Name of the time range. (Range: 1-30 characters)

Default Configuration

None

Command Mode

Standard IPv6 ACL

User Guidelines

New rules are appended to the end of the list.

Example

This example configures one permit rule for the specific address 2009:DB9:2229::79 and another rule for the addresses with the network prefix 2009:DB9:2229:5::/64.

Console(config-std-ipv6-acl)#permit host 2009:DB9:2229::79

Console(config-std-ipv6-acl)#permit 2009:DB9:2229:5::/64

Console(config-std-ipv6-acl)#

permit, deny (Extended)

This command adds a rule to an Extended IPv6 ACL. The rule sets a filter condition for packets with specific destination IP addresses, or next header type. Use the no form to remove a rule.

Syntax

{permit | deny} {any | host *source-ipv6-address* | *source-ipv6-address*[*/prefix-length*]}

{any | *destination-ipv6-address*[*/prefix-length*]} [dscp *dscp*] [next-header *next-header*] [time-range *time-range-name*]

no {permit | deny} {any | host *source-ipv6-address* | *source-ipv6-address*[*/prefix-length*]} [dscp *dscp*] [next-header *next-header*]

any – Any IP address (an abbreviation for the IPv6 prefix ::/0).

host – Keyword followed by a specific source IP address.

source-ipv6-address - An IPv6 source address or network class. The address must be formatted according to RFC 2373 "IPv6 Addressing Architecture," using 8 colon-separated 16-bit hexadecimal values. One double colon may be used in the address to indicate the appropriate number of zeros required to fill the undefined fields.

destination-ipv6-address - An IPv6 destination address or network class. The address must be formatted according to RFC 2373 "IPv6 Addressing Architecture," using 8 colon-separated 16-bit hexadecimal values. One double colon may be used in the address to indicate the appropriate number of zeros required to fill the undefined fields.

prefix-length - A decimal value indicating how many contiguous bits (from the left) of the address comprise the prefix; i.e., the network portion of the address. (Range: 0-128 for source prefix, 0-8 for destination prefix)

dscp – DSCP traffic class. (Range: 0-63)

next-header – Identifies the type of header immediately following the IPv6 header. (Range: 0-255)

time-range-name - Name of the time range. (Range: 1-30 characters)

Default Configuration

None

Command Mode

Extended IPv6 ACL

User Guidelines

- All new rules are appended to the end of the list.
- Optional internet-layer information is encoded in separate headers that may be placed between the IPv6 header and the upper-layer header in a packet. There are a small number of such extension headers, each identified by a distinct Next Header value. IPv6 supports the values defined for the IPv4 Protocol field in RFC 1700, including these commonly used headers:

0: Hop-by-Hop Options (RFC 2460)

6: TCP Upper-layer Header (RFC 1700)

17: UDP Upper-layer Header (RFC 1700)

43: Routing (RFC 2460)

44: Fragment (RFC 2460)

51: Authentication (RFC 2402)

50: Encapsulating Security Payload (RFC 2406)

60: Destination Options (RFC 2460)

Example

This example accepts any incoming packets if the destination address is 2009:DB9:2229::79/8.

Console(config-ext-ipv6-acl)#permit 2009:DB9:2229::79/8

Console(config-ext-ipv6-acl)#

This allows packets to any destination address when the DSCP value is 5.

Console(config-ext-ipv6-acl)#permit any dscp 5

Console(config-ext-ipv6-acl)#

This allows any packets sent to the destination 2009:DB9:2229::79/48 when the next header is 43.

Console(config-ext-ipv6-acl)#permit 2009:DB9:2229::79/48 next-header 43

Console(config-ext-ipv6-acl)#

show ipv6 access-list

This command displays the rules for configured IPv6 ACLs.

Syntax

show ipv6 access-list {standard | extended} [*acl-name*]

standard – Specifies a standard IPv6 ACL.

extended – Specifies an extended IPv6 ACL.

acl-name – Name of the ACL. (Maximum length: 16 characters)

Command Mode

EXEC

Example

Console#show ipv6 access-list standard

IPv6 standard access-list david:

permit host 2009:DB9:2229::79

permit 2009:DB9:2229:5::/64

Console#

ipv6 service-acl

This command binds a port to an IPv6 ACL. Use the no form to remove the port.

Syntax

ipv6 service-acl *acl-name* {in | out} [time-range *time-range-name*] [counter]

no ipv6 service-acl *acl-name* {in | out}

acl-name – Name of the ACL. (Maximum length: 16 characters)

in – Indicates that this list applies to ingress packets.

out – Indicates that this list applies to egress packets.

time-range-name - Name of the time range. (Range: 1-30 characters)

counter – Enables counter for ACL statistics.

Default Configuration

None

Command Mode

Interface Configuration (Ethernet)

User Guidelines

If a port is already bound to an ACL and you bind it to a different ACL, the switch will replace the old binding with the new one.

Example

Console(config)#interface ethernet 1/2

Console(config-if)#ipv6 service-acl standard david in

Console(config-if)#

show interfaces ipv6 access-lists

This command shows the ports assigned to IPv6 ACLs.

Command Mode

EXEC

Example

Console# show interfaces ipv6 access-lists

Interface ethernet 1/2

IPv6 standard access-list david in

Console#

29.3 MAC ACLs

The commands in this section configure ACLs based on hardware addresses, packet format, and Ethernet type. To configure MAC ACLs, first create an access list containing the required permit or deny rules, and then bind the access list to one or more ports.

mac access-list

This command adds a MAC access list and enters MAC ACL configuration mode. Use the no form to remove the specified ACL.

Syntax

[no] mac access-list *acl-name*

acl-name – Name of the ACL. (Maximum length: 16 characters, no spaces or other special characters)

Default Configuration

None

Command Mode

Global Configuration

User Guidelines

- When you create a new ACL or enter configuration mode for an existing ACL, use the permit or deny command to add new rules to the bottom of the list.
- To remove a rule, use the no permit or no deny command followed by the exact text of a previously configured rule.
- An ACL can contain up to 64 rules.

Example

Console(config)#mac access-list jerry

Console(config-mac-acl)#

permit, deny (MAC)

This command adds a rule to a MAC ACL. The rule filters packets matching a specified MAC source or destination address (i.e., physical layer address), or Ethernet protocol type. Use the no form to remove a rule.

Syntax

{permit | deny} {any | host *source* | *source address-bitmask*} {any | host *destination* | *destination address-bitmask*} [vid *vid vid-bitmask*] [ethertype *protocol* [*protocol-bitmask*]] [time-range *time-range-name*]

no {permit | deny} {any | host *source* | *source address-bitmask*} {any | host *destination* | *destination address-bitmask*} [vid *vid vid-bitmask*] [ethertype *protocol* [*protocol-bitmask*]]

NOTE: The default is for Ethernet II packets.

{permit | deny} tagged-eth2 {any | host *source* | *source address-bitmask*} {any | host *destination* | *destination address-bitmask*} [vid *vid vid-bitmask*] [ethertype *protocol* [*protocol-bitmask*]] [time-range *time-range-name*]

no {permit | deny} tagged-eth2 {any | host *source* | *source address-bitmask*}

{any | host *destination* | *destination address-bitmask*} [vid *vid vid-bitmask*] [ethertype *protocol* [*protocol-bitmask*]]

{permit | deny} untagged-eth2 {any | host *source* | *source address-bitmask*}

{any | host *destination* | *destination address-bitmask*} [ethertype *protocol* [*protocol-bitmask*]] [time-range *time-range-name*]

no {permit | deny} untagged-eth2 {any | host *source* | *source address-bitmask*} {any | host *destination* | *destination address-bitmask*} [ethertype *protocol* [*protocol-bitmask*]]

{permit | deny} tagged-802.3 {any | host *source* | *source address-bitmask*}

{any | host *destination* | *destination address-bitmask*} [vid *vid vid-bitmask*] [time-range *time-range-name*]

no {permit | deny} tagged-802.3 {any | host *source* | *source address-bitmask*}

{any | host *destination* | *destination address-bitmask*} [vid *vid vid-bitmask*]

{permit | deny} untagged-802.3 {any | host *source* | *source address-bitmask*}

{any | host *destination* | *destination address-bitmask*} [time-range *time-range-name*]

no {permit | deny} untagged-802.3 {any | host *source* | *source address-bitmask*} {any | host *destination* | *destination address-bitmask*}

tagged-eth2 – Tagged Ethernet II packets.

untagged-eth2 – Untagged Ethernet II packets.

tagged-802.3 – Tagged Ethernet 802.3 packets.

untagged-802.3 – Untagged Ethernet 802.3 packets.

any – Any MAC source or destination address.

host – A specific MAC address.

source – Source MAC address.

destination – Destination MAC address range with bitmask.

*address-bitmask*19 – Bitmask for MAC address (in hexadecimal format).

vid – VLAN ID. (Range: 1-4094)

*vid-bitmask*19 – VLAN bitmask. (Range: 1-4095)

protocol – A specific Ethernet protocol number. (Range: 600-ffff hex.)

protocol-bitmask – Protocol bitmask. (Range: 600-ffff hex.)

time-range-name - Name of the time range. (Range: 1-30 characters)

Default Configuration

None

Command Mode

MAC ACL

User Guidelines

- New rules are added to the end of the list.
- The ethertype option can only be used to filter Ethernet II formatted packets.
- A detailed listing of Ethernet protocol types can be found in RFC 1060. A few of the more common types include the following:

a. 0800 - IP

b. 0806 - ARP

c. 8137 - IPX

Example

This rule permits packets from any source MAC address to the destination address 64-9D-99-94-34-de where the Ethernet type is 0800.

Console(config-mac-acl)#permit any host 00-e0-29-94-34-de ethertype 0800

Console(config-mac-acl)#

mac service-acl

This command binds a MAC ACL to a port. Use the no form to remove the

port.

Syntax

mac service-acl *acl-name* {in | out} [time-range *time-range-name*] [counter]

acl-name – Name of the ACL. (Maximum length: 16 characters)

in – Indicates that this list applies to ingress packets.

out – Indicates that this list applies to egress packets.

time-range-name - Name of the time range. (Range: 1-30 characters)

counter – Enables counter for ACL statistics.

Default Configuration

None

Command Mode

Interface Configuration (Ethernet)

User Guidelines

If an ACL is already bound to a port and you bind a different ACL to it, the switch will replace the old binding with the new one.

Example

Console(config)#interface ethernet 1/2

Console(config-if)#mac service-acl jerry in

Console(config-if)#

show interfaces mac access-list

This command shows the ports assigned to MAC ACLs.

Command Mode

EXEC

Example

Console# show interfaces mac access-list

Interface ethernet 1/5

MAC access-list M5 in

Console#

show mac access-list

This command displays the rules for configured MAC ACLs.

Syntax

show mac access-list [*acl-name*]

acl-name – Name of the ACL. (Maximum length: 16 characters)

Command Mode

EXEC

Example

Console#show mac access-list

MAC access-list jerry:

permit any 00-e0-29-94-34-de ethertype 0800

Console#

29.4 ARP ACLs

The commands in this section configure ACLs based on the IP or MAC

address contained in ARP request and reply messages. To configure ARP ACLs, first create an access list containing the required permit or deny rules, and then bind the access list to one or more VLANs.

arp access-list

This command adds an ARP access list and enters ARP ACL configuration mode. Use the no form to remove the specified ACL.

Syntax

[no] arp access-list *acl-name*

acl-name – Name of the ACL. (Maximum length: 16 characters)

Default Configuration

None

Command Mode

Global Configuration

User Guidelines

- When you create a new ACL or enter configuration mode for an existing ACL, use the permit or deny command to add new rules to the bottom of the list. To create an ACL, you must add at least one rule to the list.
- To remove a rule, use the no permit or no deny command followed by the exact text of a previously configured rule.
- An ACL can contain up to 128 rules.

Example

Console(config)#arp access-list factory

Console(config-arp-acl)#

permit, deny (ARP)

This command adds a rule to an ARP ACL. The rule filters packets matching a specified source or destination address in ARP messages. Use the no form to remove a rule.

Syntax

[no] {permit | deny} ip {any | host *source-ip* | *source-ip ip-address-bitmask*}

mac {any | host *source-mac* | *source-mac mac-address-bitmask*} [log]

This form indicates either request or response packets.

[no] {permit | deny} request ip {any | host *source-ip* | *source-ip ip-address-bitmask*} mac {any | host *source-mac* | *source-mac mac-address-bitmask*} [log]

[no] {permit | deny} response ip {any | host *source-ip* | *source-ip ip-address-bitmask*} {any | host *destination-ip* | *destination-ip ip-address-bitmask*} mac {any | host *source-mac* | *source-mac mac-address-bitmask*} [any | host *destination-mac* | *destination-mac mac-addressbitmask*] [log]

source-ip – Source IP address.

destination-ip – Destination IP address with bitmask.

ip-address-bitmask – IPv4 number representing the address bits to match.

source-mac – Source MAC address.

destination-mac – Destination MAC address range with bitmask.

*mac-address-bitmask*20 – Bitmask for MAC address (in hexadecimal format).

log - Logs a packet when it matches the access control entry.

Default Configuration

None

Command Mode

ARP ACL

User Guidelines

New rules are added to the end of the list.

Example

This rule permits packets from any source IP and MAC address to the destination subnet address 192.168.0.0.

Console(config-arp-acl)#$permit response ip any 192.168.0.0 255.255.0.0 mac any any

Console(config-mac-acl)#

show arp access-list

This command displays the rules for configured ARP ACLs.

Syntax

show arp access-list [*acl-name*]

acl-name – Name of the ACL. (Maximum length: 16 characters)

Command Mode

EXEC

Example

Console#show arp access-list

ARP access-list factory:

permit response ip any 192.168.0.0 255.255.0.0 mac any any

Console#

29.5 ACL Information

This section describes commands used to display ACL information.

clear access-list counters

This command clears the hit counter for the rules in all ACLs, or for the rules in a specified ACL.

Syntax

clear access-list counters [*acl-name*]

acl-name – Name of the ACL. (Maximum length: 16 characters)

Command Mode

EXEC

Example

Console#clear access-list counters

Console#

show access-group

This command shows the port assignments of ACLs.

Command Mode

EXECutive

Example

Console#show access-group

Interface ethernet 1/2

IP access-list david

MAC access-list jerry

Console#

show access-list

This command shows all ACLs and associated rules.

Syntax

show access-list [[arp [*acl-name*]] | [ip [extended [*acl-name*] | standard [*acl-name*]] | [ipv6 [extended [*acl-name*] | standard [*acl-name*]] | [mac [*acl-name*]] | [tcam-utilization] | [hardware counters]]

arp – Shows ingress or egress rules for ARP ACLs.

hardware counters – Shows statistics for all ACLs.21

ip extended – Shows ingress or egress rules for Extended IPv4 ACLs.

ip standard – Shows ingress or egress rules for Standard IPv4 ACLs.

ipv6 extended – Shows ingress or egress rules for Extended IPv6 ACLs.

ipv6 standard – Shows ingress or egress rules for Standard IPv6 ACLs.

mac – Shows ingress or egress rules for MAC ACLs.

tcam-utilization – Shows the percentage of user configured ACL rules as a percentage of total ACL rules

acl-name – Name of the ACL. (Maximum length: 16 characters)

Command Mode

EXEC

Example

Console#show access-list

IP standard access-list david:

permit host 10.1.1.21

permit 168.92.0.0 255.255.15.0

IP extended access-list bob:

permit 10.7.1.1 255.255.255.0 any

permit 192.168.1.0 255.255.255.0 any destination-port 80 80

permit 192.168.1.0 255.255.255.0 any protocol tcp control-code 2 2

MAC access-list jerry:

permit any host 00-30-29-94-34-de ethertype 800 800

IP extended access-list A6:

deny tcp any any control-flag 2 2

permit any any

Console#

30. Interface Commands

These commands are used to display or set communication parameters for an Ethernet port, aggregated link, or VLAN; or perform cable diagnostics on the specified interface.

30.1 Interface Configuration

Interface

This command configures an interface type and enters interface configuration mode. Use the no form with a trunk to remove an inactive interface.

Syntax

[no] interface *interface*

interface

ethernet *unit*/*port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-28)

port-channel *channel-id* (Range: 1-12)

vlan *vlan-id* (Range: 1-4094)

Default Configuration

None

Command Mode

Global Configuration

Example

To specify port 4, enter the following command:

Console(config)#interface ethernet 1/4

Console(config-if)#

capabilities

This command advertises the port capabilities of a given interface during auto-negotiation. Use the no form with parameters to remove an advertised capability, or the no form without parameters to restore the default values.

Syntax

[no] capabilities {1000full | 100full | 100half | 10full | 10half | flowcontrol | symmetric}

1000full - Supports 1 Gbps full-duplex operation

100full - Supports 100 Mbps full-duplex operation

100half - Supports 100 Mbps half-duplex operation

10full - Supports 10 Mbps full-duplex operation

10half - Supports 10 Mbps half-duplex operation

flowcontrol - Supports flow control

symmetric - When specified, the port transmits and receives symmetric pause frames.

Default Configuration

1000BASE-T: 10half, 10full, 100half, 100full, 1000full

1000BASE-SX/LX/ZX (SFP+): 1000full

10GBASE-SR/LR/ER (SFP+): 10Gfull

Command Mode

Interface Configuration (Ethernet, Port Channel)

User Guidelines

- 10GBASE-SFP+ connections are fixed at 10G, full duplex. When auto-negotiation is enabled, the only attributes which can be advertised include flow control and symmetric pause frames.
- The 1000BASE-T standard does not support forced mode. Auto-negotiation should always be used to establish a connection over any 1000BASE-T port or trunk.
- When auto-negotiation is enabled with the negotiation command, the switch will negotiate the best settings for a link based on the capabilities command. When auto-negotiation is disabled, you must manually specify the link attributes with the speed-duplex and flowcontrol commands.

Example

The following example configures Ethernet port 5 capabilities to include 100half and 100full.

```
Console(config)#interface ethernet 1/5
Console(config-if)#capabilities 100half
Console(config-if)#capabilities 100full
Console(config-if)#capabilities flowcontrol
Console(config-if)#
```

description

This command adds a description to an interface. Use the no form to remove the description.

Syntax

description *string*

no description

string - Comment or a description to help you remember what is attached to this interface. (Range: 1-64 characters)

Default Configuration

None

Command Mode

Interface Configuration (Ethernet, Port Channel)

User Guidelines

The description is displayed by the show interfaces status command and in the running-configuration file. An example of the value which a network manager might store in this object is the name of the manufacturer, and the product name.

Example

The following example adds a description to port 4.

```
Console(config)#interface ethernet 1/4
Console(config-if)#description RD-SW#3
Console(config-if)#
```

flowcontrol

This command enables flow control. Use the no form to disable flow control.

Syntax

[no] flowcontrol

Default Configuration

Disabled

Command Mode

Interface Configuration (Ethernet, Port Channel)

User Guidelines

- 1000BASE-T does not support forced mode. Auto-negotiation should always be used to establish a connection over any 1000BASE-T port or trunk.
- Flow control can eliminate frame loss by "blocking" traffic from end stations or segments connected directly to the switch when its buffers fill. When enabled, back pressure is used for half-duplex operation and IEEE 802.3-2002 (formally IEEE 802.3x) for full-duplex operation.
- To force flow control on or off (with the flowcontrol or no flowcontrol command), use the no negotiation command to disable auto-negotiation on the selected interface.
- When using the negotiation command to enable auto-negotiation, the optimal settings will be determined by the capabilities command. To enable flow control under auto-negotiation, "flowcontrol" must be included in the capabilities list for any port.

Example

The following example enables flow control on port 5.

Console(config)#interface ethernet 1/5

Console(config-if)#flowcontrol

Console(config-if)#no negotiation

Console(config-if)#

negotiation

This command enables auto-negotiation for a given interface. Use the no form to disable auto-negotiation.

Syntax

[no] negotiation

Default Configuration

Enabled

Command Mode

Interface Configuration (Ethernet, Port Channel)

User Guidelines

- 1000BASE-T does not support forced mode. Auto-negotiation should always be used to establish a connection over any 1000BASE-T port or trunk.
- When auto-negotiation is enabled the switch will negotiate the best settings for a link based on the capabilities command. When auto-negotiation is disabled, you must manually specify the link attributes with the speed-duplex and flowcontrol commands.
- If auto-negotiation is disabled, auto-MDI/MDI-X pin signal configuration will also be disabled for the RJ-45 ports.

Example

The following example configures port 10 to use auto-negotiation.

Console(config)#interface ethernet 1/10

Console(config-if)#negotiation

Console(config-if)#

shutdown

This command disables an interface. To restart a disabled interface, use the no form.

Syntax

[no] shutdown

Default Configuration

All interfaces are enabled.

Command Mode

Interface Configuration (Ethernet, Port Channel)

User Guidelines

This command allows you to disable a port due to abnormal behavior (e.g., excessive collisions), and then re-enable it after the problem has been resolved. You may also want to disable a port for security reasons.

Example

The following example disables port 5.

Console(config)#interface ethernet 1/5

Console(config-if)#shutdown

Console(config-if)#

speed-duplex

This command configures the speed and duplex mode of a given interface when auto-negotiation is disabled. Use the no form to restore the default.

Syntax

speed-duplex {1000full | 100full | 100half | 10full | 10half}

no speed-duplex

1000full - Forces 1000 Mbps full-duplex operation

100full - Forces 100 Mbps full-duplex operation

100half - Forces 100 Mbps half-duplex operation

10full - Forces 10 Mbps full-duplex operation

10half - Forces 10 Mbps half-duplex operation

Default Configuration

- Auto-negotiation is enabled by default.
- When auto-negotiation is disabled, the default speed-duplex setting is 100full for 1000BASE-T ports

Command Mode

Interface Configuration (Ethernet, Port Channel)

User Guidelines

- The 1000BASE-T standard does not support forced mode. Auto-negotiation should always be used to establish a connection over any 1000BASE-T port or trunk. If not used, the success of the link process cannot be guaranteed when connecting to other types of switches.
- To force operation to the speed and duplex mode specified in a speed-duplex command, use the no negotiation command to disable auto-negotiation on the selected interface.
- When using the negotiation command to enable auto-negotiation, the optimal settings will be determined by the capabilities command. To set the speed/duplex mode under auto-negotiation, the required mode must be specified in the capabilities list for an interface.

Example

The following example configures port 5 to 100 Mbps, half-duplex

operation.

Console(config)#interface ethernet 1/5

Console(config-if)#speed-duplex 100half

Console(config-if)#no negotiation

Console(config-if)#

switchport packet-rate

This command configures broadcast, multicast and unknown unicast storm control. Use the no form to restore the default setting.

Syntax

switchport {broadcast | multicast | unicast} packet-rate *rate*

no switchport {broadcast | multicast | unicast}

broadcast - Specifies storm control for broadcast traffic.

multicast - Specifies storm control for multicast traffic.

unicast - Specifies storm control for unknown unicast traffic.

rate - Threshold level in Kilobits per second. (Range: Range: 64-10,000,000 Kbps; Default: 64 Kbps)

Default Configuration

Broadcast Storm Control: Enabled, packet-rate limit: 64 kbps

Multicast Storm Control: Disabled

Unknown Unicast Storm Control: Disabled

Command Mode

Interface Configuration (Ethernet)

User Guidelines

- When traffic exceeds the threshold specified for broadcast and multicast or unknown unicast traffic, packets exceeding the threshold are dropped until the rate falls back down beneath the threshold.
- Using both rate limiting and storm control on the same interface may lead to unexpected results. For example, suppose broadcast storm control is set to 500 Kbps by the command "switchport broadcast packet-rate 500," and the rate limit is set to 20000 Kbps by the command "rate-limit input 20000" on a Fast Ethernet port. Since 20000 Kbps is 1/5 of line speed (100 Mbps), the received rate will actually be 100 Kbps, or 1/5 of the 500 Kbps limit set by the storm control command. It is therefore not advisable to use both of these commands on the same interface.

Example

The following shows how to configure broadcast storm control at 600 kilobits per second:

Console(config)#interface ethernet 1/5

Console(config-if)#switchport broadcast packet-rate 600

Console(config-if)#

clear counters

This command clears statistics on an interface.

Syntax

clear counters *interface*

interface

ethernet *unit*/*port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-28)

port-channel *channel-id* (Range: 1-12)

Default Configuration

None

Command Mode

EXEC

User Guidelines

Statistics are only initialized for a power reset. This command sets the base value for displayed statistics to zero for the current management session. However, if you log out and back into the management interface, the statistics displayed will show the absolute value accumulated since the last power reset.

Example

The following example clears statistics on port 5.

Console#clear counters ethernet 1/5

Console#

show interfaces brief

This command displays a summary of key information, including operational status, native VLAN ID, default priority, speed/duplex mode, and port type for all ports.

Command Mode

EXEC

Example

Console#show interfaces brief

Interface	Type	Admin	Link-Status	Negotiation	Speed/Duplex	Group
Eth 1/ 1	1000BASE-T	Up	Down	Auto		None
Eth 1/ 2	1000BASE-T	Up	Down	Auto		None
Eth 1/ 3	1000BASE-T	Up	Down	Auto		None
Eth 1/ 4	1000BASE-T	Up	Down	Auto		None
Eth 1/ 5	1000BASE-T	Up	Down	Auto		None
Eth 1/ 6	1000BASE-T	Up	Down	Auto		None
Eth 1/ 7	1000BASE-T	Up	Down	Auto		None
Eth 1/ 8	1000BASE-T	Up	Down	Auto		None

show interfaces counters

This command displays interface statistics.

Syntax

show interfaces counters [*interface*]

interface

ethernet *unit*/*port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-28)

port-channel *channel-id* (Range: 1-12)

Default Configuration

Shows the counters for all interfaces.

Command Mode

Normal Exec, EXEC

User Guidelines

If no interface is specified, information on all interfaces is displayed.

Example

Console#show interfaces counters ethernet 1/1

Ethernet 1/ 1

Item	Counters
Octets Input	0
Octets Output	0

Unicast Input Pkts 0
Unicast Output Pkts 0
Multi-cast Input Pkts 0
Multi-cast Output Pkts 0
Broadcast Input Pkts 0
Broadcast Output Pkts 0
Discard Input Pkts 0
Discard Output Pkts 0
Alignment Errors 0
FCS Errors 0
Single Collision Frames 0
Multiple Collision Frames 0
Deferred Transmissions 0
Late Collisions 0
Excessive Collisions 0
Internal Mac Transmit Errors 0
Internal Mac Receive Errors 0
Frames Too Long 0
Carrier Sense Errors 0
Symbol Errors 0
Pause Frames Input 0
Pause Frames Output 0

Console#
show interfaces status
This command displays the status for an interface.
Syntax
show interfaces status {*interface*}
interface
ethernet *unit*/*port*
unit - Unit identifier. (Range: 1)
port - Port number. (Range: 1-28)
port-channel *channel-id* (Range: 1-12)
vlan *vlan-id* (Range: 1-4094)
Default Configuration
Shows the status for all interfaces.
Command Mode
Normal Exec, EXEC
User Guidelines
If no interface is specified, information on all interfaces is displayed.
Example
Console#show interfaces status ethernet 1/1
Port Type: 1000BASE-T
Link Status: Down

Speed-duplex Status: 1000full
Max Frame Size: 1518 bytes (1522 bytes for tagged frames)
MAC Learning Status: Enabled
Console#

show interfaces configuration

This command displays the configuration of the specified interfaces.

Syntax

show interfaces configuration {*interface*}

interface

ethernet *unit*/*port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-28)

port-channel *channel-id* (Range: 1-12)

Default Configuration

Shows all interfaces.

Command Mode

Normal Exec, EXEC

User Guidelines

If no interface is specified, information on all interfaces is displayed.

Example

This example shows the configuration setting for port 1.

Console#show interfaces configuration ethernet 1/1

Name:
Port Admin: Up
Speed-duplex Capabilities: 10half, 10full, 100half, 100full, 1000full
Nego-Speed-duplex: Auto
Flow Control: Disabled
VLAN Trunking: Disabled
MAC Learning: Enabled
Link-Status Trap: Enabled
Media Type: None
MTU: 1518
Broadcast Threshold: Disabled
Multicast Threshold: Disabled
Unknown Unicast Threshold: Disabled
Broadcast Block: Disabled
Unknown Multicast Block: Disabled
Unknown Unicast Block: Disabled
Ingress Rate Limit: Disabled, 1000000 kbits/second
Egress Rate Limit: Disabled, 1000000 kbits/second
VLAN Mode: Hybrid
Vlan Ingress filtering: Disabled
Native VLAN: 1
GVRP Status: Disabled

VLAN: 1(u)

Forbidden VLAN:

QinQ Status: Disabled

QinQ Mode: Normal

QinQ TPID: 8100 (Hex)

Console#

show transceiver

This command displays identifying information for the specified transceiver, including connector type and vendor-related parameters, as well as the temperature, voltage, bias current, transmit power, and receive power.

Syntax

show transceiver [*interface* detail]

interface

ethernet *unit*/*port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: SFP ports 25-28)

Default Configuration

Shows all SFP interfaces.

Command Mode

EXEC

User Guidelines

The switch can display diagnostic information for SFP modules which support the SFF-8472 Specification for Diagnostic Monitoring Interface for Optical Transceivers. This information allows administrators to remotely diagnose problems with optical devices. This feature, referred to as Digital Diagnostic Monitoring (DDM) in the command display, provides information on transceiver parameters including temperature, supply voltage, laser bias current, laser power, and received optical power.

Example

Console#show transceiver ethernet 1/25 detail

30.2 Cable Diagnostics

test cable-diagnostics

This command performs cable diagnostics on the specified port to diagnose any cable faults (short, open, etc.) and report the cable length.

Syntax

test cable-diagnostics interface *interface*

interface

ethernet *unit*/*port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-28)

Command Mode

EXEC

User Guidelines

- Cable diagnostics are performed using Digital Signal Processing (DSP) test methods. DSP analyses the cable by sending a pulsed signal into the cable, and then examining the reflection of that pulse.
- This cable test is only accurate for cables 7 - 140 meters long.

- The test takes approximately 5 seconds. The switch displays the results of the test immediately upon completion, including common cable failures, as well as the status and approximate length of each cable pair.
- Potential conditions which may be listed by the diagnostics include:

a. OK: Correctly terminated pair

b. Open: Open pair, no link partner

c. Short: Shorted pair

d. Not Supported: This message is displayed for any Fast Ethernet ports that are linked up, or for any Gigabit Ethernet ports linked up at a speed lower than 1000 Mbps.

e. Impedance mismatch: Terminating impedance is not in the reference range.

- Ports are linked down while running cable diagnostics.
- To ensure more accurate measurement of the length to a fault, first disable power-saving mode (using the no power-save command) on the link partner before running cable diagnostics.

Example

Console# test cable-diagnostics interface ethernet 1/25

Port Type Link Status Pair A (meters) Pair B (meters) Last Update

-------- ---- ----------- ---------------- ---------------- -----------------

Eth 1/25 GE Up OK (21) OK (21) 2009-11-13 09:44:19

Console#

show cable-diagnostics

This command shows the results of a cable diagnostics test.

Syntax

show cable-diagnostics interface [*interface*]

interface

ethernet *unit*/*port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-28)

Command Mode

EXEC

User Guidelines

- The results include common cable failures, as well as the status and approximate distance to a fault, or the approximate cable length if no fault is found.
- To ensure more accurate measurement of the length to a fault, first disable power-saving mode on the link partner before running cable diagnostics.
- For link-down ports, the reported distance to a fault is accurate to within +/- 2 meters. For link-up ports, the accuracy is +/- 10 meters.

Example

Console# show cable-diagnostics interface ethernet 1/26

Port Type Link Status Pair A (meters) Pair B (meters) Last Update

-------- ---- ----------- ---------------- ---------------- -----------------

Eth 1/26 GE Up OK (21) OK (21) 2009-11-13 09:44:19

Console#

30.3 Power Savings

power-save

This command enables power savings mode on the specified port.

Syntax

[no] power-save

Command Mode

Interface Configuration (Ethernet)

User Guidelines

- IEEE 802.3 defines the Ethernet standard and subsequent power requirements based on cable connections operating at 100 meters. Enabling power saving mode can reduce power used for cable lengths of 60 meters or less, with more significant reduction for cables of 20 meters or less, and continue to ensure signal integrity.
- Power saving mode only applies to the Gigabit Ethernet ports using copper media.
- Power savings can be enabled on Gigabit Ethernet RJ-45 ports.
- The power-saving methods provided by this switch include:

a. Power saving when there is no link partner:

Under normal operation, the switch continuously auto-negotiates to find a link partner, keeping the MAC interface powered up even if no link connection exists. When using power-savings mode, the switch checks for energy on the circuit to determine if there is a link partner. If none is detected, the switch automatically turns off the transmitter, and most of the receive circuitry (enters Sleep Mode). In this mode, the low-power energy-detection circuit continuously checks for energy on the cable. If none is detected, the MAC interface is also powered down to save additional energy. If energy is detected, the switch immediately turns on both the transmitter and receiver functions, and powers up the MAC interface.

b. Power saving when there is a link partner:

Traditional Ethernet connections typically operate with enough power to support at least 100 meters of cable even though average network cable length is shorter. When cable length is shorter, power consumption can be reduced since signal attenuation is proportional to cable length. When power-savings mode is enabled, the switch analyzes cable length to determine whether or not it can reduce the signal amplitude used on a particular link.

Note:

Power-savings mode on a active link only works when the connection speed is 100 Mbps or higher at linkup, and line length is less than 60 meters.

Note:

Power savings can only be implemented on Gigabit Ethernet ports using twisted-pair cabling. Power-savings mode on a active link only works when connection speed is 1 Gbps, and line length is less than 60 meters.

Example

Console(config)#interface ethernet 1/28

Console(config-if)#power-save

Console(config-if)#

show power-save

This command shows the configuration settings for power savings.

Syntax

show power-save [interface *interface*]

interface

ethernet *unit*/*port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-28)

Command Mode

EXEC

Example

Console#show power-save interface ethernet 1/28

Power Saving Status:

Ethernet 1/28: Enabled

Console#

31. Link Aggregation Commands

31.1 Manual Configuration Commands

port channel load-balance

This command sets the load-distribution method among ports in aggregated links (for both static and dynamic trunks). Use the no form to restore the default setting.

Syntax

port channel load-balance {dst-ip | dst-mac | src-dst-ip | src-dst-mac | src-ip | src-mac}

no port channel load-balance

dst-ip - Load balancing based on destination IP address.

dst-mac - Load balancing based on destination MAC address.

src-dst-ip - Load balancing based on source and destination IP address.

src-dst-mac - Load balancing based on source and destination MAC address.

src-ip - Load balancing based on source IP address.

src-mac - Load balancing based on source MAC address.

Default Configuration

src-dst-ip

Command Mode

Global Configuration

User Guidelines

- This command applies to all static and dynamic trunks on the switch.
- To ensure that the switch traffic load is distributed evenly across all links in a trunk, select the source and destination addresses used in the load-balance calculation to provide the best result for trunk connections:

a. dst-ip: All traffic with the same destination IP address is output on the same link in a trunk. This mode works best for switch-to-router trunk links where traffic through the switch is destined for many different hosts. Do not use this mode for switch-to-server trunk links where the destination IP address is the same for all traffic.

b. dst-mac: All traffic with the same destination MAC address is output on the same link in a trunk. This mode works best for switch-to-switch trunk links where traffic through the switch is destined for many different hosts. Do not use this mode for switchto-router trunk links where the destination MAC address is the same for all traffic.

c. src-dst-ip: All traffic with the same source and destination IP address is output on the same link in a trunk. This mode works best for switch-to-router trunk links where traffic through the switch is received from and destined for many different hosts.

d. src-dst-mac: All traffic with the same source and destination MAC address is output on the same link in a trunk. This mode works best for switch-to-switch trunk links where traffic through the switch is received from and destined for many different hosts.

e. src-ip: All traffic with the same source IP address is output on the same link in a trunk. This mode works best for switch-to-router or switch-to-server trunk links where traffic through the switch is received from many different hosts.

f. src-mac: All traffic with the same source MAC address is output on the same link in a trunk. This mode works best for switch-to-switch trunk links where traffic through the switch is received from many different hosts.

Example

Console(config)#port-channel load-balance dst-ip

Console(config)#

channel-group

This command adds a port to a port channel. Use the no form to remove a port from a port channel.

Syntax

channel-group *channel-id* mode *{on | auto}*

no channel-group

channel-id - port channel index (Range: 1-12)

mode - Specifies the mode of joining the port channel. The possible values are:

on - static.

auto - dynamic.

Default Configuration

Static port channel.

Command Mode

Interface Configuration (Ethernet)

User Guidelines

- When configuring static port channel, the switches must comply with the Cisco Ether-Channel standard.
- Use no channel-group to remove a port group from a port channel.
- Use no interface port-channel to remove a port channel from the switch.

Example

The following example creates static port channel 1 and then adds port 10:

Console(config)#interface port-channel 1

Console(config-if)#exit

Console(config)#interface ethernet 1/10

Console(config-if)#channel-group 1 mode on

Console(config-if)#

The following example adds port 10 to dynamic port channel 1(lacp):

Console(config)#interface ethernet 1/10

Console(config-if)#channel-group 1 mode auto

31.2 Dynamic Configuration Commands

lacp max-member-count

This command configures the max member of LACP group. Use the no form to restore the default setting.

Syntax

lacp max-member-count *number*

no lacp max-member-count

max-member-count – the max member of LACP group.

number – the number of max member.

Default Configuration

8

Command Mode

Interface Configuration (port-channel)

User Guidelines

- If more than max member ports are added to the same LACP group, the additional ports will be placed in standby mode, and will only be enabled if one of the active links fails.

Example

Console(config)#interface port-channel 1

Console(config-if)#lacp max-member-count 5

Console(config-if)#

lacp port-priority

This command configures LACP port priority. Use the no form to restore the default setting.

Syntax

lacp port-priority *priority*

no lacp port-priority

priority - LACP port priority is used to select a backup link. (Range: 0-65535)

Default Configuration

32768

Command Mode

Interface Configuration (Ethernet)

User Guidelines

- Setting a lower value indicates a higher effective priority.
- If an active port link goes down, the backup port with the highest priority is selected to replace the downed link. However, if two or more ports have the same LACP port priority, the port with the lowest physical port number will be selected as the backup port.
- If a LAG already exists with the maximum number of allowed port members, and LACP is subsequently enabled on another port using a higher priority than an existing member, the newly configured port will replace an existing port member that has a lower priority.

Example

Console(config)#interface ethernet 1/5

Console(config-if)#lacp port-priority 128

lacp system-priority

This command configures a port's LACP system priority. Use the no form to restore the default setting.

Syntax

lacp system-priority *priority*

no lacp system-priority

priority - This priority is used to determine link aggregation group (LAG) membership, and to identify this device to other switches during LAG negotiations. (Range: 0-65535)

Default Configuration

32768

Command Mode

Interface Configuration (port-channel)

User Guidelines

- Port must be configured with the same system priority to join the same LAG.
- System priority is combined with the switch's MAC address to form the LAG identifier. This identifier is used to indicate a specific LAG during LACP negotiations with other systems.

Example

Console(config)# interface port-channel 1

Console(config-if)#lacp system-priority 3

Console(config-if)#

31.3 Trunk Status Display Commands

show lacp

This command displays LACP information.

Syntax

show lacp [counters]

counters - Statistics for LACP protocol messages.

Default Configuration

Port Channel: all

Command Mode

EXEC

Example

Console#show lacp counters

Port Channel: 1

Eth 1/ 2

LACPDUs Sent: 12

LACPDUs Received: 6

Marker Sent: 0

Marker Received: 0

LACPDUs Unknown Pkts: 0

LACPDUs Illegal Pkts: 0

...

show port-channel load-balance

This command shows the load-distribution method used on aggregated links.

Command Mode

EXEC

Example

Console#show port-channel load-balance

Trunk Load Balance Mode: Destination IP address

Console#

32. Port Mirroring Commands

32.1 Local Port Mirroring Commands

This section describes how to mirror traffic from a source port to a target port.

port monitor

This command configures a mirror session. Use the no form to clear a mirror session.

Syntax

port monitor {*interface* [rx | tx | both] | vlan *vlan-id* |

mac-address *mac-address* | access-list *acl-name*}

no port monitor {*interface* | vlan *vlan-id* |

mac-address *mac-address* | access-list *acl-name*}

interface - ethernet *unit*/*port* (source port)

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-28)

rx - Mirror received packets.

tx - Mirror transmitted packets.

both - Mirror both received and transmitted packets.

vlan-id - VLAN ID (Range: 1-4094)

mac-address - MAC address in the form of xx-xx-xx-xx-xx-xx or xxxxxxxxxxxx.

acl-name – Name of the ACL. (Maximum length: 16 characters, no spaces or other special characters)

Default Configuration

- No mirror session is defined.
- When enabled for an interface, default mirroring is for both received and transmitted packets.
- When enabled for a VLAN or a MAC address, mirroring is restricted to received packets.

Command Mode

Interface Configuration (Ethernet, destination port)

User Guidelines

- You can mirror traffic from any source port to a destination port for real-time analysis. You can then attach a logic analyzer or RMON probe to the destination port and study the traffic crossing the source port in a completely unobtrusive manner.
- Set the destination port by specifying an Ethernet interface with the interface configuration command, and then use the port monitor command to specify the source of the traffic to mirror.
- When mirroring traffic from a port, the mirror port and monitor port speeds should match, otherwise traffic may be dropped from the monitor port. When mirroring traffic from a VLAN, traffic may also be dropped under heavy loads.
- When VLAN mirroring and port mirroring are both enabled, the target port can receive a mirrored packet twice; once from the source mirror port and again from the source mirror VLAN.
- When mirroring traffic from a MAC address, ingress traffic with the specified source address entering any port in the switch, other than the target port, will be mirrored to the destination port.
- Note that Spanning Tree BPDU packets are not mirrored to the target port.
- When mirroring VLAN traffic or packets based on a source MAC address, the target port cannot be set to the same target port as that used for basic port mirroring.

- You can create multiple mirror sessions, but all sessions must share the same destination port.
- The destination port cannot be a trunk or trunk member port.
- ACL-based mirroring is only used for ingress traffic. To mirror an ACL, follow these steps:

(1) Use the access-list command to add an ACL.

(2) Use the access-group command to add a mirrored port to access control list.

(3) Use the port monitor access-list command to specify the destination port to which traffic matching the ACL will be mirrored.

Example

The following example configures the switch to mirror all packets from port

6 to 5:

Console(config)#interface ethernet 1/5

Console(config-if)#port monitor ethernet 1/6 both

Console(config-if)#

show port monitor

This command displays mirror information.

Syntax

show port monitor [*interface* | vlan *vlan-id* |

mac-address *mac-address*]

interface - ethernet *unit*/*port* (source port)

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-28)

vlan-id - VLAN ID (Range: 1-4094)

mac-address - MAC address in the form of xx-xx-xx-xx-xx-xx or xxxxxxxxxxxx.

Default Configuration

Shows all sessions.

Command Mode

EXEC

User Guidelines

This command displays the currently configured source port, destination port, and mirror mode (i.e., RX, TX, RX/TX).

Example

The following shows mirroring configured from port 6 to port 5:

Console(config)#interface ethernet 1/5

Console(config-if)#port monitor ethernet 1/6

Console(config-if)#end

Console#show port monitor

Port Mirroring

Destination Port (listen port): Eth1/5

Source Port (monitored port): Eth1/6

Mode: RX/TX

Console#

32.2 Rspan Mirroring Commands

rspan source

Use this command to specify the source port and traffic type to be mirrored remotely. Use the no form to disable RSPAN on the specified port, or with a traffic type keyword to disable mirroring for the specified type.

Syntax

[no] rspan session *session-id* source interface *interface-list* [rx | tx | both]

session-id – A number identifying this RSPAN session. (Range: 1)

Only two mirror sessions are allowed, including both local and remote mirroring. If local mirroring is enabled with the port monitor command, then there is only one session available for RSPAN.

interface-list – One or more source ports. Use a hyphen to indicate a consecutive list of ports or a comma between non-consecutive ports.

ethernet *unit*/*port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-28)

rx - Mirror received packets.

tx - Mirror transmitted packets.

both - Mirror both received and transmitted packets.

Default Configuration

Both TX and RX traffic is mirrored

Command Mode

Global Configuration

User Guidelines

- One or more source ports can be assigned to the same RSPAN session, either on the same switch or on different switches.
- Only ports can be configured as an RSPAN source – static and dynamic trunks are not allowed.
- The source port and destination port cannot be configured on the same switch.

Example

The following example configures the switch to mirror received packets

from port 2 and 3:

Console(config)#rspan session 1 source interface ethernet 1/2

Console(config)#rspan session 1 source interface ethernet 1/3

Console(config)#

rspan destination

Use this command to specify the destination port to monitor the mirrored traffic. Use the no form to disable RSPAN on the specified port.

Syntax

rspan session *session-id* destination interface *interface* [tagged | untagged]

no rspan session *session-id* destination interface *interface*

session-id – A number identifying this RSPAN session. (Range: 1)

Only two mirror sessions are allowed, including both local and remote mirroring. If local mirroring is enabled with the port monitor command, then there is only one session available for RSPAN.

interface - ethernet *unit*/*port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-28)

tagged - Traffic exiting the destination port carries the RSPAN VLAN tag.

untagged - Traffic exiting the destination port is untagged.

Default Configuration

Traffic exiting the destination port is untagged.

Command Mode

Global Configuration

User Guidelines

- Only one destination port can be configured on the same switch per session, but a destination port can be configured on more than one switch for the same session.
- Only 802.1Q trunk or hybrid (i.e., general use) ports can be configured as an RSPAN destination port – access ports are not allowed (see switchport mode).
- Only ports can be configured as an RSPAN destination – static and dynamic trunks are not allowed.
- The source port and destination port cannot be configured on the same switch.
- A destination port can still send and receive switched traffic, and participate in any Layer 2 protocols to which it has been assigned.

Example

The following example configures port 4 to receive mirrored RSPAN traffic:

Console(config)#rspan session 1 destination interface ethernet 1/2

Console(config)#

rspan remote vlan

Use this command to specify the RSPAN VLAN, switch role (source, intermediate or destination), and the uplink ports. Use the no form to disable the RSPAN on the specified VLAN.

Syntax

[no] rspan session *session-id* remote vlan *vlan-id*

{source | intermediate | destination} uplink *interface*

session-id – A number identifying this RSPAN session. (Range: 1)

Only two mirror sessions are allowed, including both local and remote mirroring. If local mirroring is enabled with the port monitor command, then there is only one session available for RSPAN.

vlan-id - ID of configured RSPAN VLAN. (Range: 2-4092) Use the vlan rspan command to reserve a VLAN for RSPAN mirroring before enabling RSPAN with this command.

source - Specifies this device as the source of remotely mirrored traffic.

intermediate - Specifies this device as an intermediate switch, transparently passing mirrored traffic from one or more sources to one or more destinations.

destination - Specifies this device as a switch configured with a destination port which is to receive mirrored traffic for this session.

uplink - A port configured to receive or transmit remotely mirrored traffic.

interface - ethernet *unit*/*port*

ethernet *unit*/*port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-28)

Default Configuration

None

Command Mode

Global Configuration

User Guidelines

- Only 802.1Q trunk or hybrid (i.e., general use) ports can be configured as an RSPAN uplink port – access ports are not allowed (see switchport mode).
- Only one uplink port can be configured on a source switch, but there is no limitation on the number of uplink ports configured on an intermediate or destination switch.
- Only destination and uplink ports will be assigned by the switch as members of this VLAN. Ports cannot be manually assigned to an RSPAN VLAN with the switchport allowed vlan command. Nor can GVRP dynamically add port members to an RSPAN VLAN. Also, note that the show vlan command will not display any members for an RSPAN VLAN, but will only show configured RSPAN VLAN identifiers.

Example

The following example enables RSPAN on VLAN 2, specifies this device as an RSPAN destination switch, and the uplink interface as port 3:

Console(config)#rspan session 1 remote vlan 2 destination uplink ethernet 1/3

Console(config)#

no rspan session

Use this command to delete a configured RSPAN session.

Syntax

no rspan session *session-id*

session-id – A number identifying this RSPAN session. (Range: 1)

Only two mirror sessions are allowed, including both local and remote mirroring. If local mirroring is enabled with the port monitor command, then there is only one session available for RSPAN.

Command Mode

Global Configuration

User Guidelines

The no rspan session command must be used to disable an RSPAN VLAN before it can be deleted from the VLAN database (see the vlan command).

Example

Console(config)#no rspan session 1

Console(config)#

show rspan

Use this command to displays the configuration settings for an RSPAN session.

Syntax

show rspan session [*session-id*]

session-id – A number identifying this RSPAN session. (Range: 1)

Only two mirror sessions are allowed, including both local and remote mirroring. If local mirroring is enabled with the port monitor command, then there is only one session available for RSPAN.

Command Mode

EXEC

Example

Console#show rspan session

RSPAN Session ID: 1

Source Ports (mirrored ports): None

RX Only: None

TX Only: None

BOTH: None

Destination Port (monitor port): Eth 1/2

Destination Tagged Mode: Untagged

Switch Role: Destination

RSPAN VLAN: 2

RSPAN Uplink Ports: Eth 1/3

Operation Status: Up

Console#

33. Rate Limit Commands

rate-limit

This command defines the rate limit for a specific interface. Use this command without specifying a rate to restore the default rate. Use the no form to restore the default status of disabled.

Syntax

rate-limit {input | output} [*rate*]

no rate-limit {input | output}

input – Input rate for specified interface

output – Output rate for specified interface

rate – Maximum value in Kbps. (Range: 64 - 1,000,000 kbits per second for Gigabit Ethernet ports; 64 - 10,000,000 kbits per second for 10 Gigabit Ethernet ports)

Default Configuration

Disabled

Command Mode

Interface Configuration (Ethernet, Port Channel)

User Guidelines

Using both rate limiting and storm control on the same interface may lead to unexpected results. For example, suppose broadcast storm control is set to 500 Kbps by the command "switchport broadcast packet-rate 500," and the rate limit is set to 20000 Kbps by the command "rate-limit input 20000" on a Fast Ethernet port. Since 20000 Kbps is 1/5 of line speed (100 Mbps), the received rate will actually be 100 Kbps, or 1/5 of the 500 Kbps limit set by the storm control command. It is therefore not advisable to use both of these commands on the same interface.

Example

Console(config)#interface ethernet 1/1

Console(config-if)#rate-limit input 64

Console(config-if)#

34. Loopback Detection Commands

The switch can be configured to detect general loopback conditions caused by hardware problems or faulty protocol settings. When enabled, a control frame is transmitted on the participating ports, and the switch monitors inbound traffic to see if the frame is looped back.

Usage Guidelines

- The default settings for the control frame transmit interval and recover time may be adjusted to improve performance for your specific environment. The shutdown mode may also need to be changed once you determine what kind of packets are being looped back.
- General loopback detection provided by the command described in this section and loopback detection provided by the spanning tree protocol cannot both be enabled at the same time. If loopback detection is enabled for the spanning tree protocol, general loopback detection cannot be enabled on the same interface.
- When a loopback event is detected on an interface or when a interface is released from a shutdown state caused by a loopback event, a trap message is sent and the event recorded in the system log.
- Loopback detection must be enabled both globally and on an interface for loopback detection to take effect.

loopback-detection

This command enables loopback detection globally on the switch or on a specified interface. Use the no form to disable loopback detection.

Syntax

[no] loopback-detection

Default Configuration

Disabled

Command Mode

Global Configuration

Interface Configuration (Ethernet, Port Channel)

User Guidelines

Loopback detection must be enabled globally for the switch by this command and enabled for a specific interface for this function to take effect.

Example

This example enables general loopback detection on the switch, disables loopback detection provided for the spanning tree protocol on port 1, and then enables general loopback detection for that port.

Console(config)#loopback-detection

Console(config)#interface ethernet 1/1

Console(config-if)#no spanning-tree loopback-detection

Console(config-if)#loopback-detection

Console(config)#

loopback-detection mode

This command specifies shutdown by dropping packets for a port detected in loopback state or by dropping packets belonging to a VLAN detected in loopback state. Use the no form to restore the default setting.

Syntax

loopback-detection mode {port-based | vlan-based}

no loopback-detection mode

port-based - When loopback is detected on a port, the port is shut down automatically.

vlan-based - When loopback is detected on a port which a member of a specific VLAN, packets belonging to that VLAN are dropped at the port.

Default Configuration

port-based

Command Mode

Global Configuration

User Guidelines

- When using vlan-based mode, loopback detection control frames are untagged or tagged depending on the port's VLAN membership type.
- When using vlan-based mode, ingress filtering for the port is enabled automatically if not already enabled by the switchport ingress-filtering command. The port's original setting for ingress filtering will be restored when loopback detection is disabled.
- When the loopback detection mode is changed, any ports placed in shutdown state by the loopback detection process will be immediately restored to operation regardless of the remaining recover time.

Example

This example sets the loopback detection mode to VLAN based.

Console(config)#loopback-detection mode vlan-based

Console(config)#

loopback-detection recover-time

This command specifies the interval to wait before the switch automatically releases an interface from shutdown state. Use the no form to restore the default setting.

Syntax

loopback-detection recover-time *seconds*

no loopback-detection recover-time

seconds - Recovery time from shutdown state. (Range: 60-1,000,000 seconds, or 0 to disable automatic recovery)

Default Configuration

60 seconds

Command Mode

Global Configuration

User Guidelines

- When the loopback detection mode is changed, any ports placed in shutdown state by the loopback detection process will be immediately restored to operation regardless of the remaining recover time.
- If the recovery time is set to zero, all ports placed in shutdown state can be restored to operation using the loopback-detection release command. To restore a specific port, use the no shutdown command.

Example

Console(config)#loopback-detection recover-time 120

Console(config-if)#

loopback-detection transmit-interval

This command specifies the interval at which to transmit loopback detection control frames. Use the no form to restore the default setting.

Syntax

loopback-detection transmit-interval *seconds*

[no] loopback-detection transmit-interval

seconds - The transmission interval for loopback detection control frames. (Range: 1-32767 seconds)

Default Configuration

10 seconds

Command Mode

Global Configuration

Example

Console(config)#loopback-detection transmit-interval 60

Console(config)#

loopback-detection release

This command releases all interfaces currently shut down by the loopback detection feature.

Syntax

loopback-detection release

Command Mode

EXEC

Example

Console#loopback-detection release

Console(config)#

show loopback-detection

This command shows loopback detection configuration settings for the switch or for a specified interface.

Syntax

show loopback-detection [*interface*]

interface

ethernet *unit*/*port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-28)

Command Mode

EXEC

Example

Console#show loopback-detection

Loopback Detection Global Information

Global Status: Enabled

Transmit Interval: 10

Recover Time: 60

Mode: Port-based

Loopback Detection Port Information

Port Admin State Oper State

-------- ----------- ----------

Eth 1/ 1 Enabled Normal

Eth 1/ 2 Disabled Disabled

Eth 1/ 3 Disabled Disabled

...

Console#show loopback-detection ethernet 1/1

Loopback Detection Information of Eth 1/1

Admin State: Enabled

Oper State: Normal

Console#

35. Unidirectional Link Detection

COMMANDS

udld message-interval

This command configures the message interval between UDLD probe messages for ports in advertisement phase and determined to be bidirectional. Use the no form to restore the default setting.

Syntax

udld message-interval *message-interval*

no message-interval

message-interval – The interval at which a port sends UDLD probe

messages after linkup or detection phases. (Range: 7-90 seconds)

Default Configuration

15 seconds

Command Mode

Global Configuration

User Guidelines

- During the detection phase, messages are exchanged at the maximum rate of one per second. After that, if the protocol reaches a stable state and determines that the link is bidirectional, the message interval is increased to a configurable value based on a curve known as M1(t), a time-based function described in RFC 5171.
- If the link is deemed anything other than bidirectional at the end of the detection phase, this curve becomes a flat line with a fixed value of Mfast (7 seconds).
- If the link is instead deemed bidirectional, the curve will use Mfast for the first four subsequent message transmissions and then transition to an Mslow value for all other steady-state transmissions. Mslow is the value configured by this command.

Example

This example sets the message interval to 10 seconds.

Console(config)#udld message-interval 10

Console(config)#

udld aggressive

This command sets UDLD to aggressive mode on an interface. Use the no form to restore the default setting.

Syntax

[no] udld aggressive

Default Configuration

Disabled

Command Mode

Interface Configuration (Ethernet Port)

User Guidelines

UDLD can function in two modes: normal mode and aggressive mode.

- In normal mode, determination of link status at the end of the detection process is always based on information received in UDLD messages: whether that's information about the exchange of proper neighbor identification or the absence of such. Hence, albeit bound by a timer, normal mode determinations are always based on gleaned information, and as such are "event-based." If no such information can be obtained (e.g., because of a bidirectional loss of connectivity), UDLD follows a conservative approach minimize false positives during the

detection process and deems a port to be in "undetermined" state. In other words, normal mode will shut down a port only if it can explicitly determine that the associated link is faulty for an extended period of time.

- In aggressive mode, UDLD will also shut down a port if it loses bidirectional connectivity with the neighbor for the same extended period of time (as that mentioned above for normal mode) and subsequently fails repeated last-resort attempts to re-establish communication with the other end of the link. This mode of operation assumes that loss of communication with the neighbor is a meaningful network event in itself, and a symptom of a serious connectivity problem. Because this type of detection can be event-less, and lack of information cannot always be associated to an actual malfunction of the link, this mode is optional and is recommended only in certain scenarios (typically only on point-to-point links where no communication failure between two neighbors is admissible).

Example

This example enables UDLD aggressive mode on port 1.

Console(config)#interface ethernet 1/1

Console(config-if)#udld aggressive

Console(config-if)#

udld port

This command enables UDLD on an interface. Use the no form to disable UDLD on an interface.

Syntax

[no] udld port

Default Configuration

Disabled

Command Mode

Interface Configuration (Ethernet Port)

User Guidelines

- UDLD requires that all the devices connected to the same LAN segment be running the protocol in order for a potential miss-configuration to be detected and for prompt corrective action to be taken.
- Whenever a UDLD device learns about a new neighbor or receives a resynchronization request from an out-of-synch neighbor, it (re)starts the detection process on its side of the connection and sends N echo messages in reply. (This mechanism implicitly assumes that N packets are sufficient to get through a link and reach the other end, even though some of them might get dropped during the transmission.)
- Since this behavior must be the same on all the neighbors, the sender of the echoes expects to receive an echo in reply. If the detection process ends without the proper echo information being received, the link is considered to be unidirectional.

Example

Console(config)#interface ethernet 1/1

Console(config-if)#udld port

Console(config-if)#

show udld

This command shows UDLD configuration settings and operational status for the switch or for a specified interface.

Syntax

show udld [interface *interface*]

interface

ethernet *unit*/*port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-28)

Command Mode

EXEC

Example

```
Console#show udld
Message Interval: 15
Interface UDLD Mode Oper State Msg Invl
Port State Timeout
--------- -------- ---------- ------------------------------------ --------
Eth 1/ 1 Enabled Aggressive Advertisement 15 s
Bidirectional 5 s
Eth 1/ 2 Disabled Normal Disabled 7 s
Unknown 5 s
Eth 1/ 3 Disabled Normal Disabled 7 s
Unknown 5 s
Eth 1/ 4 Disabled Normal Disabled 7 s
Unknown 5 s
Eth 1/ 5 Disabled Normal Disabled 7 s
Unknown 5 s
...
Console#show udld interface ethernet 1/1
Interface UDLD Mode Oper State Msg Invl
Port State Timeout
--------- -------- ---------- ------------------------------------ --------
Eth 1/ 1 Enabled Aggressive Advertisement 15 s
Bidirectional 5 s
Console#
```

36. Address Table Commands

mac-address-table aging-time

This command sets the aging time for entries in the address table. Use the no form to restore the default aging time.

Syntax

mac-address-table aging-time *seconds*

no mac-address-table aging-time

seconds - Aging time. (Range: 6-672 seconds; 0 to disable aging)

Default Configuration

300 seconds

Command Mode

Global Configuration

User Guidelines

The aging time is used to age out dynamically learned forwarding information.

Example

Console(config)#mac-address-table aging-time 100

Console(config)#

mac-address-table static

This command maps a static address to a destination port in a VLAN. Use the no form to remove an address.

Syntax

mac-address-table static *mac-address* interface *interface* vlan *vlan-id* [*action*]

no mac-address-table static *mac-address* vlan *vlan-id*

mac-address - MAC address.

interface

ethernet *unit*/*port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-28)

port-channel *channel-id* (Range: 1-12)

vlan-id - VLAN ID (Range: 1-4094)

action -

delete-on-reset - Assignment lasts until the switch is reset.

permanent - Assignment is permanent.

Default Configuration

No static addresses are defined. The default mode is permanent.

Command Mode

Global Configuration

User Guidelines

- The static address for a host device can be assigned to a specific port within a specific VLAN. Use this command to add static addresses to the MAC Address Table. Static addresses have the following characteristics:
- Static addresses will not be removed from the address table when a given interface link is down.
- Static addresses are bound to the assigned interface and will not be moved. When a static address is seen on another interface, the address will be ignored and will not be written to the address table.

- A static address cannot be learned on another port until the address is removed with the no form of this command.

Example

Console(config)#mac-address-table static 00-e0-29-94-34-de interface ethernet

1/1 vlan 1 delete-on-reset

Console(config)#

clear mac-address-table dynamic

This command removes any learned entries from the forwarding database.

Default Configuration

None

Command Mode

EXEC

Example

Console#clear mac-address-table dynamic

Console#

show mac-address-table

This command shows classes of entries in the bridge-forwarding database.

Syntax

show mac-address-table [address *mac-address* [*mask*]] [interface *interface*] [vlan *vlan-id*] [sort {address | vlan | interface}]

mac-address - MAC address.

mask - Bits to match in the address.

interface

ethernet *unit*/*port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-28)

port-channel *channel-id* (Range: 1-12)

vlan-id - VLAN ID (Range: 1-4094)

sort - Sort by address, vlan or interface.

Default Configuration

None

Command Mode

EXEC

User Guidelines

- The MAC Address Table contains the MAC addresses associated with each interface. Note that the Type field may include the following types:

a. Learn - Dynamic address entries

b. Config - Static entry

- The mask should be hexadecimal numbers (representing an equivalent bit mask) in the form xx-xx-xx-xx-xx-xx that is applied to the specified MAC address. Enter hexadecimal numbers, where an equivalent binary bit "0" means to match a bit and "1" means to ignore a bit. For example, a mask of 00-00-00-00-00-00 means an exact match, and a mask of FF-FF-FF-FF-FF-FF means "any."
- The maximum number of address entries is 16K.

Example

Console#show mac-address-table

Total entry in system: 3

Interface MAC Address VLAN Type Life Time

--------- ----------------- ---- -------- -----------------

CPU 64-9D-99-00-00-01 1 CPU Delete on Reset

Eth 1/ 1 64-9D-99-10-90-09 1 Learn Delete on Timeout

Eth 1/ 1 64-9D-99-94-34-64 1 Learn Delete on Timeout

Console#

show mac-address-table aging-time

This command shows the aging time for entries in the address table.

Default Configuration

None

Command Mode

EXEC

Example

Console#show mac-address-table aging-time

Aging Status: Enabled

Aging Time: 300 sec.

Console#

show mac-address-table count

This command shows the number of MAC addresses used and the number of available MAC addresses for the overall system or for an interface.

Syntax

show mac-address-table count interface *interface*

interface

ethernet *unit*/*port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-28)

port-channel *channel-id* (Range: 1-12)

Default Configuration

None

Command Mode

EXEC

Example

Console#show mac-address-table count interface ethernet 1/1

MAC Entries for Port ID :1

Dynamic Address Count :2

Total MAC Addresses :2

Total MAC Address Space Available: 16384

Console#

37. Spanning Tree Commands

spanning-tree

This command enables the Spanning Tree Algorithm globally for the switch. Use the no form to disable it.

Syntax

[no] spanning-tree

Default Configuration

Spanning tree is enabled.

Command Mode

Global Configuration

User Guidelines

The Spanning Tree Algorithm (STA) can be used to detect and disable network loops, and to provide backup links between switches, bridges or routers. This allows the switch to interact with other bridging devices (that is, an STA-compliant switch, bridge or router) in your network to ensure that only one route exists between any two stations on the network, and provide backup links which automatically take over when a primary link goes down.

Example

This example shows how to enable the Spanning Tree Algorithm for the switch:

Console(config)#spanning-tree

Console(config)#

spanning-tree cisco-prestandard

This command configures spanning tree operation to be compatible with Cisco prestandard versions. Use the no form to restore the default setting.

Syntax

[no] spanning-tree cisco-prestandard

Default Configuration

Disabled

Command Mode

Global Configuration

User Guidelines

Cisco prestandard versions prior to Cisco IOS Release 12.2(25)SEC do not fully follow the IEEE standard, causing some state machine procedures to function incorrectly. The command forces the spanning tree protocol to function in a manner compatible with Cisco prestandard versions.

Example

Console(config)#spanning-tree cisco-prestandard

Console(config)#

spanning-tree forward-time

This command configures the spanning tree bridge forward time globally for this switch. Use the no form to restore the default.

Syntax

spanning-tree forward-time *seconds*

no spanning-tree forward-time

seconds - Time in seconds. (Range: 4 - 30 seconds). The minimum value is the higher of 4 or [(max-age / 2) + 1].

Default Configuration

15 seconds

Command Mode

Global Configuration

User Guidelines

This command sets the maximum time (in seconds) a port will wait before changing states (i.e., discarding to learning to forwarding). This delay is required because every device must receive information about topology changes before it starts to forward frames. In addition, each port needs time to listen for conflicting information that would make it return to the discarding state; otherwise, temporary data loops might result.

Example

Console(config)#spanning-tree forward-time 20

Console(config)#

spanning-tree hello-time

This command configures the spanning tree bridge hello time globally for this switch. Use the no form to restore the default.

Syntax

spanning-tree hello-time *time*

no spanning-tree hello-time

time - Time in seconds. (Range: 1-10 seconds). The maximum value is the lower of 10 or [(max-age / 2) - 1].

Default Configuration

2 seconds

Command Mode

Global Configuration

User Guidelines

This command sets the time interval (in seconds) at which the root device transmits a configuration message.

Example

Console(config)#spanning-tree hello-time 5

Console(config)#

spanning-tree max-age

This command configures the spanning tree bridge maximum age globally for this switch. Use the no form to restore the default.

Syntax

spanning-tree max-age *seconds*

no spanning-tree max-age

seconds - Time in seconds. (Range: 6-40 seconds)

The minimum value is the higher of 6 or [2 x (hello-time + 1)].

The maximum value is the lower of 40 or [2 x (forward-time - 1)].

Default Configuration

20 seconds

Command Mode

Global Configuration

User Guidelines

This command sets the maximum time (in seconds) a device can wait without receiving a configuration message before attempting to re-converge. All device ports (except for designated ports) should receive configuration messages at regular intervals. Any port that ages out STA information (provided in the last configuration message)

becomes the designated port for the attached LAN. If it is a root port, a new root port is selected from among the device ports attached to the network.

Example

Console(config)#spanning-tree max-age 40

Console(config)#

spanning-tree mode

This command selects the spanning tree mode for this switch. Use the no form to restore the default.

Syntax

spanning-tree mode {stp | rstp | mstp}

no spanning-tree mode

stp - Spanning Tree Protocol (IEEE 802.1D)

rstp - Rapid Spanning Tree Protocol (IEEE 802.1w)

mstp - Multiple Spanning Tree (IEEE 802.1s)

Default Configuration

rstp

Command Mode

Global Configuration

User Guidelines

- Spanning Tree Protocol

This option uses RSTP set to STP forced compatibility mode. It uses RSTP for the internal state machine, but sends only 802.1D BPDUs. This creates one spanning tree instance for the entire network. If multiple VLANs are implemented on a network, the path between specific VLAN members may be inadvertently disabled to prevent network loops, thus isolating group members. When operating multiple VLANs, we recommend selecting the MSTP option.

- Rapid Spanning Tree Protocol

RSTP supports connections to either STP or RSTP nodes by monitoring the incoming protocol messages and dynamically adjusting the type of protocol messages the RSTP node transmits, as described below:

a. STP Mode – If the switch receives an 802.1D BPDU after a port's migration delay timer expires, the switch assumes it is connected to an 802.1D bridge and starts using only 802.1D BPDUs.

b. RSTP Mode – If RSTP is using 802.1D BPDUs on a port and receives an RSTP BPDU after the migration delay expires, RSTP restarts the migration delay timer and begins using RSTP BPDUs on that port.

- Multiple Spanning Tree Protocol

a. To allow multiple spanning trees to operate over the network, you must configure a related set of bridges with the same MSTP configuration, allowing them to participate in a specific set of spanning tree instances.

b. A spanning tree instance can exist only on bridges that have compatible VLAN instance assignments.

c. Be careful when switching between spanning tree modes. Changing modes stops all spanning-tree instances for the previous mode and restarts the system in the new mode, temporarily disrupting user traffic.

Example

The following example configures the switch to use Rapid Spanning Tree:

Console(config)#spanning-tree mode rstp

Console(config)#

spanning-tree pathcost method

This command configures the path cost method used for Rapid Spanning Tree and Multiple Spanning Tree. Use the no form to restore the default.

Syntax

spanning-tree pathcost method {long | short}

no spanning-tree pathcost method

long - Specifies 32-bit based values that range from 1-200,000,000. This method is based on the IEEE 802.1w Rapid Spanning Tree Protocol.

short - Specifies 16-bit based values that range from 1-65535. This method is based on the IEEE 802.1 Spanning Tree Protocol.

Default Configuration

Long method

Command Mode

Global Configuration

User Guidelines

- The path cost method is used to determine the best path between devices. Therefore, lower values should be assigned to ports attached to faster media, and higher values assigned to ports with slower media.
- The path cost methods apply to all spanning tree modes (STP, RSTP and MSTP). Specifically, the long method can be applied to STP since this mode is supported by a backward compatible mode of RSTP.

Example

Console(config)#spanning-tree pathcost method long

Console(config)#

spanning-tree priority

This command configures the spanning tree priority globally for this switch. Use the no form to restore the default.

Syntax

spanning-tree priority *priority*

no spanning-tree priority

priority - Priority of the bridge. (Range – 0-61440, in steps of 4096; Options: 0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344, 61440)

Default Configuration

32768

Command Mode

Global Configuration

User Guidelines

Bridge priority is used in selecting the root device, root port, and designated port. The device with the highest priority (i.e., lower numeric value) becomes the STA root device. However, if all devices have the same priority, the device with the lowest MAC address will then become the root device.

Example

Console(config)#spanning-tree priority 40000

Console(config)#

spanning-tree mst configuration

This command changes to Multiple Spanning Tree (MST) configuration mode.

Default Configuration

No VLANs are mapped to any MST instance.

The region name is set the switch's MAC address.

Command Mode

Global Configuration

Example

Console(config)#spanning-tree mst configuration

Console(config-mstp)#

spanning-tree bpdu(system)

This command configures the system to flood BPDUs to all other ports on the switch or just to all other ports in the same VLAN when spanning tree is disabled globally on the switch or disabled on a specific port. Use the no form to restore the default.

Syntax

spanning-tree bpdu { flooding | filtering }

no spanning-tree bpdu

flooding - Floods BPDUs to all other ports on the switch.

filtering - Floods BPDUs to all other ports within the receiving port's native VLAN (i.e., as determined by port's PVID).

Default Configuration

Floods to all other ports in the same VLAN.

Command Mode

Global Configuration

User Guidelines

This command has no effect if BPDU flooding is disabled on a port.

Example

Console(config)#spanning-tree bpdu flooding

Console(config)#

spanning-tree transmission-limit

This command configures the minimum interval between the transmission of consecutive RSTP/MSTP BPDUs. Use the no form to restore the default.

Syntax

spanning-tree transmission-limit *count*

no spanning-tree transmission-limit

count - The transmission limit in seconds. (Range: 1-10)

Default Configuration

3

Command Mode

Global Configuration

User Guidelines

This command limits the maximum transmission rate for BPDUs.

Example

Console(config)#spanning-tree transmission-limit 4

Console(config)#

spanning-tree mst max-hops

This command configures the maximum number of hops in the region before a BPDU is discarded. Use the no form to restore the default.

Syntax

spanning-tree mst max-hops *hop-number*

hop-number - Maximum hop number for multiple spanning tree. (Range: 1-40)

Default Configuration

20

Command Mode

Global Configuration

User Guidelines

An MSTI region is treated as a single node by the STP and RSTP protocols. Therefore, the message age for BPDUs inside an MSTI region is never changed. However, each spanning tree instance within a region, and the internal spanning tree (IST) that connects these instances use a hop count to specify the maximum number of bridges that will propagate a BPDU. Each bridge decrements the hop count by one before passing on the BPDU. When the hop count reaches zero, the message is dropped.

Example

Console(config)# spanning-tree mst max-hops 30

Console(config)#

mst priority

This command configures the priority of a spanning tree instance. Use the no form to restore the default.

Syntax

mst *instance-id* priority *priority*

no mst *instance-id* priority

instance-id - Instance identifier of the spanning tree. (Range: 0-4094)

priority - Priority of the a spanning tree instance.

(Range: 0-61440 in steps of 4096; Options: 0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344, 61440)

Default Configuration

32768

Command Mode

MST Configuration

User Guidelines

- MST priority is used in selecting the root bridge and alternate bridge of the specified instance. The device with the highest priority (i.e., lowest numerical value) becomes the MSTI root device. However, if all devices have the same priority, the device with the lowest MAC address will then become the root device.
- You can set this switch to act as the MSTI root device by specifying a priority of 0, or as the MSTI alternate device by specifying a priority of 16384.

Example

Console(config-mstp)#mst 1 priority 4096

Console(config-mstp)#

mst vlan

This command adds VLANs to a spanning tree instance. Use the no form to remove the specified VLANs. Using the no form without any VLAN parameters to remove all VLANs.

Syntax

[no] mst *instance-id* vlan *vlan-range*

instance-id - Instance identifier of the spanning tree. (Range: 0-4094)

vlan-range - Range of VLANs. (Range: 1-4094)

Default Configuration

none

Command Mode

MST Configuration

User Guidelines

- Use this command to group VLANs into spanning tree instances. MSTP generates a unique spanning tree for each instance. This provides multiple pathways across the network, thereby balancing the traffic load, preventing wide-scale disruption when a bridge node in a single instance fails, and allowing for faster convergence of a new topology for the failed instance.
- By default all VLANs are assigned to the Internal Spanning Tree (MSTI 0) that connects all bridges and LANs within the MST region. This switch supports up to 32 instances. You should try to group VLANs which cover the same general area of your network. However, remember that you must configure all bridges within the same MSTI Region with the same set of instances, and the same instance (on each bridge) with the same set of VLANs. Also, note that RSTP treats each MSTI region as a single node, connecting all regions to the Common Spanning Tree.

Example

Console(config-mstp)#mst 1 vlan 2-5

Console(config-mstp)#

name

This command configures the name for the multiple spanning tree region in which this switch is located. Use the no form to clear the name.

Syntax

name *name*

name - Name of the spanning tree.

Default Configuration

Switch's MAC address

Command Mode

MST Configuration

User Guidelines

The MST region name and revision number are used to designate a unique MST region. A bridge (i.e., spanning-tree compliant device such as this switch) can only belong to one MST region. And all bridges in the same region must be configured with the same MST instances.

Example

Console(config-mstp)#name R&D

Console(config-mstp)#

revision

This command configures the revision number for this multiple spanning tree configuration of this switch. Use the no form to restore the default.

Syntax

revision *number*

number - Revision number of the spanning tree. (Range: 0-65535)

Default Configuration

0

Command Mode

MST Configuration

User Guidelines

The MST region name and revision number are used to designate a unique MST region. A bridge (i.e., spanning-tree compliant device such as this switch) can only belong to one MST region. And all bridges in the same region must be configured with the same MST instances.

Example

Console(config-mstp)#revision 1

Console(config-mstp)#

spanning-tree bpdu-filter

This command filters all BPDUs received on an edge port. Use the no form to disable this feature.

Syntax

[no] spanning-tree bpdu-filter

Default Configuration

Disabled

Command Mode

Interface Configuration (Ethernet, Port Channel)

User Guidelines

- This command filters all Bridge Protocol Data Units (BPDUs) received on an interface to save CPU processing time. This function is designed to work in conjunction with edge ports which should only connect end stations to the switch, and therefore do not need to process BPDUs. However, note that if a trunking port connected to another switch or bridging device is mistakenly configured as an edge port, and BPDU filtering is enabled on this port, this might cause a loop in the spanning tree.
- Before enabling BPDU Filter, the interface must first be configured as an edge port with the spanning-tree portfast command.

Example

Console(config)#interface ethernet 1/5

Console(config-if)#spanning-tree portfast

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

Console(config-if)#

spanning-tree bpdu-guard

This command shuts down an edge port (i.e., an interface set for fast forwarding) if it receives a BPDU. Use the no form without any keywords to disable this feature, or with a keyword to restore the default settings.

Syntax

spanning-tree bpdu-guard [auto-recovery [interval *interval*]]

no spanning-tree bpdu-guard [auto-recovery [interval]]

auto-recovery - Automatically re-enables an interface after the specified interval.

interval - The time to wait before re-enabling an interface. (Range: 30-86400 seconds)

Default Configuration

BPDU Guard: Disabled

Auto-Recovery: Disabled

Auto-Recovery Interval: 300 seconds

Command Mode

Interface Configuration (Ethernet, Port Channel)

User Guidelines

- An edge port should only be connected to end nodes which do not generate BPDUs. If a BPDU is received on an edge port, this indicates an invalid network configuration, or that the switch may be under attack by a hacker. If

an interface is shut down by BPDU Guard, it must be manually re-enabled using the no spanning-tree spanning-disabled command if the auto-recovery interval is not specified.

- Before enabling BPDU Guard, the interface must be configured as an edge port with the spanning-tree portfast command. Also note that if the edge port attribute is disabled on an interface, BPDU Guard will also be disabled on that interface.

Example

Console(config)#interface ethernet 1/5

Console(config-if)#spanning-tree portfast

Console(config-if)#spanning-tree bpdu-guard

Console(config-if)#

spanning-tree cost

This command configures the spanning tree path cost for the specified interface. Use the no form to restore the default auto-configuration mode.

Syntax

spanning-tree cost *cost*

no spanning-tree cost

cost - The path cost for the port. (Range: 0 for auto-configuration, 1-65535 for short path cost method, 1-200,000,000 for long path cost method)

Recommended STA Path Cost Range

Port Type	Short Path Cost (IEEE 802.1 D-1998)	Long Path Cost (802.1 D-2004)
Ethernet	50-600	200,000-20,000,000
Fast Ethernet	10-60	20,000-2,000,000
Gigabit Ethernet	3-10	2,000-200,000
10G Ethernet	1-5	200-20,000

Default Configuration

By default, the system automatically detects the speed and duplex mode used on each port, and configures the path cost according to the values shown below. Path cost "0" is used to indicate auto-configuration mode. When the short path cost method is selected and the default path cost recommended by the IEEE 8021w standard exceeds 65,535, the default is set to 65,535.

Default STA Path Costs

Port Type	Short Path Cost (IEEE 802.1 D-1998)	Long Path Cost (802.1 D-2004)
Ethernet	65,535	1,000,000
Fast Ethernet	65,535	100,000
Gigabit Ethernet	10,000	10,000
10G Ethernet	1,000	1,000

Command Mode

Interface Configuration (Ethernet, Port Channel)

User Guidelines

- This command is used by the Spanning Tree Algorithm to determine the best path between devices. Therefore, lower values should be assigned to ports attached to faster media, and higher values assigned to ports with slower media.
- Path cost takes precedence over port priority.
- When the path cost method is set to short, the maximum value for path cost is 65,535.

Example

Console(config)#interface ethernet 1/5

Console(config-if)#spanning-tree cost 50

Console(config-if)#

spanning-tree portfast

This command specifies an interface as an fast-start port. Use the no form to restore the default.

Syntax

spanning-tree portfast [auto]

no spanning-tree portfast

auto - Automatically determines if an interface is an fast-start port.

Default Configuration

Auto

Command Mode

Interface Configuration (Ethernet, Port Channel)

User Guidelines

You can enable this option if an interface is attached to a LAN segment that is at the end of a bridged LAN or to an end node. Since end nodes cannot cause forwarding loops, they can pass directly through to the spanning tree forwarding state. Specifying fast-start port provides quicker convergence for devices such as workstations or servers, retains the current forwarding database to reduce the amount of frame flooding required to rebuild address tables during reconfiguration events, does not cause the spanning tree to initiate reconfiguration when the interface changes state, and also overcomes other STA-related time out problems. However, remember that fast-start port should only be enabled for ports connected to an end-node device.

Example

Console(config)#interface ethernet 1/5

Console(config-if)#spanning-tree portfast

Console(config-if)#

spanning-tree link-type

This command configures the link type for Rapid Spanning Tree and Multiple Spanning Tree. Use the no form to restore the default.

Syntax

spanning-tree link-type {auto | point-to-point | shared}

no spanning-tree link-type

auto - Automatically derived from the duplex mode setting.

point-to-point - Point-to-point link.

shared - Shared medium.

Default Configuration

auto

Command Mode

Interface Configuration (Ethernet, Port Channel)

User Guidelines

- Specify a point-to-point link if the interface can only be connected to exactly one other bridge, or a shared link if it can be connected to two or more bridges.
- When automatic detection is selected, the switch derives the link type from the duplex mode. A full-duplex interface is considered a point-to-point link, while a half-duplex interface is assumed to be on a shared link.
- RSTP only works on point-to-point links between two bridges. If you designate a port as a shared link, RSTP is forbidden. Since MSTP is an extension of RSTP, this same restriction applies.

Example

Console(config)#interface ethernet 1/5

Console(config-if)#spanning-tree link-type point-to-point

spanning-tree loopback-detection

This command enables the detection and response to Spanning Tree loopback BPDU packets on the port. Use the no form to disable this

feature.

Syntax

[no] spanning-tree loopback-detection

Default Configuration

Enabled

Command Mode

Interface Configuration (Ethernet, Port Channel)

User Guidelines

- If Port Loopback Detection is not enabled and a port receives its own BPDU, then the port will drop the loopback BPDU according to IEEE Standard 802.1W-2001 9.3.4 (Note 1).
- Port Loopback Detection will not be active if Spanning Tree is disabled on the switch.

Example

Console(config)#interface ethernet 1/5

Console(config-if)#spanning-tree loopback-detection

spanning-tree loopback-detection action

This command configures the response for loopback detection to block user traffic or shut down the interface. Use the no form to restore the default.

Syntax

spanning-tree loopback-detection action {block | shutdown *duration*}

no spanning-tree loopback-detection action

block - Blocks user traffic.

shutdown - Shuts down the interface.

duration - The duration to shut down the interface. (Range: 60-86400 seconds)

Default Configuration

block

Command Mode

Interface Configuration (Ethernet, Port Channel)

User Guidelines

- If an interface is shut down by this command, and the release mode is set to "auto" with the spanning-tree loopback-detection release-mode command, the selected interface will be automatically enabled when the shutdown interval has expired.

- If an interface is shut down by this command, and the release mode is set to "manual," the interface can be re-enabled using the spanning-tree loopback-detection release command.

Example

Console(config)#interface ethernet 1/5

Console(config-if)#spanning-tree loopback-detection action shutdown 600

spanning-tree loopback-detection release-mode

This command configures the release mode for a port that was placed in the discarding state because a loopback BPDU was received. Use the no form to restore the default.

Syntax

spanning-tree loopback-detection release-mode {auto | manual}

no spanning-tree loopback-detection release-mode

auto - Allows a port to automatically be released from the discarding state when the loopback state ends.

manual - The port can only be released from the discarding state manually.

Default Configuration

auto

Command Mode

Interface Configuration (Ethernet, Port Channel)

User Guidelines

- If the port is configured for automatic loopback release, then the port will only be returned to the forwarding state if one of the following conditions is satisfied:

a. The port receives any other BPDU except for its own, or;

b. The port's link status changes to link down and then link up again, or;

c. The port ceases to receive its own BPDUs in a forward delay interval.

- If Port Loopback Detection is not enabled and a port receives its own BPDU, then the port will drop the loopback BPDU according to IEEE Standard 802.1W-2001 9.3.4 (Note 1).
- Port Loopback Detection will not be active if Spanning Tree is disabled on the switch.
- When configured for manual release mode, then a link down / up event will not release the port from the discarding state. It can only be released using the spanning-tree loopback-detection release command.

Example

Console(config)#interface ethernet 1/5

Console(config-if)#spanning-tree loopback-detection release-mode manual

Console(config-if)#

spanning-tree loopback-detection trap

This command enables SNMP trap notification for Spanning Tree loopback BPDU detections. Use the no form to restore the default.

Syntax

[no] spanning-tree loopback-detection trap

Default Configuration

Disabled

Command Mode

Interface Configuration (Ethernet, Port Channel)

Example

Console(config)#interface ethernet 1/5

Console(config-if)#spanning-tree loopback-detection trap

spanning-tree mst cost

This command configures the path cost on a spanning instance in the Multiple Spanning Tree. Use the no form to restore the default auto-configuration mode.

Syntax

spanning-tree mst *instance-id* cost *cost*

no spanning-tree mst *instance-id* cost

instance-id - Instance identifier of the spanning tree. (Range: 0-4094)

cost - Path cost for an interface. (Range: 0 for auto-configuration, 1-65535 for short path cost method, 1-200,000,000 for long path cost method)

Default Configuration

By default, the system automatically detects the speed and duplex mode used on each port, and configures the path cost according to the values shown below. Path cost "0" is used to indicate auto-configuration mode. When the short path cost method is selected and the default path cost recommended by the IEEE 8021w standard exceeds 65,535.

Command Mode

Interface Configuration (Ethernet, Port Channel)

User Guidelines

- Each spanning-tree instance is associated with a unique set of VLAN IDs.
- This command is used by the multiple spanning-tree algorithm to determine the best path between devices. Therefore, lower values should be assigned to interfaces attached to faster media, and higher values assigned to interfaces with slower media.
- Use the no spanning-tree mst cost command to specify auto-configuration mode.
- Path cost takes precedence over interface priority.

Example

Console(config)#interface Ethernet 1/5

Console(config-if)#spanning-tree mst 1 cost 50

Console(config-if)#

spanning-tree mst port-priority

This command configures the interface priority on a spanning instance in the Multiple Spanning Tree. Use the no form to restore the default.

Syntax

spanning-tree mst *instance-id* port-priority *priority*

no spanning-tree mst *instance-id* port-priority

instance-id - Instance identifier of the spanning tree. (Range: 0-4094)

priority - Priority for an interface. (Range: 0-240 in steps of 16)

Default Configuration

128

Command Mode

Interface Configuration (Ethernet, Port Channel)

User Guidelines

- This command defines the priority for the use of an interface in the multiple spanning-tree. If the path cost for all interfaces on a switch are the same, the interface with the highest priority (that is, lowest value) will be configured as an active link in the spanning tree.
- Where more than one interface is assigned the highest priority, the interface with lowest numeric identifier will be enabled.

Example

Console(config)#interface Ethernet 1/5

Console(config-if)#spanning-tree mst 1 port-priority 0

Console(config-if)#

spanning-tree bpdu(port)

This command floods BPDUs to other ports when spanning tree is disabled globally or disabled on a specific port. Use the no form to restore the default setting.

Syntax

[no] spanning-tree bpdu

Default Configuration

Enabled

Command Mode

Interface Configuration (Ethernet, Port Channel)

User Guidelines

- When enabled, BPDUs are flooded to all other ports on the switch or to all other ports within the receiving port's native VLAN as specified by the spanning-tree bpdu flooding command.
- The spanning-tree bpdu flooding command has no effect if BPDU flooding is disabled on a port by the spanning-tree bpdu command.

Example

Console(config)#interface ethernet 1/5

Console(config-if)#spanning-tree bpdu

Console(config-if)#

spanning-tree port-priority

This command configures the priority for the specified interface. Use the no form to restore the default.

Syntax

spanning-tree port-priority *priority*

no spanning-tree port-priority

priority - The priority for a port. (Range: 0-240, in steps of 16)

Default Configuration

128

Command Mode

Interface Configuration (Ethernet, Port Channel)

User Guidelines

- This command defines the priority for the use of a port in the Spanning Tree Algorithm. If the path cost for all ports on a switch are the same, the port with the highest priority (that is, lowest value) will be configured as an active link in the spanning tree.
- Where more than one port is assigned the highest priority, the port with lowest numeric identifier will be enabled.

Example

Console(config)#interface ethernet 1/5

Console(config-if)#spanning-tree port-priority 0

spanning-tree guard root

This command prevents a designated port from taking superior BPDUs into account and allowing a new STP root port to be elected. Use the no form to disable this feature.

Syntax

[no] spanning-tree guard root

Default Configuration

Disabled

Command Mode

Interface Configuration (Ethernet, Port Channel)

User Guidelines

- A bridge with a lower bridge identifier (or same identifier and lower MAC address) can take over as the root bridge at any time.
- When Root Guard is enabled, and the switch receives a superior BPDU on this port, it is set to the Discarding state until it stops receiving superior BPDUs for a fixed recovery period. While in the discarding state, no traffic is forwarded across the port.
- Root Guard can be used to ensure that the root bridge is not formed at a suboptimal location. Root Guard should be enabled on any designated port connected to low-speed bridges which could potentially overload a slower link by taking over as the root port and forming a new spanning tree topology. It could also be used to form a border around part of the network where the root bridge is allowed.
- When spanning tree is initialized globally on the switch or on an interface, the switch will wait for 20 seconds to ensure that the spanning tree has converged before enabling Root Guard.

Example

Console(config)#interface ethernet 1/5

Console(config-if)#spanning-tree portfast

Console(config-if)#spanning-tree guard root

Console(config-if)#

spanning-tree spanning-disabled

This command disables the spanning tree algorithm for the specified interface. Use the no form to re-enable the spanning tree algorithm for the specified interface.

Syntax

[no] spanning-tree spanning-disabled

Default Configuration

Enabled

Command Mode

Interface Configuration (Ethernet, Port Channel)

Example

This example disables the spanning tree algorithm for port 5.

Console(config)#interface ethernet 1/5

Console(config-if)#spanning-tree spanning-disabled

Console(config-if)#

spanning-tree loopback-detection release

This command manually releases a port placed in discarding state by loopback-detection.

Syntax

spanning-tree loopback-detection release *interface*

interface

ethernet *unit*/*port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-28)

port-channel *channel-id* (Range: 1-12)

Command Mode

EXEC

User Guidelines

Use this command to release an interface from discarding state if loopback detection release mode is set to "manual" by the spanning-tree loopback-detection release-mode command and BPDU loopback occurs.

Example

Console#spanning-tree loopback-detection release ethernet 1/1

Console#

spanning-tree protocol-migration

This command re-checks the appropriate BPDU format to send on the selected interface.

Syntax

spanning-tree protocol-migration *interface*

interface

ethernet *unit*/*port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-28)

port-channel *channel-id* (Range: 1-12)

Command Mode

EXEC

User Guidelines

If at any time the switch detects STP BPDUs, including Configuration or Topology Change Notification BPDUs, it will automatically set the selected interface to forced STP-compatible mode. However, you can also use the spanning-tree protocol-migration command at any time to manually re-check the appropriate BPDU format to send on the selected interfaces (i.e., RSTP or STP-compatible).

Example

Console#spanning-tree protocol-migration eth 1/5

Console#

show spanning-tree

This command shows the configuration for the common spanning tree (CST), for all instances within the multiple spanning tree (MST), or for a specific instance within the multiple spanning tree (MST).

Syntax

show spanning-tree [*interface* | mst *instance-id* | active | detail]

interface

ethernet *unit*/*port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-28)

port-channel *channel-id* (Range: 1-12)

instance-id - Instance identifier of the multiple spanning tree. (Range: 0-4094)

active - Shows a summary of active interface.

detail - Shows a summary of global and interface settings.

Default Configuration

None

Command Mode

EXEC

User Guidelines

- Use the show spanning-tree command with no parameters to display the spanning tree configuration for the switch for the Common Spanning Tree (CST) and for every interface in the tree.
- Use the show spanning-tree *interface* command to display the spanning tree configuration for an interface within the Common Spanning Tree (CST).
- Use the show spanning-tree mst command to display the spanning tree configuration for all instances within the Multiple Spanning Tree (MST), including global settings and settings for active interfaces.
- Use the show spanning-tree mst *instance-id* command to display the spanning tree configuration for an instance within the Multiple Spanning Tree (MST), including global settings and settings for all interfaces.

Example

```
Console#show spanning-tree
Spanning Tree Mode: RSTP
Spanning Tree Status: Enabled
 Root ID         Priority    32768
                 Address     EC:D6:8A:32:04:C0
                 Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
 Bridge ID       Priority    32768
                 Address     EC:D6:8A:32:04:C0
                 Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
Interface Role Sts      Bridge ID                       Port ID        Prio Cost        STP
--------- ---- ----- ---------------------------- ----------    --- -------- ------
Eth 1/ 1     DISB BLK     32768.EC:D6:8A:32:04:C0       128.1          128       20000 EN
Eth 1/ 2     DISB BLK     32768.EC:D6:8A:32:04:C0       128.2          128       20000 EN
Eth 1/ 3     DISB BLK     32768.EC:D6:8A:32:04:C0       128.3          128       20000 EN
Eth 1/ 4     DISB BLK     32768.EC:D6:8A:32:04:C0       128.4          128       20000 EN
Eth 1/ 5     DISB BLK     32768.EC:D6:8A:32:04:C0       128.5          128       20000 EN
Eth 1/ 6     DISB BLK     32768.EC:D6:8A:32:04:C0       128.6          128       20000 EN
Eth 1/ 7     DISB BLK     32768.EC:D6:8A:32:04:C0       128.7          128       20000 EN
Eth 1/ 8     DISB BLK     32768.EC:D6:8A:32:04:C0       128.8          128       20000 EN
Eth 1/ 9     DISB BLK     32768.EC:D6:8A:32:04:C0       128.9          128       20000 EN
Eth 1/10     DISB BLK     32768.EC:D6:8A:32:04:C0       128.10         128       20000 EN
...
This example shows a brief summary of global and interface setting for the
spanning tree.
Console#show spanning-tree detail
###### MST 0
 Spanning Tree Enabled Mode RSTP
 Default port cost method                : Short
 Root ID         Priority    32768
                 Address     EC:D6:8A:32:04:C0
                 Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
 Bridge ID       Priority    32768
```

Address EC:D6:8A:32:04:C0

Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Number of topology changes 0 last change occurred 5823 ago

Transmission Limit: 3

Flooding Behavior: filtering

Eth 1/ 1 Information

Stp Status: Enabled

Port Role/State: Disabled/Discarding

Port Priority: 128

Port Cost: Admin=0 Oper=20000

Designated Root/Cost: 32768.EC:D6:8A:32:04:C0/0

Designated Bridge/Port: 32768.EC:D6:8A:32:04:C0/128.1

Port Fast: Admin=Auto Oper=Disabled

Link Type: Admin=Auto Oper=Point-to-point

Forward Transitions: 0

Root Guard Status: Disabled

BPDU Flooding: Enabled

BPDU Guard Status/Recovery: Disabled/No-auto (300 s)

BPDU Filter Status: Disabled

TC Prop Stop: Disabled

Loopback Detection Status/Mode: Disabled/Auto

Loopback Detection Trap/Action: Disabled/Shutdown

...

show spanning-tree mst configuration

This command shows the configuration of the multiple spanning tree.

Command Mode

EXEC

Example

Console#show spanning-tree mst configuration

Mstp Configuration Information

Configuration Name: R&D

Revision Level :0

Instance VLANs

---

0 1-4094

Console#

38. ERPS Commands

erps

This command enables ERPS on the switch. Use the no form to disable this feature.

Syntax

[no] erps

Default Configuration

Disabled

Command Mode

Global Configuration

User Guidelines

ERPS must be enabled globally on the switch before it can enable on an ERPS ring using the enable command.

Example

Console(config)#erps

Console(config)#

erps domain

This command creates an ERPS ring and enters ERPS configuration mode for the specified domain. Use the no form to delete a ring.

Syntax

[no] erps domain *name*

name - Name of a specific ERPS ring. (Range: 1-12 characters)

Default Configuration

None

Command Mode

Global Configuration

User Guidelines

Up to 14 ERPS rings can be configured on the switch.

Example

Console(config)#erps domain r&d

Console(config-erps)#

control-vlan

This command specifies a dedicated VLAN used for sending and receiving ERPS protocol messages. Use the no form to remove the Control VLAN.

Syntax

[no] control-vlan *vlan-id*

vlan-id - VLAN ID (Range: 1-4094)

Default Configuration

None

Command Mode

ERPS Configuration

User Guidelines

- Configure one control VLAN for each ERPS ring. First create the VLAN to be used as the control VLAN, add the ring ports for the east and west interface as tagged members to this VLAN (switchport allowed vlan), and then use the control-vlan command to add it to the ring.
- The Control VLAN must not be configured as a Layer 3 interface (with an IP address), nor as a dynamic VLAN (with GVRP enabled). In addition, only ring ports may be added to the Control VLAN. No other ports can be members of this VLAN. Also, the ring ports of the Control VLAN must be tagged. Failure to observe these restrictions can result in a loop in the network.
- Once the ring has been activated with the enable command, the configuration of the control VLAN cannot be modified. Use the no enable command to stop the ERPS ring before making any configuration changes to the control VLAN.

Example

```
Console(config)#vlan database
Console(config-vlan)#vlan 2 name rdc media ethernet state active
Console(config-vlan)#exit
Console(config)#interface ethernet 1/12
Console(config-if)#switchport allowed vlan add 2 tagged
Console(config-if)#interface ethernet 1/11
Console(config-if)#switchport allowed vlan add 2 tagged
Console(config-if)#exit
Console(config)#erps domain rd1
Console(config-erps)#control-vlan 2
Console(config-erps)#
```

enable

This command activates the current ERPS ring. Use the no form to disable the current ring.

Syntax

[no] enable

Default Configuration

Disabled

Command Mode

ERPS Configuration

User Guidelines

- Before enabling a ring, the global ERPS function should be enabled with the erps command, the east and west ring ports configured on each node with the ring-port command, the RPL owner specified with the rpl owner command, and the control VLAN configured with the control-vlan command.
- Once enabled, the RPL owner node and non-owner node state machines will start, and the ring will enter idle state if no signal failures are detected.

Example

```
Console(config-erps)#enable
Console(config-erps)#
```

guard-timer

This command sets the guard timer to prevent ring nodes from receiving outdated R-APS messages. Use the no form to restore the default setting.

Syntax

guard-timer *milliseconds*

milliseconds - The guard timer is used to prevent ring nodes from receiving outdated R-APS messages. During the duration of the guard timer, all received R-APS messages are ignored by the ring protection control process, giving time for old messages still circulating on the ring to expire. (Range: 10-2000 milliseconds, in steps of 10 milliseconds)

Default Configuration

500 milliseconds

Command Mode

ERPS Configuration

User Guidelines

The guard timer duration should be greater than the maximum expected forwarding delay for an R-APS message to pass around the ring. A side-effect of the guard timer is that during its duration, a node will be unaware of new or existing ring requests transmitted from other nodes.

Example

Console(config-erps)#guard-timer 300

Console(config-erps)#

holdoff-timer

This command sets the timer to filter out intermittent link faults. Use the no form to restore the default setting.

Syntax

holdoff-timer *milliseconds*

milliseconds - The hold-off timer is used to filter out intermittent link faults. Faults will only be reported to the ring protection mechanism if this timer expires. (Range: 0-10000 milliseconds, in steps of 100 milliseconds)

Default Configuration

0 milliseconds

Command Mode

ERPS Configuration

User Guidelines

In order to coordinate timing of protection switches at multiple layers, a hold-off timer may be required. Its purpose is to allow, for example, a server layer protection switch to have a chance to fix the problem before switching at a client layer. When a new defect or more severe defect occurs (new Signal Failure), this event will not be reported immediately to the protection switching mechanism if the provisioned hold-off timer value is non-zero. Instead, the hold-off timer will be started. When the timer expires, whether a defect still exists or not, the timer will be checked. If one does exist, that defect will be reported to the protection switching mechanism. The reported defect need not be the same one that started the timer.

Example

Console(config-erps)#holdoff-timer 300

Console(config-erps)#

major-domain

This command specifies the ERPS ring used for sending control packets. Use the no form to remove the current setting.

Syntax

major-domain *name*

no major-domain

name - Name of the ERPS ring used for sending control packets. (Range: 1-32 characters)

Default Configuration

None

Command Mode

ERPS Configuration

User Guidelines

- This switch can support up to two rings. However, ERPS control packets can only be sent on one ring. This command is used to indicate that the current ring is a secondary ring, and to specify the major ring which will be used to send ERPS control packets.
- The Ring Protection Link (RPL) is the west port and can not be configured. So the physical port on a secondary ring must be the west port. In other words, if a domain has two physical ring ports, this ring can only be a major ring, not a secondary ring (or sub-domain) which can have only one physical ring port. This command will therefore fail if the east port is already configured (see the ring-port command).

Example

Console(config-erps)#major-domain rd0

Console(config-erps)#

meg-level

This command sets the Maintenance Entity Group level for a ring. Use the no form to restore the default setting.

Syntax

meg-level *level*

level - The maintenance entity group (MEG) level which provides a communication channel for ring automatic protection switching (R-APS) information. (Range: 0-7)

Default Configuration

1

Command Mode

ERPS Configuration

User Guidelines

- This parameter is used to ensure that received R-APS PDUs are directed for this ring. A unique level should be configured for each local ring if there are many R-APS PDUs passing through this switch.
- If CFM continuity check messages are used to monitor the link status of an ERPS ring node as specified by the mep-monitor command, then the MEG level set by the meg-level command must match the authorized maintenance level of the CFM domain to which the specified MEP belongs.

Example

Console(config-erps)#meg-level 0

Console(config-erps)#

mep-monitor

This command specifies the CCM MEPs used to monitor the link on a ring node. Use the no form to restore the default setting.

Syntax

mep-monitor {east | west} mep *mpid*

east - Connects to next ring node to the east.

west - Connects to next ring node to the west.

mpid – Maintenance end point identifier. (Range: 1-8191)

Default Configuration

None

Command Mode

ERPS Configuration

User Guidelines

- If this command is used to monitor the link status of an ERPS node with CFM continuity check messages, then the MEG level set by the meg-level command must match the authorized maintenance level of the CFM domain to which the specified MEP belongs.
- To ensure complete monitoring of a ring node, use the mep-monitor command specify the CFM MEPs used to monitor both the east and west ports of the ring node.
- If CFM determines that a MEP node which has been configured to monitor a ring port with this command has gone down, this information is passed to ERPS, which in turn process it as a ring node failure.

Example

Console(config-erps)#mep-monitor east mep 1

Console(config-erps)#

node-id

This command sets the MAC address for a ring node. Use the no form to restore the default setting.

Syntax

node-id *mac-address*

mac-address – A MAC address unique to the ring node. The MAC address must be specified in the format xx-xx-xx-xx-xx-xx or xxxxxxxxxxxx.

Default Configuration

CPU MAC address

Command Mode

ERPS Configuration

User Guidelines

The ring node identifier is informational, and does not affect ring protection switching operations. It may be used for debugging, such as to distinguish messages when a node is connected to more than one ring.

Example

Console(config-erps)#node-id 00-12-CF-61-24-2D

Console(config-erps)#

non-erps-dev-protect

This command sends non-standard health-check packets when an owner node enters protection state without any link down event having been detected through SF messages. Use the no form to disable this feature.

Syntax

[no] non-erps-dev-protect

Default Configuration

Disabled

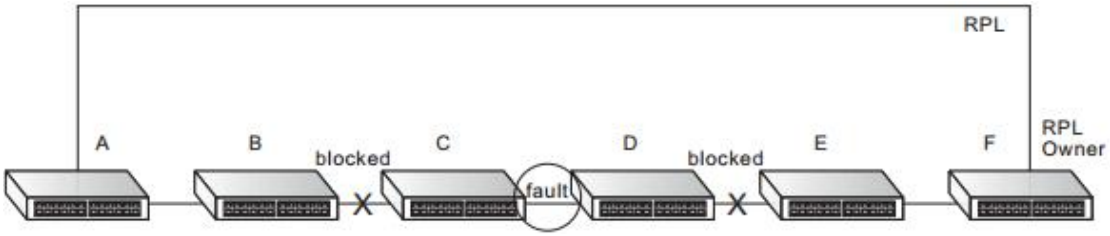
Command Mode

ERPS Configuration

User Guidelines

- The RPL owner node detects a failed link when it receives R-APS (SF - signal fault) messages from nodes adjacent to the failed link. The owner then enters protection state by unblocking the RPL. However, using this standard recovery procedure may cause a non-EPRS device to become isolated when the ERPS device adjacent to it detects a continuity check message (CCM) loss event and blocks the link between the non-ERPS device and ERPS device.

- CCMs are propagated by the Connectivity Fault Management (CFM) protocol as described under "CFM Commands". If the standard recovery procedure were used as shown in the following figure, and node E detected CCM loss, it would send an R-APS (SF) message to the RPL owner and block the link to node D, isolating that non-ERPS device.



- When non-ERPS device protection is enabled on the ring, the ring ports on the RPL owner node and non-owner nodes will not be blocked when signal loss is detected by CCM loss events.
- When non-ERPS device protection is enabled on an RPL owner node, it will send non-standard health-check packets to poll the ring health when it enters the protection state. It does not use the normal procedure of waiting to receive an R-APS (NR - no request) message from nodes adjacent to the recovered link. Instead, it waits to see if the non-standard health-check packets loop back. If they do, indicating that the fault has been resolved, the RPL will be blocked. After blocking the RPL, the owner node will still transmit an R-APS (NR, RB - ring blocked) message. ERPS-compliant nodes receiving this message flush their forwarding database and unblock previously blocked ports. The ring is now returned to Idle state.

Example

Console(config-erps)#non-erps-dev-protect

Console(config-erps)#

propagate-tc

This command enables propagation of topology change messages for a secondary ring to the primary ring. Use the no form to disable this feature.

Syntax

[no] propagate-tc

Default Configuration

Disabled

Command Mode

ERPS Configuration

User Guidelines

- When a secondary ring detects a topology change, it can pass a message about this event to the major ring. When the major ring receives this kind of message from a secondary ring, it can clear the MAC addresses on its ring ports to help the second ay ring restore its connections more quickly through protection switching.
- When the MAC addresses are cleared, data traffic may flood onto the major ring. The data traffic will become stable after the MAC addresses are learned again. The major ring will not be broken, but the bandwidth of data traffic on the major ring may suffer for a short period of time due to this flooding behavior.

Example

Console(config-erps)#propagate-tc

Console(config-erps)#

ring-port

This command configures a node's connection to the ring through the east or west interface. Use the no form to disassociate a node from the ring.

Syntax

ring-port {east | west} interface *interface*

east - Connects to next ring node to the east.

west - Connects to next ring node to the west.

interface

ethernet *unit*/*port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-28)

Default Configuration

Not associated

Command Mode

ERPS Configuration

User Guidelines

- Each node must be connected to two neighbors on the ring. For convenience, the ports connected are referred to as east and west ports. Alternatively, the closest neighbor to the east should be the next node in the ring in a clockwise direction, and the closest neighbor to the west should be the next node in the ring in a counter-clockwise direction.
- Note that a ring port cannot be configured as a member of a spanning tree, a dynamic trunk, or a static trunk.

Example

Console(config-erps)#ring-port east interface ethernet 1/12

Console(config-erps)#

rpl owner

This command configures a ring node to be the Ring Protection Link (RPL) owner or a non-owner.

Syntax

[no] rpl owner

Default Configuration

non-owner

Command Mode

ERPS Configuration

User Guidelines

- Only one RPL owner can be configured on a ring. The owner blocks traffic on the RPL during Idle state, and unblocks it during Protection state (that is, when a signal fault is detected on the ring).
- The east and west connections to the ring must be specified for all ring nodes using the ring-port command. When this switch is configured as the RPL owner, the west ring port is set as being connected to the RPL.

Example

Console(config-erps)#rpl owner

Console(config-erps)#

wtr-timer

This command sets the wait-to-restore timer which is used to verify that the ring has stabilized before blocking the RPL after recovery from a signal failure. Use the no form to restore the default setting.

Syntax

wtr-timer *minutes*

minutes - The wait-to-restore timer is used to verify that the ring has stabilized before blocking the RPL after recovery from a signal failure. (Range: 5-12 minutes)

Default Configuration

5 minutes

Command Mode

ERPS Configuration

User Guidelines

If the switch goes into ring protection state due to a signal failure, after the failure condition is cleared, the RPL owner will start the wait-to-restore timer and wait until it expires to verify that the ring has stabilized before blocking the RPL and returning to the Idle (normal operating) state.

Example

Console(config-erps)#wtr-timer 10

Console(config-erps)#

show erps

This command displays status information for all configured rings, or for a specified ring

Syntax

show erps [domain *ring-name*]

ring-name - Name of a specific ERPS ring. (Range: 1-32 characters)

Command Mode

EXEC

Example

This example displays a summary of all the ERPS rings configured on the switch.

Console#show erps

ERPS Status : Enabled

Number of ERPS Domains : 1

Domain State MEL Enabled West East RPL Owner Ctrl VLAN

---------- ---------- --- ------- -------- -------- --------- ---------

rd1 Idle 0 Yes Eth 1/12 Eth 1/10 Yes 100

rd2 Protection 0 Yes Eth 1/3 Eth 1/4 No 200

Console#

39. VLAN Commands

39.1 GVRP and Bridge Extension Commands

gvrp enable

This command enables GVRP globally for the switch. Use the no form to disable it.

Syntax

[no] gvrp enable

Default Configuration

Disabled

Command Mode

Global Configuration

User Guidelines

GVRP defines a way for switches to exchange VLAN information in order to register VLAN members on ports across the network. This function should be enabled to permit automatic VLAN registration, and to support VLANs which extend beyond the local switch.

Example

Console(config)# gvrp enable

Console(config)#

garp timer

This command sets the values for the join, leave and leaveall timers. Use the no form to restore the timers' default values.

Syntax

garp timer {join | leave | leaveall} *timer-value*

no garp timer {join | leave | leaveall}

{join | leave | leaveall} - Timer to set.

timer-value - Value of timer.

Ranges:

join: 20-1000 centiseconds

leave: 60-3000 centiseconds

leaveall: 500-18000 centiseconds

Default Configuration

join: 20 centiseconds

leave: 60 centiseconds

leaveall: 1000 centiseconds

Command Mode

Interface Configuration (Ethernet, Port Channel)

User Guidelines

- Group Address Registration Protocol is used by GVRP and GMRP to register or deregister client attributes for client services within a bridged LAN. The default values for the GARP timers are independent of the media access method or data rate. These values should not be changed unless you are experiencing difficulties with GMRP or GVRP registration/deregistration.
- Timer values are applied to GVRP for all the ports on all VLANs.

- Timer values must meet the following restrictions:

a. leave >= (3 x join)

b. leaveall > leave

NOTE: Set GVRP timers on all Layer 2 devices connected in the same network to the same values. Otherwise, GVRP may not operate successfully.

Example

Console(config)#interface ethernet 1/1

Console(config-if)#garp timer join 100

Console(config-if)#

Switchport forbidden vlan

This command configures forbidden VLANs. Use the no form to remove the list of forbidden VLANs.

Syntax

switchport forbidden vlan {add *vlan-list* | remove *vlan-list*}

no switchport forbidden vlan

add *vlan-list* - List of VLAN identifiers to add.

remove *vlan-list* - List of VLAN identifiers to remove.

vlan-list - Separate nonconsecutive VLAN identifiers with a comma and no spaces; use a hyphen to designate a range of IDs. (Range: 1-4094).

Default Configuration

No VLANs are included in the forbidden list.

Command Mode

Interface Configuration (Ethernet, Port Channel)

User Guidelines

- This command prevents a VLAN from being automatically added to the specified interface via GVRP.
- If a VLAN has been added to the set of allowed VLANs for an interface, then you cannot add it to the set of forbidden VLANs for that same interface.
- GVRP cannot be enabled for ports set to Access mode (see the switchport mode command).

Example

The following example shows how to prevent port 1 from being added to VLAN 3:

Console(config)#interface ethernet 1/1

Console(config-if)#switchport forbidden vlan add 3

Console(config-if)#

switchport gvrp

This command enables GVRP for a port. Use the no form to disable it.

Syntax

[no] switchport gvrp

Default Configuration

Disabled

Command Mode

Interface Configuration (Ethernet, Port Channel)

User Guidelines

GVRP cannot be enabled for ports set to Access mode using the switchport mode command.

Example

Console(config)#interface ethernet 1/1

Console(config-if)#switchport gvrp

Console(config-if)#

show bridge-ext

This command shows the configuration for bridge extension commands.

Default Configuration

None

Command Mode

EXEC

Example

Console#show bridge-ext

Maximum Supported VLAN Numbers: 4094

Maximum Supported VLAN ID: 4094

Extended Multicast Filtering Services: No

Static Entry Individual Port: Yes

VLAN Learning: IVL

Configurable PVID Tagging: Yes

Local VLAN Capable: No

Traffic Classes: Enabled

Global GVRP Status: Disabled

GMRP: Disabled

Console#

show garp timer

This command shows the GARP timers for the selected interface.

Syntax

show garp timer [*interface*]

interface

ethernet *unit*/*port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-28)

port-channel *channel-id* (Range: 1-12)

Default Configuration

Shows all GARP timers.

Command Mode

Normal Exec, EXEC

Example

Console#show garp timer ethernet 1/1

Eth 1/ 1 GARP Timer Status:

Join Timer: 20 centiseconds

Leave Timer: 60 centiseconds

Leave All Timer: 1000 centiseconds

Console#

show gvrp configuration

This command shows if GVRP is enabled.

Syntax

show gvrp configuration [*interface*]

interface

ethernet *unit*/*port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-28)

port-channel *channel-id* (Range: 1-12)

Default Configuration

Shows both global and interface-specific configuration.

Command Mode

Normal Exec, EXEC

Example

Console#show gvrp configuration ethernet 1/7

Eth 1/ 7:

GVRP Configuration: Disabled

Console#

39.2 Editing VLAN Groups

vlan database

This command enters VLAN database mode. All commands in this mode will take effect immediately.

Default Configuration

None

Command Mode

Global Configuration

User Guidelines

- Use the VLAN database command mode to add, change, and delete VLANs. After finishing configuration changes, you can display the VLAN settings by entering the show vlan command.
- Use the interface vlan command mode to define the port membership mode and add or remove ports from a VLAN. The results of these commands are written to the running-configuration file, and you can display this file by entering the show running-config command.

Example

Console(config)#vlan database

Console(config-vlan)#

vlan

This command configures a VLAN. Use the no form to restore the default settings or delete a VLAN.

Syntax

vlan *vlan-id* [name *vlan-name*] media ethernet [state {active | suspend}] [rspan]

no vlan *vlan-id* [name | state]

vlan-id - VLAN ID, specified as a single number, a range of consecutive numbers separated by a hyphen, or multiple numbers separated by commas. (Range: 1-4094)

name - Keyword to be followed by the VLAN name.

vlan-name - ASCII string from 1 to 32 characters.

media ethernet - Ethernet media type.

state - Keyword to be followed by the VLAN state.

active - VLAN is operational.

suspend - VLAN is suspended. Suspended VLANs do not pass packets.

rspan - Keyword to create a VLAN used for mirroring traffic from remote switches. The VLAN used for RSPAN cannot include VLAN 1 (the switch's default VLAN), nor VLAN 4094 (the VLAN used for switch clustering). For more information on configuring RSPAN through the CLI, see "RSPAN Mirroring Commands".

Default Configuration

By default only VLAN 1 exists and is active.

Command Mode

VLAN Database Configuration

User Guidelines

- no vlan *vlan-id* deletes the VLAN.
- no vlan *vlan-id* name removes the VLAN name.
- no vlan *vlan-id* state returns the VLAN to the default state (i.e., active).
- You can configure up to 4094 VLANs on the switch.

Note:

The switch allows 256 user-manageable VLANs.

Example

The following example adds a VLAN, using VLAN ID 105 and name RD5. The VLAN is activated by default.

Console(config)#vlan database

Console(config-vlan)#vlan 105 name RD5 media ethernet

Console(config-vlan)#

39.3 Configuring VLAN Interfaces

interface vlan

This command enters interface configuration mode for VLANs, which is used to configure VLAN parameters for a physical interface.

Syntax

[no] interface vlan *vlan-id*

vlan-id - ID of the configured VLAN. (Range: 1-4094)

Default Configuration

None

Command Mode

Global Configuration

Example

The following example shows how to set the interface configuration mode to VLAN 1, and then assign an IP address to the VLAN:

Console(config)#interface vlan 1

Console(config-if)#ip add 192.168.1.254 255.255.255.0

Console(config-if)#

Switchport acceptable-frame-types

This command configures the acceptable frame types for a port. Use the no form to restore the default.

Syntax

switchport acceptable-frame-types {all | tagged}

no switchport acceptable-frame-types

all - The port accepts all frames, tagged or untagged.

tagged - The port only receives tagged frames.

Default Configuration

All frame types

Command Mode

Interface Configuration (Ethernet, Port Channel)

User Guidelines

When set to receive all frame types, any received frames that are untagged are assigned to the default VLAN.

Example

The following example shows how to restrict the traffic received on port 1 to tagged frames:

Console(config)#interface ethernet 1/1

Console(config-if)#switchport acceptable-frame-types tagged

Console(config-if)#

switchport trunk allowed vlan

This command configures VLAN groups on the selected interface in trunk mode. Use the no form to restore the default.

Syntax

switchport trunk allowed vlan {all | add *vlan-list* | remove *vlan-list*}

no switchport allowed vlan

all - List all of exist vlans to add.

add *vlan-list* - List of VLAN identifiers to add.

remove *vlan-list* - List of VLAN identifiers to remove.

vlan-list - Separate nonconsecutive VLAN identifiers with a comma and no spaces; use a hyphen to designate a range of IDs. (Range: 1-4094).

Default Configuration

All ports are assigned to VLAN 1 by default.

The default frame type is untagged.

Command Mode

Interface Configuration (Ethernet, Port Channel)

User Guidelines

- you can only assign an interface to VLAN groups as a tagged member.
- If a VLAN on the forbidden list for an interface is manually added to that interface, the VLAN is automatically removed from the forbidden list for that interface.

Example

The following example shows how to add VLANs 2, 5 and 6 to the allowed list as tagged VLANs for port 1:

Console(config)#interface ethernet 1/1

Console(config-if)#switchport trunk allowed vlan add 2,5,6

Console(config-if)#

switchport trunk native vlan

This command configures the PVID (i.e., default VLAN ID) for a port in trunk mode. Use the no form to restore the default.

Syntax

switchport trunk native vlan *vlan-id*

no switchport trunk native vlan

vlan-id - Default VLAN ID for a port. (Range: 1-4094)

Default Configuration

VLAN 1

Command Mode

Interface Configuration (Ethernet, Port Channel)

User Guidelines

If an interface is assigned to a new VLAN, its PVID is automatically set to the identifier for that VLAN.

Example

The following example shows how to set the PVID for port 1 to VLAN 3:

Console(config)#interface ethernet 1/1

Console(config-if)#switchport trunk native vlan 3

Console(config-if)#

switchport hybrid allowed vlan

This command configures VLAN groups on the selected interface in hybrid mode. Use the no form to restore the default.

Syntax

switchport hybrid allowed vlan { add *vlan-list* [tagged | untagged] | remove *vlan-list*}

no switchport hybrid allowed vlan

add *vlan-list* - List of VLAN identifiers to add.

remove *vlan-list* - List of VLAN identifiers to remove.

vlan-list - Separate nonconsecutive VLAN identifiers with a comma and no spaces; use a hyphen to designate a range of IDs. (Range: 1-4094).

Default Configuration

All ports are assigned to VLAN 1 by default.

The default frame type is untagged.

Command Mode

Interface Configuration (Ethernet, Port Channel)

User Guidelines

- you can assign an interface to VLAN groups as a tagged or untagged member.
- Frames are always tagged within the switch. The tagged/untagged parameter used when adding a VLAN to an interface tells the switch whether to keep or remove the tag from a frame on egress.
- If a VLAN on the forbidden list for an interface is manually added to that interface, the VLAN is automatically removed from the forbidden list for that interface.

Example

The following example shows how to add VLANs 2 as tagged VLANs for port 1:

Console(config)#interface ethernet 1/1

Console(config-if)#switchport hybrid allowed vlan add 2 tagged

Console(config-if)#

switchport hybrid pvid

This command configures the PVID (i.e., default VLAN ID) for a port in hybrid mode. Use the no form to restore the default.

Syntax

switchport hybrid pvid *vlan-id*

no switchport hybrid pvid

vlan-id - Default VLAN ID for a port. (Range: 1-4094)

Default Configuration

VLAN 1

Command Mode

Interface Configuration (Ethernet, Port Channel)

User Guidelines

If an interface is assigned to a new VLAN, its PVID is automatically set to the identifier for that VLAN.

Example

The following example shows how to set the PVID for port 1 to VLAN 3:

Console(config)#interface ethernet 1/1

Console(config-if)#switchport hybrid pvid 3

Console(config-if)#

switchport access vlan

This command configures the PVID (i.e., default VLAN ID) for a port in access mode. Use the no form to restore the default.

Syntax

switchport access vlan *vlan-id*

no switchport access vlan

vlan-id - Default VLAN ID for a port. (Range: 1-4094)

Default Configuration

VLAN 1

Command Mode

Interface Configuration (Ethernet, Port Channel)

User Guidelines

If an interface is assigned to a new VLAN, its PVID is automatically set to the identifier for that VLAN.

Example

The following example shows how to set the PVID for port 1 to VLAN 3:

Console(config)#interface ethernet 1/1

Console(config-if)#switchport access vlan 3

Console(config-if)#

switchport ingress-filtering

This command enables ingress filtering for an interface. Use the no form to restore the default.

Syntax

[no] switchport ingress-filtering disable

Default Configuration

Disabled

Command Mode

Interface Configuration (Ethernet, Port Channel)

User Guidelines

- Ingress filtering only affects tagged frames.
- If ingress filtering is disabled and a port receives frames tagged for VLANs for which it is not a member, these frames will be flooded to all other ports (except for those VLANs explicitly forbidden on this port).

- If ingress filtering is enabled and a port receives frames tagged for VLANs for which it is not a member, these frames will be discarded.
- Ingress filtering does not affect VLAN independent BPDU frames, such as GVRP or STA. However, they do affect VLAN dependent BPDU frames, such as GMRP.

Example

The following example shows how to set the interface to port 1 and then enable ingress filtering:

Console(config)#interface ethernet 1/1

Console(config-if)#switchport ingress-filtering disable

Console(config-if)#

switchport mode

This command configures the VLAN membership mode for a port. Use the no form to restore the default.

Syntax

switchport mode {access | hybrid | trunk}

no switchport mode

access - Specifies an access VLAN interface. The port transmits and receives untagged frames on a single VLAN only.

hybrid - Specifies a hybrid VLAN interface. The port may transmit tagged or untagged frames.

trunk - Specifies a port as an end-point for a VLAN trunk. A trunk is a direct link between two switches, so the port transmits tagged frames that identify the source VLAN. Note that frames belonging to the port's default VLAN (i.e., associated with the PVID) are also transmitted as tagged frames.

Default Configuration

All ports are in access mode with the PVID set to VLAN 1.

Command Mode

Interface Configuration (Ethernet, Port Channel)

User Guidelines

Access mode is mutually exclusive with VLAN trunking (see the vlan-trunking command). If VLAN trunking is enabled on an interface, then that interface cannot be set to access mode, and vice versa.

Example

The following shows how to set the configuration mode to port 1, and then set the switchport mode to hybrid:

Console(config)#interface ethernet 1/1

Console(config-if)#switchport mode hybrid

Console(config-if)#

show vlan

This command shows VLAN information.

Syntax

show vlan [all | id *vlan-id* | name *vlan-name*]

all - All VLANs.

id - Keyword to be followed by the VLAN ID.

vlan-id - ID of the configured VLAN. (Range: 1-4094)

name - Keyword to be followed by the VLAN name.

vlan-name - ASCII string from 1 to 32 characters.

Default Configuration

Shows all VLANs.

Command Mode

Normal Exec, EXEC

Example

The following example shows how to display information for VLAN 1:

```
Console#show vlan id 1
VLAN ID: 1
Type: Static
Name: DefaultVlan
Status: Active
Ports/Port Channels : Eth1/ 1(S) Eth1/ 2(S) Eth1/ 3(S) Eth1/ 4(S) Eth1/ 5(S)
Eth1/ 6(S) Eth1/ 7(S) Eth1/ 8(S) Eth1/ 9(S) Eth1/10(S)
Eth1/11(S) Eth1/12(S) Eth1/13(S) Eth1/14(S) Eth1/15(S)
Eth1/16(S) Eth1/17(S) Eth1/18(S) Eth1/19(S) Eth1/20(S)
Eth1/21(S) Eth1/22(S) Eth1/23(S) Eth1/24(S) Eth1/25(S)
Eth1/26(S) Eth1/27(S) Eth1/28(S)
Console#
```

39.4 Configuring QinQ

dot1q-tunnel system-tunnel-control

This command sets the switch to operate in QinQ mode. Use the no form to disable QinQ operating mode.

Syntax

[no] dot1q-tunnel system-tunnel-control

Default Configuration

Disabled

Command Mode

Global Configuration

User Guidelines

QinQ tunnel mode must be enabled on the switch for QinQ interface settings to be functional.

Example

```
Console(config)#dot1q-tunnel system-tunnel-control
Console(config)#
```

switchport dot1q-tunnel mode

This command configures an interface as a QinQ tunnel port. Use the no form to disable QinQ on the interface.

Syntax

switchport dot1q-tunnel mode {access | uplink}

no switchport dot1q-tunnel mode

access – Sets the port as an 802.1Q tunnel access port.

uplink – Sets the port as an 802.1Q tunnel uplink port.

Default Configuration

Disabled

Command Mode

Interface Configuration (Ethernet, Port Channel)

User Guidelines

- QinQ tunneling must be enabled on the switch using the dot1q-tunnel system-tunnel-control command before the switchport dot1q-tunnel mode interface command can take effect.

- When a tunnel uplink port receives a packet from a customer, the customer tag (regardless of whether there are one or more tag layers) is retained in the inner tag, and the service provider's tag added to the outer tag.
- When a tunnel uplink port receives a packet from the service provider, the outer service provider's tag is stripped off, and the packet passed on to the VLAN indicated by the inner tag. If no inner tag is found, the packet is passed onto the native VLAN defined for the uplink port.

Example

Console(config)#interface ethernet 1/1

Console(config-if)#switchport dot1q-tunnel mode access

Console(config-if)#

switchport dot1q-tunnel service match cvid

This command creates a CVLAN to SPVLAN mapping entry. Use the no form to delete a VLAN mapping entry.

Syntax

switchport dot1q-tunnel service *svid* match cvid *cvid*

svid - VLAN ID for the outer VLAN tag (Service Provider VID). (Range: 1-4094)

cvid - VLAN ID for the inner VLAN tag (Customer VID). (Range: 1-4094)

Default Configuration

Default mapping uses the PVID of the ingress port on the edge router for the SPVID.

Command Mode

Interface Configuration (Ethernet, Port Channel)

Example

This example sets the SVID to 99 in the outer tag for egress packets exiting port 1 when the packet's CVID is 2.

Console(config)#interface ethernet 1/1

Console(config-if)#switchport dot1q-tunnel service 99 match cvid 2

Console(config-if)#

1. Create VLANs 100, 200 and 300.

Console(config)#vlan database

Console(config-vlan)#vlan 100,200,300 media ethernet state active

2. Enable QinQ.

Console(config)#dot1q-tunnel system-tunnel-control

3. Configure port 2 as a tagged member of VLANs 100, 200 and 300 using uplink mode.

Console(config)#interface ethernet 1/2

Console(config-if)#switchport allowed vlan add 100,200,300 tagged

Console(config-if)#switchport dot1q-tunnel mode uplink

4. Configures port 1 as an untagged member of VLANs 100, 200 and 300 using access mode.

Console(config)#interface ethernet 1/1

Console(config-if)#switchport allowed vlan add 100,200,300 untagged

Console(config-if)#switchport dot1q-tunnel mode access

5. Configure the following selective QinQ mapping entries.

Console(config)#interface ethernet 1/1

Console(config-if)#switchport dot1q-tunnel service 100 match cvid 10

Console(config-if)#switchport dot1q-tunnel service 200 match cvid 20

Console(config-if)#switchport dot1q-tunnel service 300 match cvid 30

6. Configures port 1 as member of VLANs 10, 20 and 30 to avoid filtering out incoming frames tagged with VID 10, 20 or 30 on port 1

Console(config)#interface ethernet 1/1

Console(config-if)#switchport allowed vlan add 10,20,30

7. Verify configuration settings.

Console#show dot1q-tunnel service

802.1Q Tunnel Service Subscriptions

Port Match C-VID S-VID

-------- ---------- -----

Eth 1/ 1 10 100

Eth 1/ 1 20 200

Eth 1/ 1 30 300

Step 2. Configure Switch C.

1. Create VLAN 100, 200 and 300.

Console(config)#vlan database

Console(config-vlan)#vlan 100,200,300 media ethernet state active

2. Configure port 1 and port 2 as tagged members of VLAN 100, 200 and 300.

Console(config)#interface ethernet 1/1,2

Console(config-if)#switchport allowed vlan add 100,200,300 tagged

switchport dot1q-tunnel tpid

This command sets the Tag Protocol Identifier (TPID) value of a tunnel port. Use the no form to restore the default setting.

Syntax

switchport dot1q-tunnel tpid *tpid*

no switchport dot1q-tunnel tpid

tpid – Sets the ethertype value for 802.1Q encapsulation. This identifier is used to select a nonstandard 2-byte ethertype to identify 802.1Q tagged frames. The standard ethertype value is 0x8100. (Range: 0800-FFFF hexadecimal)

Default Configuration

0x8100

Command Mode

Interface Configuration (Ethernet, Port Channel)

User Guidelines

- Use the switchport dot1q-tunnel tpid command to set a custom 802.1Q ethertype value on the selected interface. This feature allows the switch to interoperate with third-party switches that do not use the standard 0x8100 ethertype to identify 802.1Q-tagged frames. For example, 0x1234 is set as the custom 802.1Q ethertype on a trunk port, incoming frames containing that ethertype are assigned to the VLAN contained in the tag following the ethertype field, as they would be with a standard 802.1Q trunk. Frames arriving on the port containing any other ethertype are looked upon as untagged frames, and assigned to the native VLAN of that port.
- The specified ethertype only applies to ports configured in Uplink mode using the switchport dot1q-tunnel mode command. If the port is in normal mode, the TPID is always 8100. If the port is in Access mode, received packets are processes as untagged packets.

Example

Console(config)#interface ethernet 1/1

Console(config-if)#switchport dot1q-tunnel tpid 9100

Console(config-if)#

show dot1q-tunnel

This command displays information about QinQ tunnel ports.

Syntax

show dot1q-tunnel [interface *interface* [service *svid*] |

service [*svid*]]

interface

ethernet *unit*/*port*

unit - Stack unit. (Range: 1)

port - Port number. (Range: 1-28)

port-channel *channel-id* (Range: 1-12)

svid - VLAN ID for the outer VLAN tag (SPVID). (Range: 1-4094)

Command Mode

EXEC

Example

Console#show dot1q-tunnel

QinQ Status: Disabled

QinQ TPID: 8100 (Hex)

Port Mode Priority Map

-------- ------ ----------

Eth 1/ 1 None Disabled

Eth 1/ 2 None Disabled

Eth 1/ 3 None Disabled

Eth 1/ 4 None Disabled

Eth 1/ 5 None Disabled

Eth 1/ 6 None Disabled

Eth 1/ 7 None Disabled

...

Console#show dot1q-tunnel interface ethernet 1/5

Port C-VID S-VID

-------- ---------- -----

Eth 1/ 5 1 100

Console#show dot1q-tunnel service 100

802.1Q Tunnel Service Subscriptions

Port C-VID S-VID

-------- ---------- -----

Eth 1/ 5 1 100

Eth 1/ 6 1 100

Console#

39.5 Configuring VLAN Translation

switchport vlan-translation

This command maps VLAN IDs between the customer and service provider.

Syntax

switchport vlan-translation *original-vlan new-vlan*

no switchport vlan-translation *original-vlan*

original-vlan - The original VLAN ID. (Range: 1-4094)

new-vlan - The new VLAN ID. (Range: 1-4094)

Default Configuration

Disabled

Command Mode

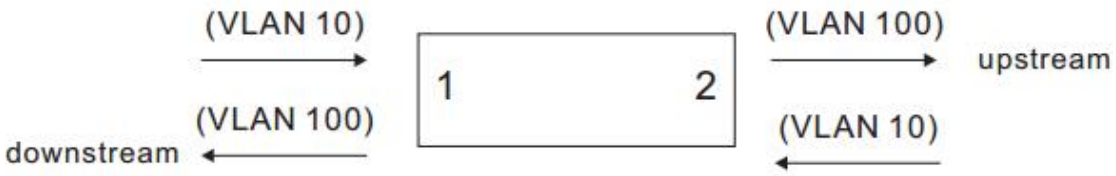
Interface Configuration (Ethernet)

User Guidelines

- If the next switch upstream does not support QinQ tunneling, then use this command to map the customer's VLAN ID to the service provider's VLAN ID for the upstream port. Similarly, if the next switch downstream does not support QinQ tunneling, then use this command to map the service provider's VLAN ID to the customer's VLAN ID for the downstream port. Note that one command maps both the *original-vlan* to *new-vlan* for ingress traffic and the *new-vlan* to *original-vlan* for egress traffic on the specified port.

For example, assume that the upstream switch does not support QinQ tunneling. If the command switchport vlan-translation 10 100 is used to map VLAN 10 to VLAN 100 for upstream traffic entering port 1, and VLAN 100 to VLAN 10 for downstream traffic leaving port 1, then the VLAN IDs will be swapped as shown below.

40. Configuring VLAN Translation



- The maximum number of VLAN translation entries is 8 per port, and up to 96 for the system. However, note that configuring a large number of entries may degrade the performance of other processes that also use the TCAM, such as IP Source Guard filter rules, Quality of Service (QoS) processes, QinQ, MAC-based VLANs, VLAN translation, or traps.
- If VLAN translation is set on an interface with this command, and the same interface is also configured as a QinQ access port with the switchport dot1q-tunnel mode command, VLAN tag assignments will be determined by the QinQ process, not by VLAN translation.

Example

This example configures VLAN translation for Port 1 as described in the

Command Usage section above.

Console(config)#vlan database

Console(config-vlan)#vlan 10 media ethernet state active

Console(config-vlan)#vlan 100 media ethernet state active

Console(config-vlan)#exit

Console(config)#interface ethernet 1/1,2

Console(config-if)#switchport allowed vlan add 10 tagged

Console(config-if)#switchport allowed vlan add 100 tagged

Console(config-if)#interface ethernet 1/1

Console(config-if)#switchport vlan-translation 10 100

Console(config-if)#end

Console#show vlan-translation

Interface Old VID New VID

--------- ------- -------

Eth 1/ 1 10 100

Console#

show vlan-translation

This command displays the configuration settings for VLAN translation.

Syntax

show vlan-translation [interface *interface*]

interface

ethernet *unit*/*port*

unit - Stack unit. (Range: 1)

port - Port number. (Range: 1-28)

Command Mode

EXEC

Example

Console#show vlan-translation

Interface Old VID New VID

--------- ------- -------

Eth 1/ 1 10 100

Console#

40.1 Configuring Port-based Traffic Segmentation

traffic-segmentation

This command enables traffic segmentation. Use the no form to disable traffic segmentation.

Syntax

[no] traffic-segmentation

Default Configuration

Disabled

Command Mode

Global Configuration

User Guidelines

- Traffic segmentation provides port-based security and isolation between ports within the VLAN. Data traffic on the downlink ports can only be forwarded to, and from, the designated uplink port(s). Data cannot pass between downlink ports in the same segmented group, nor to ports which do not belong to the same group.
- Traffic segmentation and normal VLANs can exist simultaneously within the same switch. Traffic may pass freely between uplink ports in segmented groups and ports in normal VLANs.
- When traffic segmentation is enabled, the forwarding state for the uplink and downlink ports assigned to different client sessions is shown below.
- When traffic segmentation is disabled, all ports operate in normal forwarding mode based on the settings specified by other functions such as VLANs and spanning tree protocol.
- Enter the traffic-segmentation command without any parameters to enable traffic segmentation. Then set the interface members for segmented groups using the traffic-segmentation uplink/downlink command.
- Enter no traffic-segmentation to disable traffic segmentation and clear the configuration settings for segmented groups.

Example

This example enables traffic segmentation globally on the switch.

Console(config)#traffic-segmentation

Console(config)#

traffic-segmentation session

This command creates a traffic-segmentation client session. Use the no form to remove a client session.

Syntax

[no] pvlan session *session-id*

session-id – Traffic segmentation session. (Range: 1-4)

Default Configuration

None

Command Mode

Global Configuration

Command Usage

- Use this command to create a new traffic-segmentation client session.
- Using the no form of this command will remove any assigned uplink or downlink ports, restoring these interfaces to normal operating mode.

Example

Console(config)#traffic-segmentation session 1

Console(config)#

traffic-segmentation uplink/downlink

This command configures the uplink and down-link ports for a segmented group of ports. Use the no form to remove a port from the segmented group.

Syntax

[no] traffic-segmentation [session *session-id*] {uplink *interface-list* [downlink *interface-list*] | downlink *interface-list*}

session-id – Traffic segmentation session. (Range: 1-4)

uplink – Specifies an uplink interface.

downlink – Specifies a downlink interface.

interface

ethernet *unit*/*port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-28)

port-channel *channel-id* (Range: 1-12)

Default Configuration

Session 1 if not defined

No segmented port groups are defined.

Command Mode

Global Configuration

User Guidelines

- A port cannot be configured in both an uplink and downlink list.
- A port can only be assigned to one traffic-segmentation session.
- When specifying an uplink or downlink, a list of ports may be entered by using a hyphen or comma in the *port* field. Note that lists are not supported for the *channel-id* field.
- A downlink port can only communicate with an uplink port in the same session. Therefore, if an uplink port is not configured for a session, the assigned downlink ports will not be able to communicate with any other ports.
- If a downlink port is not configured for the session, the assigned uplink ports will operate as normal ports.

Example

This example enables traffic segmentation, and then sets port 10 as the uplink and ports 5-8 as downlinks.

Console(config)#traffic-segmentation

Console(config)#traffic-segmentation uplink ethernet 1/10

downlink ethernet 1/5-8

Console(config)

traffic-segmentation uplink-to-uplink

This command specifies whether or not traffic can be forwarded between uplink ports assigned to different client sessions. Use the no form to restore the default.

Syntax

[no] traffic-segmentation uplink-to-uplink {blocking | forwarding}

blocking – Blocks traffic between uplink ports assigned to different sessions.

forwarding – Forwards traffic between uplink ports assigned to different sessions.

Default Configuration

Blocking

Command Mode

Global Configuration

Example

This example enables forwarding of traffic between uplink ports assigned to different client sessions.

Console(config)#traffic-segmentation uplink-to-uplink forwarding

Console(config)#

show traffic-segmentation

This command displays the configured traffic segments.

Command Mode

EXEC

Example

Console#show traffic-segmentation

Private VLAN Status: Enabled

Uplink-to-Uplink Mode: Forwarding

Session Uplink Ports Downlink Ports

--------- ------------------------------ ----------------------------

1 Ethernet 1/1 Ethernet 1/2

Ethernet 1/3

Ethernet 1/4

Console#

40.2 Configuring Protocol-based VLANs

protocol-vlan protocol-group (Configuring Groups)

This command creates a protocol group, or to add specific protocols to a group. Use the no form to remove a protocol group.

Syntax

protocol-vlan protocol-group *group-id* [{add | remove} frame-type *frame* protocol-type *protocol*]

no protocol-vlan protocol-group *group-id*

group-id - Group identifier of this protocol group. (Range: 1-2147483647)

frame - Frame type used by this protocol. (Options: ethernet, rfc_1042, llc_other)

protocol - Protocol type. The only option for the llc_other frame type is ipx_raw. The options for all other frames types include: arp, ip, ipv6, rarp.

Default Configuration

No protocol groups are configured.

Command Mode

Global Configuration

Example

The following creates protocol group 1, and specifies Ethernet frames with IP and ARP protocol types:

Console(config)#protocol-vlan protocol-group 1 add frame-type ethernet

protocol-type ip

Console(config)#protocol-vlan protocol-group 1 add frame-type ethernet
protocol-type arp
Console(config)#

protocol-vlan protocol-group (Configuring Interfaces)

This command maps a protocol group to a VLAN for the current interface. Use the no form to remove the protocol mapping for this interface.

Syntax

protocol-vlan protocol-group *group-id* vlan *vlan-id* priority *priority*

no protocol-vlan protocol-group *group-id* vlan

group-id - Group identifier of this protocol group. (Range: 1-2147483647)

vlan-id - VLAN to which matching protocol traffic is forwarded. (Range: 1-4094)

priority - The priority assigned to untagged ingress traffic. (Range: 0-7, where 7 is the highest priority)

Default Configuration

No protocol groups are mapped for any interface.

Command Mode

Interface Configuration (Ethernet, Port Channel)

User Guidelines

- When creating a protocol-based VLAN, only assign interfaces via this command. If you assign interfaces using any of the other VLAN commands (such as the vlan command), these interfaces will admit traffic of any protocol type into the associated VLAN.
- When MAC-based, IP subnet-based, and protocol-based VLANs are supported concurrently, priority is applied in this sequence, and then port-based VLANs last.
- When a frame enters a port that has been assigned to a protocol VLAN, it is processed in the following manner:

a. If the frame is tagged, it will be processed according to the standard rules applied to tagged frames.
b. If the frame is untagged and the protocol type matches, the frame is forwarded to the appropriate VLAN.
c. If the frame is untagged but the protocol type does not match, the frame is forwarded to the default VLAN for this interface.

Example

The following example maps the traffic entering Port 1 which matches the protocol type specified in protocol group 1 to VLAN 2.

Console(config)#interface ethernet 1/1
Console(config-if)#protocol-vlan protocol-group 1 vlan 2
Console(config-if)#

show protocol-vlan protocol-group

This command shows the frame and protocol type associated with protocol groups.

Syntax

show protocol-vlan protocol-group [*group-id*]

group-id - Group identifier for a protocol group. (Range: 1-2147483647)

Default Configuration

All protocol groups are displayed.

Command Mode

EXEC

Example

This shows protocol group 1 configured for IP over Ethernet:

Console#show protocol-vlan protocol-group

Protocol Group ID Frame Type Protocol Type

---------- ---------- ----------

1 ethernet 08 00

Console#

show interfaces protocol-vlan protocol-group

This command shows the mapping from protocol groups to VLANs for the selected interfaces.

Syntax

show interfaces protocol-vlan protocol-group [*interface*]

interface

ethernet *unit*/*port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-28)

port-channel *channel-id* (Range: 1-12)

Default Configuration

The mapping for all interfaces is displayed.

Command Mode

EXEC

Example

This shows that traffic entering Port 1 that matches the specifications for protocol group 1 will be mapped to VLAN 2:

Console#show interfaces protocol-vlan protocol-group

Port ProtocolGroup ID VLAN ID

---------- ---------- ----------

Eth 1/1 1 vlan2

Console#

40.3 Configuring IP Subnet VLANs

subnet-vlan

This command configures IP Subnet VLAN assignments. Use the no form to remove an IP subnet-to-VLAN assignment.

Syntax

subnet-vlan subnet *ip-address mask* vlan *vlan-id* [priority *priority*]

no subnet-vlan subnet {*ip-address mask* | all}

ip-address – The IP address that defines the subnet. Valid IP addresses consist of four decimal numbers, 0 to 255, separated by periods.

mask – This mask identifies the host address bits of the IP subnet.

vlan-id – VLAN to which matching IP subnet traffic is forwarded. (Range: 1-4094)

priority – The priority assigned to untagged ingress traffic. (Range: 0-7, where 7 is the highest priority)

Default Configuration

Priority: 0

Command Mode

Global Configuration

User Guidelines

- Each IP subnet can be mapped to only one VLAN ID. An IP subnet consists of an IP address and a subnet mask. The specified VLAN need not be an existing VLAN.
- When an untagged frame is received by a port, the source IP address is checked against the IP subnet-to-VLAN mapping table, and if an entry is found, the corresponding VLAN ID is assigned to the frame. If no mapping is found, the PVID of the receiving port is assigned to the frame.
- The IP subnet cannot be a broadcast or multicast IP address.
- When MAC-based, IP subnet-based, and protocol-based VLANs are supported concurrently, priority is applied in this sequence, and then port-based VLANs last.

Example

The following example assigns traffic for the subnet 192.168.12.192, mask 255.255.255.224, to VLAN 4.

Console(config)#subnet-vlan subnet 192.168.12.192 255.255.255.224 vlan 4

Console(config)#

show subnet-vlan

This command displays IP Subnet VLAN assignments.

Command Mode

EXEC

User Guidelines

- Use this command to display subnet-to-VLAN mappings.
- The last matched entry is used if more than one entry can be matched.

Example

The following example displays all configured IP subnet-based VLANs.

Console#show subnet-vlan

IP Address Mask VLAN ID Priority

--- --- --- ---

192.168.12.0 255.255.255.128 1 0

192.168.12.128 255.255.255.192 3 0

192.168.12.192 255.255.255.224 4 0

192.168.12.224 255.255.255.240 5 0

192.168.12.240 255.255.255.248 6 0

192.168.12.248 255.255.255.252 7 0

192.168.12.252 255.255.255.254 8 0

192.168.12.254 255.255.255.255 9 0

192.168.12.255 255.255.255.255 10 0

Console#

40.4 Configuring MAC Based VLANs

When using IEEE 802.1Q port-based VLAN classification, all untagged frames received by a port are classified as belonging to the VLAN whose VID (PVID) is associated with that port.

When MAC-based VLAN classification is enabled, the source address of untagged ingress frames are checked against the MAC address-to-VLAN mapping table. If an entry is found for that address, these frames are assigned to the VLAN indicated in the entry. If no MAC address is matched, the untagged frames are classified as belonging to the receiving port's VLAN ID (PVID).

mac-vlan

This command configures MAC address-to-VLAN mapping. Use the no form to remove an assignment.

Syntax

mac-vlan mac-address *mac-address* vlan *vlan-id* [priority *priority*]

no mac-vlan mac-address {*mac-address* | all}

mac-address – The source MAC address to be matched. Configured MAC addresses can only be unicast addresses. The MAC address must be specified in the format xx-xx-xx-xx-xx-xx or xxxxxxxxxxxx.

vlan-id – VLAN to which the matching source MAC address traffic is forwarded. (Range: 1-4094)

priority – The priority assigned to untagged ingress traffic. (Range: 0-7, where 7 is the highest priority)

Default Configuration

None

Command Mode

Global Configuration

User Guidelines

- The MAC-to-VLAN mapping applies to all ports on the switch.
- Source MAC addresses can be mapped to only one VLAN ID.
- Configured MAC addresses cannot be broadcast or multicast addresses.
- When MAC-based, IP subnet-based, and protocol-based VLANs are supported concurrently, priority is applied in this sequence, and then port-based VLANs last.

Example

The following example assigns traffic from source MAC address 64-9D-99-11-22-33 to VLAN 10.

Console(config)#mac-vlan mac-address 64-9D-99-11-22-33 vlan 10

Console(config)#

show mac-vlan

This command displays MAC address-to-VLAN assignments.

Command Mode

EXEC

User Guidelines

Use this command to display MAC address-to-VLAN mappings.

Example

The following example displays all configured MAC address-based VLANs.

Console#show mac-vlan

MAC Address VLAN ID Priority

----------------- -------- --------

64-9D-99-11-22-33 10 0

Console#

40.5 Configuring Voice VLANs

voice vlan

This command enables VoIP traffic detection and defines the Voice VLAN ID. Use the no form to disable the Voice VLAN.

Syntax

voice vlan *voice-vlan-id*

no voice vlan

voice-vlan-id - Specifies the voice VLAN ID. (Range: 1-4094)

Default Configuration

Disabled

Command Mode

Global Configuration

User Guidelines

- When IP telephony is deployed in an enterprise network, it is recommended to isolate the Voice over IP (VoIP) network traffic from other data traffic. Traffic isolation helps prevent excessive packet delays, packet loss, and jitter, which results in higher voice quality. This is best achieved by assigning all VoIP traffic to a single VLAN.
- VoIP traffic can be detected on switch ports by using the source MAC address of packets, or by using LLDP (IEEE 802.1AB) to discover connected VoIP devices. When VoIP traffic is detected on a configured port, the switch automatically assigns the port as a tagged member of the Voice VLAN.
- Only one Voice VLAN is supported and it must already be created on the switch before it can be specified as the Voice VLAN.
- The Voice VLAN ID cannot be modified when the global auto-detection status is enabled (see the switchport voice vlan command.

Example

The following example enables VoIP traffic detection and specifies the Voice VLAN ID as 1234.

Console(config)#voice vlan 1234

Console(config)#

voice vlan aging

This command sets the Voice VLAN ID time out. Use the no form to restore the default.

Syntax

voice vlan aging *minutes*

no voice vlan

minutes - Specifies the port Voice VLAN membership time out. (Range: 5-43200 minutes)

Default Configuration

1440 minutes

Command Mode

Global Configuration

User Guidelines

The Voice VLAN aging time is the time after which a port is removed from the Voice VLAN when VoIP traffic is no longer received on the port.

Example

The following example configures the Voice VLAN aging time as 3000 minutes.

Console(config)#voice vlan aging 3000

Console(config)#

voice vlan mac-address

This command specifies MAC address ranges to add to the OUI Telephony list. Use the no form to remove an entry from the list.

Syntax

voice vlan mac-address *mac-address* mask *mask-address* [description *description*]

no voice vlan mac-address *mac-address* mask *mask-address*

mac-address - Defines a MAC address OUI that identifies VoIP devices in the network. (For example, 01-23-45-00-00-00)

mask-address - Identifies a range of MAC addresses. (Range: 80-00-00-00-00-00 to FF-FF-FF-FF-FF-FF)

description - User-defined text that identifies the VoIP devices. (Range: 1-32 characters)

Default Configuration

None

Command Mode

Global Configuration

User Guidelines

- VoIP devices attached to the switch can be identified by the manufacturer's Organizational Unique Identifier (OUI) in the source MAC address of received packets. OUI numbers are assigned to manufacturers and form the first three octets of device MAC addresses. The MAC OUI numbers for VoIP equipment can be configured on the switch so that traffic from these devices is recognized as VoIP.
- Selecting a mask of FF-FF-FF-00-00-00 identifies all devices with the same OUI (the first three octets). Other masks restrict the MAC address range. Selecting FF-FF-FF-FF-FF-FF specifies a single MAC address.

Example

The following example adds a MAC OUI to the OUI Telephony list.

Console(config)#voice vlan mac-address 00-12-34-56-78-90 mask ff-ff-ff-00-00-
00 description A new phone

Console(config)#

switchport voice vlan

This command specifies the Voice VLAN mode for ports. Use the no form to disable the Voice VLAN feature on the port.

Syntax

switchport voice vlan {manual | auto}

no switchport voice vlan

manual - The Voice VLAN feature is enabled on the port, but the port must be manually added to the Voice VLAN.

auto - The port will be added as a tagged member to the Voice VLAN when VoIP traffic is detected on the port.

Default Configuration

Disabled

Command Mode

Interface Configuration

User Guidelines

- When auto is selected, you must select the method to use for detecting VoIP traffic, either OUI or 802.1ab (LLDP) using the switchport voice vlan rule command. When OUI is selected, be sure to configure the MAC address ranges in the Telephony OUI list using the voice vlan mac-address command.
- All ports are set to VLAN hybrid mode by default. Prior to enabling VoIP for a port (by setting the VoIP mode to Auto or Manual as described below), ensure that VLAN membership is not set to access mode using the switchport mode command.

Example

The following example sets port 1 to Voice VLAN auto mode.

Console(config)#interface ethernet 1/1

Console(config-if)#switchport voice vlan auto

Console(config-if)#

switchport voice vlan priority

This command specifies a CoS priority for VoIP traffic on a port. Use the no form to restore the default priority on a port.

Syntax

switchport voice vlan priority *priority-value*

no switchport voice vlan priority

priority-value - The CoS priority value. (Range: 0-6)

Default Configuration

6

Command Mode

Interface Configuration

User Guidelines

Specifies a CoS priority to apply to the port VoIP traffic on the Voice VLAN. The priority of any received VoIP packet is overwritten with the new priority when the Voice VLAN feature is active for the port.

Example

The following example sets the CoS priority to 5 on port 1.

Console(config)#interface ethernet 1/1

Console(config-if)#switchport voice vlan priority 5

Console(config-if)#

switchport voice vlan rule

This command selects a method for detecting VoIP traffic on a port. Use the no form to disable the detection method on the port.

Syntax

[no] switchport voice vlan rule {oui | lldp}

oui - Traffic from VoIP devices is detected by the Organizationally Unique Identifier (OUI) of the source MAC address.

lldp - Uses LLDP to discover VoIP devices attached to the port.

Default Configuration

OUI: Enabled

LLDP: Disabled

Command Mode

Interface Configuration

User Guidelines

- When OUI is selected, be sure to configure the MAC address ranges in the Telephony OUI list (see the voice vlan mac-address command. MAC address OUI numbers must be configured in the Telephony OUI list so that the switch recognizes the traffic as being from a VoIP device.
- LLDP checks that the “telephone bit” in the system capability TLV is turned on. See "LLDP Commands" for more information on LLDP.

Example

The following example enables the OUI method on port 1 for detecting VoIP traffic.

Console(config)#interface ethernet 1/1

Console(config-if)#switchport voice vlan rule oui

Console(config-if)#

switchport voice vlan security

This command enables security filtering for VoIP traffic on a port. Use the no form to disable filtering on a port.

Syntax

[no] switchport voice vlan security

Default Configuration

Disabled

Command Mode

Interface Configuration

User Guidelines

- Security filtering discards any non-VoIP packets received on the port that are tagged with the voice VLAN ID. VoIP traffic is identified by source MAC addresses configured in the Telephony OUI list, or through LLDP that discovers VoIP devices attached to the switch. Packets received from non-VoIP sources are dropped.
- When enabled, be sure the MAC address ranges for VoIP devices are configured in the Telephony OUI list (voice vlan mac-address).

Example

The following example enables security filtering on port 1.

Console(config)#interface ethernet 1/1

Console(config-if)#switchport voice vlan security

Console(config-if)#

show voice vlan

This command displays the Voice VLAN settings on the switch and the OUI Telephony list.

Syntax

show voice vlan {oui | status}

oui - Displays the OUI Telephony list.

status - Displays the global and port Voice VLAN settings.

Default Configuration

None

Command Mode

EXEC

Example

Console#show voice vlan status

Global Voice VLAN Status

Voice VLAN Status : Enabled

Voice VLAN ID : 1234

Voice VLAN aging time : 1440 minutes

Voice VLAN Port Summary

Port Mode Security Rule Priority Remaining Age

(minutes)

-------- -------- -------- --------- -------- -------------

Eth 1/ 1 Auto Enabled OUI 6 100

Eth 1/ 2 Disabled Disabled OUI 6 NA

Eth 1/ 3 Manual Enabled OUI 5 100

Eth 1/ 4 Auto Enabled OUI 6 100

Eth 1/ 5 Disabled Disabled OUI 6 NA

Eth 1/ 6 Disabled Disabled OUI 6 NA

Eth 1/ 7 Disabled Disabled OUI 6 NA

Eth 1/ 8 Disabled Disabled OUI 6 NA

Eth 1/ 9 Disabled Disabled OUI 6 NA

Eth 1/10 Disabled Disabled OUI 6 NA

Console#show voice vlan oui

OUI Address Mask Description

---------- ---------- ----------

00-12-34-56-78-9A FF-FF-FF-00-00-00 old phones

00-11-22-33-44-55 FF-FF-FF-00-00-00 new phones

00-98-76-54-32-10 FF-FF-FF-FF-FF-FF Chris' phone

Console#

41. Class of Service Commands

41.1 Priority Commands (Layer 2)

queue mode

This command sets the scheduling mode used for processing each of the class of service (CoS) priority queues. The options include strict priority, Weighted Round-Robin (WRR), or a combination of strict and weighted queuing. Use the no form to restore the default value.

Syntax

queue mode {strict | wrr | strict-wrr [*queue-type-list*]}

no queue mode

strict - Services the egress queues in sequential order, transmitting all traffic in the higher priority queues before servicing lower priority queues. This ensures that the highest priority packets are always serviced first, ahead of all other traffic.

wrr - Weighted Round-Robin shares bandwidth at the egress ports by using scheduling weights (based on the queue weight command), and servicing each queue in a round-robin fashion.

strict-wrr - Strict priority is used for the high-priority queues and WRR for the rest of the queues.

queue-type-list - Indicates if the queue is a normal or strict type. (Options: 0 indicates a normal queue, 1 indicates a strict queue)

Default Configuration

WRR

Command Mode

Global Configuration

User Guidelines

- The switch can be set to service the port queues based on strict priority, WRR, or a combination of strict and weighted queuing.
- Strict priority requires all traffic in a higher priority queue to be processed before lower priority queues are serviced.
- Weighted Round Robin (WRR) uses a predefined relative weight for each queue that determines the percentage of service time the switch services each queue before moving on to the next queue. This prevents the head-of-line blocking that can occur with strict priority queuing. Use the queue weight command to assign weights for WRR queuing to the eight priority queues.
- If Strict and WRR mode is selected, a combination of strict service is used for the high priority queues and weighted service for the remaining queues. The queues assigned to use strict priority should be specified using the Strict Mode field parameter.
- A weight can be assigned to each of the weighted queues (and thereby to the corresponding traffic priorities). This weight sets the frequency at which each queue is polled for service, and subsequently affects the response time for software applications assigned a specific priority value.
- Service time is shared at the egress ports by defining scheduling weights for WRR, or for the queuing mode that uses a combination of strict and weighted queuing. Service time is allocated to each queue by calculating a precise number of bytes per second that will be serviced on each round.
- The specified queue mode applies to all interfaces.

- Protocols used to synchronize distributed switches use packets of 1588 bytes to control the synchronization process. This switch therefore assigns packets of this size to the highest priority queue to ensure quick passage.

Example

The following example sets the queue mode to strict priority service mode:

Console(config)#queue mode strict

Console(config)#

queue weight

This command assigns weights to the eight class of service (CoS) priority queues when using weighted queuing, or one of the queuing modes that use a combination of strict and weighted queuing. Use the no form to restore the default weights.

Syntax

queue weight *weight0...weight7*

no queue weight

weight0...weight7 - The ratio of weights for queues 0 – 7 determines the weights used by the WRR scheduler. (Range: 1-255)

Default Configuration

Weights 1, 2, 4, 6, 8, 10, 12, 14 are assigned to queues 0 - 7 respectively.

Command Mode

Global Configuration

User Guidelines

- This command shares bandwidth at the egress port by defining scheduling weights for Weighted Round-Robin, or for the queuing mode that uses a combination of strict and weighted queuing.
- Bandwidth is allocated to each queue by calculating a precise number of bytes per second that will be serviced on each round.

Example

The following example shows how to assign round-robin weights of 1 - 4 to the CoS priority queues 0 - 7.

Console(config)#queue weight 1 2 3 4 5 6 7 8

Console(config)#

switchport priority default

This command sets a priority for incoming untagged frames. Use the no form to restore the default value.

Syntax

switchport priority default *default-priority-id*

no switchport priority default

default-priority-id - The priority number for untagged ingress traffic. The priority is a number from 0 to 7. Seven is the highest priority.

Default Configuration

The priority is not set, and the default value for untagged frames received on the interface is zero.

Command Mode

Interface Configuration (Ethernet, Port Channel)

User Guidelines

- The precedence for priority mapping is IP DSCP, and then default switchport priority.
- The default priority applies for an untagged frame received on a port set to accept all frame types (i.e, receives both untagged and tagged frames). This priority does not apply to IEEE 802.1Q VLAN tagged frames. If the incoming frame is an IEEE 802.1Q VLAN tagged frame, the IEEE 802.1p User Priority bits will be used.

- The switch provides eight priority queues for each port. It can be configured to use strict priority queuing, Weighted Round Robin (WRR), or a combination of strict and weighted queuing using the queue mode command. Inbound frames that do not have VLAN tags are tagged with the input port's default ingress user priority, and then placed in the appropriate priority queue at the output port. The default priority for all ingress ports is zero. Therefore, any inbound frames that do not have priority tags will be placed in queue 2 of the output port. (Note that if the output port is an untagged member of the associated VLAN, these frames are stripped of all VLAN tags prior to transmission.)

Example

The following example shows how to set a default priority on port 3 to 5:

Console(config)#interface ethernet 1/3

Console(config-if)#switchport priority default 5

Console(config-if)#

show queue mode

This command shows the current queue mode.

Command Mode

EXEC

Example

Console#show queue mode

Queue Mode : Weighted Round Robin Mode

Console#

show queue weight

This command displays the weights used for the weighted queues.

Command Mode

EXEC

Example

Console#show queue weight

Queue ID Weight

-------- ------

0 1

1 2

2 4

3 6

4 8

5 10

6 12

7 14

Console#

qos map cos-dscp

This command maps CoS/CFI values in incoming packets to per-hop behavior and drop precedence values for priority processing. Use the no form to restore the default settings.

Syntax

qos map cos-dscp *phb drop-precedence* from *cos0 cfi0...cos7 cfi7*

no qos map cos-dscp *cos0 cfi0...cos7 cfi7*

phb - Per-hop behavior, or the priority used for this router hop. (Range: 0-7)

drop-precedence - Drop precedence used in controlling traffic congestion. (Range: 0 - Green, 3 - Yellow, 1 - Red)

cos - CoS value in ingress packets. (Range: 0-7)

cfi - Canonical Format Indicator. Set to this parameter to "0" to indicate that the MAC address information carried in the frame is in canonical format. (Range: 0-1)

42. Default Configuration

Default Mapping of CoS/CFI to Internal PHB/Drop Precedence

Command Mode

Interface Configuration (Port, Static Aggregation)

User Guidelines

- The default mapping of CoS to PHB values is based on the recommended settings in IEEE 802.1p for mapping CoS values to output queues.
- Enter a value pair for the internal per-hop behavior and drop precedence, followed by the keyword "from" and then up to eight CoS/ CFI paired values separated by spaces.
- If a packet arrives with a 802.1Q header but it is not an IP packet, then the CoS/CFI-to-PHB/Drop Precedence mapping table is used to generate priority and drop precedence values for internal processing. Note that priority tags in the original packet are not modified by this command.
- The internal DSCP consists of three bits for per-hop behavior (PHB) which determines the queue to which a packet is sent; and two bits for drop precedence (namely color) which is used to control traffic congestion.
- The specified mapping applies to all interfaces.

Example

Console(config)#interface ethernet 1/5

Console(config-if)#qos map cos-dscp 0 0 from 0 1

Console(config-if)#

qos map dscp-mutation

This command maps DSCP values in incoming packets to per-hop behavior and drop precedence values for priority processing. Use the no form to restore the default settings.

Syntax

qos map dscp-mutation *phb drop-precedence* from *dscp0 ... dscp7*

no qos map dscp-mutation *dscp0 ... dscp7*

phb - Per-hop behavior, or the priority used for this router hop. (Range: 0-7)

drop-precedence - Drop precedence used in controlling traffic congestion. (Range: 0 - Green, 3 - Yellow, 1 - Red)

dscp - DSCP value in ingress packets. (Range: 0-63)

Default Configuration

Default Mapping of DSCP Values to Internal PHB/Drop Values

Command Mode

Interface Configuration (Port, Static Aggregation)

User Guidelines

- Enter a value pair for the internal per-hop behavior and drop precedence, followed by the keyword "from" and then up to eight DSCP values separated by spaces.
- This map is only used when the QoS mapping mode is set to "DSCP" by the qos map trust-mode command, and the ingress packet type is IPv4.
- Two QoS domains can have different DSCP definitions, so the DSCP-toPHB/Drop Precedence mutation map can be used to modify one set of DSCP values to match the definition of another domain. The mutation map should be applied at the receiving port (ingress mutation) at the boundary of a QoS administrative domain.
- The specified mapping applies to all interfaces.

Example

This example changes the priority for all packets entering port 1 which contain a DSCP value of 1 to a per-hop behavior of 3 and a drop precedence of 1. Referring to mapping table, note that the DSCP value for these packets is now set to 25 ($3x2^3+1$) and passed on to the egress interface.

Console(config)#interface ethernet 1/5

Console(config-if)#qos map dscp-mutation 3 1 from 1

Console(config-if)#

qos map phb-queue

This command determines the hardware output queues to use based on the internal per-hop behavior value. Use the no form to restore the default settings.

Syntax

qos map phb-queue *queue-id* from *phb0 ... phb7*

no map phb-queue *phb0 ... phb7*

phb - Per-hop behavior, or the priority used for this router hop. (Range: 0-7)

queue-id - The ID of the priority queue. (Range: 0-7, where 7 is the highest priority queue)

Default Configuration

Mapping Internal Per-hop Behavior to Hardware Queues

Command Mode

Interface Configuration (Port, Static Aggregation)

User Guidelines

- Enter a queue identifier, followed by the keyword "from" and then up to eight internal per-hop behavior values separated by spaces.
- Egress packets are placed into the hardware queues according to the mapping defined by this command.

Example

Console(config)#interface ethernet 1/5

Console(config-if)#qos map phb-queue 0 from 1 2 3

Console(config-if)#

qos map trust-mode

This command sets QoS mapping to DSCP or CoS. Use the no form to restore the default setting.

Syntax

qos map trust-mode {dscp | cos}

no qos map trust-mode

dscp - Sets the QoS mapping mode to DSCP.

cos - Sets the QoS mapping mode to CoS.

Default Configuration

CoS

Command Mode

Interface Configuration (Port)

User Guidelines

- If the QoS mapping mode is set to DSCP with this command, and the ingress packet type is IPv4, then priority processing will be based on the DSCP value in the ingress packet.
- If the QoS mapping mode is set to DSCP, and a non-IP packet is received, the packet's CoS and CFI (Canonical Format Indicator) values are used for priority processing if the packet is tagged. For an untagged packet, the default port priority is used for priority processing.

- If the QoS mapping mode is set to CoS with this command, and the ingress packet type is IPv4, then priority processing will be based on the CoS and CFI values in the ingress packet. For an untagged packet, the default port priority is used for priority processing.

Example

This example sets the QoS priority mapping mode to use DSCP based on the conditions described in the Command Usage section.

Console(config)#interface ge1/1

Console(config-if)#qos map trust-mode dscp

Console(config-if)#

show qos map cos-dscp

This command shows ingress CoS/CFI to internal DSCP map.

Syntax

show qos map cos-dscp interface *interface*

interface

ethernet *unit*/*port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-28)

port-channel *channel-id* (Range: 1-12)

Command Mode

EXEC

Example

Console#show qos map cos-dscp interface ethernet 1/5

CoS Information of Eth 1/5

CoS-DSCP map.(x,y),x: PHB,y: drop precedence:

CoS : CFI 0 1

---

0 (0,0) (0,0)

1 (1,0) (1,0)

2 (2,0) (2,0)

3 (3,0) (3,0)

4 (4,0) (4,0)

5 (5,0) (5,0)

6 (6,0) (6,0)

7 (7,0) (7,0)

Console#

show qos map dscp-mutation

This command shows the ingress DSCP to internal DSCP map.

Syntax

show qos map dscp-mutation interface *interface*

interface

ethernet *unit*/*port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-28)

port-channel *channel-id* (Range: 1-12)

Command Mode

EXEC

User Guidelines

This map is only used when the QoS mapping mode is set to "DSCP" by the qos map trust-mode command, and the ingress packet type is IPv4.

Example

The ingress DSCP is composed of "d1" (most significant digit in the left column) and "d2" (least significant digit in the top row (in other words, ingress DSCP = d1 * 10 + d2); and the corresponding Internal DSCP and drop precedence is shown at the intersecting cell in the table.

Console#show qos map dscp-mutation interface ethernet 1/5

Information of Eth 1/5

DSCP mutation map. (x,y),x: PHB,y: drop precedence:

d1: d2 0 1 2 3 4 5 6 7 8 9

0: (0,0) (0,1) (0,0) (0,3) (0,0) (0,1) (0,0) (0,3) (1,0) (1,1)

1: (1,0) (1,3) (1,0) (1,1) (1,0) (1,3) (2,0) (2,1) (2,0) (2,3)

2: (2,0) (2,1) (2,0) (2,3) (3,0) (3,1) (3,0) (3,3) (3,0) (3,1)

3: (3,0) (3,3) (4,0) (4,1) (4,0) (4,3) (4,0) (4,1) (4,0) (4,3)

4: (5,0) (5,1) (5,0) (5,3) (5,0) (5,1) (6,0) (5,3) (6,0) (6,1)

5: (6,0) (6,3) (6,0) (6,1) (6,0) (6,3) (7,0) (7,1) (7,0) (7,3)

6: (7,0) (7,1) (7,0) (7,3)

Console#

show qos map phb-queue

This command shows internal per-hop behavior to hardware queue map.

Syntax

show qos map phb-queue interface *interface*

interface

ethernet *unit*/*port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-28)

port-channel *channel-id* (Range: 1-12)

Command Mode

EXEC

Example

Console#show qos map phb-queue interface ethernet 1/5

Information of Eth 1/5

PHB-queue map:

PHB: 0 1 2 3 4 5 6 7

Queue: 2 0 1 3 4 5 6 7

Console#

show qos map trust-mode

This command shows the QoS mapping mode.

Syntax

show qos map trust-mode interface *interface*

interface

ethernet *unit*/*port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-28)

Command Mode

EXEC

Example

The following shows that the trust mode is set to CoS:

Console#show qos map trust-mode interface ethernet 1/5

Information of Eth 1/5

CoS Map Mode: CoS mode

Console#

43. Quality of Service (QoS) Commands

class-map

This command creates a class map used for matching packets to the specified class, and enters Class Map configuration mode. Use the no form to delete a class map.

Syntax

[no] class-map *class-map-name* [match-any]

class-map-name - Name of the class map. (Range: 1-32 characters)

match-any - Match any condition within a class map.

Default Configuration

None

Command Mode

Global Configuration

User Guidelines

- First enter this command to designate a class map and enter the Class Map configuration mode. Then use match commands to specify the criteria for ingress traffic that will be classified under this class map.
- One or more class maps can be assigned to a policy map. The policy map is then bound by a service policy to an interface. A service policy defines packet classification, service tagging, and bandwidth policing. Once a policy map has been bound to an interface, no additional class maps may be added to the policy map, nor any changes made to the assigned class maps with the match or set commands.

Example

This example creates a class map call "rd-class," and sets it to match packets marked for DSCP service value 3:

Console(config)#class-map rd-class match-any

Console(config-cmap)#match ip dscp 3

Console(config-cmap)#

description

This command specifies the description of a class map or policy map.

Syntax

description *string*

string - Description of the class map or policy map. (Range: 1-64 characters)

Command Mode

Class Map Configuration

Policy Map Configuration

Example

Console(config)#class-map rd-class#1

Console(config-cmap)#description matches packets marked for DSCP service value 3

Console(config-cmap)#

match

This command defines the criteria used to classify traffic. Use the no form to delete the matching criteria.

Syntax

[no] match {access-list *acl-name* | cos *cos* | ip dscp *dscp* | ip precedence *ip-precedence* | ipv6 dscp *dscp* | source-port *interface* | vlan *vlan*}

acl-name - Name of the access control list. Any type of ACL can be specified, including standard or extended IPv4/IPv6 ACLs and MAC ACLs. (Range: 1-16 characters)

cos - A Class of Service value. (Range: 0-7)

dscp - A Differentiated Service Code Point value. (Range: 0-63)

ip-precedence - An IP Precedence value. (Range: 0-7)

interface

unit/*port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-28)

vlan - A VLAN. (Range:1-4094)

Default Configuration

None

Command Mode

Class Map Configuration

User Guidelines

- First enter the class-map command to designate a class map and enter the Class Map configuration mode. Then use match commands to specify the fields within ingress packets that must match to qualify for this class map.
- If an ingress packet matches an ACL specified by this command, any deny rules included in the ACL will be ignored.
- If match criteria includes an IP ACL or IP priority rule, then a VLAN rule cannot be included in the same class map.
- If match criteria includes a MAC ACL or VLAN rule, then neither an IP ACL nor IP priority rule can be included in the same class map.
- Up to 16 match entries can be included in a class map.

Example

This example creates a class map called "rd-class#1," and sets it to match packets marked for DSCP service value 3.

Console(config)#class-map rd-class#1 match-any

Console(config-cmap)#match ip dscp 3

Console(config-cmap)#

This example creates a class map call "rd-class#2," and sets it to match packets marked for IP Precedence service value 5.

Console(config)#class-map rd-class#2 match-any

Console(config-cmap)#match ip precedence 5

Console(config-cmap)#

This example creates a class map call "rd-class#3," and sets it to match packets marked for VLAN 1.

Console(config)#class-map rd-class#3 match-any

Console(config-cmap)#match vlan 1

Console(config-cmap)#

rename

This command redefines the name of a class map or policy map.

Syntax

rename *map-name*

map-name - Name of the class map or policy map. (Range: 1-32 characters)

Command Mode

Class Map Configuration

Policy Map Configuration

Example

Console(config)#class-map rd-class#1

Console(config-cmap)#rename rd-class#9

Console(config-cmap)#

policy-map

This command creates a policy map that can be attached to multiple interfaces, and enters Policy Map configuration mode. Use the no form to delete a policy map.

Syntax

[no] policy-map *policy-map-name*

policy-map-name - Name of the policy map. (Range: 1-32 characters)

Default Configuration

None

Command Mode

Global Configuration

User Guidelines

- Use the policy-map command to specify the name of the policy map, and then use the class command to configure policies for traffic that matches the criteria defined in a class map.
- A policy map can contain multiple class statements that can be applied to the same interface with the service-policy command.
- Create a Class Map before assigning it to a Policy Map.

Example

This example creates a policy called "rd-policy," uses the class command to specify the previously defined "rd-class," uses the set command to classify the service that incoming packets will receive, and then uses the police flow command to limit the average bandwidth to 100,000 Kbps, the burst rate to 4000 bytes, and configure the response to drop any violating packets.

Console(config)#policy-map rd-policy

Console(config-pmap)#class rd-class

Console(config-pmap-c)#set cos 0

Console(config-pmap-c)#police flow 10000 4000 conform-action transmit

violate-action drop

Console(config-pmap-c)#

class

This command defines a traffic classification upon which a policy can act, and enters Policy Map Class configuration mode. Use the no form to delete a class map.

Syntax

[no] class *class-map-name*

class-map-name - Name of the class map. (Range: 1-32 characters)

Default Configuration

None

Command Mode

Policy Map Configuration

User Guidelines

- Use the policy-map command to specify a policy map and enter Policy Map configuration mode. Then use the class command to enter Policy Map Class configuration mode. And finally, use the set command and one of the police commands to specify the match criteria, where the:

a. set phb command sets the per-hop behavior value in matching packets. (This modifies packet priority for internal processing only.)

b. set cos command sets the class of service value in matching packets. (This modifies packet priority in the VLAN tag.)

c. set ip dscp command sets the IP DSCP value in matching packets. (This modifies packet priority in the IP header.)

d. police commands define parameters such as the maximum throughput, burst rate, and response to non-conforming traffic.

- Up to 16 classes can be included in a policy map.

Example

This example creates a policy called "rd-policy," uses the class command to specify the previously defined "rd-class," uses the set phb command to classify the service that incoming packets will receive, and then uses the police flow command to limit the average bandwidth to 100,000 Kbps, the burst rate to 4,000 bytes, and configure the response to drop any violating packets.

Console(config)#policy-map rd-policy

Console(config-pmap)#class rd-class

Console(config-pmap-c)#set phb 3

Console(config-pmap-c)#police flow 10000 4000 conform-action transmit

violate-action drop

Console(config-pmap-c)#

police flow

This command defines an enforcer for classified traffic based on the metered flow rate. Use the no form to remove a policer.

Syntax

[no] police flow *committed-rate committed-burst* conform-action transmit

violate-action {drop| *new-dscp*}

committed-rate - Committed information rate (CIR) in kilobits per second. (Range: 0-1000000 kbps at a granularity of 64 kbps or maximum port speed, whichever is lower)

committed-burst - Committed burst size (BC) in bytes. (Range: 64-16000000 at a granularity of 4k bytes)

conform-action - Action to take when packet is within the CIR and BC. (There are enough tokens to service the packet, the packet is set green).

violate-action - Action to take when packet exceeds the CIR and BC. (There are not enough tokens to service the packet, the packet is set red).

transmit - Transmits without taking any action.

drop - Drops packet as required by violate-action.

new-dscp - Differentiated Service Code Point (DSCP) value. (Range: 0-63)

Default Configuration

None

Command Mode

Policy Map Class Configuration

User Guidelines

- You can configure up to 16 policers (i.e., class maps) for ingress ports.
- The *committed-rate* cannot exceed the configured interface speed, and the *committed-burst* cannot exceed 16 Mbytes.
- Policing is based on a token bucket, where bucket depth (i.e., the maximum burst before the bucket overflows) is by specified the *committed-burst* field, and the average rate tokens are added to the bucket is by specified by the *committed-rate* option. Note that the token bucket functions similar to that described in RFC 2697 and RFC2698.
- The behavior of the meter is specified in terms of one token bucket (C), the rate at which the tokens are incremented (CIR – Committed Information Rate), and the maximum size of the token bucket (BC – Committed Burst Size).
- The token bucket C is initially full, that is, the token count Tc(0) = BC.
- Thereafter, the token count Tc is updated CIR times per second as follows:

If Tc is less than BC, Tc is incremented by one, else Tc is not incremented.

- When a packet of size B bytes arrives at time t, the following happens:

If Tc(t)-B ≥ 0, the packet is green and Tc is decremented by B down to the minimum value of 0, else the packet is red and Tc is not decremented.

Example

This example creates a policy called "rd-policy," uses the class command to specify the previously defined "rd-class," uses the set phb command to classify the service that incoming packets will receive, and then uses the police flow command to limit the average bandwidth to 100,000 Kbps, the burst rate to 4000 bytes, and configure the response to drop any violating packets.

Console(config)#policy-map rd-policy

Console(config-pmap)#class rd-class

Console(config-pmap-c)#set phb 3

Console(config-pmap-c)#police flow 100000 4000 conform-action transmit

violate-action drop

Console(config-pmap-c)#

police srtcm-color

This command defines an enforcer for classified traffic based on a single rate three color meter (srTCM). Use the no form to remove a policer.

Syntax

[no] police {srtcm-color-blind | srtcm-color-aware} *committed-rate committed-burst excess-burst* conform-action transmit exceed-action {drop | *new-dscp*} violate action {drop | *new-dscp*}

srtcm-color-blind - Single rate three color meter in color-blind mode.

srtcm-color-aware - Single rate three color meter in color-aware mode.

committed-rate - Committed information rate (CIR) in kilobits per second. (Range: 0-10000000 kbps at a granularity of 64 kbps or maximum port speed, whichever is lower)

committed-burst - Committed burst size (BC) in bytes. (Range: 64-16000000 at a granularity of 4k bytes)

excess-burst - Excess burst size (BE) in bytes. (Range: 64-1600000 at a granularity of 4k bytes)

conform-action - Action to take when rate is within the CIR and BC. (There are enough tokens in bucket BC to service the packet, packet is set green).

exceed-action - Action to take when rate exceeds the CIR and BC but is within the BE. (There are enough tokens in bucket BE to service the packet, the packet is set yellow.)

violate-action - Action to take when rate exceeds the BE. (There are not enough tokens in bucket BE to service the packet, the packet is set red.)

transmit - Transmits without taking any action.

drop - Drops packet as required by exceed-action or violate-action.

new-dscp - Differentiated Service Code Point (DSCP) value. (Range: 0-63)

Default Configuration

None

Command Mode

Policy Map Class Configuration

User Guidelines

- You can configure up to 16 policers (i.e., class maps) for ingress ports.
- The *committed-rate* cannot exceed the configured interface speed, and the *committed-burst* and *excess-burst* cannot exceed 16 Mbytes.

Example

This example creates a policy called "rd-policy," uses the class command to specify the previously defined "rd-class," uses the set phb command to classify the service that incoming packets will receive, and then uses the police srtcm-color-blind command to limit the average bandwidth to 100,000 Kbps, the committed burst rate to 4000 bytes, the excess burst rate to 6000 bytes, to remark any packets exceeding the committed burst size, and to drop any packets exceeding the excess burst size.

Console(config)#policy-map rd-policy

Console(config-pmap)#class rd-class

Console(config-pmap-c)#set phb 3

Console(config-pmap-c)#police srtcm-color-blind 100000 4000 6000 conform-action transmit exceed-action 0 violate-action drop

Console(config-pmap-c)#

police trtcm-color

This command defines an enforcer for classified traffic based on a two rate three color meter (trTCM). Use the no form to remove a policer.

Syntax

[no] police {trtcm-color-blind | trtcm-color-aware} *committed-rate committed-burst peak-rate peak-burst* conform-action transmit exceed-action {drop | *new-dscp*} violate action {drop | *new-dscp*}

trtcm-color-blind - Two rate three color meter in color-blind mode.

trtcm-color-aware - Two rate three color meter in color-aware mode.

committed-rate - Committed information rate (CIR) in kilobits per second. (Range: 0-1000000 kbps at a granularity of 64 kbps or maximum port speed, whichever is lower)

committed-burst - Committed burst size (BC) in bytes. (Range: 64-16000000 at a granularity of 4k bytes)

peak-rate - Peak information rate (PIR) in kilobits per second. (Range: 0-10000000 kbps at a granularity of 64 kbps or maximum port speed, whichever is lower)

peak-burst - Peak burst size (BP) in bytes. (Range: 64-16000000 at a granularity of 4k bytes)

conform-action - Action to take when rate is within the CIR and BP. (Packet size does not exceed BP and there are enough tokens in bucket BC to service the packet, the packet is set green.)

exceed-action - Action to take when rate exceeds the CIR but is within the PIR. (Packet size exceeds BC but there are enough tokens in bucket BP to service the packet, the packet is set yellow.)

violate-action - Action to take when rate exceeds the PIR. (There are not enough tokens in bucket BP to service the packet, the packet is set red.)

drop - Drops packet as required by exceed-action or violate-action.

transmit - Transmits without taking any action.

new-dscp - Differentiated Service Code Point (DSCP) value. (Range: 0-63)

Default Configuration

None

Command Mode

Policy Map Class Configuration

User Guidelines

- You can configure up to 16 policers (i.e., class maps) for ingress ports.
- The *committed-rate* and *peak-rate* cannot exceed the configured interface speed, and the *committed-burst* and *peak-burst* cannot exceed 16 Mbytes.

Example

This example creates a policy called "rd-policy," uses the class command to specify the previously defined "rd-class," uses the set phb command to classify the service that incoming packets will receive, and then uses the police trtcm-color-blind command to limit the average bandwidth to 100,000 Kbps, the committed burst rate to 4000 bytes, the peak information rate to 1,000,000 kbps, the peak burst size to 6000, to remark any packets exceeding the committed burst size, and to drop any packets exceeding the peak information rate.

Console(config)#policy-map rd-policy

Console(config-pmap)#class rd-class

Console(config-pmap-c)#set phb 3

Console(config-pmap-c)#police trtcm-color-blind 100000 4000 100000 6000 conform-action transmit exceed-action 0 violate-action drop

Console(config-pmap-c)#

set cos

This command modifies the class of service (CoS) value for a matching packet (as specified by the match command) in the packet's VLAN tag. Use the no form to remove this setting.

Syntax

[no] set cos *cos-value*

cos-value - Class of Service value. (Range: 0-7)

Default Configuration

None

Command Mode

Policy Map Class Configuration

User Guidelines

- The set cos command is used to set the CoS value in the VLAN tag for matching packets.
- The set cos and set phb command function at the same level of priority. Therefore setting either of these commands will overwrite any action already configured by the other command.

Example

This example creates a policy called "rd-policy," uses the class command to specify the previously defined "rd-class," uses the set cos command to classify the service that incoming packets will receive, and then uses the police flow command to limit the average bandwidth to 100,000 Kbps, the burst rate to 4000 bytes, and configure the response to drop any violating packets.

Console(config)#policy-map rd-policy
Console(config-pmap)#class rd-class
Console(config-pmap-c)#set cos 3
Console(config-pmap-c)#police flow 10000 4000 conform-action transmit violate-action drop
Console(config-pmap-c)#

set ip dscp

This command modifies the IP DSCP value in a matching packet (as specified by the match command). Use the no form to remove this traffic classification.

Syntax

[no] set ip dscp *new-dscp*

new-dscp - New Differentiated Service Code Point (DSCP) value. (Range: 0-63)

Default Configuration

None

Command Mode

Policy Map Class Configuration

User Guidelines

The set ip dscp command is used to set the priority values in the packet's ToS field for matching packets.

Example

This example creates a policy called "rd-policy," uses the class command to specify the previously defined "rd-class," uses the set ip dscp command to classify the service that incoming packets will receive, and then uses the police flow command to limit the average bandwidth to 100,000 Kbps, the burst rate to 4000 bytes, and configure the response to drop any violating packets.

Console(config)#policy-map rd-policy
Console(config-pmap)#class rd-class
Console(config-pmap-c)#set ip dscp 3
Console(config-pmap-c)#police flow 10000 4000 conform-action transmit violate-action drop
Console(config-pmap-c)#

set phb

This command services IP traffic by setting a per-hop behavior value for a matching packet (as specified by the match command) for internal processing. Use the no form to remove this setting.

Syntax

[no] set phb *phb-value*

phb-value - Per-hop behavior value. (Range: 0-7)

Default Configuration

None

Command Mode

Policy Map Class Configuration

Example

This example creates a policy called "rd-policy," uses the class command to specify the previously defined "rd-class," uses the set phb command to classify the service that incoming packets will receive, and then uses the police flow command to limit the average bandwidth to 100,000 Kbps, the burst rate to 4000 bytes, and configure the response to drop any violating packets.

Console(config)#policy-map rd-policy
Console(config-pmap)#class rd-class

Console(config-pmap-c)#set phb 3

Console(config-pmap-c)#police flow 10000 4000 conform-action transmit violate-action drop

Console(config-pmap-c)#

service-policy

This command applies a policy map defined by the policy-map command to the ingress or egress side of a particular interface. Use the no form to remove this mapping.

Syntax

[no] service-policy {input | output} *policy-map-name*

input - Apply to the input traffic.

output - Apply to the output traffic.

policy-map-name - Name of the policy map for this interface. (Range: 1-32 characters)

Default Configuration

No policy map is attached to an interface.

Command Mode

Interface Configuration (Ethernet, Port Channel)

User Guidelines

- Only one policy map can be assigned to an interface.
- First define a class map, then define a policy map, and finally use the service-policy command to bind the policy map to the required interface.

Example

This example applies a service policy to an ingress interface.

Console(config)#interface ethernet 1/1

Console(config-if)#service-policy input rd-policy

Console(config-if)#

show class-map

This command displays the QoS class maps which define matching criteria used for classifying traffic.

Syntax

show class-map [*class-map-name*]

class-map-name - Name of the class map. (Range: 1-32 characters)

Default Configuration

Displays all class maps.

Command Mode

EXEC

Example

Console#show class-map

Class Map match-any rd-class#1

Description:

Match ip dscp 10

Match access-list rd-access

Match ip dscp 0

Class Map match-any rd-class#2

Match ip precedence 5

Class Map match-any rd-class#3

Match vlan 1

Console#

show policy-map

This command displays the QoS policy maps which define classification criteria for incoming traffic, and may include policers for bandwidth limitations.

Syntax

show policy-map [*policy-map-name* [class *class-map-name*]]

policy-map-name - Name of the policy map. (Range: 1-32 characters)

class-map-name - Name of the class map. (Range: 1-32 characters)

Default Configuration

Displays all policy maps and all classes.

Command Mode

EXEC

Example

Console#show policy-map

Policy Map rd-policy

Description:

class rd-class

set PHB 3

Console#show policy-map rd-policy class rd-class

Policy Map rd-policy

class rd-class

set PHB 3

Console#

show policy-map interface

This command displays the service policy assigned to the specified interface.

Syntax

show policy-map interface *interface* input

interface

unit/*port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-28)

port-channel *channel-id* (Range: 1-12)

Command Mode

EXEC

Example

Console#show policy-map interface 1/5 input

Service-policy rd-policy

Console#

44. IGMP Snooping

ip igmp snooping

This command enables IGMP snooping globally on the switch or on a selected VLAN interface. Use the no form to disable it.

Syntax

[no] ip igmp snooping [vlan *vlan-id*]

vlan-id - VLAN ID (Range: 1-4094)

Default Configuration

Enabled

Command Mode

Global Configuration

User Guidelines

- When IGMP snooping is enabled globally, the per VLAN interface settings for IGMP snooping take precedence.
- When IGMP snooping is disabled globally, snooping can still be configured per VLAN interface, but the interface settings will not take effect until snooping is re-enabled globally.

Example

The following example enables IGMP snooping globally.

Console(config)#ip igmp snooping

Console(config)#

ip igmp snooping mrouter-forward-mode dynamic

This command configures mrouter ports always forward multicast streams or only forward when groups joined. Use the no form to disable it.

Syntax

[no] ip igmp snooping mrouter-forward-mode dynamic

Default Configuration

Always forward

Command Mode

Global Configuration

Example

Console(config)# ip igmp snooping mrouter-forward-mode dynamic

Console(config)#

ip igmp snooping priority

This command assigns a priority to all multicast traffic. Use the no form to restore the default setting.

Syntax

ip igmp snooping priority *priority*

no ip igmp snooping priority

priority - The CoS priority assigned to all multicast traffic. (Range: 0-6, where 6 is the highest priority)

Default Configuration

2

Command Mode

Global Configuration

User Guidelines

This command can be used to set a high priority for low-latency multicast traffic such as a video-conference, or to set a low priority for normal multicast traffic not sensitive to latency.

Example

Console(config)#ip igmp snooping priority 6

Console(config)#

ip igmp snooping proxy-reporting

This command enables IGMP Snooping with Proxy Reporting. Use the no form to restore the default setting.

Syntax

[no] ip igmp snooping proxy-reporting ip igmp snooping vlan *vlan-id* proxy-reporting {enable | disable}

no ip igmp snooping vlan *vlan-id* proxy-reporting

vlan-id - VLAN ID (Range: 1-4094)

enable - Enable on the specified VLAN.

disable - Disable on the specified VLAN.

Default Configuration

Global: Enabled

VLAN: Based on global setting

Command Mode

Global Configuration

User Guidelines

- When proxy reporting is enabled with this command, the switch performs "IGMP Snooping with Proxy Reporting" (as defined in DSL Forum TR-101, April 2006), including last leave, and query suppression. Last leave sends out a proxy query when the last member leaves a multicast group, and query suppression means that specific queries are not forwarded from an upstream multicast router to hosts downstream from this device.
- If the IGMP proxy reporting is configured on a VLAN, this setting takes precedence over the global configuration.

Example

Console(config)#ip igmp snooping proxy-reporting

Console(config)#

ip igmp snooping querier

This command enables the switch as an IGMP querier. Use the no form to disable it.

Syntax

[no] ip igmp snooping querier

Default Configuration

Enabled

Command Mode

Global Configuration

User Guidelines

- IGMP snooping querier is not supported for IGMPv3 snooping (see ip igmp snooping version).
- If enabled, the switch will serve as querier if elected. The querier is responsible for asking hosts if they want to receive multicast traffic.

Example

Console(config)#ip igmp snooping querier

Console(config)#

ip igmp snooping router-alert-option-check

This command discards any IGMPv2/v3 packets that do not include the Router Alert option. Use the no form to ignore the Router Alert Option when receiving IGMP messages.

Syntax

[no] ip igmp snooping router-alert-option-check

Default Configuration

Disabled

Command Mode

Global Configuration

User Guidelines

As described in Section 9.1 of RFC 3376 for IGMP Version 3, the Router Alert Option can be used to protect against DOS attacks. One common method of attack is launched by an intruder who takes over the role of querier, and starts overloading multicast hosts by sending a large number of group-and-source-specific queries, each with a large source list and the Maximum Response Time set to a large value.

To protect against this kind of attack, (1) routers should not forward queries. This is easier to accomplish if the query carries the Router Alert option. (2) Also, when the switch is acting in the role of a multicast host (such as when using proxy routing), it should ignore version 2 or 3 queries that do not contain the Router Alert option.

Example

Console(config)#ip igmp snooping router-alert-option-check

Console(config)#

ip igmp snooping router-port-expire-time

This command configures the querier time out. Use the no form to restore the default.

Syntax

ip igmp snooping router-port-expire-time *seconds*

no ip igmp snooping router-port-expire-time

seconds - The time the switch waits after the previous querier stops before it considers it to have expired. (Range: 1-65535; Recommended Range: 300-500)

Default Configuration

300 seconds

Command Mode

Global Configuration

Example

The following shows how to configure the time out to 400 seconds:

Console(config)#ip igmp snooping router-port-expire-time 400

Console(config)#

ip igmp snooping tcn-flood

This command enables flooding of multicast traffic if a spanning tree topology change notification (TCN) occurs. Use the no form to disable flooding.

Syntax

[no] ip igmp snooping tcn-flood

Default Configuration

Disabled

Command Mode

Global Configuration

User Guidelines

- When a spanning tree topology change occurs, the multicast membership information learned by the switch may be out of date. For example, a host linked to one port before the topology change (TC) may be moved to another port after the change. To ensure that multicast data is delivered to all receivers, by default, a switch in a VLAN (with IGMP snooping enabled) that receives a Bridge Protocol Data Unit (BPDU) with the TC bit set (by the root bridge) will enter into "multicast flooding mode" for a period of time until the topology has stabilized and the new locations of all multicast receivers are learned.
- If a topology change notification (TCN) is received, and all the uplink ports are subsequently deleted, a time out mechanism is used to delete all of the currently learned multicast channels.
- When a new uplink port starts up, the switch sends unsolicited reports for all current learned channels out through the new uplink port.
- By default, the switch immediately enters into "multicast flooding mode" when a spanning tree topology change occurs. In this mode, multicast traffic will be flooded to all VLAN ports. If many ports have subscribed to different multicast groups, flooding may cause excessive loading on the link between the switch and the end host. Flooding may be disabled to avoid this, causing multicast traffic to be delivered only to those ports on which multicast group members have been learned.
- When the spanning tree topology changes, the root bridge sends a proxy query to quickly re-learn the host membership/port relations for multicast channels. The root bridge also sends an unsolicited Multicast Router Discover (MRD) request to quickly locate the multicast routers in this VLAN.
- The proxy query and unsolicited MRD request are flooded to all VLAN ports except for the receiving port when the switch receives such packets.

Example

The following example enables TCN flooding.

Console(config)#ip igmp snooping tcn-flood

Console(config)#

ip igmp snooping tcn-query-solicit

This command instructs the switch to send out an IGMP general query solicitation when a spanning tree topology change notification (TCN) occurs. Use the no form to disable this feature.

Syntax

[no] ip igmp snooping tcn-query-solicit

Default Configuration

Disabled

Command Mode

Global Configuration

User Guidelines

- When the root bridge in a spanning tree receives a topology change notification for a VLAN where IGMP snooping is enabled, it issues a global IGMP leave message (query solicitation). When a switch receives this solicitation, it floods it to all ports in the VLAN where the spanning tree change occurred. When an upstream multicast router receives this solicitation, it will also immediately issues an IGMP general query.
- The ip igmp snooping tcn query-solicit command can be used to send a query solicitation whenever it notices a topology change, even if the switch is not the root bridge in the spanning tree.

Example

The following example instructs the switch to issue an IGMP general query whenever it receives a spanning tree topology change notification.

Console(config)#ip igmp snooping tcn query-solicit

Console(config)#

ip igmp snooping unregistered-data-flood

This command floods unregistered multicast traffic into the attached VLAN. Use the no form to drop unregistered multicast traffic.

Syntax

[no] ip igmp snooping unregistered-data-flood

Default Configuration

Disabled

Command Mode

Global Configuration

User Guidelines

Once the table used to store multicast entries for IGMP snooping and multicast routing is filled, no new entries are learned. If no router port is configured in the attached VLAN, and unregistered-flooding is disabled, any subsequent multicast traffic not found in the table is dropped, otherwise it is flooded throughout the VLAN.

Example

Console(config)#ip igmp snooping unregistered-data-flood

Console(config)#

ip igmp snooping unsolicited-report-interval

This command specifies how often the upstream interface should transmit unsolicited IGMP reports when proxy reporting is enabled. Use the no form to restore the default value.

Syntax

ip igmp snooping unsolicited-report-interval *seconds*

no ip igmp snooping version-exclusive

seconds - The interval at which to issue unsolicited reports. (Range: 1-65535 seconds)

Default Configuration

400 seconds

Command Mode

Global Configuration

User Guidelines

- When a new upstream interface (that is, uplink port) starts up, the switch sends unsolicited reports for all currently learned multicast channels out through the new upstream interface.
- This command only applies when proxy reporting is enabled.

Example

Console(config)#ip igmp snooping unsolicited-report-interval 5

Console(config)#

ip igmp snooping version

This command configures the IGMP snooping version. Use the no form to restore the default.

Syntax

ip igmp snooping [vlan *vlan-id*] version {1 | 2 | 3}

no ip igmp snooping version

vlan-id - VLAN ID (Range: 1-4094)

1 - IGMP Version 1

2 - IGMP Version 2

3 - IGMP Version 3

Default Configuration

Global: IGMP Version 2

VLAN: Not configured, based on global setting

Command Mode

Global Configuration

User Guidelines

- This command configures the IGMP report/query version used by IGMP snooping. Versions 1 - 3 are all supported, and versions 2 and 3 are backward compatible, so the switch can operate with other devices, regardless of the snooping version employed.
- If the IGMP snooping version is configured on a VLAN, this setting takes precedence over the global configuration.

Example

The following configures the global setting for IGMP snooping to version 1.

Console(config)#ip igmp snooping version 1

Console(config)#

ip igmp snooping version-exclusive

This command discards any received IGMP messages (except for multicast protocol packets) which use a version different to that currently configured by the ip igmp snooping version command. Use the no form to disable this feature.

Syntax

ip igmp snooping [vlan *vlan-id*] version-exclusive

no ip igmp snooping version-exclusive

vlan-id - VLAN ID (Range: 1-4094)

Default Configuration

Global: Disabled

VLAN: Disabled

Command Mode

Global Configuration

User Guidelines

- If version exclusive is disabled on a VLAN, then this setting is based on the global setting. If it is enabled on a VLAN, then this setting takes precedence over the global setting.
- When this function is disabled, the currently selected version is backward compatible (see the ip igmp snooping version command).

Example

Console(config)#ip igmp snooping version-exclusive

Console(config)#

ip igmp snooping vlan general-query-suppression

This command suppresses general queries except for ports attached to downstream multicast hosts. Use the no form to flood general queries to all ports except for the multicast router port.

Syntax

[no] ip igmp snooping vlan *vlan-id* general-query-suppression

vlan-id - VLAN ID (Range: 1-4094)

Default Configuration

Disabled

Command Mode

Global Configuration

User Guidelines

- By default, general query messages are flooded to all ports, except for the multicast router through which they are received.
- If general query suppression is enabled, then these messages are forwarded only to downstream ports which have joined a multicast service.

Example

Console(config)#ip igmp snooping vlan 1 general-query-suppression

Console(config)#

ip igmp snooping vlan immediate-leave

This command immediately deletes a member port of a multicast service if a leave packet is received at that port and immediate-leave is enabled for the parent VLAN. Use the no form to restore the default.

Syntax

[no] ip igmp snooping vlan *vlan-id* immediate-leave

vlan-id - VLAN ID (Range: 1-4094)

Default Configuration

Disabled

Command Mode

Global Configuration

User Guidelines

- If immediate-leave is *not* used, a multicast router (or querier) will send a group-specific query message when an IGMPv2/v3 group leave message is received. The router/querier stops forwarding traffic for that group only if no host replies to the query within the time out period. (The time out for this release is currently defined by Last Member Query Interval (fixed at one second) * Robustness Variable (fixed at 2) as defined in RFC 2236.
- If immediate-leave is enabled, the switch assumes that only one host is connected to the interface. Therefore, immediate leave should only be enabled on an interface if it is connected to only one IGMP-enabled device, either a service host or a neighbor running IGMP snooping.
- This command is only effective if IGMP snooping is enabled, and IGMPv2 or IGMPv3 snooping is used.

Example

The following shows how to enable immediate leave.

Console(config)#ip igmp snooping vlan 1 immediate-leave

Console(config)#

ip igmp snooping vlan last-memb-query-count

This command configures the number of IGMP proxy group-specific or group-and-source-specific query messages that are sent out before the system assumes there are no more local members. Use the no form to restore the default.

Syntax

ip igmp snooping vlan *vlan-id* last-memb-query-count *count*

no ip igmp snooping vlan *vlan-id* last-memb-query-count

vlan-id - VLAN ID (Range: 1-4094)

count - The number of proxy group-specific or group-and-source-specific query messages to issue before assuming that there are no more group members. (Range: 1-255)

Default Configuration

2

Command Mode

Global Configuration

User Guidelines

This command will take effect only if IGMP snooping proxy reporting or IGMP querier is enabled.

Example

Console(config)#ip igmp snooping vlan 1 last-memb-query-count 7

Console(config)#

ip igmp snooping vlan last-memb-query-intvl

This command configures the last-member-query interval. Use the no form to restore the default.

Syntax

ip igmp snooping vlan *vlan-id* last-memb-query-intvl *interval*

no ip igmp snooping vlan *vlan-id* last-memb-query-intvl

vlan-id - VLAN ID (Range: 1-4094)

interval - The interval to wait for a response to a group-specific or group-and-source-specific query message. (Range: 1-31744 tenths of a second)

Default Configuration

10 (1 second)

Command Mode

Global Configuration

User Guidelines

- When a multicast host leaves a group, it sends an IGMP leave message. When the leave message is received by the switch, it checks to see if this host is the last to leave the group by sending out an IGMP group-specific or group-and-source-specific query message, and starts a timer. If no reports are received before the timer expires, the group record is deleted, and a report is sent to the upstream multicast router.
- A reduced value will result in reduced time to detect the loss of the last member of a group or source, but may generate more bursty traffic.
- This command will take effect only if IGMP snooping proxy reporting is enabled.

Example

Console(config)#ip igmp snooping vlan 1 last-memb-query-intvl 700

Console(config)#

ip igmp snooping vlan mrd

This command enables sending of multicast router solicitation messages. Use the no form to disable these messages.

Syntax

[no] ip igmp snooping vlan *vlan-id* mrd

vlan-id - VLAN ID (Range: 1-4094)

Default Configuration

Enabled

Command Mode

Global Configuration

User Guidelines

- Multicast Router Discovery (MRD) uses multicast router advertisement, multicast router solicitation, and multicast router termination messages to discover multicast routers. Devices send solicitation messages in order to solicit advertisement messages from multicast routers. These messages are used to discover multicast

routers on a directly attached link. Solicitation messages are also sent whenever a multicast forwarding interface is initialized or re-initialized. Upon receiving a solicitation on an interface with IP multicast forwarding and MRD enabled, a router will respond with an advertisement.

- Advertisements are sent by routers to advertise that IP multicast forwarding is enabled. These messages are sent unsolicited periodically on all router interfaces on which multicast forwarding is enabled. They are sent upon the expiration of a periodic timer, as a part of a router's start up procedure, during the restart of a multicast forwarding interface, and on receipt of a solicitation message. When the multicast services provided to a VLAN is relatively stable, the use of solicitation messages is not required and may be disabled using the no ip igmp snooping vlan mrd command.
- This command may also be used to disable multicast router solicitation messages when the upstream router does not support MRD, to reduce the loading on a busy upstream router, or when IGMP snooping is disabled in a VLAN.

Example

This example disables sending of multicast router solicitation messages on VLAN 1.

Console(config)#no ip igmp snooping vlan 1 mrd

Console(config)#

ip igmp snooping vlan proxy-address

This command configures a static source address for locally generated query and report messages used by IGMP proxy reporting. Use the no form to restore the default source address.

Syntax

[no] ip igmp snooping vlan *vlan-id* proxy-address *source-address*

vlan-id - VLAN ID (Range: 1-4094)

source-address - The source address used for proxied IGMP query and report, and leave messages. (Any valid IP unicast address)

Default Configuration

0.0.0.0

Command Mode

Global Configuration

User Guidelines

IGMP Snooping uses a null IP address of 0.0.0.0 for the source of IGMP query messages which are proxied to downstream hosts to indicate that it is not the elected querier, but is only proxying these messages as defined in RFC 4541. The switch also uses a null address in IGMP reports sent to upstream ports.

Many hosts do not implement RFC 4541, and therefore do not understand query messages with the source address of 0.0.0.0. These hosts will therefore not reply to the queries, causing the multicast router to stop sending traffic to them.

To resolve this problem, the source address in proxied IGMP query and report messages can be replaced with any valid unicast address (other than the router's own address) using this command.

Rules Used for Proxy Reporting

When IGMP Proxy Reporting is disabled, the switch will use a null IP address for the source of IGMP query and report messages unless a proxy query address has been set.

When IGMP Proxy Reporting is enabled, the source address is based on the following criteria:

- If a proxy query address is configured, the switch will use that address as the source IP address in general and group-specific query messages sent to downstream hosts, and in report and leave messages sent upstream from the multicast router port.

- If a proxy query address is not configured, the switch will use the VLAN's IP address as the IP source address in general and group-specific query messages sent downstream, and use the source address of the last IGMP message received from a downstream host in report and leave messages sent upstream from the multicast router port.

Example

The following example sets the source address for proxied IGMP query messages to 10.0.1.8.

Console(config)#ip igmp snooping vlan 1 proxy-address 10.0.1.8

Console(config)#

ip igmp snooping vlan query-interval

This command configures the interval between sending IGMP general queries. Use the no form to restore the default.

Syntax

ip igmp snooping vlan *vlan-id* query-interval *interval*

no ip igmp snooping vlan *vlan-id* query-interval

vlan-id - VLAN ID (Range: 1-4094)

interval - The interval between sending IGMP general queries. (Range: 10-31740 seconds)

Default Configuration

100 (10 seconds)

Command Mode

Global Configuration

User Guidelines

- An IGMP general query message is sent by the switch at the interval specified by this command. When this message is received by downstream hosts, all receivers build an IGMP report for the multicast groups they have joined.
- This command applies when the switch is serving as the querier, or as a proxy host when IGMP snooping proxy reporting is enabled.

Example

Console(config)#ip igmp snooping vlan 1 query-interval 150

Console(config)#

ip igmp snooping vlan query-resp-intvl

This command configures the maximum time the system waits for a response to general queries. Use the no form to restore the default.

Syntax

ip igmp snooping vlan *vlan-id* query-resp-intvl *interval*

no ip igmp snooping vlan *vlan-id* query-resp-intvl

vlan-id - VLAN ID (Range: 1-4094)

interval - The maximum time the system waits for a response to general queries. (Range: 10-31744 tenths of a second)

Default Configuration

100 (10 seconds)

Command Mode

Global Configuration

User Guidelines

This command applies when the switch is serving as the querier, or as a proxy host when IGMP snooping proxy reporting is enabled.

Example

Console(config)#ip igmp snooping vlan 1 query-resp-intvl 20

Console(config)#

ip igmp snooping vlan static

This command adds a port to a multicast group. Use the no form to remove the port.

Syntax

[no] ip igmp snooping vlan *vlan-id* static *ip-address interface*

vlan-id - VLAN ID (Range: 1-4094)

ip-address - IP address for multicast group

interface

ethernet *unit*/*port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-28)

port-channel *channel-id* (Range: 1-12)

Default Configuration

None

Command Mode

Global Configuration

User Guidelines

- Static multicast entries are never aged out.
- When a multicast entry is assigned to an interface in a specific VLAN, the corresponding traffic can only be forwarded to ports within that VLAN.

Example

The following shows how to statically configure a multicast group on a port.

Console(config)#ip igmp snooping vlan 1 static 224.0.0.12 ethernet 1/5

Console(config)#

show ip igmp snooping

This command shows the IGMP snooping, proxy, and query configuration settings.

Syntax

show ip igmp snooping [vlan *vlan-id*]

vlan-id - VLAN ID (1-4094)

Command Mode

EXEC

User Guidelines

This command displays global and VLAN-specific IGMP configuration settings. See "Configuring IGMP Snooping and Query Parameters" for a description of the displayed items.

Example

The following shows the current IGMP snooping configuration:

Console#show ip igmp snooping

IGMP Snooping: Enabled

Router Port Expire Time: 300 s

Router Alert Check: Disabled

TCN Flood: Disabled

TCN Query Solicit: Disabled

Unregistered Data Flood: Disabled

802.1p Forwarding Priority: Disabled
Unsolicited Report Interval: 400 s
Version Exclusive: Disabled
Version: 2
Proxy Reporting: Disabled
Querier: Disabled
VLAN 1:

IGMP Snooping: Enabled
IGMP Snooping Running Status: Inactive
Version: Using global Version (2)
Version Exclusive: Using global status (Disabled)
Immediate Leave: Disabled
Last Member Query Interval: 10 (unit: 1/10s)
Last Member Query Count: 2
General Query Suppression: Disabled
Query Interval: 125
Query Response Interval: 100 (unit: 1/10s)
Proxy Query Address: 0.0.0.0
Proxy Reporting: Using global status (Disabled)
Multicast Router Discovery: Disabled
VLAN Static Group Port
---- --------------- --------
1 224.1.1.1 Eth 1/ 1
...

show ip igmp snooping group

This command shows known multicast group, source, and host port mappings for the specified VLAN interface, or for all interfaces if none is specified.

Syntax

show ip igmp snooping group [host-ip-addr *ip-address interface* | igmpsnp | sort-by-port | user | vlan *vlan-id* [user | igmpsnp]]

ip-address - IP address for multicast group

interface

ethernet *unit*/*port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-28)

port-channel *channel-id* (Range: 1-12)

igmpsnp - Display only entries learned through IGMP snooping.

sort-by-port - Display entries sorted by port.

user - Display only the user-configured multicast entries.

vlan-id - VLAN ID (1-4094)

Default Configuration

None

Command Mode

EXEC

User Guidelines

Member types displayed include IGMP or USER, depending on selected options.

Example

The following shows the multicast entries learned through IGMP snooping for VLAN 1.

Console#show ip igmp snooping group vlan 1

Bridge Multicast Forwarding Entry Count:1

Flag: R - Router port, M - Group member port

H - Host counts (number of hosts join the group on this port).

P - Port counts (number of ports join the group).

Up time: Group elapsed time (d:h:m:s).

Expire: Group remaining time (m:s).

VLAN Group Port Up time Expire Count

---- --------------- ----------- ----------- ------ --------

1 224.1.1.1 00:00:00:37 2(P)

Eth 1/ 1(R)

Eth 1/ 2(M) 0(H)

Console#

show ip igmp snooping statistics

This command shows IGMP snooping protocol statistics for the specified interface.

Syntax

show ip igmp snooping statistics {input [interface *interface*] | output [interface *interface*] | query [vlan *vlan-id*]}

interface

ethernet *unit*/*port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-28)

port-channel *channel-id* (Range: 1-12)

vlan *vlan-id* - VLAN ID (Range: 1-4094)

query - Displays IGMP snooping-related statistics.

Default Configuration

None

Command Mode

EXEC

Example

The following shows IGMP protocol statistics input:

Console#show ip igmp snooping statistics input interface ethernet 1/1

Interface Report Leave G Query G(-S)-S Query Drop Join Succ Group

--------- -------- -------- -------- -------------- -------- --------- ------

Eth 1/ 1 23 11 4 10 5 14 5

Console#

44.1 Static Multicast Routing

ip igmp snooping vlan mrouter

This command statically configures a (Layer 2) multicast router port on the specified VLAN. Use the no form to remove the configuration.

Syntax

[no] ip igmp snooping vlan *vlan-id* mrouter *interface*

vlan-id - VLAN ID (Range: 1-4094)

interface

ethernet *unit*/*port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-28)

port-channel *channel-id* (Range: 1-12)

Default Configuration

No static multicast router ports are configured.

Command Mode

Global Configuration

User Guidelines

- Depending on your network connections, IGMP snooping may not always be able to locate the IGMP querier. Therefore, if the IGMP querier is a known multicast router or switch connected over the network to an interface (port or trunk) on this switch, that interface can be manually configured to join all the current multicast groups.
- IGMP Snooping must be enabled globally on the switch (using the ip igmp snooping command) before a multicast router port can take effect.

Example

The following shows how to configure port 10 as a multicast router port within VLAN 1.

Console(config)#ip igmp snooping vlan 1 mrouter ethernet 1/10

Console(config)#

show ip igmp snooping mrouter

This command displays information on statically configured and dynamically learned multicast router ports.

Syntax

show ip igmp snooping mrouter [vlan *vlan-id*]

vlan-id - VLAN ID (Range: 1-4094)

Default Configuration

Displays multicast router ports for all configured VLANs.

Command Mode

EXEC

User Guidelines

Multicast router port types displayed include Static or Dynamic.

Example

The following shows the ports in VLAN 1 which are attached to multicast routers.

Console#show ip igmp snooping mrouter vlan 1

VLAN M'cast Router Port Type

---- ------------------ -------

1 Eth 1/10 Static

Console#

44.2 IGMP Filtering and Throttling

ip igmp filter (Global Configuration)

This command globally enables IGMP filtering and throttling on the switch. Use the no form to disable the feature.

Syntax

[no] ip igmp filter

Default Configuration

Disabled

Command Mode

Global Configuration

User Guidelines

- IGMP filtering enables you to assign a profile to a switch port that specifies multicast groups that are permitted or denied on the port. An IGMP filter profile can contain one or more, or a range of multicast addresses; but only one profile can be assigned to a port. When enabled, IGMP join reports received on the port are checked against the filter profile. If a requested multicast group is permitted, the IGMP join report is forwarded as normal. If a requested multicast group is denied, the IGMP join report is dropped.
- IGMP filtering and throttling only applies to dynamically learned multicast groups, it does not apply to statically configured groups.
- The IGMP filtering feature operates in the same manner when MVR is used to forward multicast traffic.

Example

Console(config)#ip igmp filter

Console(config)#

ip igmp profile

This command creates an IGMP filter profile number and enters IGMP profile configuration mode. Use the no form to delete a profile number.

Syntax

[no] ip igmp profile *profile-number*

profile-number - An IGMP filter profile number. (Range: 1-4294967295)

Default Configuration

Disabled

Command Mode

Global Configuration

User Guidelines

A profile defines the multicast groups that a subscriber is permitted or denied to join. The same profile can be applied to many interfaces, but only one profile can be assigned to one interface. Each profile has only one access mode; either permit or deny.

Example

Console(config)#ip igmp profile 19

Console(config-igmp-profile)#

permit, deny

This command sets the access mode for an IGMP filter profile. Use the no form to delete a profile number.

Syntax

{permit | deny}

Default Configuration

Deny

Command Mode

IGMP Profile Configuration

User Guidelines

- Each profile has only one access mode; either permit or deny.
- When the access mode is set to permit, IGMP join reports are processed when a multicast group falls within the controlled range. When the access mode is set to deny, IGMP join reports are only processed when a multicast group is not in the controlled range.

Example

Console(config)#ip igmp profile 19

Console(config-igmp-profile)#permit

Console(config-igmp-profile)#

range

This command specifies multicast group addresses for a profile. Use the no form to delete addresses from a profile.

Syntax

[no] range *low-ip-address* [*high-ip-address*]

low-ip-address - A valid IP address of a multicast group or start of a group range.

high-ip-address - A valid IP address for the end of a multicast group range.

Default Configuration

None

Command Mode

IGMP Profile Configuration

User Guidelines

Enter this command multiple times to specify more than one multicast address or address range for a profile.

Example

Console(config)#ip igmp profile 19

Console(config-igmp-profile)#range 239.1.1.1

Console(config-igmp-profile)#range 239.2.3.1 239.2.3.100

Console(config-igmp-profile)#

ip igmp filter (Interface Configuration)

This command assigns an IGMP filtering profile to an interface on the switch. Use the no form to remove a profile from an interface.

Syntax

[no] ip igmp filter *profile-number*

profile-number - An IGMP filter profile number. (Range: 1-4294967295)

Default Configuration

None

Command Mode

Interface Configuration

User Guidelines

- The IGMP filtering profile must first be created with the ip igmp profile command before being able to assign it to an interface.

- Only one profile can be assigned to an interface.
- A profile can also be assigned to a trunk interface. When ports are configured as trunk members, the trunk uses the filtering profile assigned to the first port member in the trunk.

Example

Console(config)#interface ethernet 1/1

Console(config-if)#ip igmp filter 19

Console(config-if)#

ip igmp max-groups

This command sets the IGMP throttling number for an interface on the switch. Use the no form to restore the default setting.

Syntax

ip igmp max-groups *number*

no ip igmp max-groups

number - The maximum number of multicast groups an interface can join at the same time. (Range: 1-255)

Default Configuration

255

Command Mode

Interface Configuration (Ethernet)

User Guidelines

- IGMP throttling sets a maximum number of multicast groups that a port can join at the same time. When the maximum number of groups is reached on a port, the switch can take one of two actions; either "deny" or "replace." If the action is set to deny, any new IGMP join reports will be dropped. If the action is set to replace, the switch randomly removes an existing group and replaces it with the new multicast group.
- IGMP throttling can also be set on a trunk interface. When ports are configured as trunk members, the trunk uses the throttling settings of the first port member in the trunk.

Example

Console(config)#interface ethernet 1/1

Console(config-if)#ip igmp max-groups 10

Console(config-if)#

ip igmp max-groups action

This command sets the IGMP throttling action for an interface on the switch.

Syntax

ip igmp max-groups action {deny | replace}

deny - The new multicast group join report is dropped.

replace - The new multicast group replaces an existing group.

Default Configuration

Deny

Command Mode

Interface Configuration (Ethernet)

User Guidelines

When the maximum number of groups is reached on a port, the switch can take one of two actions; either "deny" or "replace." If the action is set to deny, any new IGMP join reports will be dropped. If the action is set to replace, the switch randomly removes an existing group and replaces it with the new multicast group.

Example

Console(config)#interface ethernet 1/1

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

Console(config-if)#

ip igmp query-drop

This command drops any received IGMP query packets. Use the no form to restore the default setting.

Syntax

[no] ip igmp query-drop

Default Configuration

Disabled

Command Mode

Interface Configuration (Ethernet)

User Guidelines

This command can be used to drop any query packets received on the specified interface. If this switch is acting as a Querier, this prevents it from being affected by messages received from another Querier.

Example

Console(config)#interface ethernet 1/1

Console(config-if)#ip igmp query-drop

Console(config-if)#

show ip igmp filter

This command displays the global and interface settings for IGMP filtering.

Syntax

show ip igmp filter [interface *interface*]

interface

ethernet *unit*/*port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-28)

port-channel *channel-id* (Range: 1-12)

Default Configuration

None

Command Mode

EXEC

Example

Console#show ip igmp filter

IGMP filter enabled

Console#show ip igmp filter interface ethernet 1/1

Ethernet 1/1 information

IGMP Profile 19

Deny

Range 239.1.1.1 239.1.1.1

Range 239.2.3.1 239.2.3.100

Console#

show ip igmp profile

This command displays IGMP filtering profiles created on the switch.

Syntax

show ip igmp profile [*profile-number*]

profile-number - An existing IGMP filter profile number. (Range: 1-4294967295)

Default Configuration

None

Command Mode

EXEC

Example

Console#show ip igmp profile

IGMP Profile 19

IGMP Profile 50

Console#show ip igmp profile 19

IGMP Profile 19

Deny

Range 239.1.1.1 239.1.1.1

Range 239.2.3.1 239.2.3.100

Console#

show ip igmp query-drop

This command shows if the specified interface is configured to drop IGMP query packets.

Syntax

show ip igmp throttle interface [*interface*]

interface

ethernet *unit*/*port*

unit - Stack unit. (Range: 1)

port - Port number. (Range: 1-28)

port-channel *channel-id* (Range: 1-12)

Default Configuration

None

Command Mode

EXEC

User Guidelines

Using this command without specifying an interface displays all interfaces.

Example

Console#show ip igmp query-drop interface ethernet 1/1

Ethernet 1/1: Enabled

Console#

show ip igmp throttle interface

This command displays the interface settings for IGMP throttling.

Syntax

show ip igmp throttle interface [*interface*]

interface

ethernet *unit*/*port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-28)

port-channel *channel-id* (Range: 1-12)

Default Configuration

None

Command Mode

EXEC

User Guidelines

Using this command without specifying an interface displays information for all interfaces.

Example

```
Console#show ip igmp throttle interface ethernet 1/1
Eth 1/1 Information
Status: TRUE
Action: Deny
Max Multicast Groups: 32
Current Multicast Groups: 0
Console#
```

45. MLD Snooping

ipv6 mld snooping

This command enables MLD Snooping globally on the switch. Use the no form to disable MLD Snooping.

Syntax

[no] ipv6 mld snooping

Default Configuration

Disabled

Command Mode

Global Configuration

Example

The following example enables MLD Snooping:

Console(config)#ipv6 mld snooping

Console(config)#

ipv6 mld snooping querier

This command allows the switch to act as the querier for MLDv2 snooping. Use the no form to disable this feature.

Syntax

[no] ipv6 mld snooping querier

Default Configuration

Disabled

Command Mode

Global Configuration

User Guidelines

- If enabled, the switch will serve as querier if elected. The querier is responsible for asking hosts if they want to receive multicast traffic.
- An IPv6 address must be configured on the VLAN interface from which the querier will act if elected. When serving as the querier, the switch uses this IPv6 address as the query source address.
- The querier will not start or will disable itself after having started if it detects an IPv6 multicast router on the network.

Example

Console(config)#ipv6 mld snooping querier

Console(config)#

ipv6 mld snooping query-interval

This command configures the interval between sending MLD general queries. Use the no form to restore the default.

Syntax

ipv6 mld snooping query-interval *interval*

no ipv6 mld snooping query-interval

interval - The interval between sending MLD general queries. (Range: 60-125 seconds)

Default Configuration

125 seconds

Command Mode

Global Configuration

User Guidelines

- This command applies when the switch is serving as the querier.
- An MLD general query message is sent by the switch at the interval specified by this command. When this message is received by downstream hosts, all receivers build an MLD report for the multicast groups they have joined.

Example

Console(config)#ipv6 mld snooping query-interval 150

Console(config)#

ipv6 mld snooping query-max-response-time

This command configures the maximum response time advertised in MLD general queries. Use the no form to restore the default.

Syntax

ipv6 mld snooping query-max-response-time *seconds*

no ipv6 mld snooping query-max-response-time

seconds - The maximum response time allowed for MLD general queries. (Range: 5-25 seconds)

Default Configuration

10 seconds

Command Mode

Global Configuration

User Guidelines

This command controls how long the host has to respond to an MLD Query message before the switch deletes the group if it is the last member.

Example

Console(config)#ipv6 mld snooping query-max-response-time seconds 15

Console(config)#

ipv6 mld snooping robustness

This command configures the MLD Snooping robustness variable. Use the no form to restore the default value.

Syntax

ipv6 mld snooping robustness *value*

no ipv6 mld snooping robustness

value - The number of the robustness variable. (Range: 2-10)

Default Configuration

2

Command Mode

Global Configuration

User Guidelines

A port will be removed from the receiver list for a multicast service when no MLD reports are detected in response to a number of MLD queries. The robustness variable sets the number of queries on ports for which there is no report.

Example

Console(config)#ipv6 mld snooping robustness 2

Console(config)#

ipv6 mld snooping router-port-expire-time

This command configures the MLD query timeout. Use the no form to restore the default.

Syntax

ipv6 mld snooping router-port-expire-time *time*

no ipv6 mld snooping router-port-expire-time

time - Specifies the timeout of a dynamically learned router port. (Range: 300-500 seconds)

Default Configuration

300 seconds

Command Mode

Global Configuration

User Guidelines

The router port expire time is the time the switch waits after the previous querier stops before it considers the router port (i.e., the interface that had been receiving query packets) to have expired.

Example

Console(config)#ipv6 mld snooping router-port-expire-time 300

Console(config)#

ipv6 mld snooping unknown-multicast mode

This command sets the action for dealing with unknown multicast packets. Use the no form to restore the default.

Syntax

ipv6 mld snooping unknown-multicast mode {flood | to-router-port}

[no] ipv6 mld snooping unknown-multicast mode

flood - Floods the unknown multicast data packets to all ports.

to-router-port - Forwards the unknown multicast data packets to router ports.

Default Configuration

to-router-port

Command Mode

Global Configuration

User Guidelines

- When set to "flood," any received IPv6 multicast packets that have not been requested by a host are flooded to all ports in the VLAN.
- When set to "router-port," any received IPv6 multicast packets that have not been requested by a host are forwarded to ports that are connected to a detected multicast router.

Example

Console(config)#ipv6 mld snooping unknown-multicast mode flood

Console(config)#

ipv6 mld snooping version

This command configures the MLD snooping version. Use the no form to restore the default.

Syntax

ipv6 mld snooping version {1 | 2}

1 - MLD version 1.

2 - MLD version 2.

Default Configuration

Version 2

Command Mode

Global Configuration

Example

Console(config)#ipv6 mld snooping version 1

Console(config)#

ipv6 mld snooping vlan mrouter

This command statically configures an IPv6 multicast router port. Use the no form to remove the configuration.

Syntax

[no] ipv6 mld snooping vlan *vlan-id* mrouter *interface*

vlan-id - VLAN ID (Range: 1-4094)

interface

ethernet *unit*/*port*

unit - Stack unit. (Range: 1-6)

port - Port number. (Range: 1-28/52)

port-channel *channel-id* (Range: 1-16)

Default Configuration

No static multicast router ports are configured

Command Mode

Global Configuration

User Guidelines

Depending on your network connections, MLD snooping may not always be able to locate the MLD querier. Therefore, if the MLD querier is a known multicast router/switch connected over the network to an interface (port or trunk) on the switch, you can manually configure that interface to join all the current multicast groups.

Example

The following shows how to configure port 1 as a multicast router port within VLAN 1:

Console(config)#ipv6 mld snooping vlan 1 mrouter ethernet 1/1

Console(config)#

ipv6 mld snooping vlan static

This command adds a port to an IPv6 multicast group. Use the no form to remove the port.

Syntax

[no] ipv6 mld snooping vlan *vlan-id* static *ipv6-address interface*

vlan-id - VLAN ID (Range: 1-4094)

ipv6-address - An IPv6 address of a multicast group. (Format: X:X:X:X::X)

interface

ethernet *unit*/*port*

unit - Stack unit. (Range: 1-6)

port - Port number. (Range: 1-28/52)

port-channel *channel-id* (Range: 1-16)

Default Configuration

None

Command Mode

Global Configuration

Example

Console(config)#ipv6 mld snooping vlan 1 static FF00:0:0:0:0:0:0:10C ethernet 1/6

Console(config)#

ipv6 mld snooping vlan immediate-leave

This command immediately deletes a member port of an IPv6 multicast service when a leave packet is received at that port and immediate-leave is enabled for the parent VLAN. Use the no form to restore the default.

Syntax

[no] ipv6 mld snooping vlan *vlan-id* immediate-leave

vlan-id - VLAN ID (Range: 1-4094)

Default Configuration

Disabled

Command Mode

Global Configuration

User Guidelines

- If MLD immediate-leave is *not* used, a multicast router (or querier) will send a group-specific query message when an MLD group leave message is received. The router/querier stops forwarding traffic for that group only if no host replies to the query within the specified timeout period.
- If MLD immediate-leave is enabled, the switch assumes that only one host is connected to the interface. Therefore, immediate leave should only be enabled on an interface if it is connected to only one MLD-enabled device, either a service host or a neighbor running MLD snooping.

Example

The following shows how to enable MLD immediate leave.

Console(config)#interface vlan 1

Console(config-if)#ipv6 mld snooping immediate-leave

Console(config-if)#

clear ipv6 mld snooping groups dynamic

This command clears multicast group information dynamically learned through MLD snooping.

Syntax

clear ipv6 mld snooping groups dynamic

Command Mode

EXEC

User Guidelines

This command only clears entries learned though MLD snooping. Statically configured multicast address are not cleared.

Example

Console#clear ipv6 mld snooping groups dynamic

Console#

clear ipv6 mld snooping statistics

This command clears MLD snooping statistics

Syntax

clear ipv6 mld snooping statistics [interface *interface*]

interface

ethernet *unit*/*port*

unit - Stack unit. (Range: 1-6)

port - Port number. (Range: 1-28/52)

port-channel *channel-id* (Range: 1-16)

Command Mode

EXEC

Example

Console#clear ipv6 mld snooping statistics

Console#

show ipv6 mld snooping

This command shows the current MLD Snooping configuration.

Syntax

show ipv6 mld snooping

Command Mode

EXEC

Example

The following shows MLD Snooping configuration information:

Console#show ipv6 mld snooping

Service Status: Disabled

Querier Status: Disabled

Robustness: 2

Query Interval: 125 sec

Query Max Response Time: 10 sec

Router Port Expiry Time: 300 sec

Immediate Leave: Disabled on all VLAN

Unknown Flood Behavior: To Router Port

MLD Snooping Version: Version 2

Console#

show ipv6 mld snooping group

This command shows known multicast groups, member ports, and the means by

which each group was learned.

Syntax

show ipv6 mld snooping group

Command Mode

EXEC

Example

The following shows MLD Snooping group configuration information:

Console#show ipv6 mld snooping group

VLAN Multicast IPv6 Address Member port Type

---- ---------- ---------- ----------

1 FF02::01:01:01:01 Eth 1/1 MLD Snooping

1 FF02::01:01:01:02 Eth 1/1 Multicast Data

1 FF02::01:01:01:02 Eth 1/1 User

Console#

show ipv6 mld snooping group source-list

This command shows known multicast groups, member ports, the means by which each group was learned, and the corresponding source list.

Syntax

show ipv6 mld snooping group source-list

Command Mode

EXEC

Example

The following shows MLD Snooping group mapping information:

Console#show ipv6 mld snooping group source-list

Console#show ipv6 mld snooping group source-list

VLAN ID: 1

Mutlicast IPv6 Address: FF02::01:01:01:01

Member Port: Eth 1/1

Type: MLD Snooping

Filter Mode: Include

(if exclude filter mode)

Filter Timer elapse: 10 sec.

Request List: ::01:02:03:04, ::01:02:03:05, ::01:02:03:06, ::01:02:03:07

Exclude List: ::02:02:03:04, ::02:02:03:05, ::02:02:03:06, ::02:02:03:07

(if include filter mode)

Include List: ::02:02:03:04, ::02:02:03:05, ::02:02:03:06, ::02:02:03:06

Option:

Filter Mode: Include, Exclude

Console#

show ipv6 mld snooping mrouter

This command shows MLD Snooping multicast router information.

Syntax

show ipv6 mld snooping mrouter vlan *vlan-id*

vlan-id - A VLAN identification number. (Range: 1-4094)

Command Mode

EXEC

Example

Console#show ipv6 mld snooping mrouter vlan 1

VLAN Multicast Router Port Type Expire

---- --------------------- --------- ------

1 Eth 1/ 2 Static

Console#

46. MVR Commands

46.1 MVR for IPV4

mvr

This command enables Multicast VLAN Registration (MVR) globally on the switch. Use the no form of this command to globally disable MVR.

Syntax

[no] mvr

Default Configuration

Disabled

Command Mode

Global Configuration

User Guidelines

Only IGMP version 2 or 3 hosts can issue multicast join or leave messages. If MVR must be configured for an IGMP version 1 host, the multicast groups must be statically assigned using the mvr vlan group command.

Example

The following example enables MVR globally.

Console(config)#mvr

Console(config)#

mvr associated-profile

This command binds the MVR group addresses specified in a profile to an MVR domain. Use the no form of this command to remove the binding.

Syntax

[no] mvr domain *domain-id* associated-profile *profile-name*

domain-id - An independent multicast domain. (Range: 1-5)

profile-name - The name of a profile containing one or more MVR group addresses. (Range: 1-21 characters)

Default Configuration

Disabled

Command Mode

Global Configuration

Example

The following an MVR group address profile to domain 1:

Console(config)#mvr domain 1 associated-profile rd

Console(config)#

mvr domain

This command enables Multicast VLAN Registration (MVR) for a specific domain. Use the no form of this command to disable MVR for a domain.

Syntax

[no] mvr domain *domain-id*

domain-id - An independent multicast domain. (Range: 1-5)

Default Configuration

Disabled

Command Mode

Global Configuration

User Guidelines

Only IGMP version 2 or 3 hosts can issue multicast join or leave messages. If MVR must be configured for an IGMP version 1 host, the multicast groups must be statically assigned using the mvr vlan group command.

Example

The following example enables MVR for domain 1:

Console(config)#mvr domain 1

Console(config)#

mvr profile

This command maps a range of MVR group addresses to a profile. Use the no form of this command to remove the profile.

Syntax

mvr profile *profile-name start-ip-address end-ip-address*

profile-name - The name of a profile containing one or more MVR group addresses. (Range: 1-21 characters)

start-ip-address - Starting IPv4 address for an MVR multicast group. (Range: 224.0.1.0 - 239.255.255.255)

end-ip-address - Ending IPv4 address for an MVR multicast group. (Range: 224.0.1.0 - 239.255.255.255)

Default Configuration

No profiles are defined

Command Mode

Global Configuration

User Guidelines

- Use this command to statically configure all multicast group addresses that will join the MVR VLAN. Any multicast data associated an MVR group is sent from all source ports to all receiver ports that have registered to receive data from that multicast group.
- The IP address range from 224.0.0.0 to 239.255.255.255 is used for multicast streams. MVR group addresses cannot fall within the reserved IP multicast address range of 224.0.0.x.
- IGMP snooping and MVR share a maximum number of 1024 groups. Any multicast streams received in excess of this limitation will be flooded to all ports in the associated domain.

Example

The following example maps a range of MVR group addresses to a profile:

Console(config)#mvr profile rd 228.1.23.1 228.1.23.10

Console(config)#

mvr proxy-query-interval

This command configures the interval at which the receiver port sends out general queries. Use the no form to restore the default setting.

Syntax

mvr proxy-query-interval *interval*

no mvr proxy-query-interval

interval - The interval at which the receiver port sends out general queries. (Range: 2-31744 seconds)

Default Configuration

125 seconds

Command Mode

Global Configuration

User Guidelines

This command sets the general query interval at which active receiver ports send out general queries. This interval is only effective when proxy switching is enabled with the mvr proxy-switching command.

Example

This example sets the proxy query interval for MVR proxy switching.

Console(config)#mvr proxy-query-interval 250

Console(config)#

mvr priority

This command assigns a priority to all multicast traffic in the MVR VLAN. Use the no form of this command to restore the default setting.

Syntax

mvr priority *priority*

no mvr priority

priority - The CoS priority assigned to all multicast traffic forwarded into the MVR VLAN. (Range: 0-6, where 6 is the highest priority)

Default Configuration

Disabled

Command Mode

Global Configuration

User Guidelines

This command can be used to set a high priority for low-latency multicast traffic such as a video-conference, or to set a low priority for normal multicast traffic not sensitive to latency.

Example

Console(config)#mvr priority 6

Console(config)#

mvr proxy-switching

This command enables MVR proxy switching, where the source port acts as a host, and the receiver port acts as an MVR router with querier service enabled. Use the no form to disable this function.

Syntax

[no] mvr proxy-switching

Default Configuration

Enabled

Command Mode

Global Configuration

User Guidelines

- When MVR proxy-switching is enabled, an MVR source port serves as the upstream or host interface. The source port performs only the host portion of MVR by sending summarized membership reports, and automatically disables MVR router functions.
- Receiver ports are known as downstream or router interfaces. These interfaces perform the standard MVR router functions by maintaining a database of all MVR subscriptions on the downstream interface. Receiver ports must therefore be configured on all downstream interfaces which require MVR proxy service.
- When the source port receives report and leave messages, it only forwards them to other source ports.
- When receiver ports receive any query messages, they are dropped.

- When changes occurring in the downstream MVR groups are learned by the receiver ports through report and leave messages, an MVR state change report is created and sent to the upstream source port, which in turn forwards this information upstream.
- When MVR proxy switching is disabled:

a. Any membership reports received from receiver/source ports are forwarded to all source ports.

b. When a source port receives a query message, it will be forwarded to all downstream receiver ports.

c. When a receiver port receives a query message, it will be dropped.

Example

The following example enable MVR proxy switching.

Console(config)#mvr proxy-switching

Console(config)#

mvr robustness-value

This command configures the expected packet loss, and thereby the number of times to generate report and group-specific queries. Use the no form to restore the default setting.

Syntax

mvr robustness-value *value*

no mvr robustness-value

value - The robustness used for all interfaces. (Range: 1-255)

Default Configuration

2

Command Mode

Global Configuration

User Guidelines

- This command is used to set the number of times report messages are sent upstream when changes are learned about downstream groups, and the number of times group-specific queries are sent to downstream receiver ports.
- This command only takes effect when MVR proxy switching is enabled.

Example

Console(config)#mvr robustness-value 5

Console(config)#

mvr source-port-mode dynamic

This command configures the switch to only forward multicast streams which the source port has dynamcially joined. Use the no form to restore the default setting.

Syntax

[no] mvr source-port-mode dynamic

Default Configuration

Forwards all multicast streams which have been specified in a profile and bound to a domain.

Command Mode

Global Configuration

User Guidelines

- By default, the switch forwards any multicast streams within the address range set by a profile, and bound to a domain. The multicast streams are sent to all source ports on the switch and to all receiver ports that have elected to receive data on that multicast address.

- When the mvr source-port-mode dynamic command is used, the switch only forwards multicast streams which the source port has dynamically joined. In other words, both the receiver port and source port must subscribe to a multicast group before a multicast stream is forwarded to any attached client. Note that the requested streams are still restricted to the address range which has been specified in a profile and bound to a domain.

Example

Console(config)#mvr source-port-mode dynamic

Console(config)#

mvr upstream-source-ip

This command configures the source IP address assigned to all MVR control packets sent upstream on all domains or on a specified domain. Use the no form to restore the default setting.

Syntax

mvr [domain *domain-id*] upstream-source-ip *source-ip-address*

no mvr [domain *domain-id*] upstream-source-ip

domain-id - An independent multicast domain. (Range: 1-5)

source-ip-address – The source IPv4 address assigned to all MVR control packets sent upstream.

Default Configuration

All MVR reports sent upstream use a null source IP address

Command Mode

Global Configuration

Example

Console(config)#mvr domain 1 upstream-source-ip 192.168.0.3

Console(config)#

mvr vlan

This command specifies the VLAN through which MVR multicast data is received. Use the no form of this command to restore the default MVR

VLAN.

Syntax

mvr domain *domain-id* vlan *vlan-id*

no mvr domain *domain-id* vlan

domain-id - An independent multicast domain. (Range: 1-5)

vlan-id - Specifies the VLAN through which MVR multicast data is received. This is also the VLAN to which all source ports must be assigned. (Range: 1-4094)

Default Configuration

VLAN 1

Command Mode

Global Configuration

User Guidelines

- This command specifies the VLAN through which MVR multicast data is received. This is the VLAN to which all source ports must be assigned.
- The VLAN specified by this command must be an existing VLAN configured with the vlan command.
- MVR source ports can be configured as members of the MVR VLAN using the switchport allowed vlan command and switchport access vlan command, but MVR receiver ports should not be statically configured as members of this VLAN.

Example

The following example sets the MVR VLAN to VLAN 2:

Console(config)#mvr

Console(config)#mvr domain 1 vlan 2

Console(config)#

mvr immediate-leave

This command causes the switch to immediately remove an interface from a multicast stream as soon as it receives a leave message for that group. Use the no form to restore the default settings.

Syntax

[no] mvr [domain *domain-id*] immediate-leave

domain-id - An independent multicast domain. (Range: 1-5)

Default Configuration

Disabled

Command Mode

Interface Configuration (Ethernet, Port Channel)

User Guidelines

- Immediate leave applies only to receiver ports. When enabled, the receiver port is immediately removed from the multicast group identified in the leave message. When immediate leave is disabled, the switch follows the standard rules by sending a group-specific query to the receiver port and waiting for a response to determine if there are any remaining subscribers for that multicast group before removing the port from the group list.
- Using immediate leave can speed up leave latency, but should only be enabled on a port attached to only one multicast subscriber to avoid disrupting services to other group members attached to the same interface.
- Immediate leave does not apply to multicast groups which have been statically assigned to a port with the mvr vlan group command.

Example

The following enables immediate leave on a receiver port.

Console(config)#interface ethernet 1/5

Console(config-if)#mvr domain 1 immediate-leave

Console(config-if)#

mvr type

This command configures an interface as an MVR receiver or source port. Use the no form to restore the default settings.

Syntax

[no] mvr [domain *domain-id*] type {receiver | source}

domain-id - An independent multicast domain. (Range: 1-5)

receiver - Configures the interface as a subscriber port that can receive multicast data.

source - Configures the interface as an uplink port that can send and receive multicast data for the configured multicast groups.

Default Configuration

The port type is not defined.

Command Mode

Interface Configuration (Ethernet, Port Channel)

User Guidelines

- A port which is not configured as an MVR receiver or source port can use IGMP snooping to join or leave multicast groups using the standard rules for multicast filtering.
- Receiver ports can belong to different VLANs, but should not normally be configured as a member of the MVR VLAN. IGMP snooping can also be used to allow a receiver port to dynamically join or leave multicast groups not sourced through the MVR VLAN. Also, note that VLAN membership for MVR receiver ports cannot be set to access mode (see the switchport mode command).
- One or more interfaces may be configured as MVR source ports. A source port is able to both receive and send data for multicast groups which it has joined through the MVR protocol or which have been assigned through the mvr vlan group command.
- Only IGMP version 2 or 3 hosts can issue multicast join or leave messages. If MVR must be configured for an IGMP version 1 host, the multicast groups must be statically assigned using the mvr vlan group command.

Example

The following configures one source port and several receiver ports on the

switch.

```
Console(config)#interface ethernet 1/5
Console(config-if)#mvr domain 1 type source
Console(config-if)#exit
Console(config)#interface ethernet 1/6
Console(config-if)#mvr domain 1 type receiver
Console(config-if)#exit
Console(config)#interface ethernet 1/7
Console(config-if)#mvr domain 1 type receiver
Console(config-if)#
```

mvr vlan group

This command statically binds a multicast group to a port which will receive long-term multicast streams associated with a stable set of hosts. Use the no form to restore the default settings.

Syntax

[no] mvr [domain *domain-id*] vlan *vlan-id* group *ip-address*

domain-id - An independent multicast domain. (Range: 1-5)

vlan-id - Receiver VLAN to which the specified multicast traffic is flooded. (Range: 1-4094)

group - Defines a multicast service sent to the selected port.

ip-address - Statically configures an interface to receive multicast traffic from the IPv4 address specified for an MVR multicast group. (Range: 224.0.1.0 - 239.255.255.255)

Default Configuration

No receiver port is a member of any configured multicast group.

Command Mode

Interface Configuration (Ethernet, Port Channel)

User Guidelines

- Multicast groups can be statically assigned to a receiver port using this command.
- The IP address range from 224.0.0.0 to 239.255.255.255 is used for multicast streams. MVR group addresses cannot fall within the reserved IP multicast address range of 224.0.0.x.
- Only IGMP version 2 or 3 hosts can issue multicast join or leave messages. If MVR must be configured for an IGMP version 1 host, the multicast groups must be statically assigned using the mvr vlan group command.
- The MVR VLAN cannot be specified as the receiver VLAN for static bindings.

Example

The following statically assigns a multicast group to a receiver port:

Console(config)#interface ethernet 1/7

Console(config-if)#mvr domain 1 type receiver

Console(config-if)#mvr domain 1 vlan 3 group 225.0.0.5

Console(config-if)#

show mvr

This command shows information about MVR domain settings, including MVR operational status, the multicast VLAN, the current number of group addresses, and the upstream source IP address.

Syntax

show mvr [domain *domain-id*]

domain-id - An independent multicast domain. (Range: 1-5)

Default Configuration

Displays configuration settings for all MVR domains.

Command Mode

EXEC

Example

The following shows the MVR settings:

Console#show mvr

MVR 802.1p Forwarding Priority: Disabled

MVR 802.1p Forwarding Priority: Disabled

MVR Proxy Switching: Enabled

MVR Robustness Value: 1

MVR Proxy Query Interval: 125(sec.)

MVR Source Port Mode: Always Forward

MVR Domain: 1

MVR Config Status: Enabled

MVR Running Status: Active

MVR Multicast VLAN: 1

MVR Current Learned Groups: 10

MVR Upstream Source IP: 192.168.0.3

...

show mvr associated-profile

This command shows the profiles bound the specified domain.

Syntax

show mvr [domain *domain-id*] associated-profile

domain-id - An independent multicast domain. (Range: 1-5)

Default Configuration

Displays profiles bound to all MVR domains.

Command Mode

EXEC

Example

The following displays the profiles bound to domain 1:

Console#show mvr domain 1 associated-profile

Domain ID: 1

MVR Profile Name Start IP Addr. End IP Addr.

---------- ---------- ----------

rd 228.1.23.1 228.1.23.10

testing 228.2.23.1 228.2.23.10

Console#

show mvr interface

This command shows MVR configuration settings for interfaces attached to the MVR VLAN.

Syntax

show mvr [domain *domain-id*] interface

domain-id - An independent multicast domain. (Range: 1-5)

Default Configuration

Displays configuration settings for all attached interfaces.

Command Mode

EXEC

Example

The following displays information about the interfaces attached to the MVR VLAN in domain 1:

Console#show mvr domain 1 interface

MVR Domain: 1

Port Type Status Immediate Static Group Address

-------- -------- ---------- --------- ----------

Eth 1/ 1 Source Active/Forwarding

Eth 1/ 2 Receiver Inactive/Discarding Disabled 234.5.6.8(VLAN2)

Eth1/ 3 Source Inactive/Discarding

Eth1/ 1 Receiver Active/Forwarding Disabled 225.0.0.1(VLAN1)

225.0.0.9(VLAN3)

Eth1/ 4 Receiver Active/Discarding Disabled

Console#

show mvr members

This command shows information about the current number of entries in the forwarding database, detailed information about a specific multicast address, the IP address of the hosts subscribing to all active multicast groups, or the multicast groups associated with each port.

Syntax

show mvr [domain *domain-id*] members [*ip-address* | host-ip-address [*interface*] | sort-by-port [*interface*]]]

domain-id - An independent multicast domain. (Range: 1-5)

ip-address - IPv4 address for an MVR multicast group. (Range: 224.0.1.0 - 239.255.255.255)

members - The multicast groups assigned to the MVR VLAN.

host-ip-address - The subscriber IP addresses.

sort-by-port - The multicast groups associated with an interface.

interface

ethernet *unit*/*port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-28)

port-channel *channel-id* (Range: 1-12)

Default Configuration

Displays configuration settings for all domains and all forwarding entries.

Command Mode

EXEC

Example

The following shows information about the number of multicast forwarding entries currently active in domain 1:

Console#show mvr domain 1 members

MVR Domain: 1

MVR Forwarding Entry Count :1

Flag: S - Source port, R - Receiver port.

H - Host counts (number of hosts joined to group on this port).

P - Port counts (number of ports joined to group).

Up time: Group elapsed time (d:h:m:s).

Expire: Group remaining time (m:s).

Group Address VLAN Port Up time Expire Count

--------------- ---- ----------- ----------- ------ --------

234.5.6.7 1 00:00:09:17 2(P)

1 Eth 1/ 1(S)

2 Eth 1/ 2(R)

Console#

The following example shows detailed information about a specific multicast address:

Console#show mvr domain 1 members 234.5.6.7

MVR Domain: 1

MVR Forwarding Entry Count :1

Flag: S - Source port, R - Receiver port.

H - Host counts (number of hosts joined to group on this port).

P - Port counts (number of ports joined to group).

Up time: Group elapsed time (d:h:m:s).

Expire: Group remaining time (m:s).

Group Address VLAN Port Up time Expire Count

--------------- ---- ----------- ----------- ------ --------

234.5.6.7 1 2(P)

1 Eth 1/ 1(S)

2 Eth 1/ 2(R)

Console#

show mvr profile

This command shows all configured MVR profiles.

Command Mode

EXEC

Example

The following shows all configured MVR profiles:

Console#show mvr profile

MVR Profile Name Start IP Addr. End IP Addr.

-------------------- ---------------- ----------------

rd 228.1.23.1 228.1.23.10

testing 228.2.23.1 228.2.23.10

Console#

show mvr statistics

This command shows MVR protocol-related statistics for the specified interface.

Syntax

show mvr statistics {input | output} [interface *interface*]

show mvr domain *domain-id* statistics {input [interface *interface*] | output [interface *interface*] | query}

domain-id - An independent multicast domain. (Range: 1-5)

interface

ethernet *unit*/*port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-28)

port-channel *channel-id* (Range: 1-12)

vlan *vlan-id* - VLAN ID (Range: 1-4094)

query - Displays MVR query-related statistics.

Default Configuration

Displays statistics for all domains.

Command Mode

EXEC

Example

The following shows MVR protocol-related statistics received:

Console#show mvr domain 1 statistics input

MVR Domain: 1

Input Statistics:

Interface Report Leave G Query G(-S)-S Query Drop Join Succ Group

--------- -------- -------- -------- -------------- -------- --------- ------

Eth 1/ 1 23 11 4 10 5 20 9

Eth 1/ 2 12 15 8 3 5 19 4

VLAN 1 2 0 0 2 2 20 9

Console#

46.2 MVR for IPV6

mvr6 associated-profile

This command binds the MVR group addresses specified in a profile to an MVR domain. Use the no form of this command to remove the binding.

Syntax

[no] mvr6 domain *domain-id* associated-profile *profile-name*

domain-id - An independent multicast domain. (Range: 1-5)

profile-name - The name of a profile containing one or more MVR group addresses. (Range: 1-21 characters)

Default Configuration

Disabled

Command Mode

Global Configuration

User Guidelines

MRV6 domains can be associated with more than one MVR6 profile. But since MVR6 domains cannot share the group range, an MRV6 profile can only be associated with one MVR6 domain.

Example

The following an MVR group address profile to domain 1:

Console(config)#mvr6 domain 1 associated-profile rd

Console(config)#

mvr6 domain

This command enables Multicast VLAN Registration (MVR) for a specific domain. Use the no form of this command to disable MVR for a domain.

Syntax

[no] mvr6 domain *domain-id*

domain-id - An independent multicast domain. (Range: 1-5)

Default Configuration

Disabled

Command Mode

Global Configuration

User Guidelines

When MVR6 is enabled on a domain, any multicast data associated with an MVR6 group is sent from all designated source ports, to all receiver ports that have registered to receive data from that multicast group.

Example

The following example enables MVR for domain 1:

Console(config)#mvr6 domain 1

Console(config)#

mvr6 profile

This command maps a range of MVR group addresses to a profile. Use the no form of this command to remove the profile.

Syntax

mvr6 profile *profile-name start-ip-address end-ip-address*

profile-name - The name of a profile containing one or more MVR group addresses. (Range: 1-21 characters)

start-ip-address - Starting IPv6 address for an MVR multicast group. This parameter must be a full IPv6 address including the network prefix and host address bits.

end-ip-address - Ending IPv6 address for an MVR multicast group. This parameter must be a full IPv6 address including the network prefix and host address bits.

Default Configuration

No profiles are defined

Command Mode

Global Configuration

User Guidelines

- Use this command to statically configure all multicast group addresses that will join the MVR VLAN. Any multicast data associated with an MVR group is sent from all source ports, and to all receiver ports that have registered to receive data from that multicast group.

- All IPv6 addresses must be according to RFC 2373 "IPv6 Addressing Architecture," using 8 colon-separated 16-bit hexadecimal values. One double colon may be used in the address to indicate the appropriate number of zeros required to fill the undefined fields. (Note that the IP address ff02::X is reserved.)
- The MVR6 group address range assigned to a profile cannot overlap with the group address range of any other profile.

Example

The following example maps a range of MVR group addresses to a profile:

Console(config)#mvr6 profile rd ff00::1 ff00::9

Console(config)#

mvr6 proxy-query-interval

This command configures the interval at which the receiver port sends out general queries. Use the no form to restore the default setting.

Syntax

mvr proxy-query-interval *interval*

no mvr proxy-query-interval

interval - The interval at which the receiver port sends out general queries. (Range: 2-31744 seconds)

Default Configuration

125 seconds

Command Mode

Global Configuration

User Guidelines

This command sets the general query interval at which active receiver ports send out general queries. This interval is only effective when proxy switching is enabled with the mvr6 proxy-switching command.

Example

This example sets the proxy query interval for MVR proxy switching.

Console(config)#mvr profile rd 228.1.23.1 228.1.23.10

Console(config)#

mvr6 proxy-switching

This command enables MVR proxy switching, where the source port acts as a host, and the receiver port acts as an MVR router with querier service enabled. Use the no form to disable this function.

Syntax

[no] mvr6 proxy-switching

Default Configuration

Enabled

Command Mode

Global Configuration

User Guidelines

- When MVR proxy-switching is enabled, an MVR source port serves as the upstream or host interface, and the MVR receiver port serves as the querier. The source port performs only the host portion of MVR by sending summarized membership reports, and automatically disables MVR router functions.
- Receiver ports are known as downstream or router interfaces. These interfaces perform the standard MVR router functions by maintaining a database of all MVR subscriptions on the downstream interface. Receiver ports must therefore be configured on all downstream interfaces which require MVR proxy service.
- When the source port receives report and leave messages, it only forwards them to other source ports.

- When receiver ports receive any query messages, they are dropped.
- When changes occurring in the downstream MVR groups are learned by the receiver ports through report and leave messages, an MVR state change report is created and sent to the upstream source port, which in turn forwards this information upstream.
- When MVR proxy switching is disabled:

a. Any membership reports received from receiver/source ports are forwarded to all source ports.

b. When a source port receives a query message, it will be forwarded to all downstream receiver ports.

c. When a receiver port receives a query message, it will be dropped.

Example

The following example enable MVR proxy switching.

Console(config)#mvr proxy-switching

Console(config)#

mvr6 robustness-value

This command configures the expected packet loss, and thereby the number of times to generate report and group-specific queries. Use the no form to restore the default setting.

Syntax

mvr6 robustness-value *value*

no mvr6 robustness-value

value - The robustness used for all interfaces. (Range: 1-10)

Default Configuration

2

Command Mode

Global Configuration

User Guidelines

- This command is used to set the number of times report messages are sent upstream when changes are learned about downstream groups, and the number of times group-specific queries are sent to downstream receiver ports.
- This command only takes effect when MVR6 proxy switching is enabled.

Example

Console(config)#mvr6 robustness-value 5

Console(config)#

mvr6 source-port-mode dynamic

This command configures the switch to only forward multicast streams which the source port has dynamically joined. Use the no form to restore the default setting.

Syntax

[no] mvr6 source-port-mode dynamic

Default Configuration

Forwards all multicast streams which have been specified in a profile and bound to a domain.

Command Mode

Global Configuration

User Guidelines

- By default, the switch forwards any multicast streams within the address range set by a profile, and bound to a domain. The multicast streams are sent to all source ports on the switch and to all receiver ports that have elected to receive data on that multicast address.

- When the mvr6 source-port-mode dynamic command is used, the switch only forwards multicast streams which the source port has dynamically joined. In other words, both the receiver port and source port must subscribe to a multicast group before a multicast stream is forwarded to any attached client. Note that the requested streams are still restricted to the address range which has been specified in a profile and bound to a domain.

Example

Console(config)#mvr6 source-port-mode dynamic

Console(config)#

mvr6 upstream-source-ip

This command configures the source IPv6 address assigned to all MVR control packets sent upstream on the specified domain. Use the no form to restore the default setting.

Syntax

mvr6 domain *domain-id* upstream-source-ip *source-ip-address*

no mvr6 domain *domain-id* upstream-source-ip

domain-id - An independent multicast domain. (Range: 1-5)

source-ip-address – The source IPv6 address assigned to all MVR control packets sent upstream. This parameter must be a full IPv6 address including the network prefix and host address bits.

Default Configuration

All MVR reports sent upstream use a null source IP address

Command Mode

Global Configuration

User Guidelines

All IPv6 addresses must be according to RFC 2373 "IPv6 Addressing Architecture," using 8 colon-separated 16-bit hexadecimal values. One double colon may be used in the address to indicate the appropriate number of zeros required to fill the undefined fields. (Note that the IP address ff02::X is reserved.)

Example

Console(config)#mvr6 domain 1 upstream-source-ip 2001:DB8:2222:7223::72

Console(config)#

mvr6 vlan

This command specifies the VLAN through which MVR multicast data is received. Use the no form of this command to restore the default MVR VLAN.

Syntax

mvr6 domain *domain-id* vlan *vlan-id*

no mvr6 domain *domain-id* vlan

domain-id - An independent multicast domain. (Range: 1-5)

vlan-id - Specifies the VLAN through which MVR multicast data is received. This is also the VLAN to which all source ports must be assigned. (Range: 1-4094)

Default Configuration

VLAN 1

Command Mode

Global Configuration

User Guidelines

MVR source ports can be configured as members of the MVR VLAN using the switchport allowed vlan command and switchport access vlan command, but MVR receiver ports should not be statically configured as members of this VLAN.

Example

The following example sets the MVR VLAN to VLAN 1:

Console(config)#mvr6 domain 1 vlan 1

Console(config)#

mvr6 immediate-leave

This command causes the switch to immediately remove an interface from a multicast stream as soon as it receives a leave message for that group. Use the no form to restore the default settings.

Syntax

[no] mvr6 domain *domain-id* immediate-leave

domain-id - An independent multicast domain. (Range: 1-5)

Default Configuration

Disabled

Command Mode

Interface Configuration (Ethernet, Port Channel)

User Guidelines

- Immediate leave applies only to receiver ports. When enabled, the receiver port is immediately removed from the multicast group identified in the leave message. When immediate leave is disabled, the switch follows the standard rules by sending a group-specific query to the receiver port and waiting for a response to determine if there are any remaining subscribers for that multicast group before removing the port from the group list.
- Using immediate leave can speed up leave latency, but should only be enabled on a port attached to only one multicast subscriber to avoid disrupting services to other group members attached to the same interface.
- Immediate leave does not apply to multicast groups which have been statically assigned to a port with the mvr6 vlan group command.

Example

The following enables immediate leave on a receiver port.

Console(config)#interface ethernet 1/5

Console(config-if)#mvr6 domain 1 immediate-leave

Console(config-if)#

mvr6 type

This command configures an interface as an MVR receiver or source port. Use the no form to restore the default settings.

Syntax

[no] mvr6 domain *domain-id* type {receiver | source}

domain-id - An independent multicast domain. (Range: 1-5)

receiver - Configures the interface as a subscriber port that can

receive multicast data.

source - Configures the interface as an uplink port that can send and receive multicast data for the configured multicast groups. Note that the source port must be manually configured as a member of the MVR6 VLAN using the switchport allowed vlan command.

Default Configuration

The port type is not defined.

Command Mode

Interface Configuration (Ethernet, Port Channel)

User Guidelines

- A port configured as an MVR6 receiver or source port can join or leave multicast groups configured under MVR6.
- Receiver ports can belong to different VLANs, but should not be configured as a member of the MVR VLAN. Also, note that VLAN membership for MVR receiver ports cannot be set to access mode (see the switchport mode command).
- One or more interfaces may be configured as MVR source ports. A source port is able to both receive and send data for multicast groups which it has joined through the MVR6 protocol or which have been assigned through the mvr6 vlan group command. All source ports must belong to the MVR6 VLAN. Subscribers should not be directly connected to source ports.
- The same port cannot be configured as a source port in one MVR domain and as a receiver port in another domain.

Example

The following configures one source port and several receiver ports on the switch.

Console(config)#interface ethernet 1/5

Console(config-if)#mvr6 domain 1 type source

Console(config-if)#exit

Console(config)#interface ethernet 1/6

Console(config-if)#mvr6 domain 1 type receiver

Console(config-if)#exit

Console(config)#interface ethernet 1/7

Console(config-if)#mvr6 domain 1 type receiver

Console(config-if)#

mvr6 vlan group

This command statically binds a multicast group to a port which will receive long-term multicast streams associated with a stable set of hosts. Use the no form to restore the default settings.

Syntax

[no] mvr6 domain *domain-id* vlan *vlan-id* group *ip-address*

domain-id - An independent multicast domain. (Range: 1-5)

vlan-id - Receiver VLAN to which the specified multicast traffic is flooded. (Range: 1-4094)

group - Defines a multicast service sent to the selected port.

ip-address - Statically configures an interface to receive multicast traffic from the IPv6 address specified for an MVR multicast group. This parameter must be a full IPv6 address including the network prefix and host address bits.

Default Configuration

No receiver port is a member of any configured multicast group.

Command Mode

Interface Configuration (Ethernet, Port Channel)

User Guidelines

- Multicast groups can be statically assigned to a receiver port using this command. The assigned address must fall within the range set by the mvr6 associated-profile command.

- All IPv6 addresses must be according to RFC 2373 "IPv6 Addressing Architecture," using 8 colon-separated 16-bit hexadecimal values. One double colon may be used in the address to indicate the appropriate number of zeros required to fill the undefined fields. (Note that the IP address ff02::X is reserved.)
- The MVR VLAN cannot be specified as the receiver VLAN for static bindings.

Example

The following statically assigns a multicast group to a receiver port:

Console(config)#interface ethernet 1/2

Console(config-if)#mvr6 domain 1 type receiver

Console(config-if)#mvr6 domain 1 vlan 2 group ff00::1

Console(config-if)#

show mvr6

This command shows information about MVR domain settings, including MVR operational status, the multicast VLAN, the current number of group addresses, and the upstream source IP address.

Syntax

show mvr6 [domain *domain-id*]

domain-id - An independent multicast domain. (Range: 1-5)

Default Configuration

Displays configuration settings for all MVR domains.

Command Mode

EXEC

Example

The following shows the MVR settings:

Console#show mvr6

MVR6 Proxy Switching : Enabled

MVR6 Robustness Value : 1

MVR6 Domain : 1

MVR6 Config Status : Enabled

MVR6 Running Status : Active

MVR6 Multicast VLAN : 1

MVR6 Upstream Source IP : FF05::25

Console#

show mvr6 associated-profile

This command shows the profiles bound the specified domain.

Syntax

show mvr6 [domain *domain-id*] associated-profile

domain-id - An independent multicast domain. (Range: 1-5)

Default Configuration

Displays profiles bound to all MVR domains.

Command Mode

EXEC

Example

The following displays the profiles bound to domain 1:

Console#show mvr6 domain 1 associated-profile

Domain ID : 1

MVR Profile Name Start IPv6 Addr. End IPv6 Addr.

---------- ---------- ----------

rd FF00::1 FF00::9

Console#

show mvr6 interface

This command shows MVR configuration settings for interfaces attached to the MVR VLAN.

Syntax

show mvr6 [domain *domain-id*] interface

domain-id - An independent multicast domain. (Range: 1-5)

Default Configuration

Displays configuration settings for all attached interfaces.

Command Mode

EXEC

Example

The following displays information about the interfaces attached to the MVR VLAN in domain 1:

Console#show mvr6 domain 1 interface

MVR6 Domain: 1

Port Type Status Immediate Static Group Address

-------- -------- ---------- --------- ----------

Eth1/ 1 Source Active/Up

Eth1/ 2 Receiver Active/Up Disabled FF00::1(VLAN2)

Console#

show mvr6 members

This command shows information about the current number of entries in the forwarding database, or detailed information about a specific multicast address.

Syntax

show mvr6 [domain *domain-id*] members [*ip-address*]

domain-id - An independent multicast domain. (Range: 1-5)

ip-address - IPv6 address for an MVR multicast group.

Default Configuration

Displays configuration settings for all domains and all forwarding entries.

Command Mode

EXEC

Example

The following shows information about the number of multicast forwarding entries currently active in domain 1:

Console#show mvr6 domain 1 members

MVR6 Domain: 1

MVR6 Forwarding Entry Count :1

Flag: S - Source port, R - Receiver port.

H - Host counts (number of hosts join the group on this port).

P - Port counts (number of ports join the group).

Up time: Group elapsed time (d:h:m:s).

Expire: Group remaining time (m:s).

Group Address VLAN Port Up time Expire Count

---------- ---- ---------- ---------- ------ --------

FF00::1 1 2(P)

1 Eth1/ 1(S)

2 Eth1/ 2(S)

Console#

The following example shows detailed information about a specific multicast address:

Console#show mvr6 domain 1 members ff00::1

MVR6 Domain: 1

MVR6 Forwarding Entry Count :1

Flag: S - Source port, R - Receiver port.

H - Host counts (number of hosts join the group on this port).

P - Port counts (number of ports join the group).

Up time: Group elapsed time (d:h:m:s).

Expire: Group remaining time (m:s).

Group Address VLAN Port Up time Expire Count

---------- ---- ---------- ---------- ------ --------

FF00::1 1 2(P)

1 Eth1/ 1(S)

2 Eth1/ 2(S)

Console#

show mvr6 profile

This command shows all configured MVR profiles.

Command Mode

EXEC

Example

The following shows all configured MVR profiles:

Console#show mvr6 profile

MVR Profile Name Start IPv6 Addr. End IPv6 Addr.

---------- ---------- ----------

rd FF00::1 FF00::9

Console#

show mvr6 statistics

This command shows MVR protocol-related statistics for the specified interface.

Syntax

show mvr6 statistics {input | output} [interface *interface*]

show mvr6 domain *domain-id* statistics {input [interface *interface*] | output [interface *interface*] | query}

domain-id - An independent multicast domain. (Range: 1-5)

interface

ethernet *unit*/*port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-28)

port-channel *channel-id* (Range: 1-12)

vlan *vlan-id* - VLAN ID (Range: 1-4094)

query - Displays MVR query-related statistics.

Default Configuration

Displays statistics for all domains.

Command Mode

EXEC

Example

The following shows MVR protocol-related statistics received:

Console#show mvr6 domain 1 statistics input

MVR Domain: 1

Input Statistics:

Interface Report Leave G Query G(-S)-S Query Drop Join Succ Group

--------- -------- -------- -------- -------------- -------- --------- ------

Eth 1/ 1 23 11 4 10 5 20 9

Eth 1/ 2 12 15 8 3 5 19 4

VLAN 1 2 0 0 2 2 20 9

Console#

The following shows MVR protocol-related statistics sent:

Console#show mvr6 domain 1 statistics output

MVR Domain: 1

Output Statistics:

Interface Report Leave G Query G(-S)-S Query

--------- -------- -------- -------- --------------

Eth 1/ 1 12 0 1 0

Eth 1/ 2 5 1 4 1

VLAN 1 7 2 3 0

Console#

The following shows MVR query-related statistics:

Console#show mvr6 domain 1 statistics query

Querier IPv6 Address: FE80::2E0:CFF:FE00:FB/64

Querier Expire Time: 00(h):00(m):30(s)

General Query Received: 10

General Query Sent: 0

Specific Query Received: 2

Specific Query Sent: 0

Number of Reports Sent: 2

Number of Leaves Sent: 0

Console#

47. LLDP Commands

lldp

This command enables LLDP globally on the switch. Use the no form to disable LLDP.

Syntax

[no] lldp

Default Configuration

Enabled

Command Mode

Global Configuration

Example

Console(config)#lldp

Console(config)#

lldp holdtime-multiplier

This command configures the time-to-live (TTL) value sent in LLDP advertisements. Use the no form to restore the default setting.

Syntax

lldp holdtime-multiplier *value*

no lldp holdtime-multiplier

value - Calculates the TTL in seconds based on the following rule: minimum of ((Transmission Interval * Holdtime Multiplier), or 65536) (Range: 2 - 10)

Default Configuration

Holdtime multiplier: 4

TTL: 4*30 = 120 seconds

Command Mode

Global Configuration

User Guidelines

The time-to-live tells the receiving LLDP agent how long to retain all information pertaining to the sending LLDP agent if it does not transmit updates in a timely manner.

Example

Console(config)#lldp holdtime-multiplier 10

Console(config)#

lldp med-fast-start-count

This command specifies the amount of MED Fast Start LLDPDUs to transmit during the activation process of the LLDP-MED Fast Start mechanism.

Syntax

lldp med-fast-start-count *packets*

seconds - Amount of packets. (Range: 1-10 packets; Default: 4 packets)

Default Configuration

4 packets

Command Mode

Global Configuration

User Guidelines

This parameter is part of the timer which ensures that the LLDP-MED Fast Start mechanism is active for the port. LLDP-MED Fast Start is critical to the timely startup of LLDP, and therefore integral to the rapid availability of Emergency Call Service.

Example

Console(config)#lldp med-fast-start-count 6

Console(config)#

lldp notification-interval

This command configures the allowed interval for sending SNMP notifications about LLDP MIB changes. Use the no form to restore the default setting.

Syntax

lldp notification-interval *seconds*

no lldp notification-interval

seconds - Specifies the periodic interval at which SNMP notifications are sent. (Range: 5 - 3600 seconds)

Default Configuration

5 seconds

Command Mode

Global Configuration

User Guidelines

- This parameter only applies to SNMP applications which use data stored in the LLDP MIB for network monitoring or management.
- Information about changes in LLDP neighbors that occur between SNMP notifications is not transmitted. Only state changes that exist at the time of a notification are included in the transmission. An SNMP agent should therefore periodically check the value of lldpStatsRemTableLastChangeTime to detect any lldpRemTablesChange notification-events missed due to throttling or transmission loss.

Example

Console(config)#lldp notification-interval 30

Console(config)#

lldp refresh-interval

This command configures the periodic transmit interval for LLDP advertisements. Use the no form to restore the default setting.

Syntax

lldp refresh-interval *seconds*

no lldp refresh-delay

seconds - Specifies the periodic interval at which LLDP advertisements are sent. (Range: 5 - 32768 seconds)

Default Configuration

30 seconds

Command Mode

Global Configuration

Example

Console(config)#lldp refresh-interval 60

Console(config)#

lldp reinit-delay

This command configures the delay before attempting to re-initialize after LLDP ports are disabled or the link goes down. Use the no form to restore the default setting.

Syntax

lldp reinit-delay *seconds*

no lldp reinit-delay

seconds - Specifies the delay before attempting to re-initialize LLDP. (Range: 1 - 10 seconds)

Default Configuration

2 seconds

Command Mode

Global Configuration

User Guidelines

When LLDP is re-initialized on a port, all information in the remote systems LLDP MIB associated with this port is deleted.

Example

Console(config)#lldp reinit-delay 10

Console(config)#

lldp tx-delay

This command configures a delay between the successive transmission of advertisements initiated by a change in local LLDP MIB variables. Use the no form to restore the default setting.

Syntax

lldp tx-delay *seconds*

no lldp tx-delay

seconds - Specifies the transmit delay. (Range: 1 - 8192 seconds)

Default Configuration

2 seconds

Command Mode

Global Configuration

User Guidelines

- The transmit delay is used to prevent a series of successive LLDP transmissions during a short period of rapid changes in local LLDP MIB objects, and to increase the probability that multiple, rather than single changes, are reported in each transmission.
- This attribute must comply with the following rule:

(4 * tx-delay) ≤ refresh-interval

Example

Console(config)#lldp tx-delay 10

Console(config)#

lldp admin-status

This command enables LLDP transmit, receive, or transmit and receive mode on the specified port. Use the no form to disable this feature.

Syntax

lldp admin-status {rx-only | tx-only | tx-rx}

no lldp admin-status

rx-only - Only receive LLDP PDUs.

tx-only - Only transmit LLDP PDUs.

tx-rx - Both transmit and receive LLDP Protocol Data Units (PDUs).

Default Configuration

tx-rx

Command Mode

Interface Configuration (Ethernet, Port Channel)

Example

Console(config)#interface ethernet 1/1

Console(config-if)#lldp admin-status rx-only

Console(config-if)#

lldp basic-tlv management-ip-address

This command configures an LLDP-enabled port to advertise the management address for this device. Use the no form to disable this feature.

Syntax

[no] lldp basic-tlv management-ip-address

Default Configuration

Enabled

Command Mode

Interface Configuration (Ethernet, Port Channel)

User Guidelines

- The management address protocol packet includes the IPv4 address of the switch. If no management address is available, the address should be the MAC address for the CPU or for the port sending this advertisement.
- The management address TLV may also include information about the specific interface associated with this address, and an object identifier indicating the type of hardware component or protocol entity associated with this address. The interface number and OID are included to assist SNMP applications to perform network discovery by indicating enterprise specific or other starting points for the search, such as the Interface or Entity MIB.
- Since there are typically a number of different addresses associated with a Layer 3 device, an individual LLDP PDU may contain more than one management address TLV.
- Every management address TLV that reports an address that is accessible on a port and protocol VLAN through the particular port should be accompanied by a port and protocol VLAN TLV that indicates the VLAN identifier (VID) associated with the management address reported by this TLV.

Example

Console(config)#interface ethernet 1/1

Console(config-if)#lldp basic-tlv management-ip-address

Console(config-if)#

lldp basic-tlv port-description

This command configures an LLDP-enabled port to advertise its port description. Use the no form to disable this feature.

Syntax

[no] lldp basic-tlv port-description

Default Configuration

Enabled

Command Mode

Interface Configuration (Ethernet, Port Channel)

User Guidelines

The port description is taken from the ifDescr object in RFC 2863, which includes information about the manufacturer, the product name, and the version of the interface hardware/software.

Example

Console(config)#interface ethernet 1/1

Console(config-if)#lldp basic-tlv port-description

Console(config-if)#

lldp basic-tlv system-capabilities

This command configures an LLDP-enabled port to advertise its system capabilities. Use the no form to disable this feature.

Syntax

[no] lldp basic-tlv system-capabilities

Default Configuration

Enabled

Command Mode

Interface Configuration (Ethernet, Port Channel)

User Guidelines

The system capabilities identifies the primary function(s) of the system and whether or not these primary functions are enabled. The information advertised by this TLV is described in IEEE 802.1AB.

Example

Console(config)#interface ethernet 1/1

Console(config-if)#lldp basic-tlv system-capabilities

Console(config-if)#

lldp basic-tlv system-description

This command configures an LLDP-enabled port to advertise the system description. Use the no form to disable this feature.

Syntax

[no] lldp basic-tlv system-description

Default Configuration

Enabled

Command Mode

Interface Configuration (Ethernet, Port Channel)

User Guidelines

The system description is taken from the sysDescr object in RFC 3418, which includes the full name and version identification of the system's hardware type, software operating system, and networking software.

Example

Console(config)#interface ethernet 1/1

Console(config-if)#lldp basic-tlv system-description

Console(config-if)#

lldp basic-tlv system-name

This command configures an LLDP-enabled port to advertise the system name. Use the no form to disable this feature.

Syntax

[no] lldp basic-tlv system-name

Default Configuration

Enabled

Command Mode

Interface Configuration (Ethernet, Port Channel)

User Guidelines

The system name is taken from the sysName object in RFC 3418, which contains the system's administratively assigned name, and is in turn based on the system-name command.

Example

Console(config)#interface ethernet 1/1

Console(config-if)#lldp basic-tlv system-name

Console(config-if)#

lldp dot1-tlv proto-ident

This command configures an LLDP-enabled port to advertise the supported protocols. Use the no form to disable this feature.

Syntax

[no] lldp dot1-tlv proto-ident

Default Configuration

Enabled

Command Mode

Interface Configuration (Ethernet, Port Channel)

User Guidelines

This option advertises the protocols that are accessible through this interface.

Example

Console(config)#interface ethernet 1/1

Console(config-if)#no lldp dot1-tlv proto-ident

Console(config-if)#

lldp dot1-tlv proto-vid

This command configures an LLDP-enabled port to advertise port-based protocol VLAN information. Use the no form to disable this feature.

Syntax

[no] lldp dot1-tlv proto-vid

Default Configuration

Enabled

Command Mode

Interface Configuration (Ethernet, Port Channel)

User Guidelines

This option advertises the port-based protocol VLANs configured on this interface (see "Configuring Protocol-based VLANs").

Example

Console(config)#interface ethernet 1/1

Console(config-if)#no lldp dot1-tlv proto-vid

Console(config-if)#

lldp dot1-tlv pvid

This command configures an LLDP-enabled port to advertise its default VLAN ID. Use the no form to disable this feature.

Syntax

[no] lldp dot1-tlv pvid

Default Configuration

Enabled

Command Mode

Interface Configuration (Ethernet, Port Channel)

User Guidelines

The port's default VLAN identifier (PVID) indicates the VLAN with which untagged or priority-tagged frames are associated (see the switchport access vlan command).

Example

Console(config)#interface ethernet 1/1

Console(config-if)#no lldp dot1-tlv pvid

Console(config-if)#

lldp dot1-tlv vlan-name

This command configures an LLDP-enabled port to advertise its VLAN name. Use the no form to disable this feature.

Syntax

[no] lldp dot1-tlv vlan-name

Default Configuration

Enabled

Command Mode

Interface Configuration (Ethernet, Port Channel)

User Guidelines

This option advertises the name of all VLANs to which this interface has been assigned. See "switchport allowed vlan" and "protocolvlan protocol-group (Configuring Interfaces)".

Example

Console(config)#interface ethernet 1/1

Console(config-if)#no lldp dot1-tlv vlan-name

Console(config-if)#

lldp dot3-tlv link-agg

This command configures an LLDP-enabled port to advertise link aggregation capabilities. Use the no form to disable this feature.

Syntax

[no] lldp dot3-tlv link-agg

Default Configuration

Enabled

Command Mode

Interface Configuration (Ethernet, Port Channel)

User Guidelines

This option advertises link aggregation capabilities, aggregation status of the link, and the 802.3 aggregated port identifier if this interface is currently a link aggregation member.

Example

Console(config)#interface ethernet 1/1

Console(config-if)#no lldp dot3-tlv link-agg

Console(config-if)#

lldp dot3-tlv mac-phy

This command configures an LLDP-enabled port to advertise its MAC and physical layer capabilities. Use the no form to disable this feature.

Syntax

[no] lldp dot3-tlv mac-phy

Default Configuration

Enabled

Command Mode

Interface Configuration (Ethernet, Port Channel)

User Guidelines

This option advertises MAC/PHY configuration/status which includes information about auto-negotiation support/capabilities, and operational Multi-station Access Unit (MAU) type.

Example

Console(config)#interface ethernet 1/1

Console(config-if)#no lldp dot3-tlv mac-phy

Console(config-if)#

lldp dot3-tlv max-frame

This command configures an LLDP-enabled port to advertise its maximum frame size. Use the no form to disable this feature.

Syntax

[no] lldp dot3-tlv max-frame

Default Configuration

Enabled

Command Mode

Interface Configuration (Ethernet, Port Channel)

User Guidelines

Refer to "Frame Size" for information on configuring the maximum frame size for this switch.

Example

Console(config)#interface ethernet 1/1

Console(config-if)#lldp dot3-tlv max-frame

Console(config-if)#

lldp med-location civic-addr

This command configures an LLDP-MED-enabled port to advertise its location identification details. Use the no form to restore the default settings.

Syntax

lldp med-location civic-addr [[country *country-code*] | [what *device-type*] | [*ca-type ca-value*]]

no lldp med-location civic-addr [[country] | [what] | [*ca-type*]]

country-code – The two-letter ISO 3166 country code in capital ASCII letters. (Example: DK, DE or US)

device-type – The type of device to which the location applies.

0 – Location of DHCP server.

1 – Location of network element closest to client.

2 – Location of client.

ca-type – A one-octet descriptor of the data civic address value. (Range: 0-255)

ca-value – Description of a location. (Range: 1-32 characters)

Default Configuration

Not advertised

No description

Command Mode

Interface Configuration (Ethernet, Port Channel)

User Guidelines

- Use this command without any keywords to advertise location identification details.
- Use the *ca-type* to advertise the physical location of the device, that is the city, street number, building and room information. The address location is specified as a type and value pair, with the civic address (CA) type being defined in RFC 4776. The following table describes some of the CA type numbers and provides examples. Any number of CA type and value pairs can be specified for the civic address location, as long as the total does not exceed 250 characters.
- For the location options defined for *device-type*, normally option 2 is used to specify the location of the client device. In situations where the client device location is not known, 0 and 1 can be used, providing the client device is physically close to the DHCP server or network element.

Example

The following example enables advertising location identification details.

```
Console(config)#interface ethernet 1/1
Console(config-if)#lldp med-location civic-addr
Console(config-if)#lldp med-location civic-addr 1 California
Console(config-if)#lldp med-location civic-addr 2 Orange
Console(config-if)#lldp med-location civic-addr 3 Irvine
Console(config-if)#lldp med-location civic-addr 4 West Irvine
Console(config-if)#lldp med-location civic-addr 6 Exchange
Console(config-if)#lldp med-location civic-addr 18 Avenue
Console(config-if)#lldp med-location civic-addr 19 320
Console(config-if)#lldp med-location civic-addr 27 5
Console(config-if)#lldp med-location civic-addr 28 509B
Console(config-if)#lldp med-location civic-addr country US
Console(config-if)#lldp med-location civic-addr what 2
Console(config-if)#
```

lldp med-notification

This command enables the transmission of SNMP trap notifications about LLDP-MED changes. Use the no form to disable LLDP-MED notifications.

Syntax

[no] lldp med-notification

Default Configuration

Disabled

Command Mode

Interface Configuration (Ethernet, Port Channel)

User Guidelines

- This option sends out SNMP trap notifications to designated target stations at the interval specified by the lldp notification-interval command. Trap notifications include information about state changes in the LLDP MIB (IEEE

802.1AB), the LLDP-MED MIB (ANSI/TIA 1057), or organization-specific LLDP-EXT-DOT1 and LLDP-EXT-DOT3 MIBs.

- SNMP trap destinations are defined using the snmp-server host command.
- Information about additional changes in LLDP neighbors that occur between SNMP notifications is not transmitted. Only state changes that exist at the time of a trap notification are included in the transmission. An SNMP agent should therefore periodically check the value of lldpStatsRemTableLastChangeTime to detect any lldpRemTablesChange notification-events missed due to throttling or transmission loss.

Example

Console(config)#interface ethernet 1/1

Console(config-if)#lldp med-notification

Console(config-if)#

lldp med-tlv inventory

This command configures an LLDP-MED-enabled port to advertise its inventory identification details. Use the no form to disable this feature.

Syntax

[no] lldp med-tlv inventory

Default Configuration

Enabled

Command Mode

Interface Configuration (Ethernet, Port Channel)

User Guidelines

This option advertises device details useful for inventory management, such as manufacturer, model, software version and other pertinent information.

Example

Console(config)#interface ethernet 1/1

Console(config-if)#no lldp med-tlv inventory

Console(config-if)#

lldp med-tlv location

This command configures an LLDP-MED-enabled port to advertise its location identification details. Use the no form to disable this feature.

Syntax

[no] lldp med-tlv location

Default Configuration

Enabled

Command Mode

Interface Configuration (Ethernet, Port Channel)

User Guidelines

This option advertises location identification details.

Example

Console(config)#interface ethernet 1/1

Console(config-if)#lldp med-tlv location

Console(config-if)#

lldp med-tlv med-cap

This command configures an LLDP-MED-enabled port to advertise its Media Endpoint Device capabilities. Use the no form to disable this feature.

Syntax

[no] lldp med-tlv med-cap

Default Configuration

Enabled

Command Mode

Interface Configuration (Ethernet, Port Channel)

User Guidelines

This option advertises LLDP-MED TLV capabilities, allowing Media Endpoint and Connectivity Devices to efficiently discover which LLDP-MED related TLVs are supported on the switch.

Example

Console(config)#interface ethernet 1/1

Console(config-if)#lldp med-tlv med-cap

Console(config-if)#

lldp med-tlv network-policy

This command configures an LLDP-MED-enabled port to advertise its network policy configuration. Use the no form to disable this feature.

Syntax

[no] lldp med-tlv network-policy

Default Configuration

Enabled

Command Mode

Interface Configuration (Ethernet, Port Channel)

User Guidelines

This option advertises network policy configuration information, aiding in the discovery and diagnosis of VLAN configuration mismatches on a port. Improper network policy configurations frequently result in voice quality degradation or complete service disruption.

Example

Console(config)#interface ethernet 1/1

Console(config-if)#lldp med-tlv network-policy

Console(config-if)#

lldp notification

This command enables the transmission of SNMP trap notifications about LLDP changes. Use the no form to disable LLDP notifications.

Syntax

[no] lldp notification

Default Configuration

Disabled

Command Mode

Interface Configuration (Ethernet, Port Channel)

User Guidelines

- This option sends out SNMP trap notifications to designated target stations at the interval specified by the lldp notification-interval command. Trap notifications include information about state changes in the LLDP MIB (IEEE 802.1AB), or organization-specific LLDP-EXT-DOT1 and LLDP-EXT-DOT3 MIBs.
- SNMP trap destinations are defined using the snmp-server host command.
- Information about additional changes in LLDP neighbors that occur between SNMP notifications is not transmitted. Only state changes that exist at the time of a trap notification are included in the transmission. An SNMP agent should therefore periodically check the value of lldpStatsRemTableLastChangeTime to detect any lldpRemTablesChange notification-events missed due to throttling or transmission loss.

Example

Console(config)#interface ethernet 1/1

Console(config-if)#lldp notification

Console(config-if)#

show lldp config

This command shows LLDP configuration settings for all ports.

Syntax

show lldp config [detail *interface*]

detail - Shows configuration summary.

interface

ethernet *unit*/*port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-28)

port-channel *channel-id* (Range: 1-12)

Command Mode

EXEC

Example

Console#show lldp config

LLDP Global Configuation

LLDP Enabled: Yes

LLDP Transmit Interval: 30 sec.

LLDP Hold Time Multiplier: 4

LLDP Delay Interval: 2 sec.

LLDP Re-initialization Delay: 2 sec.

LLDP Notification Interval: 5 sec.

LLDP MED Fast Start Count: 4

LLDP Port Configuration

Port Admin Status Notification Enabled

-------- ------------ --------------------

Eth 1/1 Tx-Rx True

Eth 1/2 Tx-Rx True

Eth 1/3 Tx-Rx True

Eth 1/4 Tx-Rx True

Eth 1/5 Tx-Rx True

...

show lldp info local-device

This command shows LLDP global and interface-specific configuration settings for this device.

Syntax

show lldp info local-device [detail *interface*]

detail - Shows configuration summary.

interface

ethernet *unit*/*port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-28)

port-channel *channel-id* (Range: 1-12)

Command Mode

EXEC

Example

Console#show lldp info local-device

LLDP Local System Information

Chassis Type: MAC Address

Chassis ID: 64-9D-99-03-04-05

System Name:

System Description: ECS4510-28T

System Capabilities Support: Bridge

System Capabilities Enable: Bridge

Management Address: 192.168.0.101 (IPv4)

LLDP Port Information

Port PortID Type PortID Port Description

-------- ---------- ---------- ----------

Eth 1/1 MAC Address 64-9D-99-DA-FC-E9 Ethernet Port on unit 0, port 1

Eth 1/2 MAC Address 64-9D-99-DA-FC-EA Ethernet Port on unit 0, port 2

Eth 1/3 MAC Address 64-9D-99-DA-FC-EB Ethernet Port on unit 0, port 3

Eth 1/4 MAC Address 64-9D-99-DA-FC-EC Ethernet Port on unit 0, port 4

...

Console#show lldp info local-device detail ethernet 1/1

LLDP Port Information Details

Port: Eth 1/1

Port Type: MAC Address

Port ID: 64-9D-99-DA-FC-E9

Port Description: Ethernet Port on unit 0, port 1

MED Capability: LLDP-MED Capabilities

Network Policy

Location Identification

Inventory

Console#

show lldp info remote-device

This command shows LLDP global and interface-specific configuration settings for remote devices attached to an LLDP-enabled port.

Syntax

show lldp info remote-device [detail *interface*]

detail - Shows configuration summary.

interface

ethernet *unit*/*port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-28)

port-channel *channel-id* (Range: 1-12)

Command Mode

EXEC

Example

Note that an IP phone or other end-node device which advertises LLDPMED capabilities must be connected to the switch for information to be displayed in the "Device Class" and other related fields.

Console#show lldp info remote-device

LLDP Remote Devices Information

Interface Chassis ID Port ID System Name

--------- ----------------- ----------------- ----------------------

Eth 1/1 00-E0-0C-00-00-FD 00-E0-0C-00-01-02

Console#show lldp info remote-device detail ethernet 1/1

Local Port Name: Eth 1/2

Chassis Type: MAC Address

Chassis ID: 64-9D-99-18-B7-E0

Port ID Type: MAC Address

Port ID: 64-9D-99-18-B7-E1

System Name:

System Description: ECS4510-28T

Port Description: Ethernet Port on unit 0, port 1

SystemCapSupported: Bridge

SystemCapEnabled: Bridge

Remote Management Address: 192.168.0.5 (IPv4)

Remote Port VID: 1

Remote Port-Protocol VLAN:

VLAN-3: supported, enabled

Remote VLAN Name:

VLAN-1: DefaultVlan

Remote Protocol Identity (Hex):

88-CC

Remote MAC/PHY Configuration Status:

Remote port auto-neg supported: Yes

Remote port auto-neg enabled: Yes

Remote port auto-neg advertised cap (Hex): 0000

Remote port MAU type: 6

Remote Power via MDI:

Remote power class: PSE
Remote power MDI supported: Yes
Remote power MDI enabled: Yes
Remote power pair controllable: No
Remote power pairs: Spare
Remote power classification: Class1
Remote Link Aggregation:
Remote link aggregation capable: Yes
Remote link aggregation enable: No
Remote link aggregation port ID: 0
Remote Max Frame Size: 1518
LLDP-MED Capability:
Device Class: Type Not Defined
Console#
show lldp info statistics
This command shows statistics based on traffic received through all attached LLDP-enabled interfaces.
Syntax
show lldp info statistics [detail *interface*]
detail - Shows configuration summary.
interface
ethernet *unit*/*port*
unit - Unit identifier. (Range: 1)
port - Port number. (Range: 1-28)
port-channel *channel-id* (Range: 1-12)
Command Mode
EXEC
Example
Console#show lldp info statistics
LLDP Device Statistics
Neighbor Entries List Last Updated: 2450279 seconds
New Neighbor Entries Count: 1
Neighbor Entries Deleted Count: 0
Neighbor Entries Dropped Count: 0
Neighbor Entries Ageout Count: 0
Port NumFramesRecvd NumFramesSent NumFramesDiscarded
-------- -------------- ------------- ------------------
Eth 1/1 0 83 0
Eth 1/2 11 12 0
Eth 1/3 0 0 0
Eth 1/4 0 0 0
Eth 1/5 0 0 0
...
Console#show lldp info statistics detail ethernet 1/1
LLDP Port Statistics Detail

PortName: Eth 1/1

Frames Discarded: 0

Frames Invalid: 0

Frames Received: 12

Frames Sent: 13

TLVs Unrecognized: 0

TLVs Discarded: 0

Neighbor Ageouts: 0

Console#

48. CFM Commands

48.1 Defining CFM Structures

cfm ais level

This command configures the maintenance level at which Alarm Indication Signal (AIS) information will be sent within the specified MA. Use the no form restore the default setting.

Syntax

cfm ais level *level-id* md *domain-name* ma *ma-name*

no cfm ais level md *domain-name* ma *ma-name*

level-id – Maintenance level at which AIS information will be sent. (Range: 0-7)

domain-name – Domain name. (Range: 1-43 alphanumeric characters)

ma-name – Maintenance association name. (Range: 1-43 alphanumeric characters)

Default Configuration

Level 0

Command Mode

Global Configuration

User Guidelines

The configured AIS level must be higher than the maintenance level of the domain containing the specified MA.

Example

This example sets the maintenance level for sending AIS messages within the specified MA.

Console(config)#cfm ais level 4 md voip ma rd

Console(config)#

cfm ais ma

This command enables the MEPs within the specified MA to send frames with AIS information following detection of defect conditions. Use the no form to disable this feature.

Syntax

[no] cfm ais md *domain-name* ma *ma-name*

domain-name – Domain name. (Range: 1-43 alphanumeric characters)

ma-name – Maintenance association name. (Range: 1-43 alphanumeric characters)

Default Configuration

Disabled

Command Mode

Global Configuration

User Guidelines

- Each MA name must be unique within the CFM domain.
- Frames with AIS information can be issued at the client's maintenance level by a MEP upon detecting defect conditions. For example, defect conditions may include:

a. Signal failure conditions if continuity checks are enabled.

b. AIS condition or LCK condition if continuity checks are disabled.

- A MEP continues to transmit periodic frames with AIS information until the defect condition is removed.

Example

This example enables the MEPs within the specified MA to send frames with AIS information.

Console(config)#cfm ais md voip ma rd

Console(config)#

cfm ais period

This command configures the interval at which AIS information is sent. Use the no form to restore the default setting.

Syntax

cfm ais period *period* md *domain-name* ma *ma-name*

no cfm ais period md *domain-name* ma *ma-name*

period – The interval at which AIS information is sent. (Options: 1 second, 60 seconds)

domain-name – Domain name. (Range: 1-43 alphanumeric characters)

ma-name – Maintenance association name. (Range: 1-43 alphanumeric characters)

Default Configuration

1 second

Command Mode

Global Configuration

Example

This example sets the interval for sending frames with AIS information at 60 seconds.

Console(config)#cfm ais period 60 md voip ma rd

Console(config)#

cfm ais suppress alarm

This command suppresses sending frames containing AIS information following the detection of defect conditions. Use the no form to restore the default setting.

Syntax

[no] cfm ais suppress alarm md *domain-name*

ma *ma-name*

domain-name – Domain name. (Range: 1-43 alphanumeric characters)

ma-name – Maintenance association name. (Range: 1-43 alphanumeric characters)

Default Configuration

Suppression is disabled

Command Mode

Global Configuration

User Guidelines

- For multipoint connectivity, a MEP cannot determine the specific maintenance level entity that has encountered defect conditions upon receiving a frame with AIS information. More importantly, it cannot determine the associated subset of its peer MEPs for which it should suppress alarms since the received AIS information does not contain that information. Therefore, upon reception of a frame with AIS information, the MEP will suppress alarms for all peer MEPs whether there is still connectivity or not.
- However, for a point-to-point connection, a MEP has only a single peer MEP for which to suppress alarms when it receives frames with AIS information.
- If suppression is enabled by this command, upon receiving a frame with AIS information, a MEP detects an AIS condition and suppresses loss of continuity alarms associated with all its peer MEPs. A MEP resumes loss of continuity alarm generation upon detecting loss of continuity defect conditions in the absence of AIS messages.

Example

This example suppresses sending frames with AIS information.

Console(config)#cfm ais suppress alarm md voip ma rd

Console(config)#

cfm domain

This command defines a CFM maintenance domain, sets the authorized maintenance level, and enters CFM configuration mode. Use the no form to delete a CFM maintenance domain.

Syntax

cfm domain index *index* name *domain-name* level *level-id* [mip-creation *type*]

no cfm domain index *index*

index – Domain index. (Range: 1-65535)

domain-name – Domain name. (Range: 1-43 alphanumeric characters)

level-id – Authorized maintenance level for this domain. (Range: 0-7)

type – Specifies the CFM protocol's creation method for maintenance intermediate points (MIPs) in this domain:

default – MIPs can be created for any maintenance association (MA) configured in this domain on any bridge port through which the MA's VID can pass.

explicit – MIPs can be created for any MA configured in this domain only on bridge ports through which the MA's VID can pass, and only if a maintenance end point (MEP) is created at some lower MA Level.

none – No MIP can be created for any MA configured in this domain.

Default Configuration

No maintenance domains are configured.

No MIPs are created for any MA in the specified domain.

Command Mode

Global Configuration

User Guidelines

- A domain can only be configured with one name.
- Where domains are nested, an upper-level hierarchical domain must have a higher maintenance level than the ones it encompasses. The higher to lower level domain types commonly include entities such as customer, service provider, and operator.
- More than one domain can be configured at the same maintenance level, but a single domain can only be configured with one maintenance level.
- If MEPs or MAs are configured for a domain using the cfm mep command or ma index name command, they must first be removed before you can remove the domain.
- Maintenance domains are designed to provide a transparent method of verifying and resolving connectivity problems for end-to-end connections. By default, these connections run between the domain service access points (DSAPs) within each MA defined for a domain, and are manually configured using the cfm mep command. In contrast, MIPs are interconnection points that make up all possible paths between the DSAPs within an MA. MIPs are automatically generated by the CFM protocol when the *mip-creation* option in this command is set to "default" or "explicit," and the MIP creation state machine is invoked (as defined in IEEE 802.1ag). The default option allows MIPs to be created for all interconnection points within an MA, regardless of the domain's level in the maintenance hierarchy (e.g., customer, provider, or operator). While the explicit option only generates MIPs within an MA if its associated domain is not at the bottom of the maintenance hierarchy. This option is used to hide the structure of network at the lowest domain level. The diagnostic functions provided by CFM can be used to detect connectivity failures between any pair of MEPs in an MA. Using MIPs allows these failures to be isolated to smaller segments of the network. Allowing the CFM to generate MIPs exposes more of the network structure to users at higher domain levels, but can speed up the process of fault

detection and recovery. This trade-off should be carefully considered when designing a CFM maintenance structure. Also note that while MEPs are active agents which can initiate consistency check messages (CCMs), transmit loop back or link trace messages, and maintain the local CCM database. MIPs, on the other hand are passive agents which can only validate received CFM messages, and respond to loop back and link trace messages. The MIP creation method defined by the ma index name command takes precedence over the method defined by this command.

Example

This example creates a maintenance domain set to maintenance level 3, and enters CFM configuration mode for this domain.

Console(config)#cfm domain index 1 name voip level 3 mip-creation

explicit

Console(config-ether-cfm)#

cfm enable

This command enables CFM processing globally on the switch. Use the no form to disable CFM processing globally.

Syntax

[no] cfm enable

Default Configuration

Disabled

Command Mode

Global Configuration

User Guidelines

- To avoid generating an excessive number of traps, the complete CFM maintenance structure and process parameters should be configured prior to globally enabling CFM processing with this command. Specifically, the maintenance domains, maintenance associations, and MEPs should be configured on each participating bridge.
- When CFM is enabled, hardware resources are allocated for CFM processing.

Example

This example enables CFM globally on the switch.

Console(config)#cfm enable

Console(config)#

ma index name

This command creates a maintenance association (MA) within the current maintenance domain, maps it to a customer service instance (S-VLAN), and sets the manner in which MIPs are created for this service instance. Use the no form with the vlan keyword to remove the S-VLAN from the specified MA. Or use the no form with only the index keyword to remove the MA from the current domain.

Syntax

ma index *index* name *ma-name* [vlan *vlan-id* [mip-creation *type*]]

no ma index *index* [vlan *vlan-id*]

index – MA identifier. (Range: 1-2147483647)

ma-name – MA name. (Range: 1-43 alphanumeric characters)

vlan-id - Service VLAN ID. (Range: 1-4094)

type – Specifies the CFM protocol's creation method for maintenance intermediate points (MIPs) in this MA:

default – MIPs can be created for this MA on any bridge port through which the MA's VID can pass.

explicit – MIPs can be created this MA only on bridge ports through which the MA's VID can pass, and only if a maintenance end point (MEP) is created at some lower MA Level.

none – No MIP can be created for this MA.

Default Configuration

10 seconds

Command Mode

CFM Domain Configuration

User Guidelines

- The maintenance domain used to enter CFM domain configuration mode, the MA name and VLAN identifier specified by this command, and the DSAPs configured with the mep crosscheck mpid command create a unique service instance for each customer.
- If only the MA index and name are entered for this command, the MA will be recorded in the domain database, but will not function. No MEPs can be created until the MA is associated with a service VLAN.
- Note that multiple domains at the same maintenance level (see the cfm domain command) cannot have an MA on the same VLAN. Also, each MA name must be unique within the CFM-managed network.
- Before removing an MA, first remove all the MEPs configured for it (see the mep crosscheck mpid command).
- If the MIP creation method is not defined by this command, the creation method defined by the cfm domain command is applied to this MA. For a detailed description of the MIP types, refer to the Command Usage section under the cfm domain command.

Example

This example creates a maintenance association, binds it to VLAN 1, and allows MIPs to be created within this MA using the default method.

Console(config)#cfm domain index 1 name voip level 3

Console(config-ether-cfm)#ma index 1 name rd vlan 1 mip-creation default

Console(config-ether-cfm)#

ma index name-format

This command specifies the name format for the maintenance association as IEEE 802.1ag character based, or ITU-T SG13/SG15 Y.1731 defined ICCbased format. Use the no form to restore the default setting.

Syntax

ma index *index* name-format {character-string | icc-based}

no ma index *index* name-format

index – MA identifier. (Range: 1-2147483647)

character-string – IEEE 802.1ag defined character string format. This is an IETF RFC 2579 DisplayString.

icc-based – ITU-T SG13/SG15 Y.1731 defined ICC based format.

Default Configuration

character-string

Command Mode

CFM Domain Configuration

Example

This example specifies the name format as character string.

Console(config)#cfm domain index 1 name voip level 3

Console(config-ether-cfm)#ma index 1 name-format character-string

Console(config-ether-cfm)#

cfm mep

This command sets an interface as a domain boundary, defines it as a maintenance end point (MEP), and sets direction of the MEP in regard to sending and receiving CFM messages. Use the no form to delete a MEP.

Syntax

cfm mep mpid *mpid* md *domain-name* ma *ma-name* [up]

no cfm mep mpid *mpid* ma *ma-name*

mpid – Maintenance end point identifier. (Range: 1-8191)

domain-name – Domain name. (Range: 1-43 alphanumeric characters)

ma-name – Maintenance association name. (Range: 1-43 alphanumeric characters)

up – Indicates that the MEP faces inward toward the switch crossconnect matrix, and transmits CFM messages towards, and receives them from, the direction of the internal bridge relay mechanism. If the up keyword is not included in this command, then the MEP is facing away from the switch, and transmits CFM messages towards, and receives them from, the direction of the physical medium.

Default Configuration

No MEPs are configured.

The MEP faces outward (down).

Command Mode

Interface Configuration (Ethernet, Port Channel)

User Guidelines

- CFM elements must be configured in the following order: (1) maintenance domain at the same level as the MEP to be configured (using the cfm domain command), (2) maintenance association within the domain (using the ma index name command), and (3) finally the MEP using this command.
- An interface may belong to more than one domain. This command can be used to configure an interface as a MEP for different MAs in different domains.
- To change the MEP's MA or the direction it faces, first delete the MEP, and then create a new one.

Example

This example sets port 1 as a DSAP for the specified maintenance association.

```
Console(config)#interface ethernet 1/1
Console(config-if)#cfm mep mpid 1 md voip ma rd
Console(config-if)#
```

cfm port-enable

This command enables CFM processing on an interface. Use the no form to disable CFM processing on an interface.

Syntax

[no] cfm port-enable

Default Configuration

Enabled

Command Mode

Interface Configuration (Ethernet, Port Channel)

User Guidelines

- An interface must be enabled before a MEP can be created with the cfm mep command.
- If a MEP has been configured on an interface with the cfm mep command, it must first be deleted before CFM can be disabled on that interface.
- When CFM is disabled, hardware resources previously used for CFM processing on that interface are released, and all CFM frames entering that interface are forwarded as normal data traffic.

Example

This example enables CFM on port 1.

Console(config)#interface ethernet 1/1

Console(config-if)#cfm port-enable

Console(config-if)#

clear cfm ais mpid

This command clears AIS defect information for the specified MEP.

Syntax

clear cfm ais mpid *mpid* md *domain-name* ma *ma-name*

mpid – Maintenance end point identifier. (Range: 1-8191)

domain-name – Domain name. (Range: 1-43 alphanumeric characters)

ma-name – Maintenance association name. (Range: 1-43 alphanumeric characters)

Default Configuration

None

Command Mode

EXEC

User Guidelines

This command can be used to clear AIS defect entries if a MEP does not exit the AIS state when all errors are resolved.

Example

This example clears AIS defect entries on port 1.

Console#clear cfm ais mpid 1 md voip ma rd

Console(config)#

show cfm configuration

This command displays CFM configuration settings, including global settings, SNMP traps, and interface settings.

Syntax

show cfm configuration {global | traps | interface *interface*}

global – Displays global settings including CFM global status, crosscheck start delay, and link trace parameters.

traps – Displays the status of all continuity check and cross-check traps.

interface – Displays CFM status for the specified interface.

ethernet *unit*/*port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-28)

port-channel *channel-id* (Range: 1-12)

Default Configuration

None

Command Mode

EXEC

Example

This example shows the global settings for CFM.

Console#show cfm configuration global

CFM Global Status : Enabled

Crosscheck Start Delay : 10 seconds

Linktrace Cache Status : Enabled

Linktrace Cache Hold Time : 100 minutes

Linktrace Cache Size : 100 entries

Console#

show cfm md

This command displays the configured maintenance domains.

Syntax

show cfm md [level *level*]

level – Maintenance level. (Range: 0-7)

Default Configuration

None

Command Mode

EXEC

Example

This example shows all configured maintenance domains.

Console#show cfm md

MD Index MD Name Level MIP Creation Archive Hold Time (m.)

-------- -------------------- ----- ------------ ----------------------

1 rd 0 default 100

Console#

show cfm ma

This command displays the configured maintenance associations.

Syntax

show cfm ma [level *level*]

level – Maintenance level. (Range: 0-7)

Default Configuration

None

Command Mode

EXEC

User Guidelines

For a description of the values displayed in the CC Interval field, refer to the cfm cc ma interval command.

Example

This example shows all configured maintenance associations.

Console#show cfm ma

MD Name MA Index MA Name Primary VID CC Interval MIP Creation

--------------- -------- ---------------- ------------ ------------ ------------

steve 1 voip 1 4 Default

Console#

show cfm maintenance-points local

This command displays the maintenance points configured on this device.

Syntax

show cfm maintenance-points local {mep [domain *domain-name* | interface *interface* | level *level-id*] | mip [domain *domain-name* | level *level-id*]}

mep – Displays only local maintenance end points.

mip – Displays only local maintenance intermediate points.

domain-name – Domain name. (Range: 1-43 alphanumeric characters)

interface – Displays CFM status for the specified interface.

ethernet *unit*/*port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-28)

port-channel *channel-id* (Range: 1-12)

level-id – Maintenance level for this domain. (Range: 0-7)

Default Configuration

None

Command Mode

EXEC

User Guidelines

- Use the mep keyword with this command to display the MEPs configured on this device as DSAPs through the cfm mep command.
- Using the mip keyword with this command to display the MIPs generated on this device by the CFM protocol when the mip-creation method is set to either "default" or "explicit" by the cfm domain command or the ma index name command.

Example

This example shows all MEPs configured on this device for maintenance domain rd.

Console#show cfm maintenance-points local mep

MPID MD Name Level Direct VLAN Port CC Status MAC Address

---- ---------- ----- ------ ---- -------- --------- -----------

1 rd 0 UP 1 Eth 1/ 1 Enabled 64-9D-99-3A-A8-C0

Console#

show cfm maintenance-points local detail mep

This command displays detailed CFM information about a local MEP in the continuity check database.

Syntax

show cfm maintenance-points local detail mep [domain *domain-name* | interface *interface* | level *level-id*]

domain-name – Domain name. (Range: 1-43 alphanumeric characters)

interface – Displays CFM status for the specified interface.

ethernet *unit*/*port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-28)

port-channel *channel-id* (Range: 1-12)

level-id – Maintenance level for this domain. (Range: 0-7)

Default Configuration

None

Command Mode

EXEC

Example

This example shows detailed information about the local MEP on port 1.

Console#show cfm maintenance-points local detail mep interface

ethernet 1/1

MEP Settings:

MPID: 1

MD Name: vopu

MA Name: r&d

MA Name Format: Character String

Level: 0

Direction: Up

Interface: Eth 1/ 1

CC Status: Enabled

MAC Address: 64-9D-99-00-00-FD

Defect Condition: No Defect

Received RDI: False

AIS Status: Enabled

AIS Period: 1 seconds

AIS Transmit Level: Default

Suppress Alarm: Disabled

Suppressing Alarms: Disabled

Console#

show cfm maintenance-points remote detail

This command displays detailed CFM information about a remote MEP in the continuity check database.

Syntax show cfm maintenance-points remote detail {mac *mac-address* | mpid *mpid*} [domain *domain-name* | level *level-id* | ma *ma-name*]

mac-address – MAC address of a remote maintenance point. This address can be entered in either of the following formats: xxxx-xx-xx-xx-xx or xxxxxxxxxxxx

mpid – Maintenance end point identifier. (Range: 1-8191)

domain-name – Domain name. (Range: 1-43 alphanumeric characters)

level-id – Authorized maintenance level for this domain. (Range: 0-7)

ma-name – Maintenance association name. (Range: 1-43 alphanumeric characters)

Default Configuration

None

Command Mode

EXEC

User Guidelines

Use the mpid keyword with this command to display information about a specific maintenance point, or use the mac keyword to display information about all maintenance points that have the specified MAC address.

Example

This example shows detailed information about the remote MEP designated by MPID 2.

Console#show cfm maintenance-points remote detail mpid 2

MAC Address: 64-9D-99-FC-A2-73

Domain/Level: voip / 3

MA Name: rd

Primary VLAN: 1

MPID: 2

Incoming Port: Eth 1/ 2

CC Lifetime: 645 seconds

Age of Last CC Message: 2 seconds

Frame Loss: 137

CC Packet Statistics: 647/1

Port State: Up

Interface State: Up

Crosscheck Status: Enabled

Console#

48.2 Continuity Check Operations

cfm cc ma interval

This command sets the transmission delay between continuity check messages (CCMs). Use the no form to restore the default settings.

Syntax

cfm cc md *domain-name* ma *ma-name* interval *interval-level*

no cfm md *domain-name* cc ma *ma-name* interval

domain-name – Domain name. (Range: 1-43 alphanumeric characters)

ma-name – Maintenance association name. (Range: 1-43 alphanumeric characters)

interval-level – The transmission delay between connectivity check messages. The setting for this parameter is expressed as levels 4 through 7, which in turn map to specific intervals of time. (CCM lifetime field options: 4 - 100 ms, 5 - 1 sec, 6 - 10 sec, 7 – 60 sec).

Default Configuration

4 (100 ms)

Command Mode

Global Configuration

User Guidelines

- CCMs provide a means to discover other MEPs and to detect connectivity failures in an MA. If any MEP fails to receive three consecutive CCMs from any other MEPs in its MA, a connectivity failure is registered. The interval at which CCMs are issued should therefore be configured to detect connectivity problems in a timely manner, as dictated by the nature and size of the MA.
- The maintenance of a MIP CCM database by a MIP presents some difficulty for bridges carrying a large number of Service Instances, and for whose MEPs are issuing CCMs at a high frequency. For this reason, slower CCM transmission rates may have to be used.

Example

This example sets the transmission delay for continuity check messages to level 7 (60 seconds).

Console(config)#cfm cc md voip ma rd interval 7

Console(config)#

cfm cc enable

This command enables the transmission of continuity check messages (CCMs) within a specified maintenance association. Use the no form to disable the transmission of these messages.

Syntax

[no] cfm cc enable md *domain-name* ma *ma-name*

domain-name – Domain name. (Range: 1-43 alphanumeric characters)

ma-name – Maintenance association name. (Range: 1-43 alphanumeric characters)

Default Configuration

Disabled

Command Mode

Global Configuration

User Guidelines

- CCMs are multicast periodically by a MEP in order to discover other MEPs in the same MA, and to assure connectivity to all other MEPs/MIPs in the MA.
- Each CCM received is checked to verify that the MEP identifier field sent in the message does not match its own MEPID, which would indicate a duplicate MEP or network loop. If these error types are not found, the CCM is stored in the MEP's local database until aged out.
- If a maintenance point fails to receive three consecutive CCMs from any other MEP in the same MA, a connectivity failure is registered.
- If a maintenance point receives a CCM with an invalid MEPID or MA level or an MA level lower than its own, a failure is registered which indicates a configuration error or cross-connect error (i.e., overlapping MAs).

Example

This example enables continuity check messages for the specified maintenance association.

Console(config)#cfm cc enable md voip ma rd

Console(config)#

snmp-server enable traps ethernet cfm cc

This command enables SNMP traps for CFM continuity check events. Use the no form to disable these traps.

Syntax

[no] snmp-server enable traps ethernet cfm cc [config | loop | mep-down | mep-up]

config – Sends a trap if this device receives a CCM with the same MPID as its own but with a different source MAC address, indicating that a CFM configuration error exists.

loop – Sends a trap if this device receives a CCM with the same source MAC address and MPID as its own, indicating that a forwarding loop exists.

mep-down – Sends a trap if this device loses connectivity with a remote MEP, or connectivity has been restored to a remote MEP which has recovered from an error condition.

mep-up – Sends a trap if a remote MEP is discovered and added to the local database, the port state of a previously discovered remote MEP changes, or a CCM is received from a remote MEP which as an expired entry in the archived database.

Default Configuration

All continuity checks are enabled.

Command Mode

Global Configuration

User Guidelines

All mep-up traps are suppressed when cross-checking of MEPs is enabled because cross-check traps include more detailed status information.

Example

This example enables SNMP traps for mep-up events.

Console(config)#snmp-server enable traps ethernet cfm cc mep-up

Console(config)#

mep archive-hold-time

This command sets the time that data from a missing MEP is retained in the continuity check message (CCM) database before being purged. Use the no form to restore the default setting.

Syntax

mep archive-hold-time *hold-time*

hold-time – The time to retain data for a missing MEP. (Range: 1-65535 minutes)

Default Configuration

100 minutes

Command Mode

CFM Domain Configuration

User Guidelines

A change to the hold time only applies to entries stored in the database after this command is entered.

Example

This example sets the aging time for missing MEPs in the CCM database to 30 minutes.

Console(config)#cfm domain index 1 name voip level 3

Console(config-ether-cfm)#mep archive-hold-time 30

Console(config-ether-cfm)#

clear cfm maintenance-points remote

This command clears the contents of the continuity check database.

Syntax

clear cfm maintenance-points remote [domain *domain-name* | level *level-id*]

domain-name – Domain name. (Range: 1-43 alphanumeric characters)

level-id – Maintenance level. (Range: 0-7)

Default Configuration

None

Command Mode

EXEC

User Guidelines

Use this command without any keywords to clear all entries in the CCM database. Use the domain keyword to clear the CCM database for a specific domain, or the level keyword to clear it for a specific maintenance level.

Example

Console#clear cfm maintenance-points remote domain voip

Console#

clear cfm errors

This command clears continuity check errors logged for the specified maintenance domain or maintenance level.

Syntax

clear cfm errors [domain *domain-name* | level *level-id*]

domain-name – Domain name. (Range: 1-43 alphanumeric characters)

level-id – Maintenance level. (Range: 0-7)

Default Configuration

None

Command Mode

EXEC

User Guidelines

Use this command without any keywords to clear all entries in the error database. Use the domain keyword to clear the error database for a specific domain, or the level keyword to clear it for a specific maintenance level.

Example

Console#clear cfm errors domain voip

Console#

show cfm errors

This command displays the CFM continuity check errors logged on this device.

Syntax

show cfm errors [domain *domain-name* | level *level-id*]

domain-name – Domain name. (Range: 1-43 alphanumeric characters)

level-id – Authorized maintenance level for this domain. (Range: 0-7)

Default Configuration

None

Command Mode

EXEC

Example

Console#show cfm errors

Level VLAN MPID Interface Remote MAC Reason MA Name

----- ---- ---- --------- ----------------- ---------------- ----------------

5 2 40 Eth 1/1 ab.2f.9c.00.05.01 LEAK provider_1_2

Console#

48.3 Cross Check Operations

cfm mep crosscheck start-delay

This command sets the maximum delay that a device waits for remote MEPs to come up before starting the cross-check operation. Use the no form to restore the default setting.

Syntax

cfm mep crosscheck start-delay *delay*

delay – The time a device waits for remote MEPs to come up before the cross-check is started. (Range: 1-65535 seconds)

Default Configuration

30 seconds

Command Mode

Global Configuration

User Guidelines

- This command sets the delay that a device waits for a remote MEP to come up, and it starts cross-checking the list of statically configure remote MEPs in the local maintenance domain against the MEPs learned through CCMs.
- The cross-check start delay should be configured to a value greater than or equal to the continuity check message interval to avoid generating unnecessary traps.

Example

This example sets the maximum delay before starting the cross-check process.

Console(config)#cfm mep crosscheck start-delay 60

Console(config)#

snmp-server enable traps ethernet cfm crosscheck

This command enables SNMP traps for CFM continuity check events, in relation to the cross-check operations between statically configured MEPs and those learned via continuity check messages (CCMs). Use the no form to restore disable these traps.

Syntax

[no] snmp-server enable traps ethernet cfm crosscheck [ma-up | mep-missing | mep-unknown]

ma-up – Sends a trap when all remote MEPs in an MA come up.

mep-missing – Sends a trap if the cross-check timer expires and no CCMs have been received from a remote MEP configured in the static list.

mep-unknown – Sends a trap if an unconfigured MEP comes up.

Default Configuration

All continuity checks are enabled.

Command Mode

Global Configuration

User Guidelines

- For this trap type to function, cross-checking must be enabled on the required maintenance associations using the cfm mep crosscheck command.
- A mep-missing trap is sent if cross-checking is enabled (with the cfm mep crosscheck command), and no CCM is received for a remote MEP configured in the static list (with the mep crosscheck mpid command).
- A mep-unknown trap is sent if cross-checking is enabled, and a CCM is received from a remote MEP that is not configured in the static list.
- A ma-up trap is sent if cross-checking is enabled, and a CCM is received from all remote MEPs configured in the static list for this maintenance association.

Example

This example enables SNMP traps for mep-unknown events detected in

cross-check operations.

Console(config)#snmp-server enable traps ethernet cfm crosscheck mep-unknown

Console(config)#

mep crosscheck mpid

This command statically defines a remote MEP in a maintenance association. Use the no form to remove a remote MEP.

Syntax

[no] mep crosscheck mpid *mpid* ma *ma-name*

mpid – Identifier for a maintenance end point which exists on another CFM-enabled device within the same MA. (Range: 1-8191)

ma-name – Maintenance association name. (Range: 1-43 alphanumeric characters)

Default Configuration

No remote MEPs are configured.

Command Mode

CFM Domain Configuration

User Guidelines

- Use this command to statically configure remote MEPs that exist inside the maintenance association. These remote MEPs are used in the crosscheck operation to verify that all endpoints in the specified MA are operational.
- Remote MEPs can only be configured with this command if domain service access points (DSAPs) have already been created with the cfm mep command at the same maintenance level and in the same MA. DSAPs are MEPs that exist on the edge of the domain, and act as primary service access points for end-to-end cross-check, loopback, and link-trace functions.

Example

This example defines a static MEP for the specified maintenance association.

```
Console(config)#cfm domain index 1 name voip level 3
Console(config-ether-cfm)#ma index 1 name rd vlan 1
Console(config-ether-cfm)#mep crosscheck mpid 2 ma rd
Console(config-ether-cfm)#
```

cfm mep crosscheck

This command enables cross-checking between the static list of MEPs assigned to other devices within the same maintenance association and the MEPs learned through continuity check messages (CCMs). Use the disable keyword to stop the cross-check process.

Syntax

cfm mep crosscheck {enable | disable} md *domain-name* ma *ma-name*

enable – Starts the cross-check process.

disable – Stops the cross-check process.

domain-name – Domain name. (Range: 1-43 alphanumeric characters)

ma-name – MA name. (Range: 1-43 alphanumeric characters)

Default Configuration

Disabled

Command Mode

Global Configuration

User Guidelines

- Before using this command to start the cross-check process, first configure the remote MEPs that exist on other devices inside the maintenance association using the mep crosscheck mpid command. These remote MEPs are used in the cross-check operation to verify that all endpoints in the specified MA are operational.
- The cross-check process is disabled by default, and must be manually started using this command with the enable keyword.

Example

This example enables cross-checking within the specified maintenance association.

```
Console#cfm mep crosscheck enable md voip ma rd
Console#
```

show cfm maintenance-points remote crosscheck

This command displays information about remote MEPs statically configured in a cross-check list.

Syntax

show cfm maintenance-points remote crosscheck [domain *domain-name* | mpid *mpid*]

domain-name – Domain name. (Range: 1-43 alphanumeric characters)

mpid – Maintenance end point identifier. (Range: 1-8191)

Default Configuration

None

Command Mode

EXEC

Example

This example shows all remote MEPs statically configured on this device.

```
Console#show cfm maintenance-points remote crosscheck
MPID MA Name Level VLAN MEP Up Remote MAC
---- -------------------- ----- ---- ------ ------------------
2 downtown 4 2 Yes 00-0D-54-FC-A2-73
Console#
```

48.4 Link Trace Operations

cfm linktrace cache

This command enables caching of CFM data learned through link trace messages. Use the no form to disable caching.

Syntax

[no] cfm linktrace cache

Default Configuration

Enabled

Command Mode

Global Configuration

User Guidelines

- A link trace message is a multicast CFM frame initiated by a MEP, and forwarded from MIP to MIP, with each MIP generating a link trace reply, up to the point at which the link trace message reaches its destination or can no longer be forwarded.
- Use this command to enable the link trace cache to store the results of link trace operations initiated on this device. Use the cfm linktrace command to transmit a link trace message.
- Link trace responses are returned from each MIP along the path and from the target MEP. Information stored in the cache includes the maintenance domain name, MA name, MEPID, sequence number, and TTL value.

Example

This example enables link trace caching.

```
Console(config)#cfm linktrace cache
Console(config)#
```

cfm linktrace cache hold-time

This command sets the hold time for CFM link trace cache entries. Use the no form to restore the default setting.

Syntax

cfm linktrace cache hold-time *minutes*

minutes – The aging time for entries stored in the link trace cache. (Range: 1-65535 minutes)

Default Configuration

100 minutes

Command Mode

Global Configuration

User Guidelines

Before setting the aging time for cache entries, the cache must first be enabled with the cfm linktrace cache command.

Example

This example sets the aging time for entries in the link trace cache to 60 minutes.

Console(config)#cfm linktrace cache hold-time 60

Console(config)#

cfm linktrace cache size

This command sets the maximum size for the link trace cache. Use the no form to restore the default setting.

Syntax

cfm linktrace cache size *entries*

entries – The number of link trace responses stored in the link trace cache. (Range: 1-4095 entries)

Default Configuration

100 entries

Command Mode

Global Configuration

User Guidelines

- Before setting the cache size, the cache must first be enabled with the cfm linktrace cache command.
- If the cache reaches the maximum number of specified entries, or the size is set to a value less than the current number of stored entries, no new entries are added. To add additional entries, the cache size must first be increased with this command, or purged with the clear Cfm linktrace-cache command.

Example

This example limits the maximum size of the link trace cache to 500 entries.

Console(config)#cfm linktrace cache size 500

Console(config)#

cfm linktrace

This command sends CFM link trace messages to the MAC address of a remote MEP.

Syntax

cfm linktrace {dest-mep *destination-mpid* | src-mep *source-mpid* {dest-mep *destination-mpid* | *mac-address*} | *mac-address*} md *domain-name* ma *ma-name* [ttl *number*]

destination-mpid – The identifier of a remote MEP that is the target of the link trace message. (Range: 1-8191)

source-mpid – The identifier of a source MEP that will send the link trace message. (Range: 1-8191)

mac-address – MAC address of a remote MEP that is the target of the link trace message. This address can be entered in either of the following formats: xx-xx-xx-xx-xx-xx or xxxxxxxxxxxx

domain-name – Domain name. (Range: 1-43 alphanumeric characters)

ma-name – Maintenance association name. (Range: 1-43 alphanumeric characters)

number – The time to live of the linktrace message. (Range: 1-255 hops)

Default Configuration

None

Command Mode

Global Configuration

User Guidelines

- Link trace messages can be targeted to MEPs, not MIPs. Before sending a link trace message, be sure you have configured the target MEP for the specified MA.

- If the MAC address of target MEP has not been learned by any local MEP, then the linktrace may fail. Use the show cfm maintenance-points remote crosscheck command to verify that a MAC address has been learned for the target MEP.
- Link trace messages (LTMs) are sent as multicast CFM frames, and forwarded from MIP to MIP, with each MIP generating a link trace reply, up to the point at which the LTM reaches its destination or can no longer be forwarded.
- Link trace messages are used to isolate faults. However, this task can be difficult in an Ethernet environment, since each node is connected through multipoint links. Fault isolation is even more challenging since the MAC address of the target node can age out in several minutes. This can cause the traced path to vary over time, or connectivity lost if faults cause the target MEP to be isolated from other MEPs in an MA.
- When using the command line or web interface, the source MEP used by to send a link trace message is chosen by the CFM protocol. However, when using SNMP, the source MEP can be specified by the user.

Example

This example sends a link trace message to the specified MEP with a maximum hop count of 25.

Console#(config)linktrace ethernet dest-mep 2 md voip ma rd ttl 25

Console#

clear cfm linktrace-cache

This command clears link trace messages logged on this device.

Command Mode

EXEC

Example

Console#clear cfm linktrace-cache

Console#

show cfm linktrace-cache

This command displays the contents of the link trace cache.

Command Mode

EXEC

Example

Console#show cfm linktrace-cache

Hops MA IP / Alias Ingress MAC Ing. Action Relay

Forwarded Egress MAC Egr. Action

---- -------------- ---------------------- ------------------ ----------- -----

2 rd 192.168.0.6 00-12-CF-12-12-2D ingOk Hit

Not Forwarded

Console#

48.5 Loopback Operations

cfm loopback

This command sends CFM loopback messages to a MAC address for a MEP or MIP.

Syntax

cfm loopback {dest-mep *destination-mpid* | src-mep *source-mpid* {dest-mep *destination-mpid* | *mac-address*} | *mac-address*} md *domain-name* ma *ma-name* [count *transmit-count*] [size *packet-size*]

destination-mpid – The identifier of a MEP that is the target of the loopback message. (Range: 1-8191)

source-mpid – The identifier of a source MEP that will send the loopback message. (Range: 1-8191)

mac-address – MAC address of the remote maintenance point that is the target of the loopback message. This address can be entered in either of the following formats: xx-xx-xx-xx-xx-xx or xxxxxxxxxxxx

domain-name – Domain name. (Range: 1-43 alphanumeric characters)

ma-name – Maintenance association name. (Range: 1-43 alphanumeric characters)

transmit-count – The number of times the loopback message is sent. (Range: 1-1024)

packet-size – The size of the loopback message. (Range: 64-1518 bytes)

Default Configuration

Loop back count: One loopback message is sent.

Loop back size: 64 bytes

Command Mode

Global Configuration

User Guidelines

- Use this command to test the connectivity between maintenance points. If the continuity check database does not have an entry for the specified maintenance point, an error message will be displayed.
- The point from which the loopback message is transmitted (i.e., the DSAP) and the target maintenance point specified in this command must be within the same MA.
- Loop back messages can be used for fault verification and isolation after automatic detection of a fault or receipt of some other error report. Loopback messages can also used to confirm the successful restoration or initiation of connectivity. The receiving maintenance point should respond to the loop back message with a loopback reply.
- When using the command line or web interface, the source MEP used by to send a loopback message is chosen by the CFM protocol. However, when using SNMP, the source MEP can be specified by the user.

Example

This example sends a loopback message to the specified remote MEP.

Console#(config)cfm loopback dest-mep 1 md voip ma rd

Console#

48.6 Fault Generator Operations

mep fault-notify alarm-time

This command sets the time a defect must exist before a fault alarm is issued. Use the no form to restore the default setting.

Syntax

mep fault-notify alarm-time *alarm-time*

no fault-notify alarm-time

alarm-time – The time that one or more defects must be present before a fault alarm is generated. (Range: 3-10 seconds)

Default Configuration

3 seconds

Command Mode

CFM Domain Configuration

User Guidelines

A fault alarm is issued when the MEP fault notification generator state machine detects that a time period configured by this command has passed with one or more defects indicated, and fault alarms are enabled at or above the priority level set by the mep fault-notify lowest-priority command.

Example

This example set the delay time before generating a fault alarm.

Console(config)#cfm domain index 1 name voip level 3

Console(config-ether-cfm)#mep fault-notify alarm-time 10

Console(config-ether-cfm)#

mep fault-notify lowest-priority

This command sets the lowest priority defect that is allowed to generate a fault alarm. Use the no form to restore the default setting.

Syntax

mep fault-notify lowest-priority *priority*

no fault-notify lowest-priority

priority – Lowest priority default allowed to generate a fault alarm. (Range: 1-6)

Default Configuration

Priority level 2

Command Mode

CFM Domain Configuration

User Guidelines

- A fault alarm can generate an SNMP notification. It is issued when the MEP fault notification generator state machine detects that a configured time period (see the mep fault-notify alarm-time command) has passed with one or more defects indicated, and fault alarms are enabled at or above the priority level set by this command. The state machine transmits no further fault alarms until it is reset by the passage of a configured time period (see the mep fault-notify reset-time command) without a defect indication. The normal procedure upon receiving a fault alarm is to inspect the reporting MEP's managed objects using an appropriate SNMP software tool, diagnose the fault, correct it, reexamine the MEP's managed objects to see whether the MEP fault notification generator state machine has been reset, and repeat those steps until the fault is resolved.
- Only the highest priority defect currently detected is reported in the fault alarm.

Example

This example sets the lowest priority defect that will generate a fault alarm.

Console(config)#cfm domain index 1 name voip level 3

Console(config-ether-cfm)#mep fault-notify lowest-priority 1

Console(config-ether-cfm)#

mep fault-notify reset-time

This command configures the time after a fault alarm has been issued, and no defect exists, before another fault alarm can be issued. Use the no form to restore the default setting.

Syntax

mep fault-notify reset-time *reset-time*

no fault-notify reset-time

reset-time – The time that must pass without any further defects indicated before another fault alarm can be generated. (Range: 3-10 seconds)

Default Configuration

10 seconds

Command Mode

CFM Domain Configuration

Example

This example sets the reset time after which another fault alarm can be generated.

Console(config)#cfm domain index 1 name voip level 3

Console(config-ether-cfm)#mep fault-notify reset-time 7

Console(config-ether-cfm)#

show cfm fault-notify-generator

This command displays configuration settings for the fault notification generator.

Syntax

show cfm fault-notify-generator mep *mpid*

mpid – Maintenance end point identifier. (Range: 1-8191)

Default Configuration

None

Command Mode

EXEC

Example

This example shows the fault notification settings configured for one MEP.

Console#show cfm fault-notify-generator mep 1

MD Name MA Name Highest Defect Lowest Alarm Alarm Time Reset Time

---------- ---------- ---------- ---------- ---------- ----------

voip rd none macRemErrXcon 3sec. 10sec.

Console#

48.7 Delay Measure Operations

cfm delay-measure two-way

This command sends periodic delay-measure requests to a specified MEP within a maintenance association.

Syntax

cfm delay-measure two-way [src-mep *source-mpid*] {dest-mep *destination-mpid* | *mac-address*} md *domain-name* ma *ma-name* [count *transmit-count*] [interval *interval*] [size *packet-size*] [timeout *timeout*]

source-mpid – The identifier of a source MEP that will send the delay-measure message. (Range: 1-8191)

destination-mpid – The identifier of a remote MEP that is the target of the delay-measure message. (Range: 1-8191)

mac-address – MAC address of a remote MEP that is the target of the delay-measure message. This address can be entered in either of the following formats: xx-xx-xx-xx-xx-xx or xxxxxxxxxxxx

domain-name – Domain name. (Range: 1-43 alphanumeric characters)

ma-name – Maintenance association name. (Range: 1-43 alphanumeric characters)

count – The number of times to retry sending the message if no response is received before the specified timeout. (Range: 1-5)

interval – The transmission delay between delay-measure messages. (Range: 1-5 seconds)

packet-size – The size of the delay-measure message. (Range: 64-1518 bytes)

timeout - The timeout to wait for a response. (Range: 1-5 seconds)

Default Configuration

Count: 5

Interval: 1 second

Size: 64 bytes

Timeout: 5 seconds

Command Mode

Global Configuration

User Guidelines

- Delay measurement can be used to measure frame delay and frame delay variation between MEPs.
- A local MEP must be configured for the same MA before you can use this command.
- If a MEP is enabled to generate frames with delay measurement (DM) information, it periodically sends DM frames to its peer MEP in the same MA, and expects to receive DM frames back from it.
- Frame delay measurement can be made only for two-way measurements, where the MEP transmits a frame with DM request information with the TxTimeStampf (Timestamp at the time of sending a frame with DM request information), and the receiving MEP responds with a frame with DM reply information with TxTimeStampf copied from the DM request information, RxTimeStampf (Timestamp at the time of receiving a frame with DM request information), and TxTimeStampb (Timestamp at the time of transmitting a frame with DM reply information):

  Frame Delay = (RxTimeStampb-TxTimeStampf)-(TxTimeStampbRxTimeStampf)
- The MEP can also make two-way frame delay variation measurements based on its ability to calculate the difference between two subsequent two-way frame delay measurements.

Example

This example sends periodic delay-measure requests to a remote MEP.

Console#(config)cfm delay-measure two-way dest-mep 1 md voip ma rd

Type ESC to abort.

Sending 5 Ethernet CFM delay measurement message, timeout is 5 sec.

Sequence Delay Time (ms.) Delay Variation (ms.)

-------- ---------- ----------

1 < 10 0

2 < 10 0

3 < 10 0

4 40 40

5 < 10 40

Success rate is 100% (5/5), delay time min/avg/max=0/8/40 ms.

Average frame delay variation is 16 ms.

Console#

49. OAM Commands

efm oam

This command enables OAM functions on the specified port. Use the no form to disable this function.

Syntax

[no] efm oam

Default Configuration

Disabled

Command Mode

Interface Configuration

User Guidelines

- If the remote device also supports OAM, both exchange Information OAMPDUs to establish an OAM link.
- Not all CPEs support OAM functions, and OAM is therefore disabled by default. If the CPE attached to a port supports OAM, then this functionality must first be enabled by the efm oam command to gain access to other remote configuration functions.

Example

Console(config)#interface ethernet 1/1

Console(config-if)#efm oam

Console(config-if)#

efm oam critical-link-event

This command enables reporting of critical event or dying gasp. Use the no form to disable this function.

Syntax

[no] efm oam critical-link-event {critical-event | dying-gasp}

critical-event - If a critical event occurs, the local OAM entity (this switch) indicates this to its peer by setting the appropriate flag in the next OAMPDU to be sent and stores this information in its OAM event log.

dying-gasp - If an unrecoverable condition occurs, the local OAM entity indicates this by immediately sending a trap message.

Default Configuration

Enabled

Command Mode

Interface Configuration

User Guidelines

- Critical events are vendor-specific and may include various failures, such as abnormal voltage fluctuations, out-of-range temperature detected, fan failure, CRC error in flash memory, insufficient memory, or other hardware faults.
- Dying gasp events are caused by an unrecoverable failure, such as a power failure or device reset.

Note:

When system power fails, the switch will always send a dying gasp trap message prior to power down.

Example

Console(config)#interface ethernet 1/1

Console(config-if)#efm oam critical-link-event dying-gasp

Console(config-if)#

efm oam link-monitor frame

This command enables reporting of errored frame link events. Use the no form to disable this function.

Syntax

[no] efm oam link-monitor frame

Default Configuration

Enabled

Command Mode

Interface Configuration

User Guidelines

- An errored frame is a frame in which one or more bits are errored.
- If this feature is enabled and an errored frame link event occurs, the local OAM entity (this switch) sends an Event Notification OAMPDU.

Example

Console(config)#interface ethernet 1/1

Console(config-if)#efm oam link-monitor frame

Console(config-if)#

efm oam link-monitor frame threshold

This command sets the threshold for errored frame link events. Use the no form to restore the default setting.

Syntax

[no] efm oam link-monitor frame threshold *count*

count - The threshold for errored frame link events. (Range: 1-65535)

Default Configuration

1

Command Mode

Interface Configuration

User Guidelines

If this feature is enabled, an event notification message is sent if the threshold is reached or exceeded within the period specified by the efm oam link-monitor frame window command. The Errored Frame Event TLV includes the number of errored frames detected during the specified period.

Example

Console(config)#interface ethernet 1/1

Console(config-if)#efm oam link-monitor frame threshold 5

Console(config-if)#

efm oam link-monitor frame window

This command sets the monitor period for errored frame link events. Use the no form to restore the default setting.

Syntax

[no] efm oam link-monitor frame window *size*

size - The period of time in which to check the reporting threshold for errored frame link events. (Range: 10-65535 units of 10 milliseconds)

Default Configuration

10 (units of 100 milliseconds) = 1 second

Command Mode

Interface Configuration

User Guidelines

If this feature is enabled, an event notification message is sent if the threshold specified by the efm oam link-monitor frame threshold command is reached or exceeded within the period specified by this command. The Errored Frame Event TLV includes the number of errored frames detected during the specified period.

Example

This example set the window size to 5 seconds.

Console(config)#interface ethernet 1/1

Console(config-if)#efm oam link-monitor frame window 50

Console(config-if)#

efm oam mode

This command sets the OAM mode on the specified port. Use the no form to restore the default setting.

Syntax

efm oam mode {active | passive}

no efm oam mode

active - All OAM functions are enabled.

passive - All OAM functions are enabled, except for OAM discovery, and sending loopback control OAMPDUs.

Default Configuration

Active

Command Mode

Interface Configuration

User Guidelines

When set to active mode, the selected interface will initiate the OAM discovery process. When in passive mode, it can only respond to discovery messages.

Example

Console(config)#interface ethernet 1/1

Console(config-if)#efm oam mode active

Console(config-if)#

clear efm oam counters

This command clears statistical counters for various OAMPDU message types.

Syntax

clear efm oam counters [*interface-list*]

interface-list - *unit*/*port*

unit - Unit identifier. (Range: 1)

port - Port number or list of ports. To enter a list, separate nonconsecutive port identifiers with a comma and no spaces; use a hyphen to designate a range of ports. (Range: 1-28)

Command Mode

EXEC

Example

Console#clear efm oam counters

Console#

efm oam remote-loopback

This command starts or stops OAM loopback test mode to the attached CPE.

Syntax

efm oam remote-loopback {start | stop} *interface*

start - Starts remote loopback test mode.

stop - Stops remote loopback test mode.

interface - *unit*/*port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-28)

Default Configuration

None

Command Mode

Global Configuration

User Guidelines

- OAM remote loop back can be used for fault localization and link performance testing. Statistics from both the local and remote DTE can be queried and compared at any time during loop back testing.
- Use the efm oam remote-loopback start command to start OAM remote loop back test mode on the specified port. Afterwards, use the efm oam remote-loopback test command to start sending test packets. Then use the efm oam remote loopback stop command to terminate testing (if test packets are still being sent) and to terminate loop back test mode.
- The port that you specify to run this test must be connected to a peer OAM device capable of entering into OAM remote loopback mode. During a remote loopback test, the remote OAM entity loops back every frame except for OAMPDUs and pause frames.
- During loopback testing, both the switch and remote device are permitted to send OAMPDUs to the peer device and to process any OAMPDUs received from the peer.

Example

Console#(config)efm oam remote-loopback start 1/1

Loopback operation is processing, please wait.

Enter loopback mode succeeded.

Console#

efm oam remote-loopback test

This command performs a remote loopback test, sending a specified number of packets.

Syntax

efm oam remote-loopback test *interface* [*number-of-packets* [*packet-size*]]

interface - *unit*/*port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-28)

number-of-packets - Number of packets to send. (Range: 1-99999999)

packet-size - Size of packets to send. (Range: 64-1518 bytes)

Default Configuration

Number of packets: 10,000

Packet size: 64 bytes

Command Mode

Global Configuration

User Guidelines

- You can use this command to perform an OAM remote loopback test on the specified port. The port that you specify to run this test must be connected to a peer OAM device capable of entering into OAM remote loopback mode. During a remote loopback test, the remote OAM entity loops back every frame except for OAMPDUs and pause frames.

- OAM remote loopback can be used for fault localization and link performance testing. Statistics from both the local and remote DTE can be queried and compared at any time during loopback testing.
- A summary of the test is displayed after it is finished.

Example

Console#(config)efm oam remote-loopback test 1/1

Loopback test is processing, press ESC to suspend.

....

Port OAM loopback Tx OAM loopback Rx Loss Rate

---- --------------- --------------- ---------

1/2 1990 1016 48.94 %

Console#

show efm oam counters interface

This command displays counters for various OAM PDU message types.

Syntax

show efm oam counters interface [*interface-list*]

interface-list - *unit*/*port*

unit - Unit identifier. (Range: 1)

port - Port number or list of ports. To enter a list, separate nonconsecutive port identifiers with a comma and no spaces; use a hyphen to designate a range of ports. (Range: 1-28)

Command Mode

Normal Exec, EXEC

Example

Console#show efm oam counters interface 1/1

Port OAMPDU Type TX RX

---- --------------------- ---------- ----------

1/1 Information 1121 1444

1/1 Event Notification 0 0

1/1 Loopback Control 1 0

1/1 Organization Specific 76 0

Console#

show efm oam event-log interface

This command displays the OAM event log for the specified port(s) or for all ports that have logs.

show efm oam event-log interface [*interface-list*]

interface-list - *unit*/*port*

unit - Unit identifier. (Range: 1)

port - Port number or list of ports. To enter a list, separate nonconsecutive port identifiers with a comma and no spaces; use a hyphen to designate a range of ports. (Range: 1-28)

Command Mode

Normal Exec, EXEC

User Guidelines

- When a link event occurs, no matter whether the location is local or remote, this information is entered in the OAM event log.
- When the log system becomes full, older events are automatically deleted to make room for new entries.

Example

Console#show efm oam event-log interface 1/1

OAM event log of Eth 1/1:

00:24:07 2001/01/01

"Unit 1, Port 1: Dying Gasp at Remote"

Console#

show efm oam remote-loopback interface

This command displays the results of OAM remote loopback test.

Syntax

show efm oam remote-loopback interface [*interface-list*]

interface-list - *unit*/*port*

unit - Unit identifier. (Range: 1)

port - Port number or list of ports. To enter a list, separate nonconsecutive port identifiers with a comma and no spaces; use a hyphen to designate a range of ports. (Range: 1-28)

Command Mode

Normal Exec, EXEC

Example

Console#show efm oam remote-loopback interface 1/1

Port OAM loopback Tx OAM loopback Rx

---- --------------- ---------------

1/1 2300 2250

Console#

show efm oam status interface

This command displays OAM configuration settings and event counters.

Syntax

show efm oam status interface [*interface-list*] [brief]

interface - *unit*/*port*

unit - Unit identifier. (Range: 1)

port - Port number or list of ports. To enter a list, separate nonconsecutive port identifiers with a comma and no spaces; use a hyphen to designate a range of ports. (Range: 1-28)

brief - Displays a brief list of OAM configuration states.

Command Mode

Normal Exec, EXEC

Example

Console#show efm oam status interface 1/1

OAM information of Eth 1/1:

Basic Information:

Admin State: Enabled

Operation State: Operational

Mode: Active

Dying Gasp: Enabled

Critical Event: Enabled

Link Monitor (Errored Frame): Enabled

Link Monitor:

Errored Frame Window (100msec): 10

Errored Frame Threshold: 1

Console#show efm oam status interface 1/1 brief

$ = local OAM in loopback

* = remote OAM in loopback

Port Admin Mode Remote Dying Critical Errored

State Loopback Gasp Event Frame

---- ------- -------- -------- -------- -------- -------

1/1 Enabled Active Disabled Enabled Enabled Enabled

Console#

show efm oam status remote interface

This command displays information about attached OAM-enabled devices.

Syntax

show efm oam status remote interface [*interface-list*]

interface-list - *unit*/*port*

unit - Unit identifier. (Range: 1)

port - Port number or list of ports. To enter a list, separate nonconsecutive port identifiers with a comma and no spaces; use a hyphen to designate a range of ports. (Range: 1-28)

Command Mode

Normal Exec, EXEC

Example

Console#show efm oam status remote interface 1/1

Port MAC Address OUI Remote Unidirectional Link MIB Variable

Loopback Monitor Retrieval

---- ----------------- ------ -------- --------------- ------- ------------

1/1 64-9D-99-6A-07-F6 000084 Enabled Disabled Enabled Disabled

Console#

50. Domain Name Service (DNS) Commands

dns domain-list

This command defines a list of domain names that can be appended to incomplete host names (i.e., host names passed from a client that are not formatted with dotted notation). Use the no form to remove a name from this list.

Syntax

[no] dns domain-list *name*

name - Name of the host. Do not include the initial dot that separates the host name from the domain name. (Range: 1-127 characters)

Default Configuration

None

Command Mode

Global Configuration

User Guidelines

- Domain names are added to the end of the list one at a time.
- When an incomplete host name is received by the DNS service on this switch, it will work through the domain list, appending each domain name in the list to the host name, and checking with the specified name servers for a match.
- If there is no domain list, the domain name specified with the dns domain-name command is used. If there is a domain list, the default domain name is not used.

Example

This example adds two domain names to the current list and then displays the list.

Console(config)#dns domain-list sample.com.jp

Console(config)#dns domain-list sample.com.uk

Console(config)#end

Console#show dns

Domain Lookup Status:

DNS Disabled

Default Domain Name:

sample.com

Domain Name List:

sample.com.jp

sample.com.uk

Name Server List:

Console#

dns domain-lookup

This command enables DNS host name-to-address translation. Use the no form to disable DNS.

Syntax

[no] dns domain-lookup

Default Configuration

Disabled

Command Mode

Global Configuration

User Guidelines

- At least one name server must be specified before DNS can be enabled.
- If all name servers are deleted, DNS will automatically be disabled.

Example

This example enables DNS and then displays the configuration.

```
Console(config)#dns domain-lookup
Console(config)#end
Console#show dns
Domain Lookup Status:
DNS Enabled
Default Domain Name:
sample.com
Domain Name List:
sample.com.jp
sample.com.uk
Name Server List:
192.168.1.55
10.1.0.55
Console#
```

dns domain-name

This command defines the default domain name appended to incomplete host names (i.e., host names passed from a client that are not formatted with dotted notation). Use the no form to remove the current domain name.

Syntax

dns domain-name *name*

no dns domain-name

name - Name of the host. Do not include the initial dot that separates the host name from the domain name. (Range: 1-127 characters)

Default Configuration

None

Command Mode

Global Configuration

Example

```
Console(config)#dns domain-name sample.com
Console(config)#end
Console#show dns
Domain Lookup Status:
DNS Disabled
Default Domain Name:
sample.com
Domain Name List:
```

dns host

This command creates a static entry in the DNS table that maps a host name to an IP address. Use the no form to remove an entry.

Syntax

[no] dns host *name address*

name - Name of an DNS host. (Range: 1-100 characters)

address - Corresponding IP address.

Default Configuration

No static entries

Command Mode

Global Configuration

User Guidelines

Use the no dns host command to clear static entries, or the clear host command to clear dynamic entries.

Example

This example maps an IP address to a host name.

Console(config)#dns host rd5 192.168.1.55

Console(config)#end

Console#show hosts

No. Flag Type IP Address TTL Domain

---- ---- ------- --------------------- ----- ------------------------------

0 2 Address 192.168.1.55 rd5

Console#

dns name-server

This command specifies the address of one or more domain name servers to use for name-to-address resolution. Use the no form to remove a name server from this list.

Syntax

[no] dns name-server *server-address1* [*server-address2* … *server-address6*]

server-address1 - IP address of domain-name server.

server-address2 … *server-address6* - IP address of additional domain-name servers.

Default Configuration

None

Command Mode

Global Configuration

User Guidelines

The listed name servers are queried in the specified sequence until a response is received, or the end of the list is reached with no response.

Example

This example adds two domain-name servers to the list and then displays the list.

Console(config)#dns name-server 192.168.1.55 10.1.0.55

Console(config)#end

Console#show dns

Domain Lookup Status:

DNS disabled

Default Domain Name:

sample.com

Domain Name List:

sample.com.jp

sample.com.uk

Name Server List:

192.168.1.55

10.1.0.55

Console#

clear dns cache

This command clears all entries in the DNS cache.

Command Mode

EXEC

Example

Console#clear dns cache

Console#show dns cache

No. Flag Type DNS Address TTL Domain

------- ------- ------- --------------- ------- --------

Console#

clear host

This command deletes dynamic entries from the DNS table.

Syntax

clear host {*name* | *}

name - Name of the host. (Range: 1-100 characters)

* - Removes all entries.

Default Configuration

None

Command Mode

EXEC

User Guidelines

Use the clear host command to clear dynamic entries, or the no dns host command to clear static entries.

Example

This example clears all dynamic entries from the DNS table.

Console(config)#clear host *

Console(config)#

show dns

This command displays the configuration of the DNS service.

Command Mode

EXEC

Example

Console#show dns

Domain Lookup Status:

DNS enabled

Default Domain Name:

sample.com

Domain Name List:

sample.com.jp

sample.com.uk

Name Server List:

192.168.1.55

10.1.0.55

Console#

show dns cache

This command displays entries in the DNS cache.

Command Mode

EXEC

Example

Console#show dns cache

No. Flag Type IP Address TTL Host

------- ------- ------- --------------- ------- --------

3 4 Host 209.131.36.158 115 www-real.wa1.b.yahoo.com

4 4 CNAME POINTER TO:3 115 www.yahoo.com

5 4 CNAME POINTER TO:3 115 www.wa1.b.yahoo.com

Console#

show hosts

This command displays the static host name-to-address mapping table.

Command Mode

EXEC

Example

Note that a host name will be displayed as an alias if it is mapped to the same address(es) as a previously configured entry.

Console#show hosts

No. Flag Type IP Address TTL Domain

---- ---- ------- ------------------- ----- ------------------------------

0 2 Address 192.168.1.55 rd5

1 2 Address 2001:DB8:1::12 rd6

3 4 Address 209.131.36.158 65 www-real.wa1.b.yahoo.com

4 4 CNAME POINTER TO:3 65 www.yahoo.com

5 4 CNAME POINTER TO:3 65 www.wa1.b.yahoo.com

Console#

51. DHCP Commands

51.1 DHCP Client

Use the commands in this section to allow the switch's VLAN interfaces to dynamically acquire IP address information.

ip dhcp client class-id

This command specifies the DCHP client vendor class identifier for the current interface. Use the no form to remove the class identifier option from the DHCP packet.

Syntax

ip dhcp client class-id [text *text* | hex *hex*]

no ip dhcp client class-id

text - A text string. (Range: 1-32 characters)

hex - A hexadecimal value. (Range: 1-64 characters)

Default Configuration

Class identifier option enabled, with the name ECS4510-28T

Command Mode

Interface Configuration (VLAN)

User Guidelines

- Use this command without any keyword to restore the default setting.
- This command is used to identify the vendor class and configuration of the switch to the DHCP server, which then uses this information to decide on how to service the client or the type of information to return.
- The general framework for this DHCP option is set out in RFC 2132 (Option 60). This information is used to convey configuration settings or other identification information about a client, but the specific string to use should be supplied by your service provider or network administrator.
- The server should reply with Option 43 information, which encapsulates Option 66 attributes including the TFTP server name and boot file name.

Example

Console(config)#interface vlan 2

Console(config-if)#ip dhcp client class-id hex 0000e8666572

Console(config-if)#

ip dhcp restart client

This command submits a BOOTP or DHCP client request.

Default Configuration

None

Command Mode

EXEC

User Guidelines

- This command issues a BOOTP or DHCP client request for any IP interface that has been set to BOOTP or DHCP mode through the ip address command.
- DHCP requires the server to reassign the client's last address if available.
- If the BOOTP or DHCP server has been moved to a different domain, the network portion of the address provided to the client will be based on this new domain.

Example

In the following example, the device is reassigned the same address.

```
Console(config)#interface vlan 1
Console(config-if)#ip add dhcp
Console(config-if)#exit
Console#ip dhcp restart client
Console#show ip interface brief
VLAN 1 is Administrative Up - Link Up
Address is 00-E0-00-00-00-01
Index: 1001, MTU: 1500
Address Mode is DHCP
IP Address: 192.168.0.2 Mask: 255.255.255.0
Console#
```

51.2 DHCP Relay Option 82

ip dhcp relay server

This command enables DHCP relay service, and specifies the address of the servers to use. Use the no form to clear all addresses.

Syntax

ip dhcp relay server *address1* [*address2* [*address3* ...]]

no ip dhcp relay server

address - IP address of DHCP server. (Range: 1-5 addresses)

Default Configuration

None

Command Mode

Global Configuration

USAGE GUIDELINES

- DHCP relay service applies to DHCP client requests received on any configured VLAN, both the management VLAN and non-management VLANs.
- This command is used to configure DHCP relay for host devices attached to the switch. If DHCP relay service is enabled (by specifying the address for at least one DHCP server), and this switch sees a DHCP request broadcast, it inserts its own IP address into the request so the DHCP server will know the subnet where the client is located. Then, the switch forwards the packet to a DHCP server on another network. When the server receives the DHCP request, it allocates a free IP address for the DHCP client from its defined scope for the DHCP client's subnet, and sends a DHCP response back to the DHCP relay agent (i.e., this switch). This switch then passes the DHCP response received from the server to the client.
- You must specify the IP address for at least one DHCP server. Otherwise, the switch's DHCP relay agent will not forward client requests to a DHCP server. Up to five DHCP servers can be specified in order of preference.
- To terminate DHCP relay service, all configured server addresses must be cleared with the no form of this command.

Example

```
Console(config)#ip dhcp relay server 192.168.10.19
Console(config)#
```

ip dhcp relay information option

This command enables DHCP Option 82 information relay, and specifies the frame format to use for the remote-id when Option 82 information is generated by the switch. Use the no form of this command to disable this feature.

Syntax

ip dhcp relay information option [encode no-subtype] [remote-id {ip-address [encode {ascii | hex}] | mac-address [encode {ascii | hex}] | string *string*}]

no ip dhcp rely information option [encode no-subtype] [remote-id [ip-address encode] | [mac-address encode]]

encode no-subtype - Disables use of sub-type and sub-length fields in circuit-ID (CID) and remote-ID (RID) in Option 82 information.

mac-address - Includes a MAC address field for the relay agent (that is, the MAC address of the switch's CPU).

ip-address - Includes the IP address field for the relay agent (that is, the IP address of the management interface).

encode - Indicates encoding in ASCII or hexadecimal.

string - An arbitrary string inserted into the remote identifier field. (Range: 1-32 characters)

Default Configuration

Option 82: Disabled

CID/RID sub-type: Enabled

Remote ID: MAC address

Command Mode

Global Configuration

USAGE GUIDELINES

- Use this command without any keywords to enable DHCP Option 82 information relay.
- DHCP provides a relay agent information option for sending information about its DHCP clients or the relay agent itself to the DHCP server. Also known as DHCP Option 82, it allows compatible DHCP servers to use this information when assigning IP addresses, or to set other services or policies for clients.
- When Option 82 is enabled, the requesting client (or an intermediate relay agent that has used the information fields to describe itself) can be identified in the DHCP request packets forwarded by the switch and in reply packets sent back from the DHCP server. Depending on the selected frame format set for the remote-id by this command, this information may specify the MAC address, IP address, or an arbitrary string for the requesting device (that is, the relay agent in this context).
- By default, the relay agent also fills in the Option 82 circuit-id field with information indicating the local interface over which the switch received the DHCP client request, including the VLAN ID, stack unit, and port. This allows DHCP client-server exchange messages to be forwarded between the server and client without having to flood them to the entire VLAN.
- DHCP request packets received by the switch are handled as follows:

a. If a DHCP relay server has been set on the switch, when the switch receives a DHCP request packet *without* option 82 information from the management VLAN or a non-management VLAN, it will add option 82 relay information and the relay agent's address to the DHCP request packet, and then unicast it to the DHCP server.

b. If a DHCP relay server has been set on the switch, when the switch receives a DHCP request packet *with* option 82 information from the management VLAN or a non-management VLAN, it will process it according to the configured relay information option policy:

c. If the policy is "replace," the DHCP request packet's option 82 content (the RID and CID sub-option) is replaced with information provided by the switch. The relay agent address is inserted into the DHCP request packet, and the switch then unicasts this packet to the DHCP server.

d. If the policy is "keep," the DHCP request packet's option 82 content will be retained. The relay agent address is inserted into the DHCP request packet, and the switch then unicasts this packet to the DHCP server.

e. If the policy is "drop," the original DHCP request packet is flooded onto the VLAN which received the packet but is not relayed.

- DHCP reply packets received by the relay agent are handled as follows:

When the relay agent receives a DHCP reply packet with Option 82 information over the management VLAN, it first ensures that the packet is destined for it.

a. If the RID in the DHCP reply packet is not identical with that configured on the switch, the option 82 information is retained, and the packet is flooded onto the VLAN through which it was received.

b. If the RID in the DHCP reply packet matches that configured on the switch, it then removes the Option 82 information from the packet, sends it on as follows:

c. If the DHCP packet's broadcast flag is on, the switch uses the circuit-id information contained in the option 82 information fields to identify the VLAN connected to the requesting client and then broadcasts the DHCP reply packet to this VLAN.

d. If the DHCP packet's broadcast flag is off, the switch uses the circuit-id information in option 82 fields to identify the interface connected to the requesting client and unicasts the reply packet to the client.

- DHCP packets are flooded onto the VLAN which received them if DHCP relay service is enabled on the switch and any of the following situations apply:

a. There is no DHCP relay server set on the switch, when the switch receives a DHCP packet.

b. A DHCP relay server has been set on the switch, when the switch receives a DHCP request packet with a non-zero relay agent address field (that is not the address of this switch).

c. A DHCP relay server has been set on the switch, when the switch receives DHCP reply packet without option 82 information from the management VLAN.

d. The reply packet contains a valid relay agent address field (that is not the address of this switch), or receives a reply packet with a zero relay agent address through the management VLAN.

e. A DHCP relay server has been set on the switch, and the switch receives a reply packet on a non-management VLAN.

- Use the ip dhcp relay information policy command to specify how to handle DHCP client request packets which already contain Option 82 information.
- DHCP Snooping Information Option 82 and DHCP Relay Information Option 82 cannot both be enabled at the same time.

Example

This example enables Option 82, and sets the frame format of the remote ID for the option to use the MAC address of the switch's CPU.

Console(config)#ip dhcp relay information option remote-id mac-address

Console(config)#

ip dhcp relay information policy

This command specifies how to handle client requests which already contain DHCP Option 82 information.

Syntax

ip dhcp relay information policy {drop | keep | replace}

drop - Floods the original request packet onto the VLAN that received it instead of relaying it.

keep - Retains the Option 82 information in the client request, inserts the relay agent's address, and unicasts the packet to the DHCP server.

replace - Replaces the Option 82 information circuit-id and remoteid fields in the client's request with information provided by the relay agent itself, inserts the relay agent's address, and unicasts the packet to the DHCP server.

Default Configuration

drop

Command Mode

Global Configuration

USAGE GUIDELINES

- Refer to the Usage Guidelines under the ip dhcp relay information option command for information on when Option 82 information is processed by the switch.
- When the Option 82 policy is set to "keep" the original information in the request packet, the frame type specified by the ip dhcp relay information option command is ignored.

Example

This example sets the Option 82 policy to keep the client information in the request packet received by the relay agent, and forward this packet on to the DHCP server.

Console(config)#ip dhcp relay information policy keep

Console(config)#

show ip dhcp relay

This command displays the configuration settings for DHCP relay service.

Command Mode

EXEC

Example

Console#show ip dhcp relay

Status of DHCP relay information:

Insertion of relay information: enabled.

DHCP option policy: drop.

DHCP relay-server address: 192.168.0.4

0.0.0.0

0.0.0.0

0.0.0.0

0.0.0.0

DHCP sub-option format: extra subtype included

DHCP remote id sub-option: mac address (hex encoded)

Console#

52. IP Interface Commands

52.1 IPV4 Interface

ip add

This command sets the IPv4 address for the currently selected VLAN interface. Use the no form to restore the default IP address.

Syntax

ip add {*ip-address netmask* [secondary] [default-gateway *ip-address*] | bootp | dhcp}

no ip add [*ip-address netmask* [secondary] | dhcp]

ip-address - IP address

netmask - Network mask for the associated IP subnet. This mask identifies the host address bits used for routing to specific subnets.

secondary - Specifies a secondary IP address.

default-gateway - The default gateway. (Refer to the ip defaultgateway command which provides the same function)

bootp - Obtains IP address from BOOTP.

dhcp - Obtains IP address from DHCP.

Default Configuration

DHCP

Command Mode

Interface Configuration (VLAN)

User Guidelines

- An IP address must be assigned to this device to gain management access over the network or to connect the switch to existing IP subnets. A specific IP address can be manually configured, or the switch can be directed to obtain an address from a BOOTP or DHCP server. Valid IP addresses consist of four numbers, 0 to 255, separated by periods. Anything other than this format is not be accepted by the configuration program.
- An interface can have only one primary IP address, but can have many secondary IP addresses. In other words, secondary addresses need to be specified if more than one IP subnet can be accessed through this interface. Note that a secondary address cannot be configured prior to setting the primary IP address, and the primary address cannot be removed if a secondary address is still present. Also, if any router/switch in a network segment uses a secondary address, all other routers/switches in that segment must also use a secondary address from the same network or subnet address space.
- If bootp or dhcp options are selected, the system will immediately start broadcasting service requests for all VLANs configured to obtain address assignments through BOOTP or DHCP. IP is enabled but will not function until a BOOTP or DHCP reply has been received. Requests are broadcast periodically by the router in an effort to learn its IP address. (BOOTP and DHCP values can include the IP address, default gateway, and subnet mask). If the DHCP/BOOTP server is slow to respond, you may need to use the ip dhcp restart client command to re-start broadcasting service requests, or reboot the switch.

Example

In the following example, the device is assigned an address in VLAN 1.

```
Console(config)#interface vlan 1
Console(config-if)#ip add 192.168.1.5 255.255.255.0
Console(config-if)#
```

ip default-gateway

This command specifies the default gateway for destinations not found in the local routing tables. Use the no form to remove a default gateway.

Syntax

ip default-gateway *gateway*

no ip default-gateway

gateway - IP address of the default gateway

Default Configuration

No default gateway is established.

Command Mode

Global Configuration

User Guidelines

- A default gateway can only be successfully set when a network interface that directly connects to the gateway has been configured on the switch.
- A gateway must be defined if the management station is located in a different IP segment.

Example

The following example defines a default gateway for this device:

Console(config)#ip default-gateway 10.1.1.254

Console(config)#

show ip default-gateway

This command shows the IPv4 default gateway configured for this device.

Default Configuration

None

Command Mode

EXEC

Example

Console#show ip default-gateway

IP default gateway 10.1.0.254

Console#

show ip interface brief

This command displays the settings of an IPv4 interface.

Command Mode

EXEC

Example

Console#show ip interface brief

VLAN 1 is Administrative Up - Link Up

Address is 00-E0-00-00-00-01

Index: 1001, MTU: 1500

Address Mode is DHCP

IP Address: 192.168.0.2 Mask: 255.255.255.0

Console#

show ip traffic

This command displays statistics for IP, ICMP, UDP, TCP and ARP protocols.

Command Mode

EXEC

Example

Console#show ip traffic

IP Statistics:

IP received

7845 total received

header errors

unknown protocols

address errors

discards

7845 delivers

reassembly request datagrams

reassembly succeeded

reassembly failed

IP sent

forwards datagrams

9903 requests

discards

no routes

generated fragments

fragment succeeded

fragment failed

ICMP Statistics:

ICMP received

input

errors

destination unreachable messages

time exceeded messages

parameter problem message

echo request messages

echo reply messages

redirect messages

timestamp request messages

timestamp reply messages

source quench messages

address mask request messages

address mask reply messages

ICMP sent

output

errors

destination unreachable messages

time exceeded messages

parameter problem message

echo request messages

echo reply messages
redirect messages
timestamp request messages
timestamp reply messages
source quench messages
address mask request messages
address mask reply messages
UDP Statistics:
input
no port errors
other errors
output
TCP Statistics:
7841 input
input errors
9897 output
Console#

traceroute ip

This command shows the route packets take to the specified destination.

Syntax

traceroute ip *host*

host - IP address or alias of the host.

Default Configuration

None

Command Mode

EXEC

User Guidelines

- Use the traceroute ip command to determine the path taken to reach a specified destination.
- A trace terminates when the destination responds, when the maximum time out (TTL) is exceeded, or the maximum number of hops is exceeded.
- The traceroute command first sends probe datagrams with the TTL value set at one. This causes the first router to discard the datagram and return an error message. The trace function then sends several probe messages at each subsequent TTL level and displays the roundtrip time for each message. Not all devices respond correctly to probes by returning an "ICMP port unreachable" message. If the timer goes off before a response is returned, the trace function prints a series of asterisks and the "Request Timed Out" message. A long sequence of these messages, terminating only when the maximum time out has been reached, may indicate this problem with the target device.
- If the target device does not respond or other errors are detected, the switch will indicate this by one of the following messages:

a. - No Response
b. H - Host Unreachable
c. N - Network Unreachable
d. P - Protocol Unreachable
e. –Other

Example

Console#traceroute ip 192.168.0.1

Press "ESC" to abort.

Traceroute to 192.168.0.99, 30 hops max, timeout is 3 seconds

Hop Packet 1 Packet 2 Packet 3 IP Address

--- -------- -------- -------- ---------------

1 20 ms <10 ms <10 ms 192.168.0.99

Trace completed.

Console#

ping ip

This command sends (IPv4) ICMP echo request packets to another node on the network.

Syntax

ping ip *host* [count *count*] [size *size*]

host - IP address or alias of the host.

count - Number of packets to send. (Range: 1-16)

size - Number of bytes in a packet. (Range: 32-512) The actual packet size will be eight bytes larger than the size specified because the router adds header information.

Default Configuration

count: 5

size: 32 bytes

Command Mode

Normal Exec, EXEC

User Guidelines

- Use the ping ip command to see if another site on the network can be reached.
- The following are some results of the ping ip command:

a. *Normal response* - The normal response occurs in one to ten seconds, depending on network traffic.

b. *Destination does not respond* - If the host does not respond, a "timeout" appears in ten seconds.

c. *Destination unreachable* - The gateway for this destination indicates that the destination is unreachable.

d. *Network or host unreachable* - The gateway found no corresponding entry in the route table.

- When pinging a host name, be sure the DNS server has been defined and host name-to-address translation enabled. If necessary, local devices can also be specified in the DNS static host table.

Example

Console#ping ip 10.1.0.9

Type ESC to abort.

PING to 10.1.0.9, by 5 32-byte payload ICMP packets, timeout is 5 seconds

response time: 10 ms

response time: 10 ms

response time: 10 ms

response time: 10 ms

response time: 0 ms

Ping statistics for 10.1.0.9:

5 packets transmitted, 5 packets received (100%), 0 packets lost (0%)

Approximate round trip times:

Minimum = 0 ms, Maximum = 10 ms, Average = 8 ms

Console#

arp

This command adds a static entry in the Address Resolution Protocol (ARP) cache. Use the no form to remove an entry from the cache.

Syntax

arp *ip-address hardware-address*

no arp *ip-address*

ip-address - IP address to map to a specified hardware address.

hardware-address - Hardware address to map to a specified IP address. (The format for this address is xx-xx-xx-xx-xx-xx.)

Default Configuration

No default entries

Command Mode

Global Configuration

User Guidelines

- The ARP cache is used to map 32-bit IP addresses into 48-bit hardware (i.e., Media Access Control) addresses. This cache includes entries for hosts and other routers on local network interfaces defined on this router.
- The maximum number of static entries allowed in the ARP cache is 128.
- A static entry may need to be used if there is no response to an ARP broadcast message. For example, some applications may not respond to ARP requests or the response arrives too late, causing network operations to time out.
- Static entries will not be aged out nor deleted when power is reset. A static entry can only be removed through the configuration interface.

Example

Console(config)#arp 10.1.0.19 01-02-03-04-05-06

Console(config)#

arp timeout

This command sets the aging time for dynamic entries in the Address Resolution Protocol (ARP) cache. Use the no form to restore the default timeout.

Syntax

arp timeout *seconds*

no arp timeout

seconds - The time a dynamic entry remains in the ARP cache. (Range: 300-86400; 86400 seconds is one day)

Default Configuration

1200 seconds (20 minutes)

Command Mode

Global Configuration

User Guidelines

- When an ARP entry expires, it is deleted from the cache and an ARP request packet is sent to re-establish the MAC address.
- The aging time determines how long dynamic entries remain in the cache. If the timeout is too short, the switch may tie up resources by repeating ARP requests for addresses recently flushed from the table.

Example

This example sets the ARP cache timeout for 15 minutes (i.e., 900 seconds).

Console(config)#arp timeout 900

Console(config)#

clear arp-cache

This command deletes all dynamic entries from the Address Resolution Protocol (ARP) cache.

Command Mode

EXEC

Example

This example clears all dynamic entries in the ARP cache.

Console#clear arp-cache

This operation will delete all the dynamic entries in ARP Cache.

Are you sure to continue this operation (y/n)?y

Console#

show arp

This command displays entries in the Address Resolution Protocol (ARP) cache.

Command Mode

Normal Exec, EXEC

User Guidelines

This command displays information about the ARP cache. The first line shows the cache timeout. It also shows each cache entry, including the IP address, MAC address, type (dynamic, other), and VLAN interface. Note that entry type "other" indicates local addresses for this router.

Example

This example displays all entries in the ARP cache.

Console#show arp

ARP Cache Timeout: 1200 (seconds)

IP Address MAC Address Type Interface

---------- ----------- --------- ----------

10.1.0.0 FF-FF-FF-FF-FF-FF other VLAN1

10.1.0.254 64-9D-99-CD-00-00 other VLAN1

10.1.0.255 FF-FF-FF-FF-FF-FF other VLAN1

145.30.20.23 64-9D-99-30-20-10 dynamic VLAN3

Total entry: 4

Console#

52.2 IPV6 Interface

ipv6 default-gateway

This command sets an IPv6 default gateway to use when the destination is located in a different network segment. Use the no form to remove a previously configured default gateway.

Syntax

ipv6 default-gateway *ipv6-address*

no ipv6 default-gateway

ipv6-address - The IPv6 address of the default next hop router to use when the destination is located in a different network segment.

Default Configuration

No default gateway is defined

Command Mode

Global Configuration

User Guidelines

- All IPv6 addresses must be according to RFC 2373 "IPv6 Addressing Architecture," using 8 colon-separated 16-bit hexadecimal values. One double colon may be used in the address to indicate the appropriate number of zeros required to fill the undefined fields.
- The same link-local address may be used by different interfaces/nodes in different zones (RFC 4007). Therefore, when specifying a link-local address, include zone-id information indicating the VLAN identifier after the % delimiter. For example, FE80::7272%1 identifies VLAN 1 as the interface.
- An IPv6 default gateway must be defined if the destination has been assigned an IPv6 address and is located in a different IP segment.
- An IPv6 default gateway can only be successfully set when a network interface that directly connects to the gateway has been configured on the switch.

Example

The following example defines a default gateway for this device:

Console(config)#ipv6 default-gateway FE80::269:3EF9:FE19:6780%1

Console(config)#

ipv6 add

This command configures an IPv6 global unicast address and enables IPv6 on an interface. Use the no form without any arguments to remove all IPv6 addresses from the interface, or use the no form with a specific IPv6 address to remove that address from the interface.

Syntax

[no] ipv6 add *ipv6-address*[/*prefix-length*]

ipv6-address - A full IPv6 address including the network prefix and host address bits.

prefix-length - A decimal value indicating how many contiguous bits (from the left) of the address comprise the prefix (i.e., the network portion of the address).

Default Configuration

No IPv6 addresses are defined

Command Mode

Interface Configuration (VLAN)

User Guidelines

- All IPv6 addresses must be according to RFC 2373 "IPv6 Addressing Architecture," using 8 colon-separated 16-bit hexadecimal values. One double colon may be used in the address to indicate the appropriate number of zeros required to fill the undefined fields.
- To connect to a larger network with multiple subnets, you must configure a global unicast address. This address can be manually configured with this command, or it can be automatically configured using the ip ipv6 add autoconfig command.
- If a link-local address has not yet been assigned to this interface, this command will assign the specified static global unicast address and also dynamically generate a link-local unicast address for the interface. (The link-local address is made with an address prefix of FE80 and a host portion based the switch's MAC address in modified EUI-64 format.)
- If a duplicate address is detected, a warning message is sent to the console.

Example

This example specifies a full IPv6 address and prefix length.

```
Console(config)#interface vlan 1
Console(config-if)#ipv6 add 2001:DB8:2222:7272::72/96
Console(config-if)#end
Console#show ipv6 interface
VLAN 1 is up
IPv6 is enabled
Link-local address:
FE80::2E0:CFF:FE00:FD/64
Global unicast address(es):
2001:DB8:2222:7272::72/96, subnet is 2001:DB8:2222:7272::/96
Joined group address(es):
FF02::1:FF00:72
FF02::1:FF00:FD
FF02::1
IPv6 link MTU is 1500 bytes
ND DAD is enabled, number of DAD attempts: 3.
ND retransmit interval is 1000 milliseconds
ND advertised retransmit interval is 0 milliseconds
ND reachable time is 30000 milliseconds
ND advertised reachable time is 0 milliseconds
Console#
```

ipv6 add eui-64

This command configures an IPv6 address for an interface using an EUI-64 interface ID in the low order 64 bits and enables IPv6 on the interface. Use the no form without any arguments to remove all manually configured IPv6 addresses from the interface. Use the no form with a specific address to remove it from the interface.

Syntax

ipv6 add *ipv6-prefix*/*prefix-length* eui-64

no ipv6 add [*ipv6-prefix*/*prefix-length* eui-64]

ipv6-prefix - The IPv6 network portion of the address assigned to the interface.

prefix-length - A decimal value indicating how many contiguous bits (from the left) of the address comprise the prefix (i.e., the network portion of the address).

Default Configuration

No IPv6 addresses are defined

Command Mode

Interface Configuration (VLAN)

User Guidelines

- The prefix must be formatted according to RFC 2373 "IPv6 Addressing Architecture," using 8 colon-separated 16-bit hexadecimal values. One double colon may be used in the address to indicate the appropriate number of zeros required to fill the undefined fields.
- If a link local address has not yet been assigned to this interface, this command will dynamically generate a global unicast address and a linklocal address for this interface. (The link-local address is made with an address prefix of FE80 and a host portion based the switch's MAC address in modified EUI-64 format.)

- Note that the value specified in the ipv6-prefix may include some of the high-order host bits if the specified prefix length is less than 64 bits. If the specified prefix length exceeds 64 bits, then the network portion of the address will take precedence over the interface identifier.
- If a duplicate address is detected, a warning message is sent to the console.
- IPv6 addresses are 16 bytes long, of which the bottom 8 bytes typically form a unique host identifier based on the device's MAC address. The EUI-64 specification is designed for devices that use an extended 8-byte MAC address. For devices that still use a 6-byte MAC address (also known as EUI-48 format), it must be converted into EUI-64 format by inverting the universal/local bit in the address and inserting the hexadecimal number FFFE between the upper and lower three bytes of the MAC address.
- For example, if a device had an EUI-48 address of 28-9F-18-1C-82-35, the global/local bit must first be inverted to meet EUI-64 requirements (i.e., 1 for globally defined addresses and 0 for locally defined addresses), changing 28 to 2A. Then the two bytes FFFE are inserted between the OUI (i.e., company id) and the rest of the address, resulting in a modified EUI-64 interface identifier of 2A-9F-18-FF-FE-1C-82-35.
- This host addressing method allows the same interface identifier to be used on multiple IP interfaces of a single device, as long as those interfaces are attached to different subnets.

Example

This example uses the network prefix of 2001:0DB8:0:1::/64, and specifies that the EUI-64 interface identifier be used in the lower 64 bits of the address.

```
Console(config)#interface vlan 1
Console(config-if)#ipv6 add 2001:0DB8:0:1::/64 eui-64
Console(config-if)#end
Console#show ipv6 interface
VLAN 1 is up
IPv6 is enabled
Link-local address:
FE80::2E0:CFF:FE00:FD/64
Global unicast address(es):
2001:DB8::1:2E0:CFF:FE00:FD/64, subnet is 2001:DB8::1:0:0:0:0/64[EUI]
2001:DB8:2222:7272::72/96, subnet is 2001:DB8:2222:7272::/96[EUI]
Joined group address(es):
FF02::1:FF00:72
FF02::1:FF00:FD
FF02::1
IPv6 link MTU is 1500 bytes
ND DAD is enabled, number of DAD attempts: 3.
ND retransmit interval is 1000 milliseconds
ND advertised retransmit interval is 0 milliseconds
ND reachable time is 30000 milliseconds
ND advertised reachable time is 0 milliseconds
Console#
```

ipv6 add link-local

This command configures an IPv6 link-local address for an interface and enables IPv6 on the interface. Use the no form without any arguments to remove all manually configured IPv6 addresses from the interface. Use the no form with a specific address to remove it from the interface.

Syntax

ipv6 add *ipv6-address* link-local

no ipv6 add [*ipv6-address* link-local]

ipv6-address - The IPv6 address assigned to the interface.

Default Configuration

No IPv6 addresses are defined

Command Mode

Interface Configuration (VLAN)

User Guidelines

- The specified address must be formatted according to RFC 2373 "IPv6 Addressing Architecture," using 8 colon-separated 16-bit hexadecimal values. One double colon may be used in the address to indicate the appropriate number of zeros required to fill the undefined fields. And the address prefix must be in the range of FE80~FEBF.
- The address specified with this command replaces a link-local address that was automatically generated for the interface.
- You can configure multiple IPv6 global unicast addresses per interface, but only one link-local address per interface.
- If a duplicate address is detected, a warning message is sent to the console.

Example

This example assigns a link-local address of FE80::269:3EF9:FE19:6779 to VLAN 1. Note that the prefix in the range of FE80~FEBF is required for linklocal addresses, and the first 16-bit group in the host address is padded with a zero in the form 0269.

Console(config)#interface vlan 1

Console(config-if)#ipv6 add FE80::269:3EF9:FE19:6779 link-local

Console(config-if)#end

Console#show ipv6 interface

VLAN 1 is up

IPv6 is enabled

Link-local address:

FE80::269:3EF9:FE19:6779/64

Global unicast address(es):

2001:DB8::1:2E0:CFF:FE00:FD/64, subnet is 2001:DB8::1:0:0:0:0/64[EUI]

2001:DB8:2222:7272::72/96, subnet is 2001:DB8:2222:7272::/96[EUI]

Joined group address(es):

FF02::1:FF19:6779

FF02::1:FF00:72

FF02::1:FF00:FD

FF02::1

IPv6 link MTU is 1500 bytes

ND DAD is enabled, number of DAD attempts: 3.

ND retransmit interval is 1000 milliseconds

ND advertised retransmit interval is 0 milliseconds

ND reachable time is 30000 milliseconds

ND advertised reachable time is 0 milliseconds

Console#

ipv6 enable

This command enables IPv6 on an interface that has not been configured with an explicit IPv6 address. Use the no form to disable IPv6 on an interface that has not been configured with an explicit IPv6 address.

Syntax

[no] ipv6 enable

Default Configuration

IPv6 is disabled

Command Mode

Interface Configuration (VLAN)

User Guidelines

This command enables IPv6 on the current VLAN interface and automatically generates a link-local unicast address. The address prefix uses FE80, and the host portion of the address is generated by converting the switch's MAC address to modified EUI-64 format. This address type makes the switch accessible over IPv6 for all devices attached to the same local subnet.

- If a duplicate address is detected on the local segment, this interface will be disabled and a warning message displayed on the console.
- The no ipv6 enable command does not disable IPv6 for an interface that has been explicitly configured with an IPv6 address.

Example

In this example, IPv6 is enabled on VLAN 1, and the link-local address FE80::2E0:CFF:FE00:FD/64 is automatically generated by the switch.

Console(config)#interface vlan 1

Console(config-if)#ipv6 enable

Console(config-if)#end

Console#show ipv6 interface

VLAN 1 is up

IPv6 is enabled

Link-local address:

FE80::2E0:CFF:FE00:FD/64

Global unicast address(es):

2001:DB8:2222:7273::72/96, subnet is 2001:DB8:2222:7273::/96

Joined group address(es):

FF02::1:FF00:72

FF02::1:FF00:FD

FF02::1

IPv6 link MTU is 1280 bytes

ND DAD is enabled, number of DAD attempts: 3.

ND retransmit interval is 1000 milliseconds

ND advertised retransmit interval is 0 milliseconds

ND reachable time is 30000 milliseconds

ND advertised reachable time is 0 milliseconds

Console#

ipv6 mtu

This command sets the size of the maximum transmission unit (MTU) for IPv6 packets sent on an interface. Use the no form to restore the default setting.

Syntax

ipv6 mtu *size*

no ipv6 mtu

size - Specifies the MTU size. (Range: 1280-65535 bytes)

Default Configuration

1500 bytes

Command Mode

Interface Configuration (VLAN)

User Guidelines

- The maximum value set by this command cannot exceed the MTU of the physical interface, which is currently fixed at 1500 bytes.
- IPv6 routers do not fragment IPv6 packets forwarded from other routers. However, traffic originating from an end-station connected to an IPv6 router may be fragmented.
- All devices on the same physical medium must use the same MTU in order to operate correctly.
- IPv6 must be enabled on an interface before the MTU can be set.

Example

The following example sets the MTU for VLAN 1 to 1280 bytes:

Console(config)#interface vlan 1

Console(config-if)#ipv6 mtu 1280

Console(config-if)#

show ipv6 default-gateway

This command displays the current IPv6 default gateway.

Command Mode

Normal Exec, EXEC

Example

The following shows the default gateway configured for this device:

Console#show ipv6 default-gateway

IPv6 default gateway 2001:DB8:2222:7272::254

Console#

show ipv6 interface

This command displays the usability and configured settings for IPv6 interfaces.

Syntax

show ipv6 interface [brief [vlan *vlan-id* [*ipv6-prefix*/*prefix-length*]]]

brief - Displays a brief summary of IPv6 operational status and the addresses configured for each interface.

vlan-id - VLAN ID (Range: 1-4094)

ipv6-prefix - The IPv6 network portion of the address assigned to the interface. The prefix must be formatted according to RFC 2373 "IPv6 Addressing Architecture," using 8 colon-separated 16-bit hexadecimal values. One double colon may be used in the address to indicate the appropriate number of zeros required to fill the undefined fields.

prefix-length - A decimal value indicating how many of the contiguous bits (from the left) of the address comprise the prefix (i.e., the network portion of the address).

Command Mode

Normal Exec, EXEC

Example

This example displays all the IPv6 addresses configured for the switch.

```
Console#show ipv6 interface
VLAN 1 is up
IPv6 is enabled
Link-local address:
FE80::2E0:CFF:FE00:FD/64
Global unicast address(es):
2001:DB8:2222:7273::72/96, subnet is 2001:DB8:2222:7273::/96
Joined group address(es):
FF02::1:FF00:72
FF02::1:FF00:FD
FF02::1
IPv6 link MTU is 1280 bytes
ND DAD is enabled, number of DAD attempts: 3.
ND retransmit interval is 1000 milliseconds
ND advertised retransmit interval is 0 milliseconds
ND reachable time is 30000 milliseconds
ND advertised reachable time is 0 milliseconds
Console#
```

show ipv6 mtu

This command displays the maximum transmission unit (MTU) cache for destinations that have returned an ICMP packet-too-big message along with an acceptable MTU to this switch.

Command Mode

Normal Exec, EXEC

Example

The following example shows the MTU cache for this device:

```
Console#show ipv6 mtu
MTU Since Destination Address
1400 00:04:21 5000:1::3
1280 00:04:50 FE80::203:A0FF:FED6:141D
Console#
```

show ipv6 traffic

This command displays statistics about IPv6 traffic passing through this switch.

Command Mode

Normal Exec, EXEC

Example

The following example shows statistics for all IPv6 unicast and multicast traffic, as well as ICMP, UDP and TCP statistics:

```
Console#show ipv6 traffic
IPv6 Statistics:
IPv6 received
total received
header errors
```

too big errors
no routes
address errors
unknown protocols
truncated packets
discards
delivers
reassembly request datagrams
reassembly succeeded
reassembly failed
IPv6 sent
forwards datagrams
requests
discards
no routes
generated fragments
fragment succeeded
fragment failed
ICMPv6 Statistics:
ICMPv6 received
input
errors
destination unreachable messages
packet too big messages
time exceeded messages
parameter problem message
echo request messages
echo reply messages
router solicit messages
router advertisement messages
neighbor solicit messages
neighbor advertisement messages
redirect messages
group membership query messages
group membership response messages
group membership reduction messages
multicast listener discovery version 2 reports
ICMPv6 sent
output
destination unreachable messages
packet too big messages
time exceeded messages
parameter problem message
echo request messages

echo reply messages
router solicit messages
router advertisement messages
neighbor solicit messages
neighbor advertisement messages
redirect messages
group membership query messages
group membership response messages
group membership reduction messages
multicast listener discovery version 2 reports
UDP Statistics:
input
no port errors
other errors
output
Console#
clear ipv6 traffic
This command resets IPv6 traffic counters.
Command Mode
EXEC
User Guidelines
This command resets all of the counters displayed by the show ipv6 traffic command.
Example
Console#clear ipv6 traffic
Console#
ping ipv6
This command sends (IPv6) ICMP echo request packets to another node on the network.
Syntax
ping ipv6 {*ipv6-address* | *host-name*} [count *count*] [size *size*]
ipv6-address - The IPv6 address of a neighbor device. You can specify either a link-local or global unicast address formatted according to RFC 2373 "IPv6 Addressing Architecture," using 8 colon-separated 16-bit hexadecimal values. One double colon may be used in the address to indicate the appropriate number of zeros required to fill the undefined fields.
host-name - A host name string which can be resolved into an IPv6 address through a domain name server.
count - Number of packets to send. (Range: 1-16)
size - Number of bytes in a packet. (Range: 48-18024 bytes) The actual packet size will be eight bytes larger than the size specified because the router adds header information.
Default Configuration
count: 5
size: 100 bytes
Command Mode
EXEC
User Guidelines

- Use the ping ipv6 command to see if another site on the network can be reached, or to evaluate delays over the path.
- The same link-local address may be used by different interfaces/nodes in different zones (RFC 4007). Therefore, when specifying a link-local address, include zone-id information indicating the VLAN identifier after the % delimiter. For example, FE80::7272%1 identifies VLAN 1 as the interface from which the ping is sent.
- When pinging a host name, be sure the DNS server has been enabled. If necessary, local devices can also be specified in the DNS static host table.
- When using ping ipv6 with a host name, the switch first attempts to resolve the alias into an IPv6 address before trying to resolve it into an IPv4 address.

Example

Console#ping ipv6 FE80::2E0:CFF:FE00:FC%1/64

Type ESC to abort.

PING to FE80::2E0:CFF:FE00:FC%1/64, by 5 32-byte payload ICMP packets,

timeout is 3 seconds

response time: 20 ms [FE80::2E0:CFF:FE00:FC] seq_no: 1

response time: 0 ms [FE80::2E0:CFF:FE00:FC] seq_no: 2

response time: 0 ms [FE80::2E0:CFF:FE00:FC] seq_no: 3

response time: 0 ms [FE80::2E0:CFF:FE00:FC] seq_no: 4

response time: 0 ms [FE80::2E0:CFF:FE00:FC] seq_no: 5

Ping statistics for FE80::2E0:CFF:FE00:FC%1/64:

5 packets transmitted, 5 packets received (100%), 0 packets lost (0%)

Approximate round trip times:

Minimum = 0 ms, Maximum = 20 ms, Average = 4 ms

Console#

traceroute ipv6

This command shows the route packets take to the specified destination.

Syntax

traceroute ipv6 {*ipv6-address* | *host-name*}

ipv6-address - The IPv6 address of a neighbor device. You can specify either a link-local or global unicast address formatted according to RFC 2373 "IPv6 Addressing Architecture," using 8 colon-separated 16-bit hexadecimal values. One double colon may be used in the address to indicate the appropriate number of zeros required to fill the undefined fields.

host-name - A host name string which can be resolved into an IPv6 address through a domain name server.

Default Configuration

None

Command Mode

EXEC

User Guidelines

- Use the traceroute ipv6 command to determine the path taken to reach a specified destination.
- The same link-local address may be used by different interfaces/nodes in different zones (RFC 4007). Therefore, when specifying a link-local address, include zone-id information indicating the VLAN identifier after the % delimiter. For example, FE80::7272%1 identifies VLAN 1 as the interface from which the ping is sent.
- A trace terminates when the destination responds, when the maximum timeout (TTL) is exceeded, or the maximum number of hops is exceeded.

- The traceroute command first sends probe datagrams with the TTL value set at one. This causes the first router to discard the datagram and return an error message. The trace function then sends several probe messages at each subsequent TTL level and displays the roundtrip time for each message. Not all devices respond correctly to probes by returning an "ICMP port unreachable" message. If the timer goes off before a response is returned, the trace function prints a series of asterisks and the "Request Timed Out" message. A long sequence of these messages, terminating only when the maximum timeout has been reached, may indicate this problem with the target device.

Example

Console#traceroute ipv6 FE80::2E0:CFF:FE9C:CA10%1/64

Press "ESC" to abort.

Traceroute to FE80::2E0:CFF:FE9C:CA10%1/64, 30 hops max, timeout is 3

seconds, 5 max failure(s) before termination.

Hop Packet 1 Packet 2 Packet 3 IPv6 Address

--- -------- -------- -------- --

1 <10 ms <10 ms <10 ms FE80::2E0:CFF:FE9C:CA10%1/64

Trace completed.

Console#

ipv6 nd dad attempts

This command configures the number of consecutive neighbor solicitation messages sent on an interface during duplicate address detection. Use the no form to restore the default setting.

Syntax

ipv6 nd dad attempts *count*

no ipv6 nd dad attempts

count - The number of neighbor solicitation messages sent to determine whether or not a duplicate address exists on this interface. (Range: 0-600)

Default Configuration

3

Command Mode

Interface Configuration (VLAN)

User Guidelines

- Configuring a value of 0 disables duplicate address detection.
- Duplicate address detection determines if a new unicast IPv6 address already exists on the network before it is assigned to an interface.
- Duplicate address detection is stopped on any interface that has been suspended (see the vlan command). While an interface is suspended, all unicast IPv6 addresses assigned to that interface are placed in a "pending" state. Duplicate address detection is automatically restarted when the interface is administratively re-activated.
- An interface that is re-activated restarts duplicate address detection for all unicast IPv6 addresses on the interface. While duplicate address detection is performed on the interface's link-local address, the other IPv6 addresses remain in a "tentative" state. If no duplicate link-local address is found, duplicate address detection is started for the remaining IPv6 addresses.
- If a duplicate address is detected, it is set to "duplicate" state, and a warning message is sent to the console. If a duplicate link-local address is detected, IPv6 processes are disabled on the interface. If a duplicate global unicast address is detected, it is not used. All configuration commands associated with a duplicate address remain configured while the address is in "duplicate" state.

- If the link-local address for an interface is changed, duplicate address detection is performed on the new link-local address, but not for any of the IPv6 global unicast addresses already associated with the interface.

Example

The following configures five neighbor solicitation attempts for addresses configured on VLAN 1. The show ipv6 interface command indicates that the duplicate address detection process is still on-going.

Console(config)#interface vlan 1
Console(config-if)#ipv6 nd dad attempts 5
Console(config-if)#end
Console#show ipv6 interface
VLAN 1 is up
IPv6 is enabled
Link-local address:
FE80::200:E8FF:FE90:0/64
Global unicast address(es):
2009:DB9:2229::79, subnet is 2009:DB9:2229:0::/64
Joined group address(es):
FF01::1/16
FF02::1/16
FF02::1:FF00:79/104
FF02::1:FF90:0/104
IPv6 link MTU is 1500 bytes.
ND DAD is enabled, number of DAD attempts: 5.
ND retransmit interval is 1000 milliseconds
ND advertised retransmit interval is 0 milliseconds
ND reachable time is 30000 milliseconds
ND advertised reachable time is 0 milliseconds
Console#

ipv6 nd ns-interval

This command configures the interval between transmitting IPv6 neighbor solicitation messages on an interface. Use the no form to restore the default value.

Syntax

ipv6 nd ns-interval *milliseconds*

no ipv6 nd ns-interval

milliseconds - The interval between transmitting IPv6 neighbor solicitation messages. (Range: 1000-3600000)

Default Configuration

1000 milliseconds is used for neighbor discovery operations

Command Mode

Interface Configuration (VLAN)

User Guidelines

- This command specifies the interval between transmitting neighbor solicitation messages when resolving an address, or when probing the reachability of a neighbor. Therefore, avoid using very short intervals for normal IPv6 operations.

Example

The following sets the interval between sending neighbor solicitation messages to 30000 milliseconds:

Console(config)#interface vlan 1
Console(config)#pv6 nd ns-interval 30000
Console(config)#end
Console#show ipv6 interface
VLAN 1 is up
IPv6 is enabled
Link-local address:
FE80::200:E8FF:FE90:0/64
Global unicast address(es):
2009:DB9:2229::79, subnet is 2009:DB9:2229:0::/64
Joined group address(es):
FF01::1/16
FF02::1/16
FF02::1:FF00:79/104
FF02::1:FF90:0/104
IPv6 link MTU is 1500 bytes.
ND DAD is enabled, number of DAD attempts: 5.
ND retransmit interval is 1000 milliseconds
ND advertised retransmit interval is 0 milliseconds
ND reachable time is 30000 milliseconds
ND advertised reachable time is 0 milliseconds
Console#

ipv6 nd raguard

This command blocks incoming Router Advertisement and Router Redirect packets. Use the no form to disable this feature.

Syntax

[no] ipv6 nd raguard

Default Configuration

Disabled

Command Mode

Interface Configuration (Ethernet, Port Channel)

User Guidelines

- IPv6 Router Advertisements (RA) convey information that enables nodes to auto-configure on the network. This information may include the default router address taken from the observed source address of the RA message, as well as on-link prefix information. However, unintended misconfigurations, or possibly malicious attacks on the network, may lead to bogus RAs being sent, which in turn can cause operational problems for hosts on the network.
- This command can be used to block RAs and Router Redirect (RR) messages on the specified interface. Determine which interfaces are connected to known routers, and enable RA Guard on all other untrusted interfaces.

Example

Console(config)#interface ethernet 1/1
Console(config-if)#pv6 nd raguard
Console(config-if)#

ipv6 nd reachable-time

This command configures the amount of time that a remote IPv6 node is considered reachable after some reachability confirmation event has occurred.

Syntax

ipv6 nd reachable-time *milliseconds*

no ipv6 nd reachable-time

milliseconds - The time that a node can be considered reachable after receiving confirmation of reachability. (Range: 0-3600000)

Default Configuration

30000 milliseconds is used for neighbor discovery operations

Command Mode

Interface Configuration (VLAN)

User Guidelines

- The time limit configured by this command allows the switch to detect unavailable neighbors.

Example

The following sets the reachable time for a remote node to 1000 milliseconds:

Console(config)#interface vlan 1

Console(config)#pv6 nd reachable-time 1000

Console(config)#

clear ipv6 neighbors

This command deletes all dynamic entries in the IPv6 neighbor discovery cache.

Command Mode

EXEC

Example

The following deletes all dynamic entries in the IPv6 neighbor cache:

Console#clear ipv6 neighbors

Console#

show ipv6 nd raguard

This command displays the configuration setting for RA Guard.

Syntax

show ipv6 nd raguard [*interface*]

interface

ethernet *unit*/*port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-28)

port-channel *channel-id* (Range: 1-12)

Command Mode

EXEC

Example

Console#show ipv6 nd raguard interface ethernet 1/1

Interface RA Guard

--------- --------

Eth 1/ 1 Yes

Console#

show ipv6 neighbors

This command displays information in the IPv6 neighbor discovery cache.

Syntax

show ipv6 neighbors [vlan *vlan-id* | *ipv6-address*]

vlan-id - VLAN ID (Range: 1-4094)

ipv6-address - The IPv6 address of a neighbor device. You can specify either a link-local or global unicast address formatted according to RFC 2373 "IPv6 Addressing Architecture," using 8 colon-separated 16-bit hexadecimal values. One double colon may be used in the address to indicate the appropriate number of zeros required to fill the undefined fields.

Default Configuration

All IPv6 neighbor discovery cache entries are displayed.

Command Mode

EXEC

Example

The following shows all known IPv6 neighbors for this switch:

Console#show ipv6 neighbors

State: I1 - Incomplete, I2 - Invalid, R - Reachable, S - Stale, D - Delay,

P1 - Probe, P2 - Permanent, U - Unknown

IPv6 Address Age Link-layer Addr State VLAN

FE80::2E0:CFF:FE9C:CA10 4 00-E0-0C-9C-CA-10 R 1

Console#

53. IP Routing Commands

53.1 IPV4 Interface

ip route

This command configures static routes. Use the no form to remove static routes.

Syntax

ip route *destination-ip netmask next-hop* [*distance*]

no ip route {*destination-ip netmask next-hop* | *}

destination-ip – IP address of the destination network, subnetwork, or host.

netmask - Network mask for the associated IP subnet. This mask identifies the host address bits used for routing to specific subnets.

next-hop – IP address of the next hop router used for this route.

distance – An administrative distance indicating that this route can be overridden by dynamic routing information if the distance of the dynamic route is less than that configured for the static route. Note that the default administrative distances used by the dynamic unicast routing protocols is 110 for OSPF, 120 for RIP, 20 for eBGP, and 200 for iBGP. (Range: 1-255, Default: 1)

* – Removes all static routing table entries.

Default Configuration

No static routes are configured.

Command Mode

Global Configuration

User Guidelines

If both static and dynamic paths have the same lowest cost, the first route stored in the routing table, either statically configured or dynamically learned via a routing protocol, will be used.

Example

This example forwards all traffic for subnet 192.168.1.0 to the gateway router

192.168.5.254, using the default metric of 1.

Console(config)#ip route 192.168.1.0 255.255.255.0 192.168.5.254

Console(config)#

show ip route

This command displays information in the Forwarding Information Base (FIB).

Syntax

show ip route [connected | database | static | summary]

connected – Displays all currently connected entries.

database – All known routes, including inactive routes.

static – Displays all static entries.

summary – Displays a brief list of summary information about entries in the routing table, including the maximum number of entries supported, the number of connected routes, the total number of routes currently stored in the routing table, and the number of entries in the FIB.

Command Mode

EXEC

User Guidelines

- The FIB contains information required to forward IP traffic. It contains the interface identifier and next hop information for each reachable destination network prefix based on the IP routing table. When routing or topology changes occur in the network, the routing table is updated, and those changes are immediately reflected in the FIB.
- The FIB is distinct from the routing table (or, Routing Information Base), which holds all routing information received from routing peers. The forwarding information base contains unique paths only. It does not contain any secondary paths. A FIB entry consists of the minimum amount of information necessary to make a forwarding decision on a particular packet. The typical components within a forwarding information base entry are a network prefix, a router port identifier, and next hop information.
- This command only displays routes which are currently accessible for forwarding. The router must be able to directly reach the next hop, so the VLAN interface associated with any dynamic or static route entry must be up. Note that routes currently not accessible for forwarding, may still be displayed.

Example

In the following example, note that the entry for RIP displays both the distance and

metric for this route.

```
Console#show ip route
Codes: C - connected, S - static, R - RIP, B - BGP
O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default
R 10.1.1.0/24 [120/2] via 192.168.1.10, VLAN1, 00:00:14
C 127.0.0.0/8 is directly connected, lo
C 192.168.1.0/24 is directly connected, VLAN1
Console#
```

53.2 IPV6 Interface

ipv6 route

This command configures static IPv6 routes. Use the no form to remove static routes.

Syntax

[no] ipv6 route *destination-ipv6-address*/*prefix-length*

{*gateway-address* [*distance*] | *link-local-address%zone-id* [*distance*]}

destination-ipv6-address – The IPv6 address of a destination network, subnetwork, or host. This must be a full IPv6 address including the network prefix and host address bits.

prefix-length - A decimal value indicating how many contiguous bits (from the left) of the address comprise the prefix (i.e., the network portion of the

address).

gateway-address – IP address of the next hop router used for this route.

link-local-address%zone-id – a link-local address, including a zone-id indicating the VLAN identifier after the % delimiter.

distance – An administrative distance indicating that this route can be overridden by dynamic routing information if the distance of the dynamic route is less than that configured for the static route. Note that the default administrative

distances used by the dynamic unicast routing protocols is 110 for OSPF, 120 for RIP, 20 for eBGP, and 200 for iBGP. (Range: 1-255, Default: 1)

Default Configuration

No static routes are configured.

Command Mode

Global Configuration

User Guidelines

If both static and dynamic paths have the same lowest cost, the first route stored in the routing table, either statically configured or dynamically learned via a routing protocol, will be used.

Example

This example forwards all traffic for subnet 2001::/64 to the next hop router 2001:DB8:2222:7272::254, using the default metric of 1.

Console(config)#ipv6 route 2001::/64 2001:DB8:2222:7272::254

Console(config)#

show ipv6 route

This command displays information in the Forwarding Information Base (FIB).

Syntax

show ipv6 route [*ipv6-address*[/*prefix-length*] database | interface [vlan *vlan-id*] | local | ospf | static]

ipv6-address - A full IPv6 address including the network prefix and host address bits.

prefix-length - A decimal value indicating how many contiguous bits (from the left) of the address comprise the prefix (i.e., the network portion of the address).

database – All known routes, including inactive routes.

interface – Displays all routes that be accessed through this interface.

local – Displays all entries for destinations attached directly to this router.

ospf – Displays external routes imported from the Open Shortest Path First (OSPF) protocol into this routing domain.

static – Displays all static entries.

vlan-id - VLAN ID. (Range: 1-4094)

Command Mode

EXEC

User Guidelines

- The FIB contains information required to forward IP traffic. It contains the interface identifier and next hop information for each reachable destination network prefix based on the IP routing table. When routing or topology changes occur in the network, the routing table is updated, and those changes are immediately reflected in the FIB.
- The FIB is distinct from the routing table (or, Routing Information Base), which holds all routing information received from routing peers. The forwarding information base contains unique paths only. It does not contain any secondary paths. A FIB entry consists of the minimum amount of information necessary to make a forwarding decision on a particular packet. The typical components within a forwarding information base entry are a network prefix, a router port identifier, and next hop information.
- This command only displays routes which are currently accessible for forwarding. The router must be able to directly reach the next hop, so the VLAN interface associated with any dynamic or static route entry must be up.

Example

In the following example, note that the last entry displays both the distance and

metric for this route.

```
Console#show ipv6 route
Codes: C - connected, S - static, R - RIP, B - BGP
O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
C ::1/128, lo0
? FE80::/64, VLAN1 inactive
C FE80::/64, VLAN1
? FF00::/8, VLAN1 inactive
O IA 3FFF:1::/32 [110/3]
via FE80::204:FF:FE05:6, VLAN1
Console#
```

54. Stacking

stacking all renumber

This command resets the switch unit identification numbers in the stack. All stack members are numbered sequentially starting from the top unit for a non-loop stack, or starting from the Master unit for a looped stack.

Syntax

stacking all renumber

Default Configuration

The master unit is unit 1.

Command Mode

Global Configuration

User Guidelines

The system will restart after renumbering is completed.

Example

This example shows how to renumber all units.

Console(config)#stacking all renumber

Console(config)#

stacking master

This command configures a unit as the stack master. Use the no form to disable the master button.

Syntax

[no] stacking master *unit*

unit - Unit identifier. (Range: 1-6)

Default Configuration

Disabled

Command Mode

Global Configuration

User Guidelines

- The switch must be rebooted to activate this command. Note that the configured setting is not affected by changes to the start-up configuration file.
- Set the front panel 10G ports to stacking mode with the stacking enable command prior to rebooting the switch.
- If the stack has not been initialized, the master button must be disabled on all other units in the stack, and those units rebooted.
- If the stack has been initialized, and this command used to configure a new stack master, then the master button on the old master must be disabled before rebooting the stack.
- After the newly configured stack master has been rebooted, the front panel unit identifier will the updated on each unit in the stack.
- The boo-tup messages on all slave units will be halted when the master unit is rebooted, and configuration through the CLI will be restricted to the master unit.

Example

This example shows the current switch set to stack master, the switch rebooted,

and the messages displayed after the reboot process completes.

Console(config)#stacking master 1

Console#reload

...

stacking enable

This command sets the front panel 10G ports to stacking mode. Use the no form to disable this function.

Syntax

[no] stacking enable *unit*

unit - Unit identifier. (Range: 1-6)

Default Configuration

Disabled

Command Mode

Global Configuration

User Guidelines

- Use this command on all stack members.
- Use the stacking master command to specify one unit as the stack master.
- Every switch in the stack must be rebooted to activate this command. Note that the configured setting is not affected by changes to the start-up configuration file.

Example

Console(config)#stacking enable 1

Console#

show stacking master

This command shows the status of the master button.

Command Mode

EXEC

User Guidelines

- If the stack has not been initialized, "N" will be displayed in the switch ID field.
- Use the stacking master command to specify one unit as the stack master.

Example

Console#show stacking master

Switch ID Master

--------- ----------

1 Y

2 N

Console#

show stacking status

This command shows the status of the stacking button.

Command Mode

EXEC

User Guidelines

Use the stacking enable command to set the 10G ports to stacking mode.

Example

Console#show stacking status

Switch ID Config Status Active Status

--------- ---------- ----------

1 N N

Console#

https://www.fs.com