Dell PowerConnect 5500 Series

CLI Reference Guide

Regulatory Model: PC5524, PC5524P, PC5548 and PC5548P

Notes, Cautions, and Warnings

NOTE: A NOTE indicates important information that helps you make better use of your computer.

CAUTION: A CAUTION indicates potential damage to hardware or loss of data if instructions are not followed.

WARNING: A WARNING indicates a potential for property damage, personal injury, or death.

Regulatory Models: PC5524, PC5524P, PC5548 and PC5548P

May 2012 Rev. A03

Contents

1

Preface

About this Document

This CLI Reference Guide describes how to use the CLI and a list of the CLI commands and their arguments.

The CLI commands described in this document are organized according to feature groups in separate sections.

This section describes how to use the CLI. It contains the following topics:

- CLI Command Modes
- Starting the CLI
- CLI Command Conventions
- Entering Commands

CLI Command Modes

To configure devices, the CLI is divided into various command modes. Each command mode has its own set of specific commands. Entering a question mark "?" at the console prompt displays a list of commands available for that particular command mode.

A specific command, which varies from mode to mode, is used to navigate from one mode to another. The standard order to access the modes is as follows: *User EXEC* mode, *Privileged EXEC* mode, *Global Configuration* mode, and *Interface Configuration* modes.

When starting a session, the initial mode for non-privileged users is the User EXEC mode. Only a limited subset of commands is available in the User EXEC mode. This level is reserved for tasks that do not change the configuration.

Privileged users enter the Privileged EXEC mode directly using a password. This mode provides access to the device Configuration modes.

The modes are described below.

User EXEC Mode

After logging into the device, the user is automatically in *User EXEC* command mode unless the user is defined as a privileged user. In general, the *User EXEC* commands enable the user to perform basic tests, and display system information.

The user-level prompt consists of the device "host name" followed by the angle bracket (>).

```
console>
```

The default host name is "console" unless it has been changed using the **hostname** command in the *Global Configuration* mode.

Privileged EXEC Mode

Privileged access is password-protected to prevent unauthorized use, because many of the privileged commands set operating system parameters: The password is not displayed on the screen and is case sensitive.

Privileged users enter directly into the *Privileged EXEC* mode.

Use **disable** to return to the *User EXEC* mode.

Global Configuration Mode

Global Configuration mode commands apply to features that affect the system as a whole, rather than just a specific interface.

To enter the *Global Configuration* mode, enter **configure** in the Privileged EXEC mode, and press <Enter>.

The *Global Configuration* mode prompt is displayed.

```
console(config)#
```

Use **exit**, **end** or **ctrl/z** to return to the Privileged EXEC mode.

Interface Configuration Modes

Commands in the following modes perform specific interface operations:

- **Line Interface** — Contains commands to configure the management connections. These include commands such as line speed, timeout settings, etc. The *Global Configuration* mode command **line** is used to enter the *Line Configuration command* mode.
- **VLAN Database** — Contains commands to create a VLAN as a whole. The Global Configuration mode command **vlan database** is used to enter the *VLAN Database Interface Configuration* mode.
- **Management Access List** — Contains commands to define management access-lists. The *Global Configuration* mode command management access-list is used to enter the *Management Access List Configuration* mode.
- **Port Channel** — Contains commands to configure port-channels, for example, assigning ports to a VLAN or port-channel. The *Global Configuration* mode command interface **port-channel** is used to enter the *Port Channel Interface Configuration* mode.
- **SSH Public Key-Chain** — Contains commands to manually specify other device SSH public keys. The *Global Configuration* mode command crypto key pubkey-chain **ssh** is used to enter the *SSH Public Key-chain Configuration* mode.
- **Interface** — Contains commands that configure the interface. The *Global Configuration* mode command **interface** is used to enter the *Interface Configuration* mode.

Starting the CLI

The switch can be managed over a direct connection to the switch console port, or via a Telnet connection. The switch is managed by entering command keywords and parameters at the prompt. Using the switch CLI commands is similar to entering commands on a UNIX system.

If access is via a Telnet connection, ensure the device has an IP address defined, corresponding management access is granted, and the workstation used to access the device is connected to the device prior to using CLI commands.

Accessing the CLI from the Console Line

1. Start the device and wait until the startup procedure is complete. The User Exec mode is entered, and the prompt "console>" is displayed.

2. Configure the device and enter the necessary commands to complete the required tasks.
3. When finished, exit the session with the **quit** or **exit** command.

Accessing the CLI from Telnet

1. Enter **telnet** and the IP address of the device. A User Name prompt is displayed.
2. Enter the User Name and Password. You are in the Privileged Exec mode.
3. Configure the device and enter the necessary commands to complete the required tasks.
4. When finished, exit the session with the quit or exit command.

When another user is required to log onto the system, the **login** command is entered in the Privileged EXEC command mode,. This effectively logs off the current user and logs on the new user.

CLI Command Conventions

The following table describes the command syntax conventions.

[ ]	In a command line, square brackets indicates an optional entry.
{ }	In a command line, curly brackets indicate a selection of compulsory parameters separated by the | character. One option must be selected. For example: **flowcontrol {auto|on|off}** means that for the **flowcontrol** command either **auto**, **on** or **off** must be selected.
Italic font	Indicates a parameter.
<Enter>	Any individual key on the keyboard. For example click **<Enter>**.
Ctrl+F4	Any combination keys pressed simultaneously on the keyboard.

Screen Display	Indicates system messages and prompts appearing on the console.
all	When a parameter is required to define a range of ports or parameters and **all** is an option, the default for the command is **all** when no parameters are defined. For example, the command **interface range port-channel** has the option of either entering a range of channels, or selecting **all**. When the command is entered without a parameter, it automatically defaults to **all**.

Entering Commands

A CLI command is a series of keywords and arguments. Keywords identify a command, and arguments specify configuration parameters. For example, in the command "**show interfaces status gi1/0/5**" **show**, **interfaces** and **status** are keywords, **gi** is an argument that specifies the interface type, and **1/0/5** is an argument that specifies the port.

To enter commands that require parameters, enter the required parameters after the command keyword. For example, to set a password for the administrator, enter:

```
console(config)# username admin password smith
```

Help information can be displayed in the following ways:

- **Keyword Lookup** — The character ? is entered in place of a command. A list of all valid commands and corresponding help messages are displayed.
- **Partial Keyword Lookup** — A command is incomplete and the character ? is entered in place of a parameter. The matched parameters for this command are displayed.

The following describes features that assist in using the CLI:

Terminal Command Buffer

Every time a command is entered in the CLI, it is recorded on an internally managed Command History buffer. Commands stored in the buffer are maintained on a First In First Out (FIFO) basis.These commands can be

recalled, reviewed, modified, and reissued. This buffer is not preserved across device resets. The keys that can be used to access the history buffer are described in Table 1.

By default, the history buffer system is enabled, but it can be disabled at any time. For information about the command syntax to enable or disable the history buffer, see the **history** command.

There is a standard default number of commands that are stored in the buffer. The standard number of 10 commands can be increased to 256. By configuring 0, the effect is the same as disabling the history buffer system. For information about the command syntax for configuring the command history buffer, see the **history size** command.

To display the history buffer, see **show history** command.

Negating the Effect of Commands

For many configuration commands, the prefix keyword "no" can be entered to cancel the effect of a command or reset the configuration to the default value. This guide describes the negation effect for all applicable commands.

Command Completion

If the command entered is incomplete, invalid, or has missing or invalid parameters, an appropriate error message is displayed.

To complete an incomplete command, press the <Tab> button. If the characters already entered are not enough for the system to identify a single matching command, press "?" to display the available commands matching the characters already entered.

Incorrect or incomplete commands are automatically re-entered next to the cursor. If a parameter must be added, the parameter can be added to the basic command already displayed next to the cursor. The following example indicates that the command interface requires a missing parameter.

```
(config)#interface
%missing mandatory parameter
(config)#interface
```

Keyboard Shortcuts

The CLI has a range of keyboard shortcuts to assist in entering the CLI commands.

The following table describes these shortcuts:

Table 1: Keyboard Keys

Up-arrow key	Recalls commands from the history buffer, beginning with the most recent command. Repeat the key sequence to recall successively older commands.
Down-arrow key	Returns the most recent commands from the history buffer after recalling commands with the up arrow key. Repeating the key sequence will recall successively more recent commands.
Ctrl+A	Moves the cursor to the beginning of the command line.
Ctrl+E	Moves the cursor to the end of the command line.
Ctrl+Z / End	Returns back to the Privileged EXEC mode from any mode.
Backspace key	Moves the cursor back one space.
Up-arrow key	Recalls commands from the history buffer, beginning with the most recent command. Repeat the key sequence to recall successively older commands.

2

User Interface Commands

enable

The **enable** EXEC mode command enters the Privileged EXEC mode.

Syntax

enable [*privilege-level*]

Parameters

privilege-level—Specifies the privilege level at which to enter the system. (Range: 1–15)

Default Configuration

The default privilege level is 15.

Command Mode

EXEC mode

Example

The following example enters the Privileged EXEC mode.

```
Console> enable
enter password:
Console#
```

disable

The **disable** Privileged EXEC mode command leaves the Privileged EXEC mode and returns to the User EXEC mode.

Syntax

disable [*privilege-level*]

Parameters

privilege-level—Specifies the privilege level at which to enter the system. (Range: 1–15)

Default Configuration

The default privilege level is 1.

Command Mode

Privileged EXEC mode

Example

The following example returns to the User EXEC mode.

```
Console# disable
Console>
```

login

The **login** EXEC mode command changes a user's login.

Syntax

login

Command Mode

EXEC mode

Example
The following example enters Privileged EXEC mode and logs in with username 'admin'.

```
Console> login
User Name:admin
Password:*****
Console#
```

configure

The **configure** Privileged EXEC mode command enters the Global Configuration mode.

Syntax
configure [*terminal*]

Parameters
terminal—Enter the Global Configuration mode with or without the keyword terminal.

Command Mode
Privileged EXEC mode

Example
The following example enters Global Configuration mode.

```
Console# configure
Console(config)#
```

exit (Configuration)

The **exit** command exits any configuration mode to the next highest mode in the CLI mode hierarchy.

Syntax
exit

Command Mode
All commands in configuration modes.

Examples
The following examples change the configuration mode from Interface Configuration mode to Privileged EXEC mode.

```
Console(config-if)# exit
Console(config)# exit
Console#
```

```
Router(config-if)# exit
Router(config)# exit
Router#
```

exit (EXEC)

The **exit** EXEC mode command closes an active terminal session by logging off the device.

Syntax
exit

Command Mode
EXEC mode

Example
The following examples close an active terminal session.

```
Console> exit
```

```
Router> exit
```

end

The **end** command ends the current configuration session and returns to the Privileged EXEC mode.

Syntax
end

Command Mode
All configuration modes

Example
The following examples end the Global Configuration mode session and return to the Privileged EXEC mode.

```
Console(config)# end
Console#
```

```
Router(config-if)# end
Router#
```

help

The **help** command displays a brief description of the Help system.

Syntax
help

Command Mode
All command modes

Example
The following example describes the Help system.

```
Console# help
```

```
Help may be requested at any point in a command by entering
a question mark '?'. If nothing matches the currently
entered incomplete command, the help list is empty. This
indicates that there is no command matching the input as it
currently appears. If the request is within a command, press
the Backspace key and erase the entered characters to a
point where the request results in a match.

Help is provided when:

1. There is a valid command and a help request is made for
entering a parameter or argument (e.g. 'show ?'). All
possible parameters or arguments for the entered command are
then displayed.

2. An abbreviated argument is entered and a help request is
made for arguments matching the input (e.g. 'show pr?').
```

history

The **history** Line Configuration mode command enables the command history function. Use the **no** form of this command to disable the command history function.

Syntax

history

no history

Default Configuration

The history command is enabled.

Command Mode

Line Configuration mode

User Guidelines

This command enables the command history function for a specified line. Use the **terminal history** EXEC mode command to enable or disable the command history function for the current terminal session.

Example
The following example enables the command history function for Telnet.

```
Console(config)# line telnet
Console(config-line)# history
```

history size
The **history size** Line Configuration mode command changes the command history buffer size for a particular line. Use the **no** form of this command to reset the command history buffer size to the default value.

Syntax
history size *number-of-commands*

no history size

Parameters
number-of-commands—Specifies the number of commands the system records in its history buffer. (Range: 0–256)

Default Configuration
The default command history buffer size is 10 commands.

Command Mode
Line Configuration mode

User Guidelines
This command configures the command history buffer size for a particular line. Use the **terminal history size** EXEC mode command to configure the command history buffer size for the current terminal session.

The allocated command history buffer is per terminal user, and is taken from a shared buffer. If there is not enough space available in the shared buffer, the command history buffer size () cannot be increased above the default size.

Example
The following example changes the command history buffer size to 100 entries for a particular line

```
Console(config)# line telnet
Console(config-line)# history size 100
```

terminal history

The **terminal history** EXEC mode command enables the command history function for the current terminal session. Use the **no** form of this command to disable the command history function.

Syntax
terminal history

terminal no history

Default Configuration
The default configuration for all terminal sessions is defined by the **history** Line Configuration mode command.

Command Mode
EXEC mode

User Guidelines
The command enables the command history for the current session. The default is determined by the **history** Line Configuration mode command.

Example
The following example disables the command history function for the current terminal session.

```
Console> terminal no history
```

terminal history size

The **terminal history size** EXEC mode command changes the command history buffer size for the current terminal session. Use the **no** form of this command to reset the command history buffer size to the default value.

Syntax

terminal history size *number-of-commands*

terminal no history size

Parameters

number-of-commands—Specifies the number of commands the system maintains in its history buffer. (Range: 10–256)

Default Configuration

The default configuration for all terminal sessions is defined by the **history size** Line Configuration mode command.

Command Mode

EXEC mode

User Guidelines

The **terminal history size** EXEC command changes the command history buffer size for the current terminal session. Use the **history** Line Configuration mode command to change the default command history buffer size.

The maximum number of commands in all buffers is 256.

Example

The following example sets the command history buffer size to 20 commands for the current terminal session.

```
Console> terminal history size 20
```

terminal datadump

The **terminal datadump** EXEC mode command enables dumping all the output of a show command without prompting. Use the **no** form of this command to disable dumping.

Syntax

terminal datadump

terminal no datadump

Default Configuration

Dumping is disabled.

Command Mode

EXEC mode

User Guidelines

By default, a **More** prompt is displayed when the output contains more lines than can be displayed on the screen. Pressing the **Enter** key displays the next line; pressing the **Spacebar** displays the next screen of output. The **terminal datadump** command enables dumping all output immediately after entering the show command.

This command is relevant only for the current session.

Example

The following example dumps all output immediately after entering a show command.

```
Console> terminal datadump
```

debug-mode

The **debug-mode** Privileged EXEC mode command mode switches to debug mode.

Syntax
debug-mode

Command Mode
Privileged EXEC mode

Example
The following example enters Debug mode.

```
Console# debug-mode
```

show history

The **show history** EXEC mode command lists commands entered in the current session.

Syntax
show history

Command Mode
EXEC mode

User Guidelines
The buffer includes executed and unexecuted commands.

Commands are listed from the first to the most recent command.

The buffer remains unchanged when entering into and returning from configuration modes.

Example
The following example displays all the commands entered while in the current Privileged EXEC mode.

```
Console# show version
SW version 3.131 (date 23-Jul-2005 time 17:34:19)
HW version 1.0.0
Console# show clock
```

```
15:29:03 Jun 17 2005
Console# show history
show version
show clock
show history
3 commands were logged (buffer size is 10)
```

show privilege

The **show privilege** EXEC mode command displays the current privilege level.

Syntax
show privilege

Command Mode
EXEC mode

Example
The following example displays the current privilege level for the Privileged EXEC mode.

```
Console# show privilege
Current privilege level is 15
```

do

The **do** command executes an EXEC-level command from Global Configuration mode or any configuration submode.

Syntax
do *command*

Parameters
command—Specifies the EXEC-level command to execute.

Command Mode
All configuration modes

Example
The following example executes the **show vlan** Privileged EXEC mode command from Global Configuration mode.

Example

```
Console (Config)# do show vlan

Vlan  Name   Ports                     Type         Authorization
---- ---- ------------------------- --------     -------------
 1    1      gi1/0/1-39,Po1,Po2,         other        Required
             Po3,Po4,Po5,Po6,Po7,Po8
 2    2      gi1/0/1                   dynamicGvrp  Required
 10   v0010  gi1/0/1                   permanent    Not Required
 11   V0011  gi1/0/1,gi1/0/13          permanent    Required
 20   20     gi1/0/1                   permanent    Required
 30   30     gi1/0/1,gi1/0/13          permanent    Required
 31   31     gi1/0/1                   permanent    Required
 91   91     gi1/0/1,gi1/0/40          permanent    Required
 4093 guest-vlan  gi1/0/1,gi1/0/13     permanent    Guest
console(config)#s
```

banner exec

Use the **banner exec** command to specify and enable a message to be displayed when an EXEC process is created (The user has successfully logged in), use the banner exec command in Global Configuration mode. Use the **no** form of this command to delete the existing EXEC banner.

Syntax
banner exec *d message-text d*

no banner exec

Parameters

- **d**—Delimiting character of your choice—a pound sign (**#**), for example. You cannot use the delimiting character in the banner message.
- **message-text**—The message must start in a new line. You can enter multi-line messages. You can include tokens in the form of **$(token)** in the message text. Tokens are replaced with the corresponding configuration variable. Tokens are described in the User Guidelines. The message can contain up to 2000 characters (after every 510 characters, you must press <Enter> to continue).

Default Configuration

Disabled (no EXEC banner is displayed).

Command Mode

Global Configuration mode

User Guidelines

Follow this command with one or more blank spaces and a delimiting character of your choice. Then enter one or more lines of text, terminating the message with the second occurrence of the delimiting character.

When a user connects to a device, the message-of-the-day (MOTD) banner appears first, followed by the login banner and prompts. After the user logs in to the device, the EXEC banner is displayed.

Use tokens in the form of **$(token)** in the message text to customize the banner. The tokens are described in the table below:

Token	Information displayed in the banner
$(hostname)	Displays the host name for the device.
$(domain)	Displays the domain name for the device.
$(bold)	Indicates that the next text is a bold text. Using this token again indicates the end of the bold text.
$(inverse)	Indicates that the next text is an inverse text. Using this token again indicates the end of the inverse text.
$(contact)	Displays the system contact string.

$(location)	Displays the system location string.
$(mac-address)	Displays the base MAC address of the device.

Use the no exec-banner line configuration command to disable the EXEC banner on a particular line or lines.

Example

The following example sets an EXEC banner that uses tokens. The percent sign (%) is used as a delimiting character. Note that the **$(token)** syntax is replaced by the corresponding configuration variable.

```
Device(config)# banner exec %
Enter TEXT message. End with the character '%'.
$(bold)Session activated.$(bold) Enter commands at the prompt.
%
When a user logs on to the system, the following output is displayed:
Session activated. Enter commands at the prompt.
```

banner login

Use the **banner login** command in Global Configuration mode to specify and enable a message to be displayed before the username and password login prompts. Use the **no** form of this command to delete the existing Login banner.

Syntax

banner login *d message-text d*

no banner login

Parameters

- **Delimiting character of your choice**—A pound sign (#), for example. You cannot use the delimiting character in the banner message.

- **message-text**—Message text. The message must start on a new line. You can enter multi-line messages. You can include tokens in the form of **$(token)** in the message text. Tokens are replaced with the corresponding configuration variable. Tokens are described in the User Guidelines. The message can contain up to 2000 characters (after every 510 characters, you must press <Enter> to continue).

Default Configuration
Disabled (no Login banner is displayed).

Command Mode
Global Configuration mode

User Guidelines
Follow this command with one or more blank spaces and a delimiting character of your choice. Then enter one or more lines of text, terminating the message with the second occurrence of the delimiting character.

When a user connects to a device, the message-of-the-day (MOTD) banner appears first, followed by the login banner and prompts. After the user logs in to the device, the EXEC banner is displayed.

Use tokens in the form of **$(token)** in the message text to customize the banner. The tokens are described in the table below:

Token	Information displayed in the banner
$(hostname)	Displays the host name for the device.
$(domain)	Displays the domain name for the device.
$(bold)	Indicates that the next text is a bold text. Using this token again indicates the end of the bold text.
$(inverse)	Indicates that the next text is an inverse text. Using this token again indicates the end of the inverse text.
$(contact)	Displays the system contact string.
$(location)	Displays the system location string.
$(mac-address)	Displays the base MAC address of the device.

Use the **no login-banner** line configuration command to disable the Login banner on a particular line or lines.

Example

The following example sets a Login banner that uses tokens. The percent sign (%) is used as a delimiting character. Note that the **$(token)** syntax is replaced by the corresponding configuration variable.

```
Device(config)# banner login %
Enter TEXT message. End with the character '%'.
You have entered $(hostname).$(domain)
%
When the login banner is executed, the user will see the following banner:
You have entered host123.ourdomain.com
```

banner motd

Use the **banner motd** command in Global Configuration mode to specify and enable a message-of-the-day banner. Use the **no** form of this command to delete the existing MOTD banner.

Syntax

banner motd *d message-text d*

no banner motd

Parameters

- **d**—Delimiting character of your choice—a pound sign (**#**), for example. You cannot use the delimiting character in the banner message.
- **message-text**—The message must start on a new line. You can enter multi-line messages. You can include tokens in the form of **$(token)** in the message text. Tokens are replaced with the corresponding configuration variable. Tokens are described in the User Guidelines. The message can contain up to 2000 characters (after every 510 characters, you must press <Enter> to continue).

Default Configuration
Disabled (no MOTD banner is displayed).

Command Mode
Global Configuration mode

User Guidelines
Follow this command with one or more blank spaces and a delimiting character of your choice. Then enter one or more lines of text, terminating the message with the second occurrence of the delimiting character.

When a user connects to a device, the message-of-the-day (MOTD) banner appears first, followed by the login banner and prompts. After the user logs in to the device, the EXEC banner is displayed.

Use tokens in the form of **$(token)** in the message text to customize the banner. The tokens are described in the table below:

Token	Information displayed in the banner
$(hostname)	Displays the host name for the device.
$(domain)	Displays the domain name for the device.
$(bold)	Indicates that the next text is a bold text. Using this token again to indicates the end of the bold text.
$(inverse)	Indicates that the next text is an inverse text. Using this token again indicates the end of the inverse text.
$(contact)	Displays the system contact string.
$(location)	Displays the system location string.
$(mac-address)	Displays the base MAC address of the device.

Use the **no motd-banner** line configuration command to disable the MOTD banner on a particular line or lines.

Example
The following example sets an MOTD banner that uses tokens. The percent sign (%) is used as a delimiting character. Note that the **$(token)** syntax is replaced by the corresponding configuration variable.

```
Device(config)# banner motd %
Enter TEXT message. End with the character '%'.
$(bold)Upgrade$(bold) to all devices begins at March 12
%
When the login banner is executed, the user will see the following banner:
Upgrade to all devices begins at March 12
```

exec-banner

Use the **exec-banner** command in Line Configuration mode to enable the display of exec banners. Use the **no** form of this command to disable the display of exec banners.

Syntax

exec-banner

no exec-banner

Parameters

This command has no arguments or keywords.

Default Configuration

Disabled

Command Mode

Line Configuration mode

Example

```
console# configure
console(config)# line console
console(config-line)# exec-banner
console(config-line)# exit
console(config)# line telnet
console(config-line)# exec-banner
console(config-line)# exit
```

```
console(config)# line ssh
console(config-line)# exec-banner
```

login-banner

Use the **login-banner** command in Line Configuration mode to enable the display of login banners. Use the **no** form of this command to disable the display of login banners.

Syntax

login-banner

no login-banner

Parameters

This command has no arguments or keywords.

Default Configuration

Enabled

Command Mode

Line Configuration mode

Example

```
console# configure
console(config)# line console
console(config-line)# login-banner
console(config-line)# exit
console(config)# line telnet
console(config-line)# login-banner
console(config-line)# exit
console(config)# line ssh
console(config-line)# login-banner
```

motd-banner

Use the **motd-banner** command in Line Configuration mode to enable the display of message-of-the-day banners. Use the **no** form of this command to disable the display of MOTD banners.

Syntax

motd-banner

no motd-banner

Parameters

This command has no arguments or keywords.

Default Configuration

Enabled

Command Mode

Line Configuration mode

Example

```
console# configure
console(config)# line console
console(config-line)# motd-banner
console(config-line)# exit
console(config)# line telnet
console(config-line)# motd-banner
console(config-line)# exit
console(config)# line ssh
console(config-line)# motd-banner
```

show banner

Use the **show banner** command in EXEC mode to display the configuration of banners.

Syntax

show banner motd

show banner login

show banner exec

Parameters

This command has no arguments or keywords.

Command Mode

EXEC mode

Examples

```
Device> show banner motd
Banner: MOTD
Line SSH: Enabled
Line Telnet: Enabled
Line Console: Enabled
10000 giga ports switch
console#
console# show banner login
------------------------------------------------------------
Banner: Login
Line SSH: Enabled
Line Telnet: Enabled
Line Console: Enabled
console#
console# show banner exec
```

```
Banner: EXEC
Line SSH: Enabled
Line Telnet: Enabled
Line Console: Enabled
console#
```

3

Macro Commands

macro name

Use the **Macro Name** Global Configuration mode command to create a user defined macro.

Use the **no** form of this command to delete the macro definition.

Syntax

macro name *[macro-name]*

no macro name *[macro-name]*

Parameters

macro-name—Name of the macro. Macro names are case sensitive.

Default Configuration

The command has no default setting.

Command Mode

Global Configuration mode

User Guidelines

A macro can contain up to 3000 characters and up to 200 lines. Enter one macro command per line. Use the @ character to end the macro. Use the # character at the beginning of a line to enter comment text within the macro.

You can define mandatory keywords within a macro by using a help string to specify the keywords. Enter **#macro** keywords word to define the keywords that are available for use with the macro. The keyword name is case sensitive. You can enter up to three keywords separated by a space. Only the first three

keywords are visible if you enter more than three macro keywords. The command can be anywhere within the macro.

When creating a macro, do not use the **exit** or **end** commands or change the command mode using interface interface-id. Doing so might cause commands that follow **exit**, **end** or interface interface-id to be executed in a different command mode.

You can modify a macro by creating a new macro with the same name as the existing macro. The newer macro overwrites the existing macro.

Examples

The following example shows how to create a macro that defines the duplex mode and speed:

```
Switch(config) #  macro name dup
Enter macro commands one per line. End with the character '@'.
macro description dup
duplex full
speed auto
```

The following example shows how to create a macro with #macro keywords:

```
Switch(config) #  macro name duplex
Enter macro commands one per line. End with the character '@'.
macro description duplex
duplex $DUPLEX
speed $SPEED
#macro keywords $ DUPLEX $ SPEED
@
```

The following example shows how to apply the macros to an interface:

```
Switch(config-if) #  macro apply duplex $DUPLEX full $SPEED auto

Switch(config-if) #  macro apply duplex ?
    WORDkeyword to replace with value e.g. $DUPLEX, $SPEED
      <cr>
```

```
Switch(config-if) #  macro apply duplex $DUPLEX ?
    WORDValue of the first keyword to replace
      <cr>
Switch(config-if) #  macro apply duplex $DUPLEX full $SPEED ?
    WORDValue of the second keyword to replace
```

macro apply

Use the **macro apply** interface configuration command to apply a macro to an interface or to apply and trace a macro configuration on an interface.

Syntax

macro {*apply | trace*} *macro-name [parameter {value}] [parameter {value}] [parameter {value}*]

Parameters

- **apply**—Apply a macro to the specific interface.
- **trace**—Apply and trace a macro to the specific interface.
- **macro-name**—Specify the name of the macro.
- **parameter**—(Optional) Specify unique parameter values that are specific to the interface. You can enter up to three keyword-value pairs. Parameter keyword matching is case sensitive. All matching occurrences of the keyword are replaced with the corresponding value.

Default Configuration

The command has no default setting.

Command Mode

Interface Configuration mode

User Guidelines

You can use the **macro trace macro-name** Interface Configuration command to apply and show the macros running on an interface or to debug the macro to find any syntax or configuration errors.

If a command fails because of a syntax error or a configuration error the macro continues to apply t) in the interface. Use the parameter value

keywords to designate values specific to the interface when creating a macro that requires the assignment of a unique value.

Keyword matching is case sensitive. All matching occurrences of the keyword are replaced with the corresponding value. Any full match of a keyword, even if it is part of a large string, is considered a match and replaced by the corresponding value.

Some macros might contain keywords that require a parameter value. You can use the **macro apply macro-name** command to display a list of any required values in the macro. If you apply a macro without entering the keyword values, the commands are invalid and are therefore not applied.

When you apply a macro to an interface, the macro name is automatically added to the interface. You can display the applied commands and macro names by using the **show running-configuration** interface interface-id user EXEC mode command.

A macro applied to an interface range behaves the same way as a macro applied to a single interface. When a macro is applied to an interface range, it is applied sequentially to each interface within the range. If a macro command fails on one interface, it is nonetheless applied to the remaining interfaces.

Example

```
Switch(config) #  interface gigabitethernet 1/0/2
Switch(config-if) #  macro trace dup
  Applying command…  'duplex full'
  Applying command…  'speed auto'

Switch(config) # interface gigabitethernet 1/0/2
Switch(config-if) #  macro apply duplex $DUPLEX full $SPEED auto
Switch(config-if) #  exit
Switch(config) #  interface gigabitethernet 1/0/3
Switch(config-if) #  macro apply dup
Switch(config-if) #  exit
```

macro description

Use the **macro description** Interface Configuration mode command to enter a description about which macros are applied to an interface. Use the **no** form of this command to remove the description.

Syntax

macro description *text*

no macro description

Parameters

text—Description text. The text can contain up to 160 characters.

Default Configuration

The command has no default setting.

Command Mode

Interface Configuration mode

User Guidelines

When multiple macros are applied on a single interface, the description text is a concatenation of texts from a number of previously applied macros.

You can verify your setting by entering the **show parser macro description** privileged EXEC modecommand.

Example

```
Switch(config) # interface gigabitethernet 1/0/2
Switch(config-if) #  macro apply dup
Switch(config-if) #  end
Switch(config) # interface gi1/0/3
Switch(config-if) #  macro apply duplex $DUPLEX full $SPEED auto
Switch(config-if) #  end
Switch #  show parser macro description
InterfaceMacro Description
------------------------------------------------------------------
```

```
1/2     dup
1/3     duplex
------------------------------------------------------------------
Switch(config) # interface gigabitethernet 1/0/2
Switch(config-if) #  no macro description
Switch(config-if) #  end
Switch #  show parser macro description
InterfaceMacro Description
------------------------------------------------------------------
1/3     duplex
------------------------------------------------------------------
```

macro global

Use the **macro global** Global Configuration command to apply a macro to a switch or to apply and trace a macro configuration on a switch.

Syntax

macro global {*apply | trace*} *macro-name [parameter {value}] [parameter {value}] [parameter {value}*]

Parameters

- **apply**—Apply a macro to the switch.
- **trace**—Apply and trace a macro to the switch.
- **macro-name**—Specify the name of the macro.
- **paramete**—(Optional) Specify unique parameter values that are specific to the switch. You can enter up to three keyword-value pairs. Parameter keyword matching is case sensitive. All matching occurrences of the keyword are replaced with the corresponding value.

Default Configuration

The command has no default setting.

Command Mode

Global Configuration mode

User Guidelines

You can use the **macro global trace macro-name** Global Configuration mode command to apply and show the macros running on the switch or to debug the macro in order to locate any syntax or configuration errors.

If a command fails because of a syntax error or a configuration error when you apply a macro, the macro nonetheless continues to apply the remaining commands to the interface.

Use the parameter value keywords to designate values specific to the switch when creating a macro that requires the assignment of unique value.

Keyword matching is case sensitive. All matching occurrences of the keyword are replaced with the corresponding value. Any full match of a keyword, even if it is part of a large string, is considered a match and replaced by the corresponding value.

Some macros might contain keywords that require a parameter value. You can use the **macro global apply macro-name** command to display a list of any required values in the macro. If you apply a macro without entering the keyword values, the commands are considered invalid and are not applied.

When you apply a macro to the switch, the macro name is automatically added to the switch. You can display the applied commands and macro names by using the **show running-configuration** interface user EXEC mode command.

macro global description

Use the **macro global description** Global Configuration command to enter a description about which macros are applied to the switch. Use the **no** form of this command to remove the description.

Syntax

macro global description *text*

no macro global description

Parameters

text—Description text. The text can contain up to 160 characters.

Default Configuration
The command has no default setting.

Command Mode
Global Configuration mode

User Guidelines
When multiple global macros are applied to a switch, the global description text is a concatenation of texts from a number of previously applied macros.

You can verify your settings by entering the **show parser macro description** privileged EXEC mode command.

show parser macro

Use the **show parser macro** User EXEC mode command to display the parameters for all configured macros or for one macro on the switch.

Syntax
show parser macro [*{brief | description [interface interface-id] | name macro-name}*]

Parameters

- **brief**—(Optional) Display the name of each macro.
- **description [interface]**—(Optional) Display all macro descriptions.
- **interface-id**—Or the description of a specific interface.
- **name macro-name**—(Optional) Display information about a single macro identified by the macro name.

Command Mode
User EXEC mode

4

System Management Commands

ping

Use the **ping** command to send ICMP echo request packets to another node on the network.

Syntax

ping [**ip**] *{ipv4-address | hostname} [size packet_size] [count packet_count] [timeout time_out]*

ping ipv6 *{ipv6-address | hostname} [size packet_size] [count packet_count] [timeout time_out]*

Parameters

- **ip**—Use IPv4 to check the network connectivity.
- **ipv6**—Use IPv6 to check the network connectivity.
- **ipv4-address**—IPv4 address to ping.
- **ipv6-address**—Unicast or multicast IPv6 address to ping. When the IPv6 address is a Link Local address (IPv6Z address), the outgoing interface name must be specified. Refer to the User Guidelines for the interface name syntax.
- **hostname**—Hostname to ping (160 characters. Maximum label size: 63.)
- **packet_size**—Number of bytes in the packet not including the VLAN tag. The default is 64 bytes. (IPv4:64-1518, IPv6: 68-1518)
- **packet_count**—Number of packets to send, from 1 to 65535 packets. The default is 4 packets. If 0 is entered, it pings until stopped (0–65535).
- **time-out**—Timeout in milliseconds to wait for each reply, from 50 to 65535 milliseconds. The default is 2000 milliseconds (50–65535).

Command Mode
EXEC mode

User Guidelines
Press **Esc** to stop pinging. Following are sample results of the ping command:

- **Destination does not respond**—If the host does not respond, a "no answer from host" appears within 10 seconds.
- **Destination unreachable**—The gateway for this destination indicates that the destination is unreachable.
- **Network or host unreachable**—The switch found no corresponding entry in the route table.

The format of an **IPv6Z** address is: *<ipv6-link-local-address>%<interface-name>*

- **interface-name** = *vlan<integer> | ch<integer> | isatap<integer> | <physical-port-name> | 0*
- **integer** = *<decimal-number> | <integer><decimal-number>*
- **decimal-number** = *0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9*
- **physical-port-name** = Designated port number, for example gi1/0/1

When using the ping **ipv6** command to check network connectivity of a directly attached host using its link local address, the egress interface may be specified in the **IPv6Z** format. If the egress interface is not specified, the default interface is selected. Specifying interface zone=0 is equivalent to not defining an egress interface.

When using the ping **ipv6** command with MC address, the information displayed is taken from all received echo responses.

Examples

```
Console> ping ip 10.1.1.1
Pinging 10.1.1.1 with 64 bytes of data:

64 bytes from 10.1.1.1: icmp_seq=0. time=11 ms
64 bytes from 10.1.1.1: icmp_seq=1. time=8 ms
64 bytes from 10.1.1.1: icmp_seq=2. time=8 ms
```

```
64 bytes from 10.1.1.1: icmp_seq=3. time=7 ms

----10.1.1.1 PING Statistics----
4 packets transmitted, 4 packets received, 0% packet loss
round-trip (ms) min/avg/max = 7/8/11

Console> ping ip yahoo.com
Pinging yahoo.com [66.218.71.198] with 64 bytes of data:

64 bytes from 10.1.1.1: icmp_seq=0. time=11 ms
64 bytes from 10.1.1.1: icmp_seq=1. time=8 ms
64 bytes from 10.1.1.1: icmp_seq=2. time=8 ms
64 bytes from 10.1.1.1: icmp_seq=3. time=7 ms

----10.1.1.1 PING Statistics----
4 packets transmitted, 4 packets received, 0% packet loss
round-trip (ms) min/avg/max = 7/8/11

Console> ping ip oob/176.16.1.1
Pinging oob/176.16.1.1 with 64 bytes of data:

64 bytes from oob/176.16.1.1: icmp_seq=0. time=5 ms
64 bytes from oob/176.16.1.1: icmp_seq=1. time=5 ms
64 bytes from oob/176.16.1.1: icmp_seq=2. time=5 ms
64 bytes from oob/176.16.1.1: icmp_seq=3. time=5 ms

----10.1.1.1 PING Statistics----
4 packets transmitted, 4 packets received, 0% packet loss
round-trip (ms) min/avg/max = 5/5/5

console> ping ipv6 3003::11
Pinging 3003::11 with 64 bytes of data:

64 bytes from 3003::11: icmp_seq=1. time=0 ms
64 bytes from 3003::11: icmp_seq=2. time=50 ms
64 bytes from 3003::11: icmp_seq=3. time=0 ms
```

```
64 bytes from 3003::11: icmp_seq=4. time=0 ms

----3003::11 PING Statistics----
4 packets transmitted, 4 packets received, 0% packet loss
round-trip (ms) min/avg/max = 0/12/50

console> ping ipv6 FF02::1
Pinging FF02::1 with 64 bytes of data:

64 bytes from 3003::11: icmp_seq=1. time=0 ms
64 bytes from 3003::33: icmp_seq=1. time=70 ms
64 bytes from 3003::11: icmp_seq=2. time=0 ms
64 bytes from 3003::55: icmp_seq=1. time=1050 ms
64 bytes from 3003::33: icmp_seq=2. time=70 ms
64 bytes from 3003::55: icmp_seq=2. time=1050 ms
64 bytes from 3003::11: icmp_seq=3. time=0 ms
64 bytes from 3003::33: icmp_seq=3. time=70 ms
64 bytes from 3003::11: icmp_seq=4. time=0 ms
64 bytes from 3003::55: icmp_seq=3. time=1050 ms
64 bytes from 3003::33: icmp_seq=4. time=70 ms
64 bytes from 3003::55: icmp_sq=4. time=1050 ms

---- FF02::1 PING Statistics----
4 packets transmitted, 12 packets received
```

traceroute

To discover (?) the routes that packets will take when traveling to their destination, use the **traceroute** EXEC command.

Syntax

traceroute ip *{ipv4-address | hostname} [size packet_size] [ttl max-ttl] [count packet_count] [timeout time_out] [source ip-address] [tos tos*]

traceroute ipv6 *{ipv6-address | hostname} [size packet_size] [ttl max-ttl] [count packet_count] [timeout time_out] [source ip-address] [tos tos*]

Parameters

- **ip**—Use IPv4 to discover the route.
- **ipv6**—Use IPv6 to discover the route.
- **ipv4-address**—IPv4 address of the destination host. (Range: Valid IP address)
- **ipv6-address**—IPv6 address of the destination host.
- **hostname**—Hostname of the destination host. (Range: 1–160 characters. Maximum label size: 63.)
- **packet_size**—Number of bytes in the packet not including the VLAN tag. The default is 64 bytes. (IPv4:64-1518, IPv6: 68-1518)
- **ttl max-ttl**—The largest TTL value that can be used. The default is 30. The **traceroute** command terminates when the destination is reached or when this value is reached. (Range: 1–255)
- **count packet_count**—The number of probes to be sent at each TTL level. The default count is 3. (Range: 1–10)
- **timeout time_out**—The number of seconds to wait for a response to a probe packet. The default is 3 seconds. (Range: 1–60)
- **source ip-address**—One of the interface addresses of the device to use as a source address for the probes. The device will normally pick what it feels is the best source address to use. (Range: Valid IP address)
- **tos tos**—The Type-Of-Service byte in the IP Header of the packet.(Range: 0—255)

Command Mode

EXEC mode

User Guidelines

The traceroute command works by taking advantage of the error messages generated by routers when a datagram exceeds its time-to-live (TTL) value.

The traceroute command starts by sending probe datagrams with a TTL value of one. This causes the first router to discard the probe datagram and send back an error message. The traceroute command sends several probes at each TTL level and displays the round-trip time for each.

The traceroute command sends out one probe at a time. Each outgoing packet can result in one or two error messages. A "time exceeded" error message indicates that an intermediate router has seen and discarded the probe. A "destination unreachable" error message indicates that the destination node has received the probe and discarded it because it could not deliver the packet. If the timer goes off before a response comes in, the traceroute command prints an asterisk (*).

The traceroute command terminates when the destination responds, when the maximum TTL is exceeded, or when the user interrupts the trace with Esc.

The traceroute command is not relevant to IPv6 link local addresses.

Example

```
Router> traceroute ip umaxp1.physics.lsa.umich.edu
Type Esc to abort.
Tracing the route to umaxp1.physics.lsa.umich.edu (141.211.101.64)
   1 i2-gateway.stanford.edu (192.68.191.83)  0 msec 0 msec 0 msec
   2 STAN.POS.calren2.NET (171.64.1.213) 0 msec 0 msec 0 msec
   3 SUNV--STAN.POS.calren2.net (198.32.249.73) 1 msec 1 msec 1 msec
   4 Abilene--QSV.POS.calren2.net (198.32.249.162)  1 msec 1 msec 1 msec
   5 kscyng-snvang.abilene.ucaid.edu (198.32.8.103)  33 msec 35 msec 35
msec
   6 iplsng-kscyng.abilene.ucaid.edu (198.32.8.80)   47 msec 45 msec 45
msec
   7 so-0-2-0x1.aa1.mich.net (192.122.183.9)  56 msec  53 msec 54 msec
   8 atm1-0x24.michnet8.mich.net (198.108.23.82)  56 msec 56 msec 57 msec
   9 * * *
  10 A-ARB3-LSA-NG.c-SEB.umnet.umich.edu (141.211.5.22) 58 msec 58 msec 58
msec
  11 umaxp1.physics.lsa.umich.edu (141.211.101.64)  62 msec 63 msec 63 msec
Trace completed
```

The following table describes the significant fields shown in the display:

Field	Description
1	Indicates the sequence number of the router in the path to the host.
i2-gateway.stanford.edu	Host name of this router.
192.68.191.83	IP address of this router.
1 msec 1 msec 1 msec	Round-trip time for each of the probes that are sent.

The following are characters that can appear in the traceroute command output:

Field	Description
*	The probe timed out.
?	Unknown packet type.
A	Administratively unreachable. Usually, this output indicates that an access list is blocking traffic.
F	Fragmentation required and DF is set.
H	Host unreachable.
N	Network unreachable.
P	Protocol unreachable.
Q	Source quench.
R	Fragment reassembly time exceeded
S	Source route failed.
U	Port unreachable.

telnet

The **telnet** EXEC mode command enables logging on to a host that supports Telnet.

Syntax

telnet {*ip-address* | *hostname*} [*port*] [*keyword ...*]

Parameters

- **ip-address**—Specifies the destination host IP address.
- **hostname**—Specifies the destination host name. (Length: 1-160 characters. Maximum label length: 63 characters.)
- **port**—Specifies the decimal TCP port number or one of the keywords listed in the Ports table in the User Guidelines.
- **keyword**—Specifies the one or more keywords listed in the Keywords table in the User Guidelines.

Default Configuration

The default port is the Telnet port (23) on the host.

By default, Telnet is enabled.

Command Mode

EXEC mode

User Guidelines

Telnet software supports special Telnet commands in the form of Telnet sequences that map generic terminal control functions to operating system-specific functions. To enter a Telnet sequence, press the escape sequence keys (Ctrl-shift-6) followed by a Telnet command character.

Special Telnet Sequences

Telnet Sequence	Purpose
Ctrl-shift-6-b	Break
Ctrl-shift-6-c	Interrupt Process (IP)
Ctrl-shift-6-h	Erase Character (EC)
Ctrl-shift-6-o	Abort Output (AO)
Ctrl-shift-6-t	Are You There? (AYT)
Ctrl-shift-6-u	Erase Line (EL)

At any time during an active Telnet session, available Telnet commands can be listed by pressing the Ctrl-shift-6-? keys at the system prompt.

A sample of this list follows. Note that the Ctrl-shift-6 sequence appears as ^ ^ on the screen.

```
Console> 'Ctrl-shift-6' ?
[Special telnet escape help]
^^ B sends telnet BREAK
^^ C sends telnet IP
^^ H sends telnet EC
^^ O sends telnet AO
^^ T sends telnet AYT
^^ U sends telnet EL
Ctrl-shift-6 x suspends the session (return to system
command prompt)
```

Several concurrent Telnet sessions can be opened, enabling switching between the sessions. To open a subsequent session, the current connection has to be suspended by pressing the escape sequence keys (Ctrl-shift-6) and x to return to the system command prompt. Then open a new connection with the telnet EXEC mode command.

This command lists concurrent Telnet connections to remote hosts that were opened by the current Telnet session to the local device. It does not list Telnet connections to remote hosts that were opened by other Telnet sessions.

Keywords Table

Options	Description
/echo	Enables local echo.
/quiet	Prevents onscreen display of all messages from the software.
/source-interface	Specifies the source interface.

Options	Description
/stream	Turns on stream processing, which enables a raw TCP stream with no Telnet control sequences. A stream connection does not process Telnet options and can be appropriate for connections to ports running UNIX-to-UNIX Copy Program (UUCP) and other non-Telnet protocols.
Ctrl-shift-6 x	Returns to the System Command Prompt.

Ports Table

Keyword	Description	Port Number
BGP	Border Gateway Protocol	179
chargen	Character generator	19
cmd	Remote commands	514
daytime	Daytime	13
discard	Discard	9
domain	Domain Name Service	53
echo	Echo	7
exec	Exec	512
finger	Finger	79
ftp	File Transfer Protocol	21
ftp-data	FTP data connections	20
gopher	Gopher	70
hostname	NIC hostname server	101
ident	Ident Protocol	113
irc	Internet Relay Chat	194
klogin	Kerberos login	543
kshell	Kerberos shell	544
login	Login	513
lpd	Printer service	515
nntp	Network News Transport Protocol	119

Keyword	Description	Port Number
pim-auto-rp	PIM Auto-RP	496
pop2	Post Office Protocol v2	109
pop3	Post Office Protocol v3	110
smtp	Simple Mail Transport Protocol	25
sunrpc	Sun Remote Procedure Call	111
syslog	Syslog	514
tacacs	TAC Access Control System	49
talk	Talk	517
telnet	Telnet	23
time	Time	37
uucp	Unix-to-Unix Copy Program	540
whois	Nickname	43
www	World Wide Web	80

Example

The following example displays logging in to IP address 176.213.10.50 via Telnet.

```
Console> telnet 176.213.10.50
Esc U sends telnet EL
```

resume

The **resume** EXEC mode command enables switching to another open Telnet session.

Syntax

resume [*connection*]

Parameters

connection—Specifies the connection number. (Range: 1-4 connections.)

Default Configuration
The default connection number is that of the most recent connection.

Command Mode
EXEC mode

Example
The following command switches to open Telnet session number 1.

```
Console> resume 1
```

hostname

The **hostname** Global Configuration mode command specifies or modifies the device host name. Use the **no** form of the command to remove the existing host name.

Syntax
hostname *name*

no hostname

Parameters
Name—specifies The Device Host Name. (Length: 1-160 Characters. Maximum label length: 63 characters.)

Default Configuration
No host name is defined.

Command Mode
Global Configuration mode

Example
The following example specifies the device host name as 'enterprise'.

```
Console(config)# hostname enterprise
enterprise(config)#
```

reload

The **reload** Privileged EXEC mode command reloads the operating system.

Syntax

reload [**slot** *stack-member-number]*

Command Mode

Privileged EXEC mode

Parameters

stack-member-number —Specifies the new master unit number. (Range: 1–8). If unspecified, reloads all the units.

Example

The following example reloads the operating system on all units.

```
Console# reload
This command will reset the whole system and disconnect your
current session. Do you want to continue? (y/n) [n]
```

stack master

The **stack master** Global Configuration mode command forces a stack master selection. Use the **no** form of this command to restore the default configuration.

Syntax

stack master unit *unit*

no stack master

Parameters

unit —Specifies the new master unit number. (Range: 1–2)

Default Configuration

The default is no forced master.

Command Mode
Global Configuration mode

Example
The following example forces the stack master to be unit 2.

```
Console(config)# stack master unit 2
```

system light

Use the **system light** EXEC command to light LEDs on a specific unit.

Syntax
system light [*unit unit-number] [duration seconds*]

system light stop

Parameters

- **unit-number**—Specify unit number or all.
- **seconds**—The number of seconds to light the LEDs. If unspecified, defaults to 5 seconds. (Range: 2–6)
- **stop**—Stop lighting the LEDs.

Command Mode
EXEC mode

switch renumber

Use the **switch renumber** Global Configuration command to change the unit ID of a specific unit.

Syntax
switch *current-unit-number renumber new-unit-number*

Parameters

- **current-unit-number**—Specify Unit number. (Range: 1–8)

- **new-unit-number**—The new unit number. (Range: 1–8)

Command Mode
Global Configuration mode

show switch

The **show switch** EXEC mode command displays stack status information for the stack or stack member.

Syntax
show switch [*stack-member-number*]

Parameters
stack-member-number— Specifies the unit number. (Range: 1–6)

Command Mode
EXEC mode

Example
The following examples display the stack status information.

```
Console> show switch

Unit   MAC Address         SW      Master    Up-     Down    Status
----   -----------------   ------  ------    link    link    ------
                                              -----   -----
1      00:00:b0:87:12:11   3.30    Enabled   2       3       Slave
3      00:00:b0:87:12:13   3.30    Forced    1       4       Master
4      00:00:b0:87:12:14   3.30    Enabled   3       5       Slave
5      00:00:b0:87:12:15   3.30    Enabled   4       6       Slave
6      00:00:b0:87:12:16   3.30    Enabled   5       7       Slave
7      00:00:b0:87:12:17   3.30    Enabled   6       8       Slave
8      00:00:b0:87:12:18   3.30    Enabled   7       2       Slave
2      00:00:b0:87:12:12   3.30    Enabled   8       1       Slave
```

```
Configured order: Unit 1 at Top, Unit 2 at bottom

Console> show switch 1

Unit 1:
MAC address: 00:00:b0:87:12:11
Master: Forced.
Product: Fonseca 48. Software: 3.30
Uplink unit: 8. Downlink unit: 2.
Status: Master
Active image: image-1.
Selected for next boot: image-2.
```

service cpu-utilization

The **service cpu-utilization** Global Configuration mode command enables measuring CPU utilization. Use the **no** form of this command to restore the default configuration.

Syntax

service cpu-utilization

no service cpu-utilization

Default Configuration

Measuring CPU utilization is disabled.

Command Mode

Global Configuration mode

User Guidelines

Use the **show cpu utilization** Privileged EXEC command to view information on CPU utilization.

Example
The following example enables measuring CPU utilization.

```
Console(config)# service cpu-utilization
```

show cpu utilization

The **show cpu utilization** Privileged EXEC mode command displays information about CPU utilization.

Syntax
show cpu utilization

Command Mode
Privileged EXEC mode

User Guidelines
Use the **service cpu-utilization** Global Configuration mode command to enable measuring CPU utilization.

Example
The following example displays CPU utilization information.

```
Console# show cpu utilization
CPU utilization service is on.
CPU utilization
------------------------------------------------
five seconds: 5%; one minute: 3%; five minutes: 3%
```

clear cpu counters

The **clear cpu counters** EXEC mode command clears traffic counters to and from the CPU.

Syntax
clear cpu counters

Command Mode
EXEC mode

Example
The following example clears the CPU traffic counters.

```
Console# clear cpu counters
```

service cpu-counters

The **service cpu-counters** Global Configuration mode command enables traffic counting to and from the CPU. To disable counting, use the **no** form of this command.

Syntax
service cpu-counters

no service cpu-counters

Command Mode
Global Configuration mode

User Guidelines
Use the **show cpu counters** command to display the CPU traffic counters.

Example
The following example enables counting CPU traffic.

```
Console(config)# service cpu-counters
```

show cpu counters

The **show cpu counters** EXEC mode command displays traffic counter information to and from the CPU.

Syntax
show cpu counters

Command Mode
EXEC mode

User Guidelines
Use the **service cpu-counters** command to enable traffic counting to and from the CPU.

Example
The following example displays the CPU traffic counters.

```
Console# show cpu counters

CPU counters are active.

In Octets: 987891
In Unicast Packets: 3589
In Multicast Packets: 29
In Broadcast Packets: 8

Out Octets: 972181
Out Unicast Packets: 3322
Out Multicast Packets: 22
Out Broadcast Packets: 8
```

show users

The **show users** EXEC mode command displays information about the active users.

Syntax
show users

Command Mode
EXEC mode

Example
The following example displays information about the active users.

```
Console# show users

Username        Protocol     Location
----------      ----------   -----------
Bob             Serial
John            SSH          172.16.0.1
Robert          HTTP         172.16.0.8
Betty           Telnet       172.16.1.7
Sam                          172.16.1.6
```

show sessions

The **show sessions** EXEC mode command displays open Telnet sessions.

Syntax
show sessions

Command Mode
EXEC mode

User Guidelines
The command displays Telnet sessions to remote hosts opened by the current Telnet session to the local device. It does not display Telnet sessions to remote hosts opened by other Telnet sessions to the local device.

Example
The following example displays open Telnet sessions.

```
Console# show sessions

Connection    Host             Address       Port    Byte
----------    -------------    ----------    -----   ----
1             Remote router    172.16.1.1    23      89
2             172.16.1.2       172.16.1.2    23      8
```

The following table describes significant fields shown above.

Field	Description
Connection	The connection number.
Host	The remote host to which the device is connected through a Telnet session.
Address	The remote host IP address.
Port	The Telnet TCP port number.
Byte	The number of unread bytes for the user to see on the connection.

show system

The **show system** EXEC mode command displays system information.

Syntax
show system [**unit** *unit*]

Parameters
unit unit — Specifies the unit number. (Range: 1–8)

Command Mode
EXEC mode

Example

The following example displays the system information.

```
console# show system
Unit          Type
---- ----------------------
 1     PowerConnect 5524
 2     PowerConnect 5524
 3     PowerConnect 5524
 4     PowerConnect 5524
 5     PowerConnect 5524
 6     PowerConnect 5524
 7     PowerConnect 5524
 8     PowerConnect 5524


Unit Main Power Supply Redundant Power Supply
---- ----------------- ----------------------
 1          OK
 2          OK
 3          OK
 4          OK
 5          OK
 6          OK
 7          OK
 8          OK            NOT OPERATIONAL
Unit  Fans Status
---- -------------
 1        OK
 2        OK
 3        OK
 4        OK
 5       IDLE
 6        OK
 7        OK
 8      FAILURE
```

```
Unit   Temperature (Celsius)   Temperature Sensor
                               Status
---- ------------------------- ---------------
 1             47                       OK
 2             45                       OK
 3             49                       OK
 4             36                       OK
 5             35                       OK
 6             45                       OK
 7             40                       OK
 8             56                       OK


Unit     Up time
---- ---------------
 1     00,00:31:24
 2     00,00:31:19
 3     00,00:31:24
 4     00,00:31:24
 5     00,00:31:24
 6     00,00:31:24
 7     00,00:31:25
 8     00,00:31:25

console# show system unit 2
System Type:                          PowerConnect 5548
System Up Time (days,hour:min:sec):   08,23:03:46
System Contact:
System Name:
System Location:
System MAC Address:                   00:99:88:66:33:33
System Object ID:                     1.3.6.1.4.1.674.10895.3031
Type:                                 PowerConnect 5548
Main Power Supply Status:             OK
```

```
Fans Status:                          OK
          Unit Temperature (Celsius) Status
------------  ------------------   -------------
           2   42                   OK
```

show version

The **show version** EXEC mode command displays system version information.

Syntax

show version [**unit** *unit*]

Parameters

unit *unit* — Specifies the unit number. (Range: 1–8)

Command Mode

EXEC mode

Example

The following example displays system version information.

```
console > show version
Unit       SW Version    Boot Version     HW Version
------     ----------    ------------     ----------
1          3.131         2.178            1.0.0
2          3.131         2.178            1.0.0
```

system resources routing

The **system resources routing** Global Configuration mode command configures the routing table maximum size. Use the **no** form of this command to return to the default size.

Syntax

system resources routing *routes hosts interfaces*

no system resources routing

Parameters

- **routes**—Specifies the maximum number of remote networks in the routing table.
- **hosts**—Specifies the maximum number of directly attached hosts.
- **interfaces**—Specifies the maximum number of IP interfaces.

Default Configuration
Hosts: 200, Routes: 64, IP Interfaces: 32

Command Mode
Global Configuration mode

User Guidelines
The settings are effective after reboot.

Example
The following example configures the routing table maximum size.

```
Console# system resources routing 20 23 5
```

show system resources routings

The **show system resources routings** EXEC mode command displays system routing resources information.

Syntax
show system resources routings

Command Mode
EXEC mode

Example
The following example displays the system routing resources information.

```
Console> show system resources routings

Parameters          Current value         After reboot Value
--------------      ----------------      ------------------
Hosts:              100                   100
Routes:             32                    32
IP Interfaces:      32                    32
```

show system tcam utilization

The **show system tcam utilization** EXEC mode command displays the Ternary Content Addressable Memory (TCAM) utilization.

Syntax
show system tcam utilization [*unit unit*]

Parameters
unit unit—Specifies the unit number. (Range: 1–8)

Command Mode
EXEC mode

Example
The following example displays TCAM utilization information.

```
Console> show system tcam utilization
System: 75%

Unit   TCAM utilization [%]
----   --------------------
1      58
2      57
```

show system defaults

Use the **show system defaults** command to display system defaults.

Syntax

show system defaults [*section*]

Parameters

section—Show information for specific session only. Available values are: management, 802.1x, port, fdb, port-mirroring, spanning-tree, vlan, voice-vlan, ip-addressing, network-security and qos-acl.

Command Mode

EXEC mode

Examples

```
console# show system defaults
System Mode: Router
Maximum units in stack: 8
# Management defaults
Telnet: Enabled (Maximum 4 sessions, shared with SSH)
SSH: Enabled (Maximum 4 sessions, shared with Telnet)
HTTP: Enabled, port 80 (Maximum 27 sessions)
HTTPS: Disabled
SNMP: Enabled.
      User: first
SNMP version: V3
SNMP Local Engine ID: 0000000001
SNMP Notifications: Enabled
SNMP Authentication Notifications: Enabled
Console: Enabled.
Cryptographic keys are not generated
HTTPS certificate is not generated
Management ACL: No ACL is defined
AAA Telnet authentication login: Local user data base
```

```
AAA HTTP authentication login: Local data base
AAA HTTPS authentication login: Local data base
Radius accounting: Disabled
Radius: No server is defined
Tacacs: No server is defined
Syslog: No server is defined
Logging: Enabled
Logging to console: Informational messages
Logging to internal buffer: Informational messages
Logging to file: Error messages
Logging to remote server: Informational messages
Maximum no. of syslog messages: 200
SNTP: supported
SNTP Port No.: 123
SNTP Interface: Enabled
IP Domain Naming System: Enabled
DHCP Server: Enabled
DHCP Auto Configuration: Enabled
DHCP Option 67: Enabled
DHCP Option 82: Disabled

# IPv6 defaults

# 802.1x defaults
802.1X is disabled
Mode: Multiple host
Guest VLAN: Not defined

# Interface defaults in present unit
48 GE regular
2 10G fiberOptics
PoE: Enabled
POE mode: Port Limit
Duplex: Full
Negotiation: Enabled
Flow control: Off
```

```
Mdix mode: auto
LAGs: No LAG is defined
Storm control: Disabled
Storm control mode: unknown unicast, broadcast, multicast
Port security: Disabled
LLDP: Enabled
LLDPDU Handeling: Filtering
Jumbo frames: Disabled
Port-Channel Load Balancing: Layer 2

# Bridging defaults
Maximum 16K entries
Aging time: 5 minutes
iSCSI: Enabled
iSCSI cos: 5, with no remark

# Multicast defaults
Multicast filtering: Disabled
IGMP snooping: Disabled
IGMP Querier: Disabled
Multicast TV Vlan Interface: disabled

# Port monitoring defaults
Port monitor is not defined
Maximum source port: 4
Maximum destination ports for mirroring: 2

# Spanning tree defaults
Spanning tree is Enabled
Spanning tree mode is Classic
Spanning tree interface: Enabled
Port fast: Disabled
BPDU handling: Filtering
BPDU Guard: Disabled

# Vlan defaults
```

```
Maximum Vlans: 4094
Default VLAN: Enabled
Default VLAN id: 1
GVRP: Disabled
Port mode: undefined
PVID: 1
VLAN membership: 1

# Voice vlan defaults
Voice VLAN: Disabled
Cos: 6 with no remark
OUI table:
00:E0:BB    3COM
00:03:6B    Cisco
00:E0:75    Veritel
00:D0:1E    Pingtel
00:01:E3    Simens
00:60:B9    NEC/Philips
00:0F:E2    Huawei-3COM
00:09:6E    Avaya

# Network security defaults
DHCP snooping: Disabled
ARP inspection: Disabled
ARP inspection Validation: Disabled

# DOS attacks

# IP addressing defaults
No IP interface is defined

# QOS and ACLs defaults
QoS mode is basic
QoS Basic Trust Mode: CoS
QoS Advanced Trust Mode: CoS-DSCP
Queue default mapping:
```

```
cos  qid:
 0    2
 1    1
 2    1
 3    3
 4    4
 5    5
 6    6
 7    7
```

show tech-support

Use the **show tech-support** command to display system and configuration information you can provide to the Technical Assistance Center when reporting a problem.

Syntax

show tech-support [*config*] [*memory*]

Parameters

Memory—Displays memory and processor state data.

Config—Displays switch configuration within the CLI commands supported on the device.

Default Configuration

By default, this command displays the output for technical-support-related show commands. Use keywords to specify the type of information to be displayed. If you do not specify any parameters, the system displays all configuration and memory data.

Command Types

Switch command.

Command Mode

EXEC mode

User Guidelines

Caution: Avoid running multiple **show tech-support** commands on a switch or multiple switches on the network segment. Doing so may cause starvation of some time sensitive protocols, like STP.

The show tech-support command may timeout if the configuration file output takes longer to display than the configured session timeout time. If this happens, enter a set logout timeout value of **0** to disable automatic disconnection of idle sessions or enter a longer timeout value.

The show tech-support command output is continuous, it does not display one screen at a time. To interrupt the output, press Esc.

If you specify the **config** keyword, the show tech-support command displays a list of the commands supported on the device.

```
If user specifies the memory keyword, the show tech-support command
displays the output:
flash info (dir if existed, or flash mapping)
show bootvar
buffers info (like print os buff)
memory info (like print os mem)
proc info (lie print os tasks)
versions of software components
show cpu utilization
```

system fans always-on

Use the **system fans always-on** Global Configuration command to set the system fans to On regardless of device temperature. Use the **no** form of the command to return to default.

Syntax

system fans always-on [*unit unit*]

no system fans always-on

Parameters

unit unit—Unit number or all. If unspecified, defaults to all. (Range: 1–8)

Default Configuration
Automatic mode; The system fan speed depends on the temperature of the device.

Command Mode
Global Configuration mode

show system fans

Use the **show system fans** EXEC command to view the fans' status

Syntax
show system fans

Command Mode
EXEC mode

Example

```
console>show system fans
Unit  Temperature       Speed       Admin state      Oper state
      (Celsius)         (RPM)
---   ---------------  ----------  --------------    -----------
1     30                8000        auto              on
2     40                8000        on                on
```

asset-tag

The **asset-tag** Global Configuration mode command assigns an asset-tag to a device. Use the **no** form of this command to restore the default setting.

Syntax
asset-tag [**unit** *unit*] *tag*

no asset-tag [**unit** *unit]*

Parameters

- **unit** —Specifies the unit number. (Range: 1–8)
- **tag**—Specifies the device asset-tag.

Default Configuration
No asset tag is defined.

The default unit number is the master unit number.

Command Mode
Global Configuration mode

Example
The following example assigns the asset-tag 2365491870 to the device.

```
Console(config)# asset-tag 2365491870
```

show system id

The **show system id** EXEC mode command displays the system identity information.

Syntax
show system id [*unit unit*]

Parameters
unit unit—Specifies the unit number. (Range: 1–8)

Command Mode
EXEC mode

Example

The following example displays the system identity information.

```
Console> show system id
Unit             Service tag      Serial number  Asset tag
------           ------------     ------------    -----------
1                89788978         8936589782     7843678957
2                                 3216523877     5621987728
```

5

Clock Commands

clock set

The **clock set** Privileged EXEC mode command manually sets the system clock.

Syntax

clock set *hh:mm:ss* {[*day month*] | [*month day*]} *year*

Parameters

- **hh:mm:ss**—Specifies the current time in hours (military format), minutes, and seconds. (Range: hh: 0-23, mm: 0-59, ss: 0-59)
- **day**—Specifies the current day of the month. (Range: 1-31)
- **month**—Specifies the current month using the first three letters of the month name. (Range: Jan–Dec)
- **year**—Specifies the current year. (Range: 2000–2037)

Command Mode

Privileged EXEC mode

User Guidelines

The user should enter the local clock time and date.

Example

The following example sets the system time to 13:32:00 on March 7th, 2005.

```
Console# clock set 13:32:00 7 Mar 2005
```

clock source

The **clock source** Global Configuration mode command configures an external time source for the system clock. Use the **no** form of this command to disable the external time source.

Syntax

clock source {**sntp**}

no clock source

Parameters

sntp—Specifies that an SNTP server is the external clock source.

Default Configuration

There is no external clock source.

Command Mode

Global Configuration mode

Example

The following example configures an SNTP server as an external time source for the system clock.

```
Console(config)# clock source sntp
```

clock timezone

Use the **clock timezone** Global Configuration command to set the time zone for display purposes. Use the **no** form of this command to set the time to Coordinated Universal Time (UTC) or Greenwich Mean Time (GMT), which is the same.

Syntax

clock timezone *zone hours-offset [minutes-offset]*

no clock timezone

Parameters

- **zone**—The acronym of the time zone.(Range: Up to 4 characters)
- **hours-offset**—Hours difference from UTC. (Range: (-12)–(+13))
- **minutes-offset**—Minutes difference from UTC. (Range: 0–59)

Default Configuration

Offset is **0**.

Acronym is empty.

Command Mode

Global Configuration mode

User Guidelines

The system internally keeps time in UTC, so this command is used only for display purposes and when the time is manually set.

Example

```
console(config)# clock timezone abc +2 minutes 32
```

clock summer-time

Use one of the formats of the **clock summer-time** Global Configuration command to configure the system to automatically switch to summer time (daylight saving time). Use the **no** form of this command to configure the software not to automatically switch to summer time.

Syntax

clock summer-time *zone recurring {usa | eu | {week day month hh:mm week day month hh:mm}} [offset]*

clock summer-time *zone date date month year hh:mm date month year hh:mm [offset]*

clock summer-time *zone date month date year hh:mm month date year hh:mm [offset]*

no clock summer-time

Parameters

- **zone**—The acronym of the time zone to be displayed when summer time is in effect. (Range: Up to 4 characters)
- **recurring**—Indicates that summer time should start and end on the corresponding specified days every year.
- **date**—Indicates that summer time should start on the first specific date listed in the command and end on the second specific date in the command.
- **usa**—The summer time rules are the United States rules.
- **eu**—The summer time rules are the European Union rules.
- **week**—Week of the month. Can be 1–4, first, last.
- **day**—Day of the week (first three letters by name, such as Sun). (characters)
- **date**—Date of the month. (Range: 1–31)
- **month**—Month (first three letters by name, such as Feb). (characters)
- **year**—year (no abbreviation). (Range: 2000–2097)
- **hh:mm**—Time (military format) in hours and minutes. (Range: hh:mmhh: 0-23, mm: 0-59)
- offset—Number of minutes to add during summer time (default is 60). (Range: 1440)

Default Configuration

Summer time is disabled.

Command Mode

Global Configuration mode

User Guidelines

In both the date and recurring forms of the command, the first part of the command specifies when summer time begins, and the second part specifies

when it ends. All times are relative to the local time zone. The start time is relative to standard time. The end time is relative to summer time. If the starting month is chronologically after the ending month, the system assumes that you are in the southern hemisphere.

USA rule for daylight saving time:

- From 2007:
  - Start: Second Sunday in March
  - End: First Sunday in November
  - Time: 2 am local time
- Before 2007:
  - Start: First Sunday in April
  - End: Last Sunday in October
  - Time: 2 am local time

Example

```
console(config)# clock summer-time abc date apr 1 2010 09:00 aug 2 2010
09:00
```

```
EU rule for daylight saving time:
```

- Start: Last Sunday in March
- End: Last Sunday in October
- Time: 1.00 am (01:00) Greenwich Mean Time (GMT)

sntp authentication-key

The **sntp authentication-key** Global Configuration mode command defines an authentication key for Simple Network Time Protocol (SNTP). Use the **no** form of this command to remove the authentication key for SNTP.

Syntax

sntp authentication-key *key-number* **md5** *key-value*

no sntp authentication-key *key-number*

Parameters

- **key-number**—Specifies the key number. (Range: 1–4294967295)
- **key-value**—Specifies the key value. (Length: 1–8 characters)

Default Configuration
No authentication key is defined.

Command Mode
Global Configuration mode

Examples
The following example defines the authentication key for SNTP.

```
Console(config)# sntp authentication-key 8 md5 ClkKey
```

```
Device(config)# sntp authentication-key 8 md5 ClkKey
Device(config)# sntp trusted-key 8
Device(config)# sntp authenticate
```

sntp authenticate

The **sntp authenticate** Global Configuration mode command enables authentication for received Simple Network Time Protocol (SNTP) traffic from servers. Use the **no** form of this command to disable the feature.

Syntax
sntp authenticate

no sntp authenticate

Default Configuration
Authentication is disabled.

Command Mode
Global Configuration mode

User Guidelines
The command is relevant for both unicast and broadcast.

Examples
The following example enables authentication for received SNTP traffic.

```
Console(config)# sntp authenticate
```

```
Device(config)# sntp authentication-key 8 md5 ClkKey
Device(config)# sntp trusted-key 8
Device(config)# sntp authenticate
```

sntp trusted-key
The **sntp trusted-key** Global Configuration mode command authenticates the system identity with which Simple Network Time Protocol (SNTP) synchronizes. Use the **no** form of this command to disable system identity authentication.

Syntax
sntp trusted-key *key-number*

no sntp trusted-key *key-number*

Parameters
key-number—Specifies the key number of the authentication key to be trusted. (Range: 1–4294967295)

Default Configuration
No keys are trusted.

Command Mode
Global Configuration mode

User Guidelines
The command is relevant for both received unicast and broadcast.

Examples
The following example authenticates key 8.

```
Console(config)# sntp trusted-key 8
```

```
Device(config)# sntp authentication-key 8 md5 ClkKey
Device(config)# sntp trusted-key 8
Device(config)# sntp authenticate
```

sntp client poll timer

The **sntp client poll timer** Global Configuration mode command sets the polling time for the Simple Network Time Protocol (SNTP) client. Use the no form of this command to restore the default configuration.

Syntax
sntp client poll timer *seconds*

no sntp client poll timer

Parameters
seconds—Specifies the polling interval in seconds. (Range: 60–86400)

Default Configuration
The default polling interval is 1024 seconds.

Command Mode
Global Configuration mode

Example
The following example sets the polling time for the SNTP client to 120 seconds.

```
Console(config)# sntp client poll timer 120
```

sntp broadcast client enable

The **sntp broadcast client enable** Global Configuration mode command enables Simple Network Time Protocol (SNTP) broadcast clients. Use the no form of this command to disable SNTP broadcast clients.

Syntax

sntp broadcast client enable

no sntp broadcast client enable

Default Configuration

The SNTP broadcast client is disabled.

Command Mode

Global Configuration mode

User Guidelines

Use the **sntp client enable** Interface Configuration mode command to enable the SNTP client on a specific interface.

Example

The following example enables the SNTP broadcast clients.

```
Console(config)# sntp broadcast client enable
```

sntp anycast client enable

The **sntp anycast client enable** Global Configuration mode command enables the SNTP anycast client. Use the **no** form of this command to disable the SNTP anycast client.

Syntax

sntp anycast client enable

no sntp anycast client enable

Default Configuration
The SNTP anycast client is disabled.

Command Mode
Global Configuration mode

User Guidelines
The polling time is configured with the **sntp client poll timer** Global Configuration mode command.

Use the **sntp client enable** Interface Configuration mode command to enable the SNTP client on a specific interface.

Example
The following example enables SNTP anycast clients.

```
Console(config)# sntp anycast client enable
```

sntp client enable

The **sntp client enable** Global Configuration mode command enables the Simple Network Time Protocol (SNTP) broadcast and anycast client on an interface. Use the **no** form of this command to disable the SNTP client.

Syntax
sntp client enable {*interface-id*}

no sntp client enable {*interface-id*}

Parameters
interface-id—Specifies an interface ID, which can be one of the following types: Ethernet port, Port-channel or VLAN.

Default Configuration
The SNTP client is disabled on an interface.

Command Mode
Global Configuration mode

User Guidelines

The **sntp broadcast client enable** Global Configuration mode command globally enables broadcast clients.

The **sntp anycast client enable** Global Configuration mode command globally enables anycast clients.

Example

The following example enables the SNTP broadcast and anycast client on gigabitethernet port gi1/0/3

```
Console(config)# sntp client enable gigabitethernet 1/0/3
```

sntp client enable (Interface)

To enable the Simple Network Time Protocol (SNTP) broadcast and anycast client on an interface, use the **sntp client enable** Interface Configuration command. Use the **no** form of this command to disable the SNTP client.

The **sntp client enable** Interface Configuration (Ethernet, Port-channel, VLAN) mode command enables the Simple Network Time Protocol (SNTP) broadcast and anycast client on an interface. Use the **no** form of this command to disable the SNTP client.

Syntax

sntp client enable

no sntp client enable

Default Configuration

The SNTP client is disabled on an interface.

Command Mode

Interface Configuration (Ethernet, Port-channel, VLAN) mode

User Guidelines

The **sntp broadcast client enable** Global Configuration mode command globally enables broadcast clients.

The **sntp anycast client enable** Global Configuration mode command globally enables anycast clients.

Example
The following example enables the SNTP broadcast and anycast client on an interface.

```
Console(config-if)# sntp client enable
```

sntp unicast client enable

The **sntp unicast client enable** Global Configuration mode command enables the device to use Simple Network Time Protocol (SNTP) predefined unicast clients. Use the **no** form of this command to disable the SNTP unicast clients.

Syntax
sntp unicast client enable

no sntp unicast client enable

Default Configuration
The SNTP unicast client is disabled.

Command Mode
Global Configuration mode

User Guidelines
Use the **sntp server** Global Configuration mode command to define SNTP servers.

Example
The following example enables the device to use Simple Network Time Protocol (SNTP) unicast clients.

```
Console(config)# sntp unicast client enable
```

sntp unicast client poll

The **sntp unicast client poll** Global Configuration mode command enables polling for the Simple Network Time Protocol (SNTP) predefined unicast clients. Use the **no** form of this command to disable the polling for the SNTP client.

Syntax

sntp unicast client poll

no sntp unicast client poll

Default Configuration

Polling is disabled.

Command Mode

Global Configuration mode

User Guidelines

Polling time is configured with the **sntp client poll timer** Global Configuration mode command.

Example

The following example enables polling for SNTP predefined unicast clients.

```
Console(config)# sntp unicast client poll
```

sntp server

The **sntp server** Global Configuration mode command configures the device to use the Simple Network Time Protocol (SNTP) to request and accept Network Time Protocol (NTP) traffic from a specified server. Use the **no** form of this command to remove a server from the list of SNTP servers.

Syntax

sntp server {*ipv4-address* | *ipv6-address* | *ipv6z-address* | *hostname*} [*poll*] [*key keyid*]

no sntp server {*ipv4-address* | *ipv6-address* | *ipv6z-address* | *hostname*}

Parameters

- **ipv4-address**—Specifies the server IPv4 address.
- **ipv6-address**—Specifies the server IPv6 address. A Link Local address (IPv6Z address) can be defined.
- **pv6z-address**—Specifies the IPv6Z address to ping. The IPv6Z address format is: *ipv6-link-local-address*}%{*interface-name*}. The subparameters are:
  - **ipv6-link-local-address**—Specifies the IPv6 Link Local address.
  - **interface-name**—Specifies the outgoing interface name. The interface name has the format: *vlan* {*integer*} | *ch* {*integer*} | *isatap* {*integer*} | {*physical-port-name*}. The subparameter integer has the format: {*decimal-digit*} | {*integer*}{*decimal-digit*}. (Range for the decimal-digit: 0–9)
- **hostname**—Specifies the server hostname. Only translation to IPv4 addresses is supported. (Length: 1–158 characters. Maximum label length: 63 characters)
- **poll**—Enables polling.
- **key keyid**—Specifies the Authentication key to use when sending packets to this peer. (Range:1–4294967295)

Default Configuration
No servers are defined.

Command Mode
Global Configuration mode

User Guidelines
Up to 8 SNTP servers can be defined.

The **sntp unicast client enable** Global Configuration mode command enables predefined unicast clients.

The **sntp unicast client poll** Global Configuration mode command globally enables polling.

Polling time is configured with the **sntp client poll timer** Global Configuration mode command.

The format of an IPv6Z address is: *<ipv6-link-local-address>%<interface-name>*.

interface-name = *vlan<integer> / ch<integer> / isatap<integer> / <physical-port-name> / 0*

integer = *<decimal-number> / <integer><decimal-number>*

decimal-number = *0 / 1 / 2 / 3 / 4 / 5 / 6 / 7 / 8 / 9*

physical-port-name = Designated port number, for example:gi1/0/16.

If the egress interface is not specified, the default interface is selected. Specifying interface zone=0 is equal to not defining an egress interface.

Example

The following example configures the device to accept SNTP traffic from the server on 192.1.1.1.

```
Console(config)# sntp server 192.1.1.1
```

sntp port

The **sntp port** Global Configuration mode command specifies a Simple Network Time Protocol (SNTP) User Datagram Protocol (UDP) port. Use the **no** form of this command to use the SNTP server default port.

Syntax

sntp port *port-number*

no sntp port

Parameters

port-number—Specifies the UDP port number used by an SNTP server. (Range 1–65535)

Default Configuration

The default port number is 123.

Command Mode
Global Configuration mode

Example
The following example specifies that port 321 of the SNTP server is the UDP port.

```
Console(config)# sntp port 321
```

show clock

The **show clock** EXEC mode command displays the time and date from the system clock.

Syntax
show clock [*detail*]

Parameters
detail—Displays the TimeZone and SummerTime configuration.

Command Mode
EXEC mode

Example
The following example displays the system time and date.

```
Console> show clock
15:29:03 PDT(UTC-7) Jun 17 2002
Time source is SNTP

Console> show clock detail
15:29:03 PDT(UTC-7) Jun 17 2002
Time source is SNTP

Time zone:
```

```
Acronym is PST
Offset is UTC-8

Summertime:
Acronym is PDT
Recurring every year.
Begins at first Sunday of April at 2:00.
Ends at last Sunday of October at 2:00.
Offset is 60 minutes.

DHCP timezone: Disabled
```

```
Device> show clock detail
15:29:03 PDT(UTC-7) Jun 17 2002
Time source is SNTP

Timezone (DHCP):
Acronym is PST
Offset is UTC-8

Timezone (static):
Acronym is PST
Offset is UTC-8

Summertime (Static):
Acronym is PDT
Recurring every year.
Begins at first Sunday of April at 2:00.
Ends at last Sunday of October at 2:00.
Offset is 60 minutes.

DHCP timezone: Enabled
```

show sntp configuration

The **show sntp configuration** Privileged EXEC mode command displays the Simple Network Time Protocol (SNTP) configuration on the device.

Syntax

show sntp configuration

Command Mode

Privileged EXEC mode

Example

The following example displays the device's current SNTP configuration.

```
console# show sntp configuration
SNTP port : 123 .
Polling interval: 1024 seconds.
No MD5 authentication keys.
Authentication is not required for synchronization.
No trusted keys.
Unicast Clients: Enabled
Unicast Clients Polling: Enabled
Server              Polling   Encryption Key
--------------------------- ---------- --------------
1.1.1.121            Disabled     Disabled
Broadcast Clients: disabled
Anycast Clients: disabled
No Broadcast Interfaces.
console#
```

show sntp status

The **show sntp status** Privileged EXEC mode command displays the Simple Network Time Protocol (SNTP) servers status.

Syntax
show sntp status

Command Mode
Privileged EXEC mode

Example
The following examples display the SNTP servers status.

```
Console# show sntp status

Clock is synchronized, stratum 4, reference is 176.1.1.8, unicast
Reference time is AFE2525E.70597B34 (00:10:22.438 PDT Jul 5 1993)

Unicast servers:
Server        Status      Last response           Offset     Delay
                                                  [mSec]     [mSec]
--------      -------     --------------------    -----      ------
176.1.1.8     Up          19:58:22.289            7.33       117.79
                          PDT Feb 19 2005


176.1.8.17    Unknown     12:17.17.987            8.98       189.19
                          PDT Feb 19 2005
Anycast server:
Server        Interface   Status   Last response  Offset     Delay
                                                  [mSec]     [mSec]
--------      -------     -----    -------------  -----      ------
176.1.11.8    VLAN 118    Up       9:53:21.789    7.19       119.89
                                   PDT Feb 19
                                   2005
Broadcast:
Server        Interface           Last response
---------     ---------           ----------------------------
176.9.1.1     VLAN 119            19:17:59.792
                                  PDT Feb 19 2002
```

```
Device# show sntp status
Clock is synchronized, stratum 4, reference is 176.1.1.8, unicast
Reference time is AFE2525E.70597B34 (00:10:22.438 PDT Jul 5 1993)
```

6

Configuration/Image File Commands

copy

The **copy** Privileged EXEC mode command copies files from a source to a destination.

Syntax

copy *source-url destination-url [snmp]*

Parameters

- **source-url**—Specifies the source file location URL or source file reserved keyword to be copied. (Length: 1–160 characters)
- **destination-url**—Specifies the destination file URL or destination file reserved keyword. (Length: 1–160 characters)
- **snmp**—Specifies that the destination/source file is in SNMP format. Used only when copying from/to startup-config.

The following table displays URL options.

Keyword	Source or Destination
flash://	Source or destination URL for flash memory. This is the default URL If a URL is specified without a prefix.
running-config	Currently running configuration file.
startup-config	Startup configuration file.
image	Image file. If specified as the source file, it is the active image file. If specified as the destination file, it is the non-active image file.

Keyword	Source or Destination
boot	Boot file.
tftp://	Source or destination URL for a TFTP network server. The syntax for this alias is *tftp://host/[directory]/filename*. The host can be either an IP address or a host name.
usb://	Copy to a file on the USB device. The syntax is: usb://*directory*/*filename*
xmodem:	Source for the file from a serial connection that uses the Xmodem protocol.
unit://*member*/**image**	Image file on one of the units. To copy from the master to all units, specify * in the member field.
unit://*member*/**boot**	Boot file on one of the units. To copy from the master to all units, specify * in the member field
unit://*member*/**startup-config**	Configuration file used during initialization (startup) on one of the units.
null:	Null destination for copies or files. A remote file can be copied to null to determine its size.
mirror-config	Mirrored configuration file
WORD<1-128>	Specify URL prefixes.

Command Mode

Privileged EXEC mode

User Guidelines

The location of a file system dictates the format of the source or destination URL.

The entire copying process may take several minutes and differs from protocol to protocol and from network to network.

If the IPv6 address is a Link Local address (IPv6Z address), the outgoing interface name must be specified. The format of an IPv6Z address is: {*ipv6-link-local-address*}%{*interface-name*}. The subparameters are:

- **ipv6-link-local-address**—Specifies the IPv6 Link Local address.

- **interface-name**—Specifies the outgoing interface name. The interface name has the format: *vlan*{*integer*} | *ch*{*integer*} | *isatap{integer*} | {*physical-port-name*}.The subparameter *integer* has the format: {*decimal-digit*} | {*integer*}{*decimal-digit*}. *decimal-digit* has the range 0–9

If the egress interface is not specified, the default interface is selected. Specifying **interface zone=0** is equal to not defining an egress interface.

Understanding Invalid Combinations of Source and Destination

Some invalid combinations of source and destination exist. Specifically, if one of the following conditions exists:

- The source file and destination file are the same file.
- **xmodem:** is the destination file. The source file can be copied to **image**, **boot** and **null:** only.
- **tftp://** is the source file and destination file on the same copy.
- ***.prv** files cannot be copied.
- The source or destination is a slave unit (except for image and boot files).
- **mirror-config** cannot be used as a destination

The following table describes the copy characters:

Character	Description
!	For network transfers, indicates that the copy process is taking place. Each exclamation point indicates successful transfer of ten packets (512 bytes each).
.	For network transfers, indicates that the copy process timed out. Generally, several periods in a row means that the copy process may fail.s

Copying an Image File from a Server to Flash Memory

Use the **copy** *source-url* **image** command to copy an image file from a server to flash memory.

Copying a Boot File from a Server to Flash Memory

Use the **copy** *source-url* **boot** command to copy a boot file from a server to flash memory.

Copying a Configuration File from a Server to the Running Configuration File

Use the **copy** *source-url* **running-config** command to load a configuration file from a network server to the running device configuration file. The commands in the loaded configuration file are added to those in the running configuration file as if the commands were typed in the command-line interface (CLI). The resulting configuration file is a combination of the previous running configuration and the loaded configuration files, with the loaded configuration file taking precedence.

Copying a Configuration File from a Server to the Startup Configuration

Use the **copy** *source-url* **startup-config** command to copy a configuration file from a network server to the device startup configuration file. The startup configuration file is replaced by the copied configuration file.

Storing the Running or Startup Configuration on a Server

Use the **copy running-config** *destination-url* command to copy the current configuration file to a network server using TFTP, .

Use the **copy startup-config** *destination-url* command to copy the startup configuration file to a network server.

Saving The Running Configuration To The Startup Configuration

Use the **copy running-config startup-config** command to copy the running configuration to the startup configuration file.

-Backing Up the Running Configuration or Startup Configuration to a Backup Configuration file

Use the **copy running-config** *file* command to back up the running configuration to a backup configuration file.

Use the **copy startup-config** *file* command to back up the startup configuration to a backup configuration file.

Examples

The following example copies system image file1 from the TFTP server 172.16.101.101 to a non-active image file.

```
Console# copy tftp://172.16.101.101/file1 image

Accessing file 'file1' on 172.16.101.101...
```

```
Loading file1 from 172.16.101.101:
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!! [OK]
Copy took 0:01:11 [hh:mm:ss]
```

Copying an Image from a Server to Flash Memory

The following example copies a system image named file1 from the TFTP server with an IP address of 172.16.101.101 to a non-active image file.

```
Router# copy tftp://172.16.101.101/file1 image
Accessing file 'file1' on 172.16.101.101...
Loading file1 from 172.16.101.101:
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!! [OK]
Copy took 0:01:11 [hh:mm:ss]
```

write memory

Use the **write memory** Privileged EXEC mode command to save the running configuration to the startup configuration file.

Syntax
write memory

Parameters
This command has no arguments or keywords.

Command Mode
Privileged EXEC mode

Examples
The following example copies system image file1 from the TFTP server 172.16.101.101 to a non-active image file.

```
Console# write memory
```

Overwrite file [startup-config] ?[Yes/press any key for no]....15-Sep-2010 11:27

:48 %COPY-I-FILECPY: Files Copy - source URL running-config destination URL flas

h://startup-config

15-Sep-2010 11:27:50 %COPY-N-TRAP: The copy operation was completed successfully

Copy succeeded

delete

The **delete** Privileged EXEC mode command deletes a file from a flash memory device.

Syntax
delete *url*

Parameters

url—Specifies the location URL or reserved keyword of the file to be deleted. (Length: 1–160 characters)

The following table displays keywords and URL prefixes:

Keyword	Source or Destination
flash://	URL of the flash memory. This is the default URL if a URL is specified without a prefix.
usb://	URL of the USB memory.
startup-config	Startup configuration file.
WORD	Specify URL prefixes.

Command Mode

Privileged EXEC mode

User Guidelines

*.sys, *.prv, **image-1** and **image-2** files cannot be deleted.

Example

The following example deletes the file called 'test' from the flash memory.

```
Console# delete flash:test
Delete flash:test? [confirm]
```

pwd

Use the **pwd** Privileged EXECmode command to display a full, clarified path to the current directory.

Parameters

This command has no arguments or keywords.

Command Mode

EXEC mode

dir

The **dir** Privileged EXEC mode command displays the list of files on a flash file system.

Syntax

dir

dir *[directory-path]*

Command Mode

Privileged EXEC mode

Example

The following example displays the list of files on a flash file system

```
Total size of flash: 33292288 bytes
Free size of flash: 20708893 bytes


console# dir
Directory of flash:

File Name      Permission  Size  Data Size  Modified
               Flash
------------------ ----------   ---------- --------------------
tmp            rw       524288      104     01-Jan-2010 05:35:04
image-1        rw      10485760  10485760   01-Jan-2010 06:10:23
image-2        rw      10485760  10485760   01-Jan-2010 05:43:54
dhcpsn.prv     --       262144      --      01-Jan-2010 05:25:07
sshkeys.prv    --       262144      --      04-Jan-2010 06:05:00
syslog1.sys    r-       524288      --      01-Jan-2010 05:57:00
syslog2.sys    r-       524288      --      01-Jan-2010 05:57:00
directry.prv   --       262144      --      01-Jan-2010 05:25:07
startup-config rw       786432     1081     01-Jan-2010 10:05:34

Total size of flash: 66322432 bytes
Free size of flash: 42205184 bytes
```

```
console#
```

more

The **more** Privileged EXEC mode command displays a file.

Syntax

more *url*

Parameters

url—Specifies the location URL or reserved keyword of the source file to be displayed. (Length: 1–160 characters).

The following table displays options for the URL parameter:

Keyword	Source or Destination
flash://	Source or destination URL for flash memory. If a URL is specified without a prefix, this is the default URL.
running-config	Current running configuration file.
startup-config	Startup configuration file.
mirror-config	Mirrored configuration file.
usb:	Universal Serial Bus (USB) File System

Command Mode

Privileged EXEC mode

User Guidelines

Files are displayed in ASCII format, except for the images, which are displayed in a hexadecimal format.

***.prv** files cannot be displayed.

Example

The following example displays the running configuration file contents.

```
console# more running-config
no spanning-tree
interface range gi1/0/1-48
speed 1000
exit
no lldp run
line console
exec-timeout 0
exit
```

cd

Use the **cd** Privileged EXEC mode command to change the current directory.

cd *new-directory*

Parameters

new-directory—The new directory. The new directory path may be specificed as either a Full Clarified Path or a Relative Path.

Command Mode

Privileged EXEC mode

User Guidelines

When command **cd** changes the current file system, the current directory of the previous file system is saved and when the command specifying only the file system (for example, **cd usb:**) sets the file system as current, the current directory is restored.

Example

```
console cd usb://private/conf
console pwd
usb://private/conf
console cd ..
console pwd
usb://private
console# cd flash:
```

```
console pwd
flash://
console cd usb:
console pwd
usb://private
console# cd flash://
```
console pwd
```
flash:\\
console cd usb://
console pwd
usb://
```

rename

The **rename** Privileged EXEC mode command renames a file.

Syntax

rename *url new-url*

Parameters

- **url**—Specifies the file location URL. (Length: 1–160 characters)
- **new-url**—Specifies the file's new URL. (Length: 1–160 characters)

The following table displays options for the URL parameter:

Keyword	Source or Destination
flash://	URL for flash memory. If a URL is specified without a prefix, this is the default URL.
usb:	Universal Serial Bus (USB) File System
WORD	Specify URL prefixes.

Command Mode

Privileged EXEC mode

User Guidelines

***.sys** and ***.prv** files cannot be renamed.

Example
The following example renames the configuration file.

```
Console# rename configuration.bak m-config.bak
```

boot system

The **boot system** Privileged EXEC mode command specifies the active system image file that is loaded by the device at startup.

Syntax
boot system *{ image-1 | image-2 } [switch number | all]*

Parameters

- **switch number—**Specifies the unit number. If unspecified, defaults to the master unit number.
- **image-1**—Specifies that image-1 is loaded as the system image during the next device startup.
- **image-2**—Specifies that image-2 is loaded as the system image during the next device startup.

Default Configuration
This command has no default configuration.

The default unit number is the master unit number.

Command Mode
Privileged EXEC mode

User Guidelines
Use the **show bootvar** command to determine which image is the active image.

Example
The following example specifies that **image-1** is the active system image file loaded by the device at startup.

```
Console# boot system image-1
```

show running-config
The **show running-config** Privileged EXEC mode command displays the current running configuration file contents.

Syntax
show running-config

Parameters
This command has no arguments or keywords.

Command Mode
Privileged EXEC mode

Example
The following example displays the running configuration file contents.

```
Console# show running-config
no spanning-tree
interface range gi1/0/1-48
speed 1000
exit
no lldp run
interface vlan 1
ip address 1.1.1.1 255.0.0.0
exit
line console
exec-timeout 0
exit
console#
```

show startup-config

The **show startup-config** Privileged EXEC mode command displays the startup configuration file contents.

Syntax

show startup-config

Command Mode

Privileged EXEC mode

Example

The following example displays the startup configuration file contents.

```
Console# show startup-config
no spanning-tree
interface range gi1/0/1-48
speed 1000
exit
no lldp run
interface vlan 1
ip address 1.1.1.1 255.0.0.0
exit
line console
exec-timeout 0
exit
console#
```

show bootvar

The **show bootvar** EXEC mode command displays the active system image file that is loaded by the device at startup.

Syntax

show bootvar *[unit unit]*

Parameters

unit unit—Specifies the unit number.

Command Mode

EXEC mode

Example

The following example displays the active system image file that is loaded by the device at startup.

```
Console# show bootvar

Unit    Image     Filename   Version    Date                 Status
----    -----     --------   -------    -------------------  -----------
1       1         file1      3.1.31     23-Jul-2002          Active
                                        17:34:19

1       2         file2      3.2.19     22-Jan-2003          Not
                                        19:22:32             active*


2       1         file1      3.1.31     23-Jul-2002          Not active
                                        17:34:19


2       2         file2      3.2.19     22-Jan-2003          Active
                                        19:22:32

"*": Designates that the image was selected for the next boot.
```

7

Auto-Update and Auto-Configuration

boot host auto-config

Use the **boot host auto-config** Global Configuration mode command to enable the support of auto configuration via DHCP. Use the **no** form of this command to disable DHCP auto configuration.

Syntax

boot host auto-config

no boot host auto-config

Parameters

This command has no arguments or key words.

Command Mode

Global Configuration mode

Default Configuration

Enabled by default.

boot host auto-update

Use the **boot host auto-update** Global Configuration mode command to enable the support of auto updated via DHCP. Use the **no** form of this command to disable DHCP auto configuration.

Syntax

boot host auto-update

no boot host auto-update

Parameters

This command has no arguments or key words.

Command Mode

Global Configuration mode

Default Configuration

Enabled by default.

boot host dhcp

Use the **boot host dhcp** Global Configuration mode command to force the mechanism used to download a configuration file at the next system startup. Use the **no** form of this command to restore the host configuration file to the default.

Syntax

boot host dhcp

no boot host dhcp

Parameters

This command has no arguments or key words.

Command Mode

Global Configuration mode

User Guidelines

Configuring **boot host dhcp** does not take effect until the next reboot.

boot host auto-save

Use the **boot host auto-save** Global Configuration mode command to enable automatic saving Running in Startup after download. Use the **no** form of this command restore default behavior.

Syntax

boot host auto-save

no boot host auto-save

Parameters

This command has no arguments or key words.

Command Mode

Global Configuration mode

Default Configuration

Disable

show boot

Use the **show boot** Privilege EXEC mode command to show the status of the IP DHCP Auto Config process.

Syntax

show boot

Parameters

This command has no keywords or arguments.

Command Mode

Privilege EXEC mode

Examples

```
console# show boot
```

```
Auto Config
-----------
Config Download via DHCP: enable
Next Boot Config Download via DHCP: force

Auto Config State: Finished
TFTP Server IP address: 1.2.20.2
Configuration filename: /config/configfile1.cfg

      Auto Update
      -----------
Image Download via DHCP: enabled
```

```
console# show boot
Auto Config
-----------
Config Download via DHCP: enable
Next Boot Config Download via DHCP: default
Auto Config State: Opening <hostname>-config file

            Auto Update
            -------------
Image Download via DHCP: enabled
```

```
Example 3.
console# show boot
Auto Config
-----------
Config Download via DHCP: enable
Next Boot Config Download via DHCP: default
Auto Config State: Downloading configuration file

Auto Update
-----------
```

```
Image Download via DHCP: enabled
```

```
console# show boot
Auto Config
-----------
Config Download via DHCP: enable
Next Boot Config Download via DHCP: default
Auto Config State: Searching hostname in indirect configuration file

Auto Update
-----------
Image Download via DHCP: enabled
```

```
console# show boot
Auto Config
-----------
Config Download via DHCP: enable
Next Boot Config Download via DHCP: default
Auto Config State: Quit – failed all steps of finding existing
configuration file

Auto Update
-----------
Image Download via DHCP: enabled
```

```
console# show boot
Auto Config
-----------
Config Download via DHCP: enable
Next Boot Config Download via DHCP: default

Auto Update
-----------
Image Download via DHCP: enabled
Auto Update State: Downloaded indirect image file
```

```
console# show boot
Auto Config
-----------
Config Download via DHCP: enable
Next Boot Config Download via DHCP: default

Auto Update
-----------
Image Download via DHCP: enabled
Auto Update State: Downloading image file
```

```
console# show boot
Auto Config
-----------
Config Download via DHCP: enable
Next Boot Config Download via DHCP: default
Auto Config State: Finished
TFTP Server IP address: 1.2.20.2
Configuration filename: /config/configfile1.cfg


Auto Update
-----------
Image Download via DHCP: enabled
Auto Update State: Downloading image file
```

---

ip dhcp tftp-server ip addr

Use the **ip dhcp tftp-server ip addr** Global Configuration mode command to set the TFTP server's IP address, used by a switch when it has not been received from the DHCP server. Use the **no** form of this command to remove the address.

Syntax

ip dhcp tftp-server ip addr ip-addr

no ip dhcp tftp-server ip-addr

Parameters
ip-addr IP—Address of TFTP server

Default Configuration
No IP address

Command Mode
Global Configuration mode

ip dhcp tftp-server file

Use the **ip dhcp tftp-server file** Global Configuration mode command to set the full file name on the TFTP server by a switch when it has not been received from the DHCP server. Use the **no** form of this command to remove the name.

Syntax
ip dhcp tftp-server file *file-path*

no ip dhcp tftp-server file

Parameters
file-path—full file name on TFTP server

Default Configuration
No file name

Command Mode
Global Configuration mode

show ip dhcp tftp-server

Use the **show ip dhcp tftp-server** EXEC mode command to display information about the TFTP server.

Syntax
show ip dhcp tftp-server

Command Mode
EXEC

Example

```
console# show ip dhcp tftp server
tftp server address
active       1.1.1.1 from sname
manual       2.2.2.2
file path on tftp server
active       conf/conf-file from option 67
```

8

Management ACL Commands

management access-list

The **management access-list** Global Configuration mode command configures a management access list and enters the Management Access-List Configuration command mode. Use the **no** form of this command to delete an access list.

Syntax

management access-list *name*

no management access-list *name*

Parameters

name—Specifies the access list name. (Length: 1–32 characters)

Command Mode

Global Configuration mode

User Guidelines

Use this command to configure a management access list. This command enters the Management Access-List Configuration mode, where the denied or permitted access conditions are defined with the **deny** and **permit** commands.

If no match criteria are defined, the default value is **deny**.

When re-entering the access-list context, the new rules are entered at the end of the access list.

Use the **management access-class** command to select the active access list.

The active management list cannot be updated or removed.

For IPv6 management traffic that is tunneled in IPv4 packets, the management ACL is applied first on the external IPv4 header (rules with service field are ignored), and then again on the inner IPv6 header.

Example

The following example creates a management access list called **mlist**, configures management gigabitethernet interfaces 1/0/1 and 1/0/9, and makes the new access list the active list.

```
Console(config)# management access-list mlist
Console(config-macl)# permit gi1/0/1
Console(config-macl)# permit gi1/0/9
Console(config-macl)# exit
Console(config)# management access-class mlist
```

The following example creates a management access list called 'mlist', configures all interfaces to be management interfaces except `gigabitethernet interfaces 1/0/1 and 1/0/9`, and makes the new access list the active list.

```
Console(config)# management access-list mlist
Console(config-macl)# deny gigabitethernet 1/0/1
Console(config-macl)# deny gigabitethernet 1/0/9
Console(config-macl)# permit
Console(config-macl)# exit
Console(config)# management access-class mlist
```

permit (Management)

The **permit Management** Access-List Configuration mode command sets conditions for the management access list.

Syntax

permit *[interface-id] [service service]*

permit ip-source {*ipv4-address* | *ipv6-address*|*ipv6-prefix-length*} *[mask {mask | prefix-length}] [interface-id] [service service]*

Parameters

- interface-id:—Specify an interface ID. The interface ID can be one of the following types: Ethernet port, Port-channel or VLAN
- **service** *service* — Specifies the service type. Possible values are: Telnet, SSH, HTTP, HTTPS and SNMP.
- *ipv4-address*— Specifies the source IPv4 address.
- *ipv6-address/ipv6-prefix-length*— Specifies the source IPv6 address and source IPv6 address prefix length. The prefix length must be preceded by a forward slash (/). The parameter is optional.
- **mask** *mask* — Specifies the source IPv4 address network mask. This parameter is relevant only to IPv4 addresses.
- **mask** *prefix-length* — Specifies the number of bits that comprise the source IPv4 address prefix. The prefix length must be preceded by a forward slash (/). This parameter is relevant only to IPv4 addresses. (Range: 0–32)

Command Mode

Management Access-List Configuration mode

User Guidelines

Rules with ethernet, VLAN, and port-channel parameters are valid only if an IP address is defined on the appropriate interface.

Example

The following example permits all ports in the access list called **mlist**

```
Console(config)# management access-list mlist
Console(config-macl)# permit
```

deny (Management)

The **deny** Management Access-List Configuration mode command sets conditions for the management access list.

Syntax

deny *[interface-id] [service service]*

deny ip-source *{ipv4-address | ipv6-address/ipv6-prefix-length} [mask {mask | prefix-length}] [interface-id] [service service]*

Parameters

- **interface-id**—Specifies an interface ID. The interface ID can be one of the following types: Ethernet port, Port-channel or VLAN
- **service service**—Specifies the service type. Possible values are: Telnet, SSH, HTTP, HTTPS and SNMP.
- **ipv4-address**—Specifies the source IPv4 address.
- **ipv6-address/ipv6-prefix-length**—Specifies the source IPv6 address and source IPv6 address prefix length. The prefix length must be preceded by a forward slash (/). The parameter is optional.
- **mask mask**—Specifies the source IPv4 address network mask. The parameter is relevant only to IPv4 addresses.
- **mask prefix-length**—Specifies the number of bits that comprise the source IPv4 address prefix. The prefix length must be preceded by a forward slash (/). The parameter is relevant only to IPv4 addresses. (Range: 0–32)

Command Mode

Management Access-List Configuration mode

User Guidelines

Rules with ethernet, VLAN, and port-channel parameters are valid only if an IP address is defined on the appropriate interface.

Example

The following example denies all ports in the access list called **mlist**.

```
Console(config)# management access-list mlist
Console(config-macl)# deny
```

management access-class

The **management access-class** Global Configuration mode command restricts management connections by defining the active management access list. To disable management connection restrictions, use the **no** form of this command.

Syntax

management access-class {**console-only** | *name*}

no management access-class

Parameters

- **console-only**—Specifies that the device can be managed only from the console.
- **name**—Specifies the access list name to be used. (Length: 1–32 characters)

Default Configuration

The default configuration is no management connection restrictions.

Command Mode

Global Configuration mode

Example

The following example defines an access list called **mlist** as the active management access list.

```
Console(config)# management access-class mlist
```

show management access-list

The **show management access-list** Privileged EXEC mode command displays management access lists.

Syntax

show management access-list [*name*]

Parameters

name—Specifies the name of a management access list to be displayed. (Length: 1–32 characters)

Command Mode

Privileged EXEC mode

Example

The following example displays the **mlist** management access list.

```
Console# show management access-list mlist
console-only
------------
deny
! (Note: all other access implicitly denied)
mlist
-----
permit gi1/0/1
permit gi1/0/9
! (Note: all other access implicitly denied)
console#
```

show management access-class

The **show management access-class** Privileged EXEC mode command displays information about the active management access list.

Syntax

show management access-class

Command Mode

Privileged EXEC mode

Example

The following example displays the active management access list information.

```
Console# show management access-class
Management access-class is enabled, using access list mlist
```

9

SNMP Commands

snmp-server

Use the **snmp-server server** Global Configuration mode command to enable the device to be configured by SNMP. Use the **no** form of this command to disable this function.

Syntax

snmp-server server

no snmp-server server

Parameters

This command has no arguments or keywords.

Default

Enabled

Command Mode

Global Configuration mode

Example

```
snmp-server server
======================
console(config)# snmp-server server
```

snmp-server community

Use the **snmp-server community** Global Configuration mode command to set up the community access string to permit access to the Simple Network

Management Protocol command. Use the **no** form of this command to remove the specified community string.

Syntax

snmp-server community *string [view view-name] [ro | rw | su] {ipv4-address| ipv6-address} [mask | prefix-length] [type router | oob]*

snmp-server community-group *string group-name [ipv4-address| ipv6-address] [mask | prefix-length] [type router | oob]*

no snmp-server community *string [ipv4-address| ipv6-address]*

Parameters

- **string**—Community string that acts like a password and permits access to the SNMP protocol. (Range: 1–20 characters)
- **ro**—Specifies read-only access (default)
- **rw**—Specifies read-write access
- **su**—Specifies SNMP administrator access
- **view view-name**—Specifies the name of a view to be configured using the command **snmp-server view** (no specific order of the command configurations is imposed on the user). The view defines the objects available to the community. It is not relevant for **su**, which has access to the whole MIB. If unspecified, all the objects, except the community-table and SNMPv3 user and access tables, are available. (Range: 1–30 characters)
- **ipv4-address**—Management station IPv4 address. The default is all IP addresses.
- **ipv6-address**—Management station IPv4 address. The default is all IP addresses.
- **mask**—Specifies the mask of the IPv4 address. This is not a network mask, but rather a mask that defines which bits of the packet's source address are compared to the configured IP address. If unspecified, it defaults to 255.255.255.255. The command returns an error if the mask is specified without an IPv4 address.
- **prefix-length**—Specifies the number of bits that comprise the IPv4 address prefix. If unspecified, it defaults to 32. The command returns an error if the prefix-length is specified without an IPv4 address.

- **group-name**—Specifies the name of a group that should be configured using the command **snmp-server group** with v1 or v2 parameter (no specific order of the two command configurations is imposed on the user). The group defines the objects available to the community. (Range: 1–30 characters)
- **type router**—Specifies that SNMP requests for duplicate tables configure the router tables. This is the default.
- **type oob**—Specifies that SNMP requests for duplicate tables configure the oob tables.

Default
No community is defined

Command Mode
Global Configuration mode

User Guidelines
You can't specify view-name for su, which has access to the whole MIB.

You can use the view-name to restrict the access rights of a community string.

The logical key of the command is the pair (community, ip-address). If ip-address is omitted then the key is (community, All-Ips).

By specifying the view-name parameter, the software:

- Generates an internal security-name.
- Maps the internal security-name for SNMPv1 and SNMPv2 security models to an internal group-name.
- Maps the internal group-name for SNMPv1 and SNMPv2 security models to view-name (read-view and notify-view always, and for rw for write-view also),

You can use the group-name to restrict the access rights of a community string. By specifying the group-name parameter the software:

- Generates an internal security-name.
- Maps the internal security-name for SNMPv1 and SNMPv2 security models to the group-name.

The **snmp-server community-group** command and **snmp-server** user command for v1 and v2 are equivalent. You should use the **snmp-server community-group** command when you want to configure the ipv4-address|ipv6-address management addresses.

The Type keyword is used for a different purpose. Therefore, when defining an SNMP community, the administrator must indicate which tables are being configured. If Type is router, it means that the device's tables are being configured.

Example

```
snmp-server community
=========================
console(config)# snmp-server community abcd su 1.1.1.121 mask 255.0.0.0
console(config)# snmp-server community-group tom abcd 1.1.1.122 prefix 8
```

snmp-server view

The **snmp-server view** Global Configuration mode command creates or updates a Simple Network Management Protocol (SNMP) server view entry. Use the **no** form of this command to remove an SNMP server view entry.

Syntax

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

no snmp-server view *view-name* [*oid-tree*]

Parameters

- **view-name**—Specifies the label for the view record that is being created or updated. The name is used to reference the record. (Length: 1–30 characters)
- **oid-tree**—Specifies the ASN.1 subtree object identifier to be included or excluded from the view. To identify the subtree, specify a text string consisting of numbers, such as 1.3.6.2.4, or a word, such as System. Replace a single sub-identifier with the asterisk (*) wildcard to specify a subtree family; for example 1.3.*.4.
- **included**—Specifies that the view type is included.

- **excluded**—Specifies that the view type is excluded.

Default Configuration
Default and DefaultSuper are the default view names.

Command Mode
Global Configuration mode

User Guidelines
This command can be entered multiple times for the same view record.

The command logical key is the pair (view-name, oid-tree).

The number of views is limited to 64.

Default and DefaultSuper views are reserved for internal software use and cannot be deleted or modified.

Example
The following example creates a view that includes all objects in the MIB-II system group except for sysServices (System 7) and all objects for interface 1 in the MIB-II interface group.

```
Console(config)# snmp-server view user-view system included
Console(config)# snmp-server view user-view system.7 excluded
Console(config)# snmp-server view user-view ifEntry.*.1
included
```

snmp-server group

The **snmp-server group** Global Configuration mode command configures a new Simple Network Management Protocol (SNMP) group or a table that maps SNMP users to SNMP views. Use the **no** form of this command, remove a specified SNMP group.

Syntax
snmp-server group *groupname* {*v1 | v2 | v3 {noauth | auth | priv} [notify notifyview]*} *[read readview] [write writeview]*

no snmp-server group *groupname {v1 | v2 | v3 [noauth | auth | priv]} [context name]*

Parameters

- **groupname**—Specifies the group name. (Length: 1–30 characters)
- **v1**—Specifies the SNMP Version 1 security model.
- **v2**—Specifies the SNMP Version 2 security model.
- **v3**—Specifies the SNMP Version 3 security model.
- **noauth**—Specifies no packet authentication. Applicable only to the SNMP Version 3 security model.
- **auth**—Specifies packet authentication without encryption. Applicable only to the SNMP Version 3 security model.
- **priv**—Specifies packet authentication with encryption. Applicable only to the SNMP Version 3 security model.
- **notify notifyview**—Specifies the view name that enables specifying an inform or a trap. Applicable only to the SNMP Version 3 security model. (Length: 1–30 characters)
- **read readview**—Specifies the view name that enables viewing only the agent contents. (Length: 1–30 characters)
- **write writeview**—Specifies the view name that enables entering data and configuring the agent contents. (Length: 1–30 characters)

Default Configuration

No group entry exists.

If **notifyview** is not specified, nothing is defined for the notify view.

If **readview** is not specified, all objects except for the community-table and SNMPv3 user and access tables are available.

If **writeview** is not specified, nothing is defined for the write view.

Command Mode

Global Configuration mode

User Guidelines

The command logical key is (**groupname, snmp-version, security-level**). For snmp-version v1/v2 the security-level is always **noauth**.

The **Router** context is translated to "" context in the MIB.

Example

The following example attaches a group called user-group to SNMPv3 and assigns to the group the privacy security level and read access rights to a view called user-view.

```
Console(config)# snmp-server group user-group v3 priv read user-
view
```

snmp-server user

Use the **snmp-server user** Global Configuration mode command to configure a new SNMP Version 3 user. Use the **no** form of the command to remove a user.

Syntax

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

no snmp-server user *username [remote host]*

Parameters

- **username**—The name of the user on the host that connects to the agent. (Range: Up to 20 characters)
- **groupname**—The name of the group to which the user belongs. The group should be configured using the command **snmp-server group** with v3 parameters (no specific order of the 2 command configurations is imposed on the user). (Range: Up to 30 characters)
- **remote host**—IP address of the remote SNMP host.
- **v1**—Specifies that v1 is to be used.
- **v2c**—Specifies that v2c is to be used.

- **v3**—Specifies that v3 is to be used.
- **encrypted**—Specifies whether the password appears in encrypted format.
- **auth**—Specifies which authentication level is to be used.
- **md5**—Specifies the HMAC-MD5-96 authentication level.
- **Sha**—Specifies the HMAC-SHA-96 authentication level.
- **auth-password**—Specifies the authentication password.

Parameters Range engineid-string5 - 32 characters.

auth-passwordUp to 32 characters.

Default
No group entry exists.

Command Mode
Global configuration

User Guidelines
If **auth md5** or **auth sha** is specified, both authentication and privacy are enabled for the user.

When you enter a **show running-config** command, you do not see a line for this user. To see if this user has been added to the configuration, type the **show snmp user** command.

An SNMP EngineID should be defined in order to add users to the device.

Changing or removing the value of **snmpEngineID** deletes the SNMPv3 users' database.

The logical key of the command is Username.

Configuring a remote host is required in order to send informs to that host. A configured remote host is also able to manage the device (besides getting the informs)

To configure a remote user, specify the IP address for the remote SNMP agent of the device where the user resides. Also, before you configure remote users for a particular agent, configure the SNMP engine ID, using the **snmp-server engineID remote** command. The remote agent's SNMP engine ID is needed when computing the authentication and privacy digests from the password. If

the remote engine ID is not configured first, the configuration command fails.

Example

```
snmp-server user
====================
console(config)# snmp-server user tom acbd v1
console(config)# snmp-server user tom acbd v2c
console(config)# snmp-server engineid local default
The engine-id must be unique within your administrative domain.
Do you wish to continue? [Y/N]
y
The SNMPv3 database will be erased. Do you wish to continue? [Y/N]
y
console(config)# snmp-server user tom acbd v3
```

snmp-server filter

The **snmp-server filter** Global Configuration mode command creates or updates a Simple Network Management Protocol (SNMP) server filter entry. Use the **no** form of this command to remove the specified SNMP server filter entry.

Syntax

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

no snmp-server filter *filter-name* [*oid-tree*]

Parameters

- **filter-name**—Specifies the label for the filter record that is being updated or created. The name is used to reference the record. (Length: 1–30 characters)

- **oid-tree**—Specifies the ASN.1 subtree object identifier to be included or excluded from the view. To identify the subtree, specify a text string consisting of numbers, such as 1.3.6.2.4, or a word, such as System. Replace a single sub-identifier with the asterisk (*) wildcard to specify a subtree family; for example, 1.3.*.4.
- **included**—Specifies that the filter type is included.
- **excluded**—Specifies that the filter type is excluded.

Default Configuration
No view entry exists.

Command Mode
Global Configuration mode

User Guidelines
This command can be entered multiple times for the same filter record. If an object identifier is included in two or more lines, later lines take precedence. The command's logical key is the pair (filter-name, oid-tree).

Example
The following example creates a filter that includes all objects in the MIB-II system group except for sysServices (System 7) and all objects for interface 1 in the MIB-II interfaces group.

```
Console(config)# snmp-server filter filter-name system included
Console(config)# snmp-server filter filter-name system.7 excluded
Console(config)# snmp-server filter filter-name ifEntry.*.1
included
```

snmp-server host

Use the **snmp-server host** Global Configuration mode command to specify the recipient of a Simple Network Management Protocol notification operation. Use the **no** form of this command to remove the specified host.

Syntax

snmp-server host *{ ipv4-address | ipv6-address| hostname} [traps | informs] [version {1 | 2c | 3 [auth | noauth | priv]}] community-string [udp-port port] [filter filtername] [timeout seconds] [retries retries]*

no snmp-server host *{ ipv4-address | ipv6-address| hostname} [traps | informs] [version {1 | 2c | 3}]*

Parameters

- **pv4-address**—IPv4 address of the host (the targeted recipient).
- **ipv6-address**—Pv6 address of the host (the targeted recipient). When the IPv6 address is a Link Local address (IPv6Z address), the outgoing interface name must be specified. Refer to the User Guidelines for the interface name syntax.
- **hostname**—Hostname of the host. (Range: 1–158 characters. Maximum label size: 63)
- **trap**—Sends SNMP traps to this host (default).
- **informs**—Sends SNMP informs to this host. Not applicable to SNMPv1.
- **1**—SNMPv1 traps are used.
- **2c**—SNMPv2 traps are used
- **3**—SNMPv2 traps are used
- **community-string**—Password-like community string sent with the notification operation. (Range: 1–20 characters)
- **noauth**—Specifies no authentication of a packet.
- **auth**—Specifies authentication of a packet without encrypting it.
- **priv**—Specifies authentication of a packet with encryption.
- **udp-port port**—UDP port of the host to use. The default is 162. (Range: 1–65535)
- **filter filtername**—A string that is the name of the filter that defines the filter for this host. If unspecified, nothing is filtered. The filter should be defined using the command **snmp-server filter** (no specific order of the command configurations is imposed on the user). (Range: Up to 30 characters)

- **timeout seconds**—Number of seconds to wait for an acknowledgment before resending informs. The default is 15 seconds. The parameter is relevant only for informs. (Range: 1–300)
- **retries retries**—Maximum number of times to resend an inform request, when a response is not received for a generated message. The default is 3. The parameter is relevant only for informs. (Range: 0–255)

Command Mode
Global Configuration mode

User Guidelines
The logical key of the command is the pair (ip-address/hostname, traps/informs, version).

When configuring snmp v1 or v2 notifications recipient the software would automatically generate a notification view for that recipient for all the MIB. (.For SNMPv3 the software doesn't automatically create a user nor a notify view. Use the commands **snmp-server user**, **snmp-server group** and **snmp-server view** in Global Configuration mode to create a user, a group or a notify group respectively.

The format of an IPv6Z address is: *<ipv6-link-local-address>%<interface-name>*

interface-name = *vlan<integer>* / *ch<integer>* / *isatap<integer>* / *<physical-port-name>* / *0*

integer = *<decimal-number>* / *<integer><decimal-number>*

decimal-number = 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9

physical-port-name = Designated port number, for example 1/0/16

If the egress interface is not specified, the default interface is selected. Specifying interface zone=0 is equal to not defining an egress interface.

Example
The following defines a host at the IP address displayed.

```
console(config)# snmp-server host 1.1.1.121 abc
```

snmp-server engineID local

The **snmp-server engineID local** Global Configuration mode command specifies the Simple Network Management Protocol (SNMP) engineID on the local device. Use the **no** form of this command to remove the configured engine ID.

Syntax

snmp-server engineID local {*engineid-string* | *default*}

no snmp-server engineID local

Parameters

- **engineid-string**—Specifies a concatenated hexadecimal character string identifying the engine ID. Each byte in a hexadecimal character string is two hexadecimal digits. Bytes are separated by a period or colon. If an odd number of hexadecimal digits are entered, the system automatically prefixes the digit 0 to the string. (Length: 5–32 characters, 9–64 hexadecimal digits)
- **default**—Specifies that the engine ID is created automatically based on the device MAC address.

Default Configuration

The engine ID is not configured.

If SNMPv3 is enabled using this command, and the default is specified, the default engine ID is defined per standard as:

- First 4 octets: First bit = 1, the rest is IANA Enterprise number = 674.
- Fifth octet: Set to 3 to indicate the MAC address that follows.
- Last 6 octets: The device MAC address.

Command Mode

Global Configuration mode

User Guidelines

To use SNMPv3, specify an engine ID for the device. Any ID can be specified or use a default string, which is generated using the device MAC address.

As the EngineID should be unique within an administrative domain, the following guidelines are recommended:

- For standalone devices, use the default keyword to configure the Engine ID.
- For stackable systems, configure an EngineID, and verify that it is unique within the administrative domain.

Changing or removing the value of **snmpEngineID** deletes the SNMPv3 users database.

The SNMP EngineID cannot be all 0x0 or all 0xF or 0x000000001

Example

The following example enables SNMPv3 on the device and sets the device local engine ID to the default value.

```
Console(config)# snmp-server engineID local default
```

snmp-server engineID remote

To specify the Simple Network Management Protocol (SNMP) engine ID of a remote SNMP device, use the **snmp-server engineID remote** Global Configuration mode command. Use the **no** form of this command to remove the configured engine ID.

Syntax

snmp-server engineID remote *{ipv4-ip-address | ipv6 address} engineid-string*

no snmp-server engineID remote *{ipv4-ip-address | ipv6 address}*

Parameters

- **ipv4-ip-address | ipv6 address**—Pv4 or IPv6 address of the remote device
- **engineid-string**—The character string that identifies the engine ID. The engine ID is a concatenated hexadecimal string. Each byte in hexadecimal character strings is two hexadecimal digits. Each byte can be separated by

a period or colon. If the user enters an odd number of hexadecimal digits, the system automatically prefixes the hexadecimal string with a zero. (Range: engineid-string5–32 characters. 9–64 hexadecimal digits)

Default Configuration
The EngineID is not configured.

Command Mode
Global Configuration mode

User Guidelines
A remote engine ID is required when an SNMP version 3 inform is configured. The remote engine ID is used to compute the security digest for authenticating and encrypting packets sent to a user on the remote host.

snmp-server enable traps

Use the **snmp-server enable traps** Global Configuration mode command to enable the device to send SNMP traps. Use the **no** form of the command to disable SNMP traps.

Syntax
snmp-server enable traps

no snmp-server enable traps

Default Configuration
SNMP traps are enabled.

Command Mode
Global Configuration mode

Example
The following example enables SNMP traps.

```
Console(config)# snmp-server enable traps
```

snmp-server trap authentication

Use the **snmp-server trap authentication** Global Configuration mode command to enable the device to send SNMP traps when authentication fails. Use the **no** form of this command to disable SNMP failed authentication traps.

Syntax

snmp-server trap authentication

no snmp-server trap authentication

Default Configuration

SNMP failed authentication traps are enabled.

Command Mode

Global Configuration mode

Example

The following example enables SNMP failed authentication traps.

```
Console(config)# snmp-server trap authentication
```

snmp-server contact

Use the **snmp-server contact** Global Configuration mode command to configure the system contact (sysContact) string. Use the **no** form of the command to remove the system contact information.

Syntax

snmp-server contact *text*

no snmp-server contact

Parameters

text—Specifies the string describing system contact information. (Length: 1–160 characters)

Command Mode
Global Configuration mode

Example
The following example configures the system contact point called Technical_Support.

```
Console(config)# snmp-server contact Technical_Support
```

snmp-server location

Use the **snmp-server location** Global Configuration mode command to configure the system location string. Use the **no** form of this command to remove the location string.

Syntax
snmp-server location *text*

no snmp-server location

Parameters
text—Specifies a string describing system location information. (Length: 1–160 characters)

Command Mode
Global Configuration mode

Example
The following example defines the device location as New_York.

```
Console(config)# snmp-server location New_York
```

snmp-server set

Use the **snmp-server set** Global Configuration mode command to define the SNMP MIB value.

Syntax
snmp-server set *variable-name name value* [*name2 value2* ...]

Parameters
- **variable-name**—Specifies the SNMP MIB variable name, which must be a valid string.
- **name value**—Specifies a list of name and value pairs. Each name and value must be a valid string. In the case of scalar MIBs, there is only a single name-value pair. In the case of an entry in a table, there is at least one name-value pair, followed by one or more fields.

Command Mode
Global Configuration mode

User Guidelines
Although the CLI can set any required configuration, there might be a situation where an SNMP user sets a MIB variable that does not have an equivalent command. To generate configuration files that support those situations, use the **snmp-server set** command.

Example
The following example configures the scalar MIB sysName with the value TechSupp.

```
Console(config)# snmp-server set sysName sysname TechSupp
```

show snmp
Use the **show snmp** Privileged EXEC mode command to display the SNMP status.

Syntax
show snmp

Command Mode
Privileged EXEC mode

Example

The following example displays the SNMP communications status.

```
Console# show snmp
SNMP is enabled

Community-       Community-Access    View name          IP Address     Type
String
--------------
                 ----------------    ------------       ----------     ----
public           read only           user-view          All            Router
private          read write          Default            172.16.1.1/1   Router
private          su                  DefaultSuper       0              Router
                                                        172.16.1.1

Community-       Group name          IP address         Type
string
--------------
                 ----------          ----------         ------
public           user-group          All                Router

Traps are enabled.
Authentication trap is enabled.
Version 1,2 notifications

Target Address   Type    Community   Version    UDP     Filter   TO     Retries
                                                Port    name     Sec
--------------   ----    ---------   ------     ---     ------   ---    -------
192.122.173.42   Trap    public      2          162              15     3
192.122.173.42   Info    public      2          162              15     3
                 rm


Version 3 notifications

Target Address   Type    Username    Security   UDP     Filter   TO     Retries
                                     Level      Port    name     Sec
--------------   ----    --------    ------     ---     -----    ---    -------
192.122.173.42   Info    Bob         Priv       162              15     3
                 rm


System Contact: Robert
System Location: Marketing
```

The following table describes the significant fields shown in the display.

Field	Description
Community-string	The community access string permitting access to the SNMP protocol.
Community-access	The access type—read-only, read-write, super access.
IP Address	The management station IP Address.
Trap-Rec-Address	The targeted recipient.
Trap-Rec-Community	The statistics sent with the notification operation.
Version	The SNMP version (1 or 2) for the sent trap.

show snmp engineID

Use the **show snmp engineID** Privileged EXEC mode command to display the local Simple Network Management Protocol (SNMP) engine ID.

Syntax

show snmp engineID

Command Mode

Privileged EXEC mode

Example

The following example displays the SNMP engine ID.

```
Console # show snmp engineID
Local SNMP engineID: 08009009020C0B099C075878
#Editor: If snmp-server engineID remote command is supported
add the following line
IP address     Remote SNMP engineID
-----------    ------------------------------
172.16.1.1     08009009020C0B099C075879
```

show snmp views

Use the **show snmp views** Privileged EXEC mode command to display the configured SNMP views.

Syntax

show snmp views [*viewname*]

Parameters

viewname—Specifies the view name. (Length: 1–30 characters)

Command Mode

Privileged EXEC mode

Example

The following example displays the configured SNMP views.

```
Console# show snmp views

Name                OID Tree                    Type
-----------------   ----------------------      ----------
Default             iso                         Included
Default             snmpNotificationMIB         Excluded
```

show snmp groups

Use the **show snmp groups** Privileged EXEC mode command to display the configured SNMP groups.

Syntax

show snmp groups [*groupname*]

Parameters

groupname—Specifies the group name. (Length: 1–30 characters)

Command Mode
Privileged EXEC mode

Example
The following example displays the configured SNMP groups.

```
Console# show snmp groups

Name                    Security                Views

                 Model     Level       Read      Write     Notify
-------------    -----     ----        -------   -------   -------
user-group       V3        priv        Default   ""        ""
managers-group   V3        priv        Default   Default   ""
```

The following table describes significant fields shown above.

Field		Description
Name		Group name.
Security Model		SNMP model in use (v1, v2 or v3).
Security Level		Packet authentication with encryption. Applicable to SNMP v3 security only.
Views	Read	View name enabling viewing the agent contents. If unspecified, all objects except the community-table and SNMPv3 user and access tables are available.
	Write	View name enabling data entry and managing the agent contents.
	Notify	View name enabling specifying an inform or a trap.

show snmp filters

Use the **show snmp filters** Privileged EXEC mode command to display the configured SNMP filters.

Syntax
show snmp filters [*filtername*]

Parameters
filtername—Specifies the filter name. (Length: 1–30 characters)

Command Mode
Privileged EXEC mode

Example
The following example displays the configured SNMP filters.

```
Console# show snmp filters

Name           OID Tree                  Type
------------   ---------------------     ---------
user-filter    1.3.6.1.2.1.1             Included
user-filter    1.3.6.1.2.1.1.7           Excluded
user-filter    1.3.6.1.2.1.2.2.1.*.1     Included
```

show snmp users

Use the **show snmp users** Privileged EXEC mode command to display the configured SNMP users.

Syntax
show snmp users [*username*]

Parameters
username—Specifies the user name. (Length: 1–30 characters)

Command Mode
Privileged EXEC mode

Example

The following example displays the configured SNMP users.

```
Console# show snmp users

                        Auth
Name      Group name    Method      Remote
------    ------------  -------     ------------------------
John      user-group    md5
John      user-group    md5         08009009020C0B099C075879
```

10

RSA and Certificate Commands

crypto key generate dsa

The **crypto key generate dsa** Global Configuration mode command generates DSA key pairs.

Syntax

crypto key generate dsa

Default Configuration

DSA key pairs do not exist.

Command Mode

Global Configuration mode

User Guidelines

DSA keys are generated in pairs - one public DSA key and one private DSA key.

If the device already has DSA keys, a warning is displayed with a prompt to replace the existing keys with new keys.

This command is not saved in the router configuration. However, the keys generated by this command are saved in the private configuration (which is never displayed to the user or backed up to another device).

Example

The following example generates DSA key pairs.

```
Console(config)# crypto key generate dsa
```

crypto key generate rsa

The **crypto key generate rsa** Global Configuration mode command generates RSA key pairs.

Syntax

crypto key generate rsa

Default Configuration

RSA key paris do not exist.

Command Mode

Global Configuration mode

User Guidelines

RSA keys are generated in pairs - one public RSA key and one private RSA key.

If the device already has RSA keys, a warning is displayed with a prompt to replace the existing keys with new keys.

This command is not saved in the router configuration; however, the keys generated by this command are saved in the private configuration (which is never displayed to the user or backed up to another device).

Example

The following example generates RSA key pairs.

```
Console(config)# crypto key generate rsa
```

show crypto key mypubkey

The **show crypto key mypubkey** Privileged EXEC mode command displays the device SSH public keys.

Syntax

show crypto key mypubkey *[rsa / dsa]*

Parameters

- **rsa**—Displays the RSA key.
- **dsa**—Displays the DSA key.

Command Mode
Privileged EXEC mode

Example
The following example displays the SSH public RSA keys on the device.

```
Console# show crypto key mypubkey rsa
RSA key data:
005C300D 06092A86 4886F70D 01010105 00034B00 30480241 00C5E23B 55D6AB22
04AEF1BA A54028A6 9ACC01C5 129D99E4 64CAB820 847EDAD9 DF0B4E4C 73A05DD2
BD62A8A9 FA603DD2 E2A8A6F8 98F76E28 D58AD221 B583D7A4 71020301 87685768
Fingerprint(Hex): 77:C7:19:85:98:19:27:96:C9:CC:83:C5:78:89:F8:86
Fingerprint(Bubble Babble): yteriuwt jgkljhglk yewiury hdskjfryt
gfhkjglk
```

crypto certificate generate

The **crypto certificate generate** Global Configuration mode command generates a self-signed certificate for HTTPS.

Syntax
crypto certificate *number* **generate** *[key-generate [length]] [passphrase string] [cn common- name] [ou organization-unit] [or organization] [loc location] [st state] [cu country] [duration days*]

Parameters

- **number**—Specifies the certificate number. (Range: 1–2)
- **key-generate**—Regenerates SSL RSA key.
- **length**—Specifies the SSL's RSA key length. (Range: 512–2048)
- **passphrase string**—Specifies the passphrase used for exporting the certificate in PKCS12 file format. (Length: 8–96 characters)

- **cn common-name**—Specifies the fully qualified device URL or IP address. (Length: 1–64 characters)
- **ou organization-unit**—Specifies the organization-unit or department name. (Length: 1–64 characters)
- **or organization**—Specifies the organization name. (Length: 1–64 characters)
- **loc location**—Specifies the location or city name. (Length: 1–64 characters)
- **st state**—Specifies the state or province name. (Length: 1–64 characters)
- **cu country**—Specifies the country name. (Length: 2 characters)
- **duration days**—Specifies the number of days a certification is valid. (Range: 30–3650)

Default Configuration

The default certificate number is 1.

The default SSL's RSA key length is 1024.

If **passphrase string** is not specified, the certificate is not exportable.

If **cn common-name** is not specified, it defaults to the device's lowest static IPv6 address (when the certificate is generated), or to the device's lowest static IPv4 address if there is no static IPv6 address, or to 0.0.0.0 if there is no static IP address.

If **duration days** is not specified, it defaults to 365 days.

Command Mode

Global Configuration mode

User Guidelines

This command is not saved in the router configuration. However, the certificate and keys generated by this command are saved in the private configuration (which is never displayed to the user or backed up to another device).

When exporting a RSA key pair to a PKCS#12 file, the RSA key pair is as secure as the passphrase. Keep the passphrase secure.

If the RSA key does not exist, you must use the parameter **key-generate**.

Example

The following example generates a self-signed certificate for HTTPS.

```
Console# crypto certificate generate key-generate
```

crypto certificate request

The **crypto certificate request** Privileged EXEC mode command generates and displays a certificate request for HTTPS.

Syntax

crypto certificate *number* **request** *common-name [ou organization-unit] [or organization] [loc location] [st state] [cu country]*

Parameters

- **number**—Specifies the certificate number. (Range: 1–2)
- **common-name**—Specifies the device's fully qualified URL or IP address. (Length: 1–64 characters)
- **ou organization-unit**—Specifies the organization-unit or department name. (Length: 1–64 characters)
- **or organization**—Specifies the organization name. (Length: 1–64 characters)
- **loc location**—Specifies the location or city name. (Length: 1–64 characters)
- **st state**—Specifies the state or province name. (Length: 1–64 characters)
- **cu country**—Specifies the country name. (Length: 2 characters)

Command Mode

Privileged EXEC mode

User Guidelines

Use this command to export a certificate request to a Certification Authority. The certificate request is generated in Base64-encoded X.509 format.

Before generating a certificate request, first generate a self-signed certificate using the **crypto certificate generate** Global Configuration mode command to generate the keys. The certificate fields must be re-entered.

After receiving the certificate from the Certification Authority, use the **crypto certificate import** Global Configuration mode command to import the certificate into the device. This certificate replaces the self-signed certificate.

Example
The following example displays the certificate request for HTTPS.

```
Console# crypto certificate 1 request
-----BEGIN CERTIFICATE REQUEST-----
MIwTCCASoCAQAwYjELMAkGA1UEBhMCUFAxCzAJBgNVBAgTAkNDMQswCQYDVQQH
EwRDEMMAoGA1UEChMDZGxkMQwwCgYDVQQLEwNkbGQxCzAJBgNVBAMTAmxkMRAw
DgKoZIhvcNAQkBFgFsMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQC8ecwQ
HdML0831i0fh/F0MV/Kib6Sz5p+3nUUenbfHp/igVPmFM+1nbqTDekb2ymCu6K
aKvEbVLF9F2LmM7VPjDBb9bb4jnxkvwW/wzDLvW2rsy5NPmH1QVl+8Ubx3GyCm
/oW93BSOFwxwEsP58kf+sPYPy+/8wwmoNtDwIDAQABoB8wHQYJKoZIhvcNAQkH
MRDjEyMwgICCAgICAICAgIMA0GCSqGSIb3DQEBBAUAA4GBAGb8UgIx7rB05m+2
m5ZZPhIwl8ARSPXwhVdJexFjbnmvcacqjPG8pIiRV6LkxryGF2bVU3jKEipcZa
g+uNpyTkDt3ZVU72pjz/fa8TF0n3
-----END CERTIFICATE REQUEST-----

CN= router.gm.com
0= General Motors
C= US
```

crypto certificate import

The **crypto certificate import** Global Configuration mode command imports a certificate signed by a Certification Authority for HTTPS.

Syntax
crypto certificate *number* **import**

Parameters

number—Specifies the certificate number. (Range: 1–2)

Command Mode

Global Configuration mode

User Guidelines

To end the session, use a blank line.

The imported certificate must be based on a certificate request created by the **crypto certificate request** privileged EXEC command.

If the public key found in the certificate does not match the device's SSL RSA key, the command fails.

This command is not saved in the router configuration. However, the certificate imported by this command is saved in the private configuration (which is never displayed to the user or backed up to another device).

Example

The following example imports a certificate signed by Certification Authority for HTTPS.

```
Console(config)# crypto certificate 1 import
-----BEGIN CERTIFICATE-----
dHmUgUm9vdCBDZXJ0aWZpZXIwXDANBgkqhkiG9w0BAQEFAANLADBIAkEAp4HS
nnH/xQSGA2ffkRBwU2XIxb7n8VPsTm1xyJ1t11a1GaqchfMqqe0kmfhcoHSWr
yf1FpD0MWOTgDAwIDAQABo4IBojCCAZ4wEwYJKwYBBAGCNxQCBAYeBABDAEEw
CwR0PBAQDAgFGMA8GA1UdEwEB/wQFMAMBAf8wHQYDVR0OBBYEFAf4MT9BRD47
ZvKBAEL9Ggp+6MIIBNgYDVR0fBIIBLTCCASkwgdKggc+ggcyGgclsZGFwOi8v
L0VByb3h5JTIwU29mdHdhcmUlMjBSb290JTIwQ2VydGlmaWVyLENOPXNlcnZl
-----END CERTIFICATE-----

Certificate imported successfully.
Issued to: router.gm.com
Issued by: www.verisign.com
Valid from: 8/9/2003 to 8/9/2004
Subject: CN= router.gm.com, 0= General Motors, C= US
```

```
Finger print: DC789788 DC88A988 127897BC BB789788
```

crypto certificate export pkcs12

The **crypto certificate export pkcs12** Privileged EXEC mode command exports the certificate and the RSA keys within a PKCS12 file.

Syntax

crypto certificate *number* **export pkcs12**

Parameters

number—Specifies the certificate number. (Range: 1–2)

Command Mode

Privileged EXEC mode

User Guidelines

The **crypto certificate export** pkcs12 command creates a PKCS 12 file that contains the certificate and an RSA key pair.

The passphrase for the export is determined when the key is generated.

The certificate and key pair are exported in a standard PEM-format PKCS12 file. This format can be converted to and from the binary PFX file used by Windows and Linux by using the **openssl** command-line tool. See an open source OpenSSL user manual (man pkcs12) for more information.

Example

The following example exports the certificate and the RSA keys within a PKCS12 file.

```
Console# crypto certificate 1 export pkcs12
Bag Attributes
localKeyID: 0C 75 81 77 5A 31 53 D1 FF 4E 26 BE 8D 4A FD 8B 22 9F 45 D4
subject=/C=us/ST= /L= /CN= /O= /OU=
issuer= /C=us/ST= /L= /CN= /O= /OU=
-----BEGIN CERTIFICATE-----
MIIBfDCCASYCAQAwDQYJKoZIhvcNAQEEBQAwSTELMAkGA1UEBhMCdXMxCjAIBgNV
```

```
BAgTASAxCjAIBgNVBAcTASAxCjAIBgNVBAMTASAxCjAIBgNVBAoTASAxCjAIBgNV
BAsTASAwHhcNMDQwMjA3MTU1NDQ4WhcNMDUwMjA2MTU1NDQ4WjBJMQswCQYDVQQG
EwJ1czEKMAgGA1UECBMBIDEKMAgGA1UEBxMBIDEKMAgGA1UEAxMBIDEKMAgGA1UE
ChMBIDEKMAgGA1UECxMBIDBcMA0GCSqGSIb3DQEBAQUAA0sAMEgCQQCZXP/tk3e/
jrulfZw8q8T2oS5ymrEIes/sRJE8uahTBJqKu1VHqRYJR3VYa/03HSJ741w5MzPI
iuWZzrbbuXAxAgMBAAEwDQYJKoZIhvcNAQEEBQADQQBQ+GTLeN1p1kARxI4C1fTU
efig3ffZ/tjW5q1t1r5F6zNv/GuXWw7rGzmRyoMXDcYp1TaA4gAIFQCpFGqiSbAx
-----END CERTIFICATE-----
Bag Attributes
localKeyID: 0C 75 81 77 5A 31 53 D1 FF 4E 26 BE 8D 4A FD 8B 22 9F 45 D4
Key Attributes: <No Attributes>
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: DES-EDE3-CBC,085DCBF3A41D2669
dac0m9jqEp1DM50sIDb8Jq1jxW/1P0kqSxuMhc25OdBE/1fPBg9VSvV1ARaYt16W
bX67UyJ8t7HHF3AowjcWzElQ5GJgSQ0VemsqsRQzjpCTb090rx+cNwVfIvjoedgQ
Mtl5+fKIAcqsfEgEGJNXQ4jEzsXAkwfQLFfgt47O3IpkUn0AxrQzutJDOcC28Uxp
raMVTVSlSkJIvaPuXJxdZ279tDMwZffILBfKCJGACT5V5/4WEqDkrF+uuF9/oxm2
5SVL8TvUmXB/3hX4UoaXtxAhuyOdhh1kyyZSpw9BPPR/8bc/wUYERh7+7JXLKHpd
ueeu3znfIX4dDeti8B3xYvvE8kGZjxFN1cC3zc3JsD0IVu1LkyiAa93P4LPEvAwG
Fw1LqmGiiqw9JM/tzc6kYkZXylFzCrSVf2exP+/tEvM=
-----END RSA PRIVATE KEY-----
```

crypto certificate import pkcs12

The **crypto certificate import pkcs12** Privileged EXEC mode command imports the certificate and the RSA keys within a PKCS12 file.

Syntax

crypto certificate *number* **import pkcs12** *passphrase*

Parameters

- **number**—Specifies the certificate number. (Range: 1–2)
- **passphrase**—Specifies the passphrase used to encrypt the PKCS12 file for export. (Length: 8–96 characters)

Command Mode
Privileged EXEC mode

User Guidelines
Use the passphrase that was exported by the crypto certificate export pkcs12 command.

NOTE: This passphrase is saved for later exports.

Example
The following example imports the certificate and the RSA keys within a PKCS12 file.

```
Console# crypto certificate 1 import pkcs12 passphrase
Bag Attributes
localKeyID: 0C 75 81 77 5A 31 53 D1 FF 4E 26 BE 8D 4A FD 8B 22 9F 45 D4
subject=/C=us/ST= /L= /CN= /O= /OU=
issuer= /C=us/ST= /L= /CN= /O= /OU=
-----BEGIN CERTIFICATE-----
MIIBfDCCASYCAQAwDQYJKoZIhvcNAQEEBQAwSTELMAkGA1UEBhMCdXMxCjAIBgNV
BAgTASAxCjAIBgNVBAcTASAxCjAIBgNVBAMTASAxCjAIBgNVBAoTASAxCjAIBgNV
BAsTASAwHhcNMDQwMjA3MTU1NDQ4WhcNMDUwMjA2MTU1NDQ4WjBJMQswCQYDVQQG
EwJ1czEKMAgGA1UECBMBIDEKMAgGA1UEBxMBIDEKMAgGA1UEAxMBIDEKMAgGA1UE
ChMBIDEKMAgGA1UECxMBIDBcMA0GCSqGSIb3DQEBAQUAA0sAMEgCQQCZXP/tk3e/
jrulfZw8q8T2oS5ymrEIes/sRJE8uahTBJqKu1VHqRYJR3VYa/03HSJ741w5MzPI
iuWZzrbbuXAxAgMBAAEwDQYJKoZIhvcNAQEEBQADQQBQ+GTLeN1p1kARxI4C1fTU
efig3ffZ/tjW5q1t1r5F6zNv/GuXWw7rGzmRyoMXDcYp1TaA4gAIFQCpFGqiSbAx
-----END CERTIFICATE-----
Bag Attributes
localKeyID: 0C 75 81 77 5A 31 53 D1 FF 4E 26 BE 8D 4A FD 8B 22 9F 45 D4
Key Attributes: <No Attributes>
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: DES-EDE3-CBC,085DCBF3A41D2669
dac0m9jqEp1DM50sIDb8Jq1jxW/1P0kqSxuMhc25OdBE/1fPBg9VSvV1ARaYt16W
bX67UyJ8t7HHF3AowjcWzElQ5GJgSQ0VemsqsRQzjpCTb090rx+cNwVfIvjoedgQ
Mtl5+fKIAcqsfEgEGJNXQ4jEzsXAkwfQLFfgt47O3IpkUn0AxrQzutJDOcC28Uxp
```

```
raMVTVSlSkJIvaPuXJxdZ279tDMwZffILBfKCJGACT5V5/4WEqDkrF+uuF9/oxm2
5SVL8TvUmXB/3hX4UoaXtxAhuyOdhh1kyyZSpw9BPPR/8bc/wUYERh7+7JXLKHpd
ueeu3znfIX4dDeti8B3xYvvE8kGZjxFN1cC3zc3JsD0IVu1LkyiAa93P4LPEvAwG
Fw1LqmGiiqw9JM/tzc6kYkZXylFzCrSVf2exP+/tEvM=
-----END RSA PRIVATE KEY-----
```

show crypto certificate mycertificate

The **show crypto certificate mycertificate** Privileged EXEC mode command displays the device SSL certificates.

Syntax

show crypto certificate mycertificate [*number*]

Parameters

number—Specifies the certificate number. (Range: 1–2

Command Mode

Privileged EXEC mode

Example

The following example displays SSL certificate # 1 present on the device.

```
Console# show crypto certificate mycertificate 1
-----BEGIN CERTIFICATE-----
dHmUgUm9vdCBDZXJ0aWZpZXIwXDANBgkqhkiG9w0BAQEFAANLADBIAkEAp4HS
nnH/xQSGA2ffkRBwU2XIxb7n8VPsTm1xyJ1t11a1GaqchfMqqe0kmfhcoHSWr
yf1FpD0MWOTgDAwIDAQABo4IBojCCAZ4wEwYJKwYBBAGCNxQCBAYeBABDAEEw
CwR0PBAQDAgFGMA8GA1UdEwEB/wQFMAMBAf8wHQYDVR0OBBYEFAf4MT9BRD47
ZvKBAEL9Ggp+6MIIBNgYDVR0fBIIBLTCCASkwgdKggc+ggcyGgclsZGFwOi8v
L0VByb3h5JTIwU29mdHdhcmUlMjBSb290JTIwQ2VydGlmaWVyLENOPXNlcnZl
-----END CERTIFICATE-----

Issued by: www.verisign.com
Valid from: 8/9/2003 to 8/9/2004
Subject: CN= router.gm.com, 0= General Motors, C= US
```

```
Finger print: DC789788 DC88A988 127897BC BB789788
```

11

Web Server Commands

ip http server

The **ip http server** Global Configuration mode command enables configuring and monitoring the device from a web browser. Use the **no** form of this command to disable this function.

Syntax

ip http server

no ip http server

Default Configuration

HTTP server is enabled.

Command Mode

Global Configuration mode

Example
The following example enables configuring the device from a web browser.

```
Console(config)# ip http server
```

ip http port

The **ip http port** Global Configuration mode command specifies the TCP port used by the web browser interface. Use the **no** form of this command to restore the default configuration.

Syntax
ip http port *port-number*

no ip http port

Parameters
port-numberPort number—For use by the HTTP server. (Range: 0–65534)

Default Configuration
The default port number is 80.

Command Mode
Global Configuration mode

Example
The following example configures the http port number as 100.

```
Console(config)# ip http port 100
```

ip http timeout-policy

Use the **ip http timeout-policy** Global Configuration mode command to set the interval for the system to wait for user input in http sessions before automatic logoff. Use the **no** form of this command to return to the default value.

Syntax

ip http timeout-policy *idle seconds*

no ip http timeout-policy

Parameters

seconds—Specifies the maximum number of seconds that a connection is kept open if no data is received or response data cannot be sent out. (Range: 0–86400)

Default

600 seconds

Command Mode

Global Configuration mode

User Guidelines

This command also configures the timeout-policy for HTTPS.

To specify no timeout, enter the **ip http timeout-policy 0** command.

Example

The following example configures the http port number as 100.

```
Console(config)# ip http timeout-policy 0
```

ip http secure-server

Use the **ip http secure-server** Global Configuration mode command to enable the device to be configured securely from a browser, and to also enable the device to be monitored or have its configuration modified securely from a browser,. Use the **no** form of this command to disable this function.

Syntax

ip http secure-server

no ip http secure-server

Parameters
This command has no arguments or keywords.

Default
Disabled

Command Mode
Global Configuration mode

User Guidelines
Use the **crypto certificate generate** command to generate an HTTPS certificate.

Example

```
console(config)# ip http secure-server
```

ip http secure-port

To specify the TCP port to be used by the secure web browser interface, use the **ip http secure-port** Global Configuration mode command. To use the default port, use the **no** form of this command.

Syntax
ip http secure-port *port-number*

no ip http secure-port

Parameters
port-number—Port number for use by the HTTPS server (Range: 0–65534)

Default
The default port number is 443.

Command Mode
Global Configuration mode

Example

```
console(config)# ip http secure-port 1234
```

ip https certificate

The **ip https certificate** Global Configuration mode command configures the active certificate for HTTPS. Use the **no** form of this command to restore the default configuration.

Syntax

ip https certificate *number*

no ip https certificate

Parameters

number—Specifies the certificate number. (Range: 1–2)

Default Configuration

The default certificate number is 1.

Command Mode

Global Configuration mode

User Guidelines

Use the **crypto certificate generate** command to generate a HTTPS certificate.

Example

The following example configures the active certificate for HTTPS.

```
Console(config)# ip https certificate 2
```

show ip http

The **show ip http** EXEC mode command displays the HTTP server configuration.

Syntax
show ip http

Command Mode
EXEC mode

Example
The following example displays the HTTP server configuration.

```
Console# show ip http
HTTP server enabled
Port: 80
Interactive timeout: 10 minutes
```

show ip https

The **show ip https** Privileged EXEC mode command displays the HTTPS server configuration.

Syntax
show ip https

Command Mode
Privileged EXEC mode

Example
The following example displays the HTTPS server configuration.

```
Console# show ip https
HTTPS server enabled
```

```
Port: 443
Interactive timeout: Follows the HTTP interactive timeout
(10 minutes)


Certificate 1 is active
Issued by: www.verisign.com
Valid from: 8/9/2003 to 8/9/2004
Subject: CN= router.gm.com, 0= General Motors, C= US
Finger print: DC789788 DC88A988 127897BC BB789788

Certificate 2 is inactive
Issued by: self-signed
Valid from: 8/9/2003 to 8/9/2004
Subject: CN= router.gm.com, 0= General Motors, C= US
Finger print: 1873B936 88DC3411 BC8932EF 782134BA
```

12

Telnet, SSH and Slogin Commands

ip telnet server

The **ip telnet server** Global Configuration mode command enables the device to be configured from a Telnet server. Use the **no** form of this command to disable the device configuration from a Telnet server.

Syntax

ip telnet server

no ip telnet server

Default Configuration

Device configuration from a Telnet server is enabled.

Command Mode

Global Configuration mode

User Guidelines

To control the device configuration by SSH, use the **ip ssh server** Global Configuration mode command.

Example

The following example enables the device to be configured from a Telnet server.

```
Console(config)# ip telnet server
```

ip ssh port

The **ip ssh port** Global Configuration mode command specifies the port used by the SSH server. Use the **no** form of this command to restore the default configuration.

Syntax

ip ssh port *port-number*

no ip ssh port

Parameters

port-number—Specifies the port number to be used by the SSH server. (Range: 1–65535)

Default Configuration

The default port number is 22.

Command Mode

Global Configuration mode

Example

The following example specifies that port number 8080 is used by the SSH server.

```
Console(config)# ip ssh port 8080
```

ip ssh server

The **ip ssh server** Global Configuration mode command enables the device to be configured from an SSH server. Use the **no** form of this command to disable the device configuration from a SSH server,.

Syntax

ip ssh server

no ip ssh server

Default Configuration
Device configuration from an SSH server is enabled.

Command Mode
Global Configuration mode

User Guidelines
If encryption keys are not generated, the SSH server is in standby until the keys are generated. To generate SSH server keys, use the **crypto key generate dsa** and **crypto key generate rsa** Global Configuration mode commands.

Example
The following example enables configuring the device from a SSH server.

```
Console(config)# ip ssh server
```

ip ssh pubkey-auth

The **ip ssh pubkey-auth** Global Configuration mode command enables public key authentication of incoming SSH sessions. Use the **no** form of this command to disable this function.

Syntax
ip ssh pubkey-auth

no ip ssh pubkey-auth

Default Configuration
Public Key authentication of incoming SSH sessions is disabled.

Command Mode
Global Configuration mode

User Guidelines
AAA authentication is independent.

Example
The following example enables public key authentication for incoming SSH sessions.

```
Console(config)# ip ssh pubkey-auth
```

crypto key pubkey-chain ssh

The **crypto key pubkey-chain ssh** Global Configuration mode command enters the SSH Public Key-chain Configuration mode. This mode is used to manually specify other device public keys such as SSH client public keys.

Syntax
crypto key pubkey-chain ssh

Default Configuration
Keys do not exist.

Command Mode
Global Configuration mode

User Guidelines
Use this command when you want to manually specify SSH client's public keys.

Example
The following example enters the SSH Public Key-chain Configuration mode and manually configures the RSA key pair for SSH public key-chain to 'bob'.

```
Console(config)# crypto key pubkey-chain ssh
Console(config-pubkey-chain)# user-key bob
Console(config-pubkey-key)# key-string rsa
AAAAB3NzaC1yc2EAAAADAQABAAABAQCvTnRwPWl
Al4kpqIw9GBRonZQZxjHKcqKL6rMlQ+
ZNXfZSkvHG+QusIZ/76ILmFT34v7u7ChFAE+
Vu4GRfpSwoQUvV35LqJJk67IOU/zfwOl1g
```

```
kTwml75QR9gHujS6KwGN2QWXgh3ub8gDjTSq
muSn/Wd05iDX2IExQWu08licglk02LYciz
+Z4TrEU/9FJxwPiVQOjc+KBXuR0juNg5nFYsY
0ZCk0N/W9a/tnkm1shRE7Di71+w3fNiOA
6w9o44t6+AINEICBCCA4YcF6zMzaT1wefWwX6f+
Rmt5nhhqdAtN/4oJfce166DqVX1gWmN
zNR4DYDvSzg0lDnwCAC8Qh

Fingerprint: a4:16:46:23:5a:8d:1d:b5:37:59:eb:44:13:b9:33:e9
```

user-key

The **user-key** SSH Public Key-string Configuration mode command specifies which SSH public key is manually configured. Use the **no** form of this command to remove an SSH public key.

Syntax

user-key *username {rsa | dsa}*

no user-key *username*

Parameters

- **username**—Specifies the remote SSH client username. (Length: 1–48 characters)
- **rsa**—Specifies that the RSA key pair is manually configured.
- **dsa**—Specifies that the DSA key pair is manually configured.

Default Configuration

No SSH public keys exist.

Command Mode

SSH Public Key-string Configuration mode

User Guidelines

Follow this command with the **key-string** SSH Public Key-String Configuration mode command to specify the key.

Please note that after entering this command, the existing key is deleted even if no new key is defined by the **key-string** command

Exampe
The following example enables manually configuring an SSH public key for SSH public key-chain **bob**.

```
Console(config)# crypto key pubkey-chain ssh
Console(config-pubkey-chain)# user-key bob rsa
Console(config-pubkey-key)# key-string row
AAAAB3NzaC1yc2EAAAADAQABAAABAQCvTnRwPWl
```

key-string

The **key-string** SSH Public Key-string Configuration mode command manually specifies an SSH public key.

Syntax
key-string *[row key-string]*

Parameters

- **row**—Specifies the SSH public key row by row.
- **key-string**—Specifies the key in UU-encoded DER format. UU-encoded DER format is the same format as in the authorized_keys file used by OpenSSH. (Length:0–160)

Default Configuration
Keys do not exist.

Command Mode
SSH Public Key-string Configuration mode

User Guidelines
Use the **key-string** SSH Public Key-string Configuration mode command without the **row** parameter to specify which SSH public key is to be

interactively configured next. Enter a row with no characters to complete the command.

Use the **key-string row** SSH Public Key-string Configuration mode command to specify the SSH public key, row by row. Each row must begin with a **key-string row** command.

The UU-encoded DER format is the same format as in the authorized_keys file used by OpenSSH.

Example

The following example enters public key strings for SSH public key client 'bob'.

```
Console(config)# crypto key pubkey-chain ssh
Console(config-pubkey-chain)# user-key bob rsa
Console(config-pubkey-key)# key-string
AAAAB3NzaC1yc2EAAAADAQABAAABAQCvTnRwPWl
Al4kpqIw9GBRonZQZxjHKcqKL6rMlQ+
ZNXfZSkvHG+QusIZ/76ILmFT34v7u7ChFAE+
Vu4GRfpSwoQUvV35LqJJk67IOU/zfwOl1g
kTwml75QR9gHujS6KwGN2QWXgh3ub8gDjTSq
muSn/Wd05iDX2IExQWu08licglk02LYciz
+Z4TrEU/9FJxwPiVQOjc+KBXuR0juNg5nFYsY
0ZCk0N/W9a/tnkm1shRE7Di71+w3fNiOA
6w9o44t6+AINEICBCCA4YcF6zMzaT1wefWwX6f+
Rmt5nhhqdAtN/4oJfce166DqVX1gWmN
zNR4DYDvSzg0lDnwCAC8Qh

Fingerprint: a4:16:46:23:5a:8d:1d:b5:37:59:eb:44:13:b9:33:e9

Console(config)# crypto key pubkey-chain ssh
Console(config-pubkey-chain)# user-key bob rsa
Console(config-pubkey-key)# key-string row AAAAB3Nza
Console(config-pubkey-key)# key-string row C1yc2
```

show ip ssh

The **show ip ssh** Privileged EXEC mode command displays the SSH server configuration.

Syntax
show ip ssh

Command Mode
Privileged EXEC mode

Example
The following example displays the SSH server configuration.

```
Console# show ip ssh

SSH server enabled. Port: 22
RSA key was generated.
DSA (DSS) key was generated.

SSH Public Key Authentication is enabled.

Active incoming sessions:
IP address   SSH           Version    Cipher     Auth code
---------    username      -------    ------     ----------
172.16.0.1   -----------   1.5        3DES       HMAC-SHA1
             John Brown
```

The following table describes the significant fields shown in the display.

Field	Description
IP address	The client address
SSH username	The user name
Version	The SSH version number

Field	Description
Cipher	The encryption type (3DES, Blowfish, RC4)
Auth Code	The authentication Code (HMAC-MD5, HMAC-SHA1)

show crypto key pubkey-chain ssh

The **show crypto key pubkey-chain ssh** Privileged EXEC mode command displays SSH public keys stored on the device.

Syntax

show crypto key pubkey-chain ssh *[username username] [fingerprint {bubble-babble | hex}]*

Parameters

- **username username**—Specifies the remote SSH client username. (Length: 1–48 characters)
- **fingerprint {bubble-babble | hex}**—Specifies the fingerprint display format. The possible values are:
  - **bubble-babble**—Specifies that the fingerprint is displayed in Bubble Babble format.
  - **hex**—Specifies that the fingerprint is displayed in hexadecimal format.

Default Configuration

The default fingerprint format is hexadecimal.

Command Mode

Privileged EXEC mode

Example

The following examples display SSH public keys stored on the device.

```
Console# show crypto key pubkey-chain ssh

Username
--------
```

```
bob
john
Fingerprint
-------------------------------------------
9A:CC:01:C5:78:39:27:86:79:CC:23:C5:98:59:F1:86
98:F7:6E:28:F2:79:87:C8:18:F8:88:CC:F8:89:87:C8

Console# show crypto key pubkey-chain ssh username bob
Username: bob
Key: 005C300D 06092A86 4886F70D 01010105 00034B00 30480241
00C5E23B 55D6AB22 04AEF1BA A54028A6 9ACC01C5 129D99E4
Fingerprint:
9A:CC:01:C5:78:39:27:86:79:CC:23:C5:98:59:F1:86
```

13

Line Commands

line

The **line** Global Configuration mode command identifies a specific line for configuration and enters the Line Configuration command mode.

Syntax

line *{console | telnet | ssh}*

Parameters

- **console**—Enters the console terminal line mode.
- **telnet**—Configures the device as a virtual terminal for remote console access (Telnet).
- **ssh**—Configures the device as a virtual terminal for secured remote console access (SSH).

Command Mode

Global Configuration mode

Example

The following example configures the device as a virtual terminal for remote (Telnet) console access.

```
Console(config)# line telnet
Console(config-line)#
```

speed

The **speed** Line Configuration mode command sets the line baud rate. Use the **no** form of this command to restore the default configuration.

Syntax

speed *bps*

no speed

Parameters

bps—Specifies the baud rate in bits per second (bps). Possible values are 2400, 4800, 9600, 19200, 38400, 57600, and 115200.

Default Configuration

The default speed is 9600 bps.

Command Mode

Line Configuration (console) mode

User Guidelines

The configured speed is applied when Autobaud is disabled. This configuration applies to the current session only.

Example

The following example configures the line baud rate as 9600 bits per second.

```
Console(config-line)# speed 9600
```

autobaud

The **autobaud** Line Configuration mode command sets the line for automatic baud rate detection (autobaud). Use the **no** form of this command to disable automatic baud rate detection.

Syntax

autobaud

no autobaud

Default Configuration
Automatic baud rate detection is disabled.

Command Mode
Line Configuration mode

User Guidelines
To start communication using Autobaud, press the **Enter** key twice.

Example
The following example enables autobaud.

```
Console(config)# line console
Console(config-line)# autobaud
```

exec-timeout

The **exec-timeout** Line Configuration mode command sets the session idle time interval, during which the system waits for user input before automatic logoff. Use the **no** form of this command to restore the default configuration.

Syntax
exec-timeout *minutes* [*seconds*]

no exec-timeout

Parameters

- **minutes**—Specifies the number of minutes. (Range: 0-65535)
- **seconds**—Specifies the number of seconds. (Range: 0-59)

Default Configuration
The default idle time interval is 10 minutes.

Command Mode
Line Configuration mode

User Guidelines
To specify no timeout, enter the **exec-timeout** 0 0 command.

Example
The following example sets the HTTP session idle time interval before automatic logoff to 20 minutes.

```
Console(config)# line console
Console(config-line)# exec-timeout 20
```

show line

The **show line** EXEC mode command displays line parameters.

Syntax
show line *[console | telnet | ssh]*

Parameters

- **console**—Displays the console configuration.
- **telnet**—Displays the Telnet configuration.
- **ssh**—Displays the SSH configuration.

Default Configuration
If the line is not specified, all line configuration parameters are displayed.

Command Mode
EXEC mode

Example
The following example displays the line configuration.

```
Console> show line

Console configuration:
```

```
Interactive timeout: Disabled
History: 10
Baudrate: 9600
Databits: 8
Parity: none
Stopbits: 1

Telnet configuration:

Telnet is enabled.
Interactive timeout: 10 minutes 10 seconds
History: 10

SSH configuration:

SSH is enabled.
Interactive timeout: 10 minutes 10 seconds
History: 10
```

14

AAA Commands

aaa authentication login

The **aaa authentication login** Global Configuration mode command sets an authentication method applied during login. Use the **no** form of this command to restore the default authentication method.

Syntax

aaa authentication login *{default | list-name} method* [*method2 ...*]

no aaa authentication login *{default | list-name}*

Parameters

- **default**—Uses the listed authentication methods that follow this argument as the default method list when a user logs in.
- **list-name**—Specifies a name for a list of authentication methods activated when a user logs in. (Length: 1–12 characters)
- **method [method2 ...]**—Specifies a list of methods that the authentication algorithm tries, in the given sequence. The additional authentication methods are used only if the previous method returns an error, not if it fails. To ensure that the authentication succeeds even if all methods return an error, specify **none** as the final method in the command line. Select one or more methods from the following list**:**

Keyword	Description
enable	Uses the enable password for authentication.
line	Uses the line password for authentication.
local	Uses the local username database for authentication.

none	Uses no authentication.
radius	Uses the list of all RADIUS servers for authentication.
tacacs	Uses the list of all TACACS+ servers for authentication.

Default Configuration

The local user database is the default authentication method. This is the same as entering the command **aaa authentication login local**.

NOTE: If an authentication method is not defined, console users can log in without any authentication verification.

Command Mode

Global Configuration mode

User Guidelines

The default and additional list names created with the **aaa authentication login** command are used with the **login authentication** command.

Create a list by entering the **aaa authentication login** list-name method command for a particular protocol, where list-name is any character string used to name) this list. The method argument identifies the list of methods that the authentication algorithm tries, in the given sequence.

The additional methods of authentication are used only if the previous method returns an error, not if it fails. Specify **none** as the final method in the command line to ensure that the authentication succeeds even if all methods return an error.

Example

The following example sets the authentication login methods.

```
Console (config)# aaa authentication login default radius local
enable none
```

aaa authentication enable

The **aaa authentication enable** Global Configuration mode command sets an authentication method for accessing higher privilege levels. To restore the default authentication method, use the **no** form of this command.

Syntax

aaa authentication enable *{default | list-name} method* [*method2 ...*]

no aaa authentication enable *{default | list-name}*

Parameters

- **default**—Uses the listed authentication methods that follow this argument as the default method list, when accessing higher privilege levels.
- **list-name** —Specifies a name for the list of authentication methods activated when a user accesses higher privilege levels. (Length: 1–12 characters)
- **method [method2 ...]**—Specifies a list of methods that the authentication algorithm tries, in the given sequence. The additional authentication methods are used only if the previous method returns an error, not if it fails. Specify **none** as the final method in the command line to ensure that the authentication succeeds, even if all methods return an error. Select one or more methods from the following list:

Keyword	Description
enable	Uses the enable password for authentication.
line	Uses the line password for authentication.
none	Uses no authentication.
radius	Uses the list of all RADIUS servers for authentication. Uses username "$enabx$." where x is the privilege level.
tacacs	Uses the list of all TACACS servers for authentication. Uses username "$enabx$." where x is the privilege level.

Default Configuration

The **enable password** command is the default authentication login method. This is the same as entering the command **aaa authentication enable default enable**.

On a console, the enable password is used if a password exists. If no password is set, authentication still succeeds. This is the same as entering the command **aaa authentication enable default enable none**.

Command Mode

Global Configuration mode

User Guidelines

The default and additional list names created with the **aaa authentication enable** command are used with the **enable authentication** command.

All **aaa authentication enable default** requests sent by the device to a RADIUS or TACACS+ server include the username **$enabx$**., where **x** is the requested privilege level.

Create a list by entering the **aaa authentication enable** list-name method command where list-name is any character string used to name this list. The method argument identifies the list of methods that the authentication algorithm tries, in the given sequence.

The additional methods of authentication are used only if the previous method returns an error, not if it fails. Specify **none** as the final method in the command line to ensure that the authentication succeeds even if all methods return an error.

Example

The following example sets the enable password for authentication for accessing higher privilege levels.

```
Console(config)# aaa authentication enable default enable
```

login authentication

The **login authentication** Line Configuration mode command specifies the login authentication method list for a remote Telnet or console session. Use the **no** form of this command to restore the default authentication method.

Syntax

login authentication *{default | list-name}*

no login authentication

Parameters

- **default**—Uses the default list created with the **aaa authentication login** command.
- **list-name**—Uses the specified list created with the **aaa authentication login** command. (Length: 1–12 characters).

Default Configuration

The default is the **aaa authentication login** command default.

Command Mode

Line Configuration mode

Example

The following example specifies the login authentication method for a console session.

```
Console(config)# line console
Console(config-line)# login authentication default
```

enable authentication

The **enable authentication** Line Configuration mode command specifies the authentication method for accessing a higher privilege level from a remote Telnet or console. Use the **no** form of this command to restore the default authentication method.

Syntax

enable authentication *{default | list-name}*

no enable authentication

Parameters

- **default**—Uses the default list created with the **aaa authentication enable** command.
- **list-name**—Uses the specified list created with the **aaa authentication enable** command. (Length: 1–12 characters).

Default Configuration

The default is the **aaa authentication enable** command default.

Command Mode

Line Configuration mode

Example

The following example specifies the authentication method when accessing a higher privilege level from a console.

```
Console(config)# line console
Console(config-line)# enable authentication default
```

ip http authentication

The **ip http authentication** Global Configuration mode command specifies authentication methods for HTTP server access. Use the **no** form of this command to restore the default authentication method.

Syntax

ip http authentication aaa login-authentication *method1 [method2...]*

no ip http authentication aaa login-authentication

Parameters

method [**method2** ...]—Specifies a list of methods that the authentication algorithm tries, in the given sequence. The additional authentication

methods are used only if the previous method returns an error, not if it fails. Specify **none** as the final method in the command line to ensure that the authentication succeeds, even if all methods return an error. Select one or more methods from the following list:

Keyword	Description
local	Uses the local username database for authentication.
none	Uses no authentication.
radius	Uses the list of all RADIUS servers for authentication.
tacacs	Uses the list of all TACACS+ servers for authentication.

Default Configuration

The local user database is the default authentication login method. This is the same as entering the **ip http authentication local** command.

Command Mode

Global Configuration mode

User Guidelines

The command is relevant for HTTP and HTTPS server users.

The additional methods of authentication are used only if the previous method returns an error, not if it fails. Specify **none** as the final method in the command line to ensure that the authentication succeeds, even if all methods return an error.

Example

The following example specifies the HTTP access authentication methods.

```
Console(config)# ip http authentication aaa login-authentication
radius local
```

show authentication methods

The **show authentication methods** Privileged EXEC mode command displays information about the authentication methods.

Syntax
show authentication methods

Command Mode
Privileged EXEC mode

Example
The following example displays the authentication configuration.

```
Console# show authentication methods

Login Authentication Method Lists
---------------------------------
Default: Radius, Local, Line
Console_Login: Line, None

Enable Authentication Method Lists
----------------------------------
Default: Radius, Enable
Console_Enable: Enable, None

Line                  Login Method List   Enable Method List
--------------        -----------------   ------------------
Console               Console_Login       Console_Enable
Telnet                Default             Default
SSH                   Default             Default

HTTP: Radius, local
HTTPS: Radius, local
Dot1x: Radius
```

password

The **password** Line Configuration mode command specifies a password on a line, also known as access method, such as a console or Telnet. Use the **no** form of this command to return to the default password.

Syntax

password *password [encrypted]*

no password

Parameters

- **password**—Specifies the password for this line. (Length: 0–159 characters)
- **encrypted**—Specifies that the password is encrypted and copied from another device configuration.

Default Configuration

No password is defined.

Command Mode

Line Configuration mode

Example

The following example specifies the password 'secret' on a console.

```
Console(config)# line console
Console(config-line)# password secret
```

service password-recovery

Use the **service password-recovery** global configuration mode command to enable full functionality of the password-recovery mechanism. Use the **no service password-recovery** command to allow password-recovery mechanism without keeping the configuration and user files.

Syntax

service password-recovery

no service password-recovery

Parameters

N/A

Default Configuration
The full service password recovery is enabled by default.

Command Mode
Gobal Configuration mode

User Guidelines
This mechanism allows an end user, with physical access to the console port of the device, to enter the boot menu and trigger the password recovery process. The following functionality occurs:

- If password recovery is enabled, the user can access the boot menu and trigger the password recovery in the boot menu. All configuration files and user files are kept.
- If password recovery is disabled, the user still can access the boot menu and trigger the password recovery in the boot menu. However, the configuration files and user files are removed, and the following log message is generated to the terminal: "All the configuration and user files were removed"

Example
The following command disables password recovery:

```
console# no service password recovery
Note that choosing to use Password recovery option in the
Boot Menu during the boot process will remove the
configuration files and the user files. Would you like to
continue ? Y/N.
```

enable password

Use the **enable password** Global Configuration mode command to set a local password to control access to normal and privilege levels. Use the **no** form of this command to return to the default password.

Syntax

enable password *[* ***level*** *privilege-level] { password | encrypted encrypted-password }*

no enable password *[level level]*

Parameters

- **level** *privilege-level*—Level for which the password applies. If not specified the level is 15. (Range: 1–15)
- **password**—Password for this level. (Range: 0–159 chars)
- **encrypted-password**—Encrypted password you enter, copied from another device configuration.

Default

Default for **level** is 15.

Command Mode

Global Configuration mode

Example

```
console(config)# enable password level 15 let-me-in
```

username

Use the **username** Global Configuration mode command to establish a username-based authentication system. Use the **no** form to remove a user name.

Syntax

username *name { nopassword | **password** password | **privilege** privilege-level | **password encrypted** encrypted-password }*

username *name*

no username *name*

Parameters

- **name**—The name of the user. (Range: 1–20 characters)
- **nopassword**—No password is required for this user to log in.
- **password**—The authentication password for the user. (Range: 1–159)
- **password-encrypted**—Encrypted password you enter, copied from another device configuration.
- **privilege** *privilege-level*—Privilege level for which the password applies. If not specified the level is 15. (Range: 1–15)

Default
No user is defined.

Command Mode
Global Configuration mode

Example

```
console(config)# username tom privilege 15 password 1234
```

show user accounts

The **show user accounts** Privileged EXEC mode command displays information about the users local database.

Syntax
show user accounts

Command Mode
Privileged EXEC mode

Example
The following example displays information about the users local database.

```
Console# show user accounts


Username        Privilege
--------        ---------
Bob             15
Robert          15
Smith           15
```

The following table describes the significant fields shown in the display:

Field	Description
Username	The user name.
Privilege	The user's privilege level.

aaa accounting login

Use the **aaa accounting login** command in Global Configuration mode to enable accounting of device management sessions. Use the **no** form of this command to disable accounting.

Syntax
aaa accounting login *start-stop group radius*

no aaa accounting login *start-stop group radius*

Parameters
This command has no arguments or keywords.

Default
Disabled

Command Mode
Global Configuration mode

User Guidelines

This command enables the recording of device management sessions (Telnet, serial and WEB but not SNMP).

It records only users that were identified with a username (e.g. a user that was logged in with a line password is not recorded).

If accounting is activated, the device sends a "start"/"stop" messages to a Radius server when a user logs in / logs out respectively.

The device uses the configured priorities of the available Radius servers in order to select the Radius server.

The following table describes the supported Radius accounting Attributes Values, and when they are sent by the switch.

Name	Start	Stop	Description
User-Name (1)	Yes	Yes	User's identity.
NAS-IP-Address (4)	Yes	Yes	The switch IP address that is used for the session with the Radius server.
Class (25)	Yes	Yes	Arbitrary value is included in all accounting packets for a specific session.
Called-Station-ID (30)	Yes	Yes	The switch IP address that is used for the management session.
Calling-Station-ID (31)	Yes	Yes	The user IP address.
Acct-Session-ID (44)	Yes	Yes	A unique accounting identifier.
Acct-Authentic (45)	Yes	Yes	Indicates how the supplicant was authenticated.
Acct-Session-Time (46)	No	Yes	Indicates how long the user was logged in.
Acct-Terminate-Cause (49)	No	Yes	Reports why the session was terminated.

Example

```
console(config)# aaa accounting login start-stop group radius
```

aaa accounting dot1x

To enable accounting of 802.1x sessions, use the **aaa accounting dot1x** Global Configuration mode command. Use the **no** form of this command to disable accounting.

Syntax

aaa accounting dot1x *start-stop group radius*

no aaa accounting dot1x *start-stop group radius*

Parameters

This command has no arguments or keywords.

Default

Disabled

Command Mode

Global Configuration mode

User Guidelines

This command enables the recording of 802.1x sessions.

If accounting is activated, the device sends a “start”/“stop” messages to a Radius server when a user logs in / logs out to the network, respectively.

The device uses the configured priorities of the available Radius servers in order to select the Radius server.

If a new replaces an old supplicant (even if the port state remains authorized), the software sends a “stop” message for the old supplicant and a “start” message for the new supplicant.

In multiple sessions mode (dot1x multiple-hosts authentication), the software sends “start”/“stop” messages for each authenticated supplicant.

In multiple hosts mode (dot1x multiple-hosts), the software sends “start”/“stop” messages only for the supplicant that has been authenticated.

The software does not send “start”/“stop” messages if the port is force-authorized.

The software does not send “start”/“stop” messages for hosts that are sending traffic on the guest VLAN or on the unauthenticated VLANs.

The following table describes the supported Radius accounting Attributes Values and when they are sent by the switch.

Name	Start	Stop	Description
User-Name (1)	Yes	Yes	Supplicant’s identity.
NAS-IP-Address (4)	Yes	Yes	The switch IP address that is used for the session with the Radius server.
NAS-Port (5)	Yes	Yes	The switch port from where the supplicant has logged in.
Class (25)	Yes	Yes	Arbitrary value is included in all accounting packets for a specific session.
Called-Station-ID (30)	Yes	Yes	The switch MAC address.
Calling-Station-ID (31)	Yes	Yes	The supplicant MAC address.
Acct-Session-ID (44)	Yes	Yes	A unique accounting identifier.
Acct-Authentic (45)	Yes	Yes	Indicates how the supplicant was authenticated.
Acct-Session-Time (46)	No	Yes	Indicated how long the supplicant was logged in.
Acct-Terminate-Cause (49)	No	Yes	Reports why the session was terminated.
Nas-Port-Type (61)	Yes	Yes	Indicates the supplicant physical port type.

Example

```
console(config)# aaa accounting dot1x start-stop group radius
```

show accounting

The **show accounting** EXEC mode command displays information about the accounting status.

Syntax

show accounting

Command Mode

EXEC mode

Example

The following example displays information about the accounting status.

```
Console# show accounting

Login: Radius
802.1x: Disabled
```

passwords min-length

The **passwords min-length** Global Configuration mode command configures the minimal password length in the local database. Use the **no** form of this command to remove the restriction.

Syntax

passwords min-length *length*

no passwords min-length

Parameters

length—Specifies the minimal length required for passwords. (Range: 8-64)

Default Configuration

There is no minimal length requirement until this command is executed.

Command Mode
Global Configuration mode

User Guidelines
The setting is relevant to local user passwords, line passwords, and enable passwords.

The software checks the minimum length requirement when defining a password in an unencrypted format, or when a user tries to log in.

Note that if a password is inserted in encrypted format, the minimum length requirement is checked during user login only.

Passwords that were defined before defining the minimum length requirement are only checked during user login.

Example
The following example configures the minimal required password length to 8 characters.

```
Console (config)# passwords min-length 8
```

passwords strength-check enable

Use the **passwords strength-check enable** Global Configuration mode command to enforce minimum password strength. The no form of this command disables enforcing password strength.

Syntax
passwords strength-check enable

no passwords strength-check enable

Parameters
This command has no arguments or keywords

Default
Disabled

Command Mode
Global Configuration mode

User Guidelines
If password strength is enabled, the user is forced to enter passwords that:

- Contain characters from user-defined several character classes (uppercase letters, lowercase letters, numbers, and special characters available on a standard keyboard).
- Contain no character that is repeated more than user-defined times consecutively.

The user can control the above attributes of password strength with specific commands.

Example
The following example enables password strength and configures the character classes to 3.

```
Console (config)# passwords strength-check enable
Console (config)# passwords strength minimum character-classes 3
```

passwords strength minimum character-classes

Use the **passwords strength minimum character-classes** Global Configuration mode command to configure the minimal classes required for passwords in the local database. Use the **no** form to remove the requirement.

Syntax
passwords strength minimum character-classes *number*

no passwords strength minimum character-classes

Parameters
number—The minimal length required for passwords.(Range: 0–4)

Default
0

Command Mode
Global Configuration mode

User Guidelines
The setting is relevant to local users' passwords, line passwords and enable passwords.

The software checks the minimum length requirement when you define a password in an unencrypted format.

The classes are: upper case letters, lower case letters, numbers and special characters.

passwords strength max-limit repeated-characters

Use the **passwords strength max-limit repeated-characters** Global Configuration mode command to configure the maximum number of characters in the new password that can be repeated consecutively. Use the **no** form to remove the requirement.

Syntax
passwords strength max-limit repeated-characters *number*

no passwords strength max-limit repeated-characters

Parameters
number—The maximum number of characters in the new password that can be repeated consecutively. (Range: 1–16)

Default
1

Command Mode
Global Configuration mode

User Guidelines
The setting is relevant to local users' passwords, line passwords and enable passwords. The software checks the maximum number of characters in the new password that can be repeated consecutively.

passwords aging

Use the **passwords aging** Global Configuration mode command to enforce password aging. Use the **no** form of this command to return to default.

Syntax
passwords aging *days*

no passwords aging

Parameters
days—Specifies the number of days before a password change is forced. You can use 0 to disable aging. (Range: 0–365)

Default
Disabled

Command Mode
Global Configuration mode

User Guidelines
Aging is relevant only to users of the local database with privilege level 15 and to "enable" a password of privilege level 15.

Example
The following example configures the aging time to be 24.

```
Console (config)# passwords aging 24
```

passwords history

The **passwords history** Global Configuration mode command configures the number of password changes required before a password can be reused. Use the **no** form of this command to remove the requirement.

Syntax

passwords history *number*

no passwords history

Parameters

number—Specifies the number of password changes required before a password can be reused. (Range: 1–8)

Default Configuration

Password history is disabled.

Command Mode

Global Configuration mode

User Guidelines

The setting is relevant to local users' passwords, line passwords and enable passwords.

Password history is not checked during a configuration download.

The password history is kept even if the password history check is disabled.

The password history for a user is kept as long as the user is defined.

Example

The following example sets the number of password changes required before a password can be reused to 10.

```
Console(config)# passwords history 10
```

passwords history hold-time

The **passwords history hold-time** Global Configuration mode command configures the duration that a password is relevant for tracking passwords history. Use the **no** form of this command to return to the default configuration.

Syntax

passwords history hold-time *days*

no passwords history hold-time

Parameters

days—Specifies the number of days a password is relevant for tracking passwords history. (Range: 1–365)

Default Configuration

Command Mode

Global Configuration mode

User Guidelines

The setting is relevant to local users' passwords, line passwords and enable passwords.

The passwords are not deleted from the history database when they are not relevant for the password history tracking. Increasing the hold time might "return back" passwords.

Example

The following example configures the duration that a password is relevant for tracking passwords history.

```
Console(config)# passwords history hold-time 10
```

passwords lockout

The **passwords lockout** Global Configuration mode command enables user account lockout after a series of authentication failures. Use the **no** form of this command to disable the lockout feature.

Syntax

passwords lockout *number*

no passwords lockout

Parameters

number—Specifies the number of authentication failures before the user account is locked-out. (Range: 1–5)

Default Configuration

Lockout is disabled.

Command Mode

Global Configuration mode

User Guidelines

The setting is relevant to local users' passwords, line passwords and enable passwords.

The account is not locked out for access from the local console.

A user with privilege level 15 can release accounts that are locked out by using the **set username active**, **set enable-password active** and **set line active** Privileged EXEC mode commands.

Disabling lockout unlocks all users.

Re-enabling lockout resets the authentication failures counters.

Changing the authentication failures threshold does not reset the counters.

Example
The following example enables user account lockout after 3 successive authentication failures.

```
Console(config)# passwords lockout 3
```

aaa login-history file

The **aaa login-history file** Global Configuration mode command enables writing to the login history file. Use the **no** form of this command to disable writing to the login history file.

Syntax
aaa login-history file

no aaa login-history file

Default Configuration
Writing to the login history file is enabled.

Command Mode
Global Configuration mode

User Guidelines
The login history is stored in the device internal buffer.

Example
The following example enables writing to the login history file.

```
Console(config)# aaa login-history file
```

set username active

The **set username active** Privileged EXEC mode command reactivates a locked out user account.

Syntax
set username *name* **active**

Parameters
name—Specifies the user name: (Length: 1–20 characters)

Default Configuration
There is no default configuration for this command.

Command Mode
Privileged EXEC mode

Example
The following example reactivates user 'Bob'.

```
Console(config)# set username Bob active
```

set line active

The **set line active** Privileged EXEC mode command reactivates a locked out line.

Syntax
set line *{console | telnet | ssh}* **active**

Parameters

- **console**—Reactivates the console terminal line.
- **telnet**—Reactivates the virtual terminal for remote (Telnet) console access.
- **ssh**—Reactivates the virtual terminal for secured remote (SSH) console access.

Default Configuration
There is no default configuration for this command.

Command Mode
Privileged EXEC mode

Example
The following example reactivates the virtual terminal for remote (Telnet) console access.

```
Console(config)# set line telnet active
```

set enable-password active

The **set enable-password active** Privileged EXEC mode command reactivates a locked out local password.

Syntax
set enable-password *level* **active**

Parameters
level—Specifies the privilege level to which the password applies. (Range 1–15)

Default Configuration
There is no default configuration for this command.

Command Mode
Privileged EXEC mode

Example
The following example reactivates a local password that applies to privilege level 1.

```
Console(config)# set enable-password 1 active
```

show passwords configuration

The **show passwords configuration** Privileged EXEC mode command displays information about the password management configuration.

Syntax

show passwords configuration

Parameters

Command Mode

Privileged EXEC mode

Example

```
Console# show passwords configuration
Passwords aging is enabled with aging time 180 days.
Minimal length: 8
Minimum character classes: 4
Maximal number of repeated characters: 2
History: 10
History hold time: 365 days
Lockout control: Disabled
Enable Passwords
Level   Lockout
-----  ---------
1       1
15      0

Line Passwords
Line    Lockout
-----   ------------
Console-
Telnet  LOCKOUT
SSH     0
```

The following table describes the significant fields shown in the display:

Field	Description
Minimal length	The minimal length required for passwords in the local database.
Minimal character classes	The minimal number of different types of characters (special characters, integers and so on) required to be part of the password.
Maximum number of repeated characters	The maximum number of times a singe character can be repeated in the password.
History	The number of password changes required before a password in the local database can be reused.
History hold time	The duration that a password is relevant for tracking password history.
Lockout control	The user account lockout control status after a series of authentication failures.
Level	The applied password privilege level.
Aging	The password aging time in days.
Expiry date	The password expiration date.
Lockout	If lockout control is enabled, the specific number of times a user failed to enter the correct password since the last successful login is displayed. If the user is locked out, "LOCKOUT" is displayed.
Line	The applied password line type.

show users login-history

The **show users login-history** Privileged EXEC mode command displays information about the user's login history.

Syntax

show users login-history *[username name]*

Parameters

name—Name of the user. (Range: 1–20 characters)

Command Mode
Privileged EXEC mode

Example
The following example displays information about the users' login history.

```
Console# show users login-history

File save: Enabled.

Login Time              Username    Protocol     Location
--------------------    ----------  ----------   ------------
Jan 18 2004 23:58:17    Robert      HTTP         172.16.1.8
Jan 19 2004 07:59:23    Robert      HTTP         172.16.0.8
Jan 19 2004 08:23:48    Bob         Serial
Jan 19 2004 08:29:29    Robert      HTTP         172.16.0.8
Jan 19 2004 08:42:31    John        SSH          172.16.0.1
Jan 19 2004 08:49:52    Betty       Telnet       172.16.1.7
```

15

RADIUS Commands

radius-server host

Use the **radius-server host** Global Configuration mode command to specify a RADIUS server host. Use the no form of the command to delete the specified RADIUS server host.

Syntax

radius-server host *{ipv4-address | ipv6-address | ipv6z-address | hostname} [auth-port auth-port-number] [timeout timeout] [retransmit retries] [deadtime deadtime] [key key-string] [source {ipv4-address | ipv6-address}] [priority priority] [usage {login | 802.1x | all}*]

no radius-server host {*ipv4-address* | *ipv6-address* | *hostname*}

Parameters

- **ipv4-address**—Specifies the RADIUS server host IPv4 address.
- **ipv6-address**—Specifies the RADIUS server host IPv6 address.
- **ipv6z-address**—Specifies the RADIUS server host IPv6Z address. The IPv6Z address format is: **{ipv6-link-local-address}%{interface-name}**. The subparameters are:
  - **ipv6-link-local-address**—Specifies the IPv6 Link Local address.
  - **interface-name**—Specifies the outgoing interface name. The interface name has the format: **vlan{integer} | ch{integer} | isatap{integer} | {physical-port-name}**.
  - The subparameter **integer** has the format: **{decimal-digit} | {integer}{decimal-digit}**. **decimal-digit** has the range 0–9.

- **hostname**—Specifies the RADIUS server host name. Translation to IPv4 addresses only is supported. (Length: 1–158 characters. Maximum label length: 63 characters)
- **auth-port auth-port-number**—Specifies the port number for authentication requests. If the port number is set to 0, the host is not used for authentication. (Range: 0–65535)
- **timeout timeout**—Specifies the timeout value in seconds. (Range: 1–30)
- **retransmit retries**—Specifies the retransmit value. (Range: 1–10)
- **deadtime deadtime**—Specifies the length of time in minutes during which a RADIUS server is skipped over by transaction requests. (Range: 0–2000)
- **key key-string**—Specifies the authentication and encryption key for all RADIUS communications between the device and the RADIUS server. This key must match the encryption used on the RADIUS daemon. To specify an empty string, enter "". (Length: 0–128 characters)
- **source {ipv4-address | ipv6-address}**—Specifies the source IPv4 or IPv6 address to use for communication. 0.0.0.0 is interpreted as a request to use the IP address of the outgoing IP interface.
- **priority priority**—Specifies the order in which servers are used, where 0 has the highest priority. (Range: 0–65535)
- **usage {login | 802.1x | all}**—Specifies the RADIUS server usage type. The possible values are:
  - **login**—Specifies that the RADIUS server is used for user login parameters authentication.
  - **802.1x**—Specifies that the RADIUS server is used for 802.1x port authentication.
  - **all**—Specifies that the RADIUS server is used for user login parameters authentication and 802.1x port authentication.

Default Configuration

No RADIUS host is specified; the global **radius-server** command values are the default values.

The default authentication port number is 1812.

If **timeout** is not specified, the global value is used.

If **retransmit** is not specified, the global value is used.

If **key-string** is not specified, the global value is used.

If the **source** value is not specified, the global value is used.

The default usage type is **all**.

Command Mode
Global Configuration mode

User Guidelines
To specify multiple hosts, multiple **radius-server host** commands can be used.

If no host-specific **timeout, retries, deadtime** or **key-string** values are specified, the global values apply to each RADIUS server host.

The **source** parameter address type must be the same as that of the **host** parameter.

Example
The following example specifies a RADIUS server host with IP address 192.168.10.1, authentication request port number 20, and a 20-second timeout period.

```
Console(config)# radius-server host 192.168.10.1 auth-port 20
timeout 20
```

radius-server key

Use the **radius-server key** Global Configuration mode command to set the authentication and encryption key for all RADIUS communications between the device and the RADIUS daemon. Use the **no** form of this command to restore the default configuration.

Syntax
radius-server key [*key-string*]

no radius-server key

Parameters

key-string—Specifies the authentication and encryption key for all RADIUS communications between the device and the RADIUS server. This key must match the encryption used on the RADIUS daemon. (Range: 0–128 characters)

Default Configuration

The key-string is an empty string.

Command Mode

Global Configuration mode

Example

The following example defines the authentication and encryption key for all RADIUS communications between the device and the RADIUS daemon.

```
Console(config)# radius-server key enterprise-server
```

radius-server retransmit

Use the **radius-server retransmit** Global Configuration mode command to specify the number of times the software searches the list of RADIUS server hosts. Use the no form of this command to restore the default configuration.

Syntax

radius-server retransmit *retries*

no radius-server retransmit

Parameters

retries—Specifies the retransmit value. (Range: 1–10)

Default Configuration

The software searches the list of RADIUS server hosts 3 times.

Command Mode

Global Configuration mode

Example
The following example configures the number of times the software searches all RADIUS server hosts as 5.

```
console(config)# radius-server retransmit 5
```

radius-server source-ip
Use the **radius-server source-ip** Global Configuration mode command to specify the source IP address used for communication with RADIUS servers. Use the no form of this command to restore the default configuration.

Syntax
radius-server source-ip {*source*}

no radius-server source-ip {*source*}

Parameters
source—Specifies the source IP address.

Default Configuration
The source IP address is the IP address of the outgoing IP interface.

Command Mode
Global Configuration mode

User Guidelines
If there is no available IP interface of the configured IP source address, an error message is issued when attempting to communicate with the IP address.

Example
The following example configures the source IP address used for communication with all RADIUS servers to 10.1.1.1.

```
console(config)# radius-server source-ip 10.1.1.1
```

radius-server source-ipv6

Use the **radius-server source-ipv6** Global Configuration mode command to specify the source IPv6 address used for communication with RADIUS servers. Use the no form of this command to restore the default configuration.

Syntax

radius-server source-ipv6 {*source*}

no radius-server source-ipv6 {*source*}

Parameters

source—Specifies the source IPv6 address.

Default Configuration

The source IP address is the IP address of the outgoing IP interface.

Command Mode

Global Configuration mode

User Guidelines

If there is no available IP interface of the configured IP source address, an error message is issued when attempting to communicate with the IP address.

Example

The following example configures the source IP address used for communication with all RADIUS servers to 3ffe:1900:4545:3:200:f8ff:fe21:67cf.

```
console(config)# radius-server source-ipv6
3ffe:1900:4545:3:200:f8ff:fe21:67cf
```

radius-server timeout

Use the **radius-server timeout** Global Configuration mode command to set the time interval during which the device waits for a server host to reply. Use the **no** form of this command to restore the default configuration.

Syntax

radius-server timeout *timeout*

no radius-server timeout

Parameters

timeout—Specifies the timeout value in seconds. (Range: 1–30)

Default Configuration

The default timeout value is 3 seconds.

Command Mode

Global Configuration mode

Example

The following example sets the timeout interval on all RADIUS servers to 5 seconds.

```
Console(config)# radius-server timeout 5
```

radius-server deadtime

Use the **radius-server deadtime** Global Configuration mode command to configure the time interval during which unavailable RADIUS servers are skipped over by transaction requests. This improves RADIUS response time when servers are unavailable. Use the **no** form of this command to restore the default configuration.

Syntax

radius-server deadtime *deadtime*

no radius-server deadtime

Parameters
deadtime—Specifies the time interval in minutes during which a RADIUS server is skipped over by transaction requests. (Range: 0–2000)

Default Configuration
The default deadtime interval is 0.

Command Mode
Global Configuration mode

Example
The following example sets all RADIUS server deadtimes to 10 minutes.

```
Console(config)# radius-server deadtime 10
```

show radius-servers

Use the **show radius-servers** Privileged EXEC mode command to display the RADIUS server settings.

Syntax
show radius-servers

Command Mode
Privileged EXEC mode

Example

The following example displays RADIUS server settings.

```
Console# show radius-servers

            Port   Port
IP address  Auth   Acct   Time     Retrans   Dead     Source  Priority  Usage
----------  ----   ----   Out      mit       time     IP      --------  -----
172.16.1.1  1812   1813   -----    -------   ------   ------  1         All
172.16.1.2  1812   1813   Global   Global    Global   Global  2         All
                          11       8         Global   Global


Global values
--------------
TimeOut: 3
Retransmit: 3
Deadtime: 0
Source IP: 172.16.8.1
```

16

TACACS+ Commands

tacacs-server host

Use the **tacacs-server host** Global Configuration mode command to specify a TACACS+ host. Use the **no** form of this command to delete the specified TACACS+ host.

Syntax

tacacs-server host {*ip-address* | *hostname*} *[single-connection] [port port-number] [timeout timeout] [key key-string] [source {source}] [priority priority]*

no tacacs-server host {*ip-address* | *hostname*}

Parameters

- **ip-address**—Specifies the TACACS+ server host IP address.
- **hostname**—Specifies the TACACS+ server host name. (Length: 1?158 characters. Maximum label length: 63 characters)
- **single-connection**—Specifies that a single open connection is maintained between the device and the daemon, instead of the device opening and closing a TCP connection to the daemon each time it communicates.
- **port port-number**—Specifies the server port number. If the port number is 0, the host is not used for authentication. (Range: 0–65535)
- **timeout timeout**—Specifies the timeout value in seconds. (Range: 1–30)
- **key key-string**—Specifies the authentication and encryption key for all TACACS+ communications between the device and the TACACS+ server. This key must match the encryption used on the TACACS+ daemon. To specify an empty string, enter "". (Length: 0?128 characters)

- **source {source}**—Specifies the source IP to use for the communication. 0.0.0.0 indicates a request to use the outgoing IP interface IP address.
- **priority priority**—Specifies the order in which the TACACS+ servers are used, where 0 is the highest priority. (Range: 0–65535)

Default Configuration

No TACACS+ host is specified.

The default **port-number** is 49.

If **timeout** is not specified, the global value is used.

If **key-string** is not specified, the global value is used.

If **source** is not specified, the global value is used.

Command Mode

Global Configuration mode

User Guidelines

Multiple **tacacs-server host** commands can be used to specify multiple hosts.

If no host-specific timeout, key, or source values are specified, the global values apply to each host. Example

The following example specifies a TACACS+ host.

```
Console(config)# tacacs-server host 172.16.1.1
```

tacacs-server key

Use the **tacacs-server key** Global Configuration mode command to ses the authentication encryption key used for all TACACS+ communications between the device and the TACACS+ daemon. Use the **no** form of this command to disable the key.

Syntax

tacacs-server key *key-string*

no tacacs-server key

Parameters

key-string—Specifies the authentication and encryption key for all TACACS+ communications between the device and the TACACS+ server. This key must match the encryption used on the TACACS+ daemon. (Length: 0–128 characters)

Default Configuration

The default key is an empty string.

Command Mode

Global Configuration mode

Example

The following example sets Enterprise as the authentication encryption key for all TACACS+ servers.

```
Console(config)# tacacs-server key enterprise
```

tacacs-server timeout

Use the **tacacs-server timeout** Global Configuration mode command to set the interval during which the device waits for a TACACS+ server to reply. Use the **no** form of this command to restore the default configuration.

Syntax

tacacs-server timeout *timeout*

no tacacs-server timeout

Parameters

timeout—Specifies the timeout value in seconds. (Range: 1–30)

Default Configuration

The default timeout value is 5 seconds.

Command Mode

Global Configuration mode

Example
The following example sets the timeout value to 30 for all TACACS+ servers.

```
Console(config)# tacacs-server timeout 30
```

tacacs-server source-ip

Use the **tacacs-server source-ip** Global Configuration mode command to configure the source IP address to be used for communication with TACACS+ servers. Use the no form of this command to restore the default configuration.

Syntax
tacacs-server source-ip {*source*}

no tacacs-server source-ip {*source*}

Parameters
source—Specifies the source IP address. (Range: Valid IP address)

Default Configuration
The default source IP address is the outgoing IP interface address.

Command Mode
Global Configuration mode

User Guidelines
If the configured IP source address has no available IP interface, an error message is issued when attempting to communicate with the IP address.

Example
The following example specifies the source IP address for all TACACS+ servers.

```
Console(config)# tacacs-server source-ip 172.16.8.1
```

show tacacs

Use the **show tacacs** Privileged EXEC mode command to display configuration and statistical information for a TACACS+ server.

Syntax

show tacacs [*ip-address*]

Parameters

ip-address—Specifies the TACACS+ server name or IP address.

Default Configuration

If **ip-address** is not specified, information for all TACACS+ servers is displayed.

Command Mode

Privileged EXEC mode

Example

The following example displays configuration and statistical information for all TACACS+ servers.

```
Console# show tacacs

IP address   Status     Port   Single        Time     Source   Priority
                               Connection    Out      IP
--------     --------   ---    ---------              -------  ------
172.16.1.1   Connected  49     No            -----    -----    1
                                             Global   Global

Global values
-------------
TimeOut: 3
Source IP: 172.16.8.1
```

17

Syslog Commands

logging on

Use the **logging on** Global Configuration mode command to control error message logging. This command sends debug or error messages to a logging process, which logs messages asynchronously to designated locations for the process that generated the messages. Use the **no** form of this command to disable the logging process.

Syntax

logging on

no logging on

Default Configuration

Message logging is enabled.

Command Mode

Global Configuration mode

User Guidelines

The logging process controls the logging messages distribution at various destinations, such as the logging buffer, logging file or syslog server. Logging on and off at these destinations can be individually configured using the **logging buffered**, **logging file**, and **logging** Global Configuration mode commands. However, if the **logging on** command is disabled, no messages are sent to these destinations. Only the console receives messages.

Example
The following example enables logging error messages.

```
Console(config)# logging on
```

Logging host

Use the **logging host** global configuration command to log messages to a syslog server. Use the **no** form of this command to delete the syslog server with the specified address from the list of syslogs.

Syntax
logging host *{ipv4-address | ipv6-address | hostname} [port port] [severity level] [facility facility] [description text]*

no logging host *{ipv4-address | ipv6-address | hostname}*

Parameters

- **ipv4-address**—IPv4 address of the host to be used as a syslog server.
- **ipv6-address**—Pv6 address of the host to be used as a syslog server. When the IPv6 address is a Link Local address (IPv6Z address), the outgoing interface name must be specified. Refer to the User Guidelines for the interface name syntax.
- **hostname**—Hostname of the host to be used as a syslog server. Only translation to IPv4 addresses is supported. (Range: 1–158 characters. Maximum label size: 63)
- **port**—Port number for syslog messages. If unspecified, the port number defaults to 514. (Range: 1–65535)
- **level**—Limits the logging of messages to the syslog servers to a specified level: emergencies, alerts, critical, errors, warnings, notifications, informational, debugging.
- **facility**—The facility that is indicated in the message. It can be one of the following values: local0, local1 , local2 , local3 , local4 , local5 , local 6, local7. If unspecified, the port number defaults to local7.
- text—Description of the syslog server. (Range: Up to 64 characters)

Default
No messages are logged to a syslog server host.

Command Mode
Global Configuration mode

User Guidelines
You can use multiple syslog servers.

The format of an IPv6Z address is: *<ipv6-link-local-address>%<interface-name>*

interface-name = *vlan<integer> | ch<integer> | isatap<integer> | <physical-port-name> | 0*

integer = *<decimal-number> | <integer><decimal-number>*

decimal-number = 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9

physical-port-name = Designated port number, for example 1/0/16.

If the egress interface is not specified, the default interface is selected. Specifying interface zone=0 is equal to not defining an egress interface.

Examples

```
console(config)# logging host 1.1.1.121
```

```
console(config)# logging host 3000::100
```

logging console

Use the **logging console** Global Configuration mode command to limit messages logged to the console to messages with a specific severity level. Use the **no** form of this command to disable logging limiting to the console.

Syntax
logging console *level*

no logging console

Parameters

level—Specifies the severity level of logged messages displayed on the console. The possible values are: emergencies, alerts, critical, errors, warnings, notifications, informational and debugging.

Default Configuration

The default severity level is informational.

Command Mode

Global Configuration mode

Example

The following example limits logging messages displayed on the console to messages with severity level errors.

```
Console(config)# logging console errors
```

logging buffered

Use the **logging buffered** Global Configuration mode command to limit the syslog message display from an internal buffer to messages with a specific severity leve, and to define the buffer sizel. Use the **no** form of this command to cancel using the buffer and returning the buffer size to defult

Syntax

logging buffered [*buffer-size*] [severity-*level*]

no logging buffered

Parameters

buffer-size—Specifies the maximum number of messages stored in the history table. (Range: 20–400)

severity-*level*—Specifies the severity level of messages logged in the buffer. The possible values are: emergencies, alerts, critical, errors, warnings, notifications, informational and debugging.

Default Configuration
The default severity level is informational.

Command Mode
Global Configuration mode

User Guidelines
All the syslog messages are logged to the internal buffer. This command limits the messages displayed to the user.

Example
The following example limits the syslog message display from an internal buffer to messages with severity level **debugging**.

```
Console(config)# logging buffered debugging
```

clear logging

Use the **clear logging** Privileged EXEC mode command to clear messages from the internal logging buffer.

Syntax
clear logging

Command Mode
Privileged EXEC mode

Example
The following example clears messages from the internal logging buffer.

```
Console# clear logging
Clear logging buffer [confirm]
```

logging file

Use the **logging file** Global Configuration mode command to limit syslog messages sent to the logging file to messages with a specific severity level. Use the **no** form of this command to cancel using the buffer.

Syntax

logging file *level*

no logging file

Parameters

level—Specifies the severity level of syslog messages sent to the logging file. The possible values are: emergencies, alerts, critical, errors, warnings, notifications, informational and debugging.

Default Configuration

The default severity level is errors.

Command Mode

Global Configuration mode

Example

The following example limits syslog messages sent to the logging file to messages with severity level alerts.

```
Console(config)# logging file alerts
```

clear logging file

Use the **clear logging file** Privileged EXEC mode command to clear messages from the logging file.

Syntax

clear logging file

Command Mode
Privileged EXEC mode

Example
The following example clears messages from the logging file.

```
Console# clear logging file
Clear Logging File [y/n]
```

aaa logging

Use the **aaa logging** Global Configuration mode command to enable logging AAA login events. Use the **no** form of this command to disable logging AAA login events.

Syntax
aaa logging *{login}*

no aaa logging *{login}*

Parameters
login—Enables logging messages related to successful AAA login events, unsuccessful AAA login events and other AAA login-related events.

Default Configuration
Logging of AAA login events is enabled.

Command Mode
Global Configuration mode

User Guidelines
This command enables logging messages related to successful login events, unsuccessful login events and other login-related events. Other types of AAA events are not subject to this command.

Example
The following example enables logging messages related to AAA login events.

```
Console(config)# aaa logging login
```

file-system logging

Use the **file-system logging** Global Configuration mode command to enable the logging of file system events. Use the **no** form of this command to disable logging file system events.

Syntax
file-system logging *{copy | delete-rename}*

no file-system logging *{copy | delete-rename}*

Parameters

- **copy**—Specifies logging messages related to file copy operations.
- **delete-rename**—Specifies logging messages related to file deletion and renaming operations.

Default Configuration
Logging file system events is enabled.

Command Mode
Global Configuration mode

Example
The following example enables logging messages related to file copy operations.

```
Console(config)# file-system logging copy
```

management logging

Use the **management logging** Global Configuration mode command to enable logging Management Access List (ACL) deny events. Use the **no** form of this command to disable logging management access list events.

Syntax

management logging {*deny*}

no management logging {*deny*}

Parameters

deny—Enables logging messages related to management ACL deny actions.

Default Configuration

Logging management ACL deny events is enabled.

Command Mode

Global Configuration mode

User Guidelines

Other management ACL events are not subject to this command.

Example

The following example enables logging messages related to management ACL deny actions.

```
Console(config)# management logging deny
```

show logging

Use the **show logging** Privileged EXEC mode command to display the logging status and the syslog messages stored in the internal buffer.

Syntax

show logging

Command Mode
Privileged EXEC mode

Example
The following example displays the logging status and the syslog messages stored in the internal buffer.

```
console# show logging
Logging is enabled.
Console Logging: Level info. Console Messages: 0 Dropped.
Buffer Logging: Level info. Buffer Messages: 61 Logged, 61 Displayed, 200
Max.
File Logging: Level error. File Messages: 898 Logged, 64 Dropped.
4 messages were not logged

Application filtering control
Application            Event                 Status
--------------------   ----------------      ---------
AAA                    Login                 Enabled
File system            Copy                  Enabled
File system            Delete-Rename         Enabled
Management ACL         Deny                  Enabled

Aggregation: Disabled.
Aggregation aging time: 300 Sec

01-Jan-2010 05:29:46 :%INIT-I-Startup: Warm Startup
01-Jan-2010 05:29:02 :%LINK-I-Up:  Vlan 1
01-Jan-2010 05:29:02 :%LINK-I-Up:  gi1/0/48
01-Jan-2010 05:29:02 :%LINK-I-Up:  gi1/0/47
01-Jan-2010 05:29:00 :%LINK-W-Down:  gi1/0/48
```

show logging file

Use the **show logging file** Privileged EXEC mode command to display the logging status and the syslog messages stored in the logging file.

Syntax
show logging file

Command Mode
Privileged EXEC mode

Example
The following example displays the logging status and the syslog messages stored in the logging file.

```
Logging is enabled.
Console Logging: Level info. Console Messages: 0 Dropped.
Buffer Logging: Level info. Buffer Messages: 61 Logged, 61 Displayed, 200
Max.
File Logging: Level error. File Messages: 898 Logged, 64 Dropped.
4 messages were not logged

Application filtering control
Application             Event                 Status
-----------------       ----------------      ---------
AAA                     Login                 Enabled
File system             Copy                  Enabled
File system             Delete-Rename         Enabled
Management ACL          Deny                  Enabled


Aggregation: Disabled.
Aggregation aging time: 300 Sec

01-Jan-2010 05:57:00 :%SSHD-E-ERROR: SSH error: key_read: type mismatch:
encoding error

01-Jan-2010 05:56:36 :%SSHD-E-ERROR: SSH error: key_read: type mismatch:
encoding error

01-Jan-2010 05:55:37 :%SSHD-E-ERROR: SSH error: key_read: type mismatch:
encoding error
```

```
01-Jan-2010 05:55:03 :%SSHD-E-ERROR: SSH error: key_read: key_from_blob
bgEgGnt9
z6NHgZwKI5xKqF7cBtdl1xmFgSEWuDhho5UedydAjVkKS5XR2... failed

01-Jan-2010 05:55:03 :%SSHD-E-ERROR: SSH error: key_from_blob: invalid key
type.

01-Jan-2010 05:56:34 :%SSHD-E-ERROR: SSH error: bad sigbloblen 58 !=
SIGBLOB_LEN
console#
```

show syslog-servers

Use the **show syslog-servers** Privileged EXEC mode command to display the syslog server settings.

Syntax

show syslog-servers

Command Mode

Privileged EXEC mode

Example

The following example displays the syslog server settings.

```
console# show syslog-servers

Device Configuration
----------------------------

IP address    Port   Severity  Facility Description
------------ ----   --------- -------- --------------
1.1.1.121     514    info      local7
3000::100     514    info      local7

console#
```

18

RMON Commands

show rmon statistics

Use the **show rmon statistics** EXEC mode command to display RMON Ethernet statistics.

Syntax

show rmon statistics *{interface-id}*

Parameters

interface-id—Specifies an interface ID. The interface ID can be one of the following types: Ethernet port or Port-channel.

Command Mode

EXEC mode

Example

The following example displays RMON Ethernet statistics for gigabitethernet port 1/0/1.

```
console# show rmon statistics gi1/0/1
Port gi1/0/1
Dropped: 0
Octets: 0                       Packets: 0
Broadcast: 0                    Multicast: 0
CRC Align Errors: 0             Collisions: 0
Undersize Pkts: 0               Oversize Pkts: 0
Fragments: 0                    Jabbers: 0
64 Octets: 0                    65 to 127 Octets: 1
```

```
128 to 255 Octets: 1              256 to 511 Octets: 1
512 to 1023 Octets: 0             1024 to max Octets: 0
```

The following table describes the significant fields displayed.

Field	Description
Dropped	The total number of events in which packets were dropped by the probe due to lack of resources. Note that this number is not necessarily the number of packets dropped. It is the number of times this condition was detected.
Octets	The total number of octets of data (including those in bad packets) received on the network (excluding framing bits but including FCS octets).
Packets	The total number of packets (including bad packets, broadcast packets, and multicast packets) received.
Broadcast	The total number of good packets received and directed to the broadcast address. This does not include multicast packets.
Multicast	The total number of good packets received and directed to a multicast address. This number does not include packets directed to the broadcast address.
CRC Align Errors	The total number of packets received with a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets, inclusive, but with either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error).
Collisions	The best estimate of the total number of collisions on this Ethernet segment.
Undersize Pkts	The total number of packets received, less than 64 octets long (excluding framing bits, but including FCS octets) and otherwise well formed.
Oversize Pkts	The total number of packets received, longer than 1518 octets (excluding framing bits, but including FCS octets) and otherwise well formed.

Field	Description
Fragments	The total number of packets received, less than 64 octets in length (excluding framing bits but including FCS octets) and either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error).
Jabbers	The total number of packets received, longer than 1518 octets (excluding framing bits, but including FCS octets), and either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error).
64 Octets	The total number of packets (including bad packets) received that are 64 octets in length (excluding framing bits but including FCS octets).
65 to 127 Octets	The total number of packets (including bad packets) received that are between 65 and 127 octets in length inclusive (excluding framing bits but including FCS octets).
128 to 255 Octets	The total number of packets (including bad packets) received that are between 128 and 255 octets in length inclusive (excluding framing bits but including FCS octets).
256 to 511 Octets	The total number of packets (including bad packets) received that are between 256 and 511 octets in length inclusive (excluding framing bits but including FCS octets).
512 to 1023 Octets	The total number of packets (including bad packets) received that were between 512 and 1023 octets in length inclusive (excluding framing bits but including FCS octets).
1024 to max	The total number of packets (including bad packets) received that were between 1024 octets and the maximum frame size in length inclusive (excluding framing bits but including FCS octets).

rmon collection stats

Use the **rmon collection stats** Interface Configuration mode command to enable Remote Monitoring (RMON) MIB history group of statistics on an

interface. Use the **no** form of this command to remove a specified RMON history group of statistics.

Syntax

rmon collection stats index *[owner ownername] [buckets bucket-number] [interval seconds]*

no rmon collection stats *index*

Parameters

- **index**—The requested group of statistics index.(Range: 1–65535)
- **owner ownername**—Records the name of the owner of the RMON group of statistics. If unspecified, the name is an empty string. (Range: Valid string)
- **buckets bucket-number**—A value associated with the number of buckets specified for the RMON collection history group of statistics. If unspecified, defaults to 50.(Range: 1–50)
- **interval seconds**—The number of seconds in each polling cycle. If unspecified, defaults to 1800 (Range: 1–3600).

Command Mode

Interface Configuration (Ethernet, Port-channel) mode. Cannot be configured for a range of interfaces (range context).

show rmon collection stats

Use the **show rmon collection stats** EXEC mode command to display the requested RMON history group statistics.

Syntax

show rmon collection stats *[interface-id]*

Parameters

interface-id—Specifies an interface ID. The interface ID can be one of the following types: Ethernet port or Port-channel.

Command Mode
EXEC mode

Example
The following example displays all RMON history group statistics.

```
Console# show rmon collection stats
Index   Interface    Interval   Requested   Granted   Owner
                                Samples     Samples
-----   ---------    --------   ---------   --------  -------
1       gi1/0/1      30         50          50        CLI
2       gi1/0/1      1800       50          50        Manager
```

The following table describes the significant fields shown in the display.

Field	Description
Index	An index that uniquely identifies the entry.
Interface	The sampled Ethernet interface.
Interval	The interval in seconds between samples.
Requested Samples	The requested number of samples to be saved.
Granted Samples	The granted number of samples to be saved.
Owner	The entity that configured this entry.

show rmon history

Use the **show rmon history** EXEC mode command to display RMON Ethernet history statistics.

Syntax
show rmon history *index {throughput | errors | other} [period seconds*]

Parameters

- **index**—Specifies the set of samples to display. (Range: 1–65535)
- **throughput**—Displays throughput counters.

- **errors**—Displays error counters.
- **other**—Displays drop and collision counters.
- **period seconds**—Specifies the period of time in seconds to display. (Range: 1–2147483647)

Command Mode
EXEC mode

Example
The following examples display RMON Ethernet history statistics for index 1

```
Console# show rmon history 1 throughput

Sample Set: 1               Owner: CLI
Interface: gi1/0/1          Interval: 1800
Requested samples: 50       Granted samples: 50


Maximum table size: 500

Time           Octets       Packets     Broadcast    Multicast    Util
------------   -------      -------     --------     ---------    ----
Jan 18 2005    303595962    357568      3289         7287         19%
21:57:00       287696304    275686      2789         5878         20%
Jan 18 2005
21:57:30

Console# show rmon history 1 errors

Sample Set: 1               Owner: Me
Interface:gi1/0/1           Interval: 1800
Requested samples: 50       Granted samples: 50

Maximum table size: 500 (800 after reset)

Time           CRC Align    Under       Oversize     Fragments    Jabbers
                            size
------------   -------      -----       --------     ---------    ----
Jan 18 2005    1            1           0            49           0
21:57:00

Jan 18 2005    1            1           0            27           0
21:57:30
```

```
Console# show rmon history 1 other

Sample Set: 1                Owner: Me
Interface: gi1/0/1           Interval: 1800
Requested samples: 50        Granted samples: 50

Maximum table size: 500

Time                         Dropped     Collisions
-------------------          ------      ----------
Jan 18 2005 21:57:00         3           0
Jan 18 2005 21:57:30         3           0
```

The following table describes significant fields shown in the display:

Field	Description
Time	Date and Time the entry is recorded.
Octets	The total number of octets of data (including those in bad packets and excluding framing bits but including FCS octets) received on the network.
Packets	The number of packets (including bad packets) received during this sampling interval.
Broadcast	The number of good packets received during this sampling interval that were directed to the broadcast address.
Multicast	The number of good packets received during this sampling interval that were directed to a multicast address. This number does not include packets addressed to the broadcast address.
Utilization	The best estimate of the mean physical layer network utilization on this interface during this sampling interval, in hundredths of a percent.
CRC Align	The number of packets received during this sampling interval that had a length (excluding framing bits but including FCS octets) between 64 and 1518 octets, inclusive, but had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error).
Undersize	The number of packets received during this sampling interval that were less than 64 octets long (excluding framing bits but including FCS octets) and were otherwise well formed.

Field	Description
Oversize	The number of packets received during this sampling interval that were longer than 1518 octets (excluding framing bits but including FCS octets) but were otherwise well formed.
Fragments	The total number of packets received during this sampling interval that were less than 64 octets in length (excluding framing bits but including FCS octets) and had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error), or a bad FCS with a non-integral number of octets (Alignment Error). It is normal for etherHistoryFragments to increment because it counts both runts (which are normal occurrences due to collisions) and noise hits.
Jabbers	The number of packets received during this sampling interval that were longer than 1518 octets (excluding framing bits but including FCS octets), and had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error).
Dropped	The total number of events in which packets were dropped by the probe due to lack of resources during this sampling interval. This number is not necessarily the number of packets dropped, it is the number of times this condition has been detected.
Collisions	The best estimate of the total number of collisions on this Ethernet segment during this sampling interval.

rmon alarm

Use the **rmon alarm** Global Configuration mode command to configure alarm conditions. Use the **no** form of this command to remove an alarm.

Syntax

rmon alarm *index mib-object-id interval rthreshold fthreshold revent fevent [type {absolute | delta}]*
[startup {rising | rising-falling | falling}] [owner name]

no rmon alarm *index*

Parameters

- **index**—Specifies the alarm index. (Range: 1–65535)

- **mib-object-id**—Specifies the object identifier of the variable to be sampled. (Valid OID)
- **interval**—Specifies the interval in seconds during which the data is sampled and compared with rising and falling thresholds. (Range: 1–4294967295)
- **rthreshold**—Specifies the rising threshold value. (Range: 0–4294967295)
- **fthreshold**—Specifies the falling threshold value. (Range: 0–4294967295)
- **revent**—Specifies the index of the event triggered when a rising threshold is crossed. (Range: 0–65535)
- **fevent**—Specifies the index of the event triggered when a falling threshold is crossed. (Range: 0–65535)
- **type** {**absolute** | **delta**}—Specifies the method used for sampling the selected variable and calculating the value to be compared against the thresholds. The possible values are:
  - **absolute**—Specifies that the selected variable value is compared directly with the thresholds at the end of the sampling interval.
  - **delta**—Specifies that the selected variable value of the last sample is subtracted from the current value, and the difference is compared with the thresholds.
- **startup** {**rising** | **rising-falling** | **falling**}—Specifies the alarm that may be sent when this entry becomes valid. The possible values are:
  - **rising**—Specifies that if the first sample (after this entry becomes valid) is greater than or equal to **rthreshold**, a single rising alarm is generated.
  - **rising-falling**—Specifies that if the first sample (after this entry becomes valid) is greater than or equal to ***rthreshold***, a single rising alarm is generated. If the first sample (after this entry becomes valid) is less than or equal to **fthreshold**, a single falling alarm is generated.
  - **fallin** —Specifies that if the first sample (after this entry becomes valid) is less than or equal to **fthreshold**, a single falling alarm is generated.
- **owner name**—Specifies the name of the person who configured this alarm. (Valid string)

Default Configuration
The default method type is **absolute**.

The default startup direction is **rising-falling**.

If the owner **name** is not specified, it defaults to an empty string.

Command Mode
Global Configuration mode

Example
The following example configures an alarm with index 1000, MIB object ID D-Link, sampling interval 360000 seconds (100 hours), rising threshold value 1000000, falling threshold value 1000000, rising threshold event index 10, falling threshold event index 10, absolute method type and rising-falling alarm.

```
console(config)# rmon alarm 1000 1.3.6.1.2.1.2.2.1.10.1 360000 1000000
1000000 10 20
```

show rmon alarm-table

Use the **show rmon alarm-table** EXEC mode command to display a summary of the alarms table.

Syntax
show rmon alarm-table

Command Mode
EXEC mode

Example
The following example displays the alarms table.

```
Console# show rmon alarm-table

Index      OID                       Owner
-----      ----------------------    -------
1          1.3.6.1.2.1.2.2.1.10.1    CLI
2          1.3.6.1.2.1.2.2.1.10.1    Manager
3          1.3.6.1.2.1.2.2.1.10.9    CLI
```

The following table describes the significant fields shown in the display:

Field	Description
Index	An index that uniquely identifies the entry.
OID	Monitored variable OID.
Owner	The entity that configured this entry.

show rmon alarm

Use the **show rmon alarm** EXEC mode command to display alarm configuration.

Syntax
show rmon alarm *number*

Parameters
number—Specifies the alarm index. (Range: 1–65535)

Command Mode
EXEC mode

Example
The following example displays RMON 1 alarms.

```
Console# show rmon alarm 1
Alarm 1
-------
OID: 1.3.6.1.2.1.2.2.1.10.1
Last sample Value: 878128
Interval: 30
Sample Type: delta
Startup Alarm: rising
Rising Threshold: 8700000
Falling Threshold: 78
Rising Event: 1
Falling Event: 1
Owner: CLI
```

The following table describes the significant fields shown in the display:

Field	Description
Alarm	Alarm index.
OID	Monitored variable OID.
Last Sample Value	The value of the statistic during the last sampling period. For example, if the sample type is **delta**, this value is the difference between the samples at the beginning and end of the period. If the sample type is **absolute**, this value is the sampled value at the end of the period.
Interval	The interval in seconds over which the data is sampled and compared with the rising and falling thresholds.
Sample Type	The method of sampling the variable and calculating the value compared against the thresholds. If the value is **absolute**, the variable value is compared directly with the thresholds at the end of the sampling interval. If the value is **delta**, the variable value at the last sample is subtracted from the current value, and the difference is compared with the thresholds.

Field	Description
Startup Alarm	The alarm that may be sent when this entry is first set. If the first sample is greater than or equal to the rising threshold, and startup alarm is equal to rising or rising-falling, then a single rising alarm is generated. If the first sample is less than or equal to the falling threshold, and startup alarm is equal falling or rising-falling, then a single falling alarm is generated.
Rising Threshold	The sampled statistic rising threshold. When the current sampled value is greater than or equal to this threshold, and the value at the last sampling interval is less than this threshold, a single event is generated.
Falling Threshold	The sampled statistic falling threshold. When the current sampled value is less than or equal to this threshold, and the value at the last sampling interval is greater than this threshold, a single event is generated.
Rising Event	The event index used when a rising threshold is crossed.
Falling Event	The event index used when a falling threshold is crossed.
Owner	The entity that configured this entry.

rmon event

Use the **rmon event** Global Configuration mode command to configure an event. Use the **no** form of this command to remove an event.

Syntax

rmon event *index {none | log | trap | log-trap} [community text] [description text] [owner name]*

no rmon event index

Parameters

- **index**—Specifies the event index. (Range: 1–65535)
- **none**— pecifies that no notification is generated by the device for this event.
- **log**—Specifies that a notification entry is generated in the log table by the device for this event.

- **trap**—Specifies that an SNMP trap is sent to one or more management stations by the device for this event.
- **log-trap**—Specifies that an entry is generated in the log table and an SNMP trap is sent to one or more management stations by the device for this event.
- **community text**—Specifies the SNMP community to which an SNMP trap is sent. (Octet string;
length: 0–127 characters)
- **description text**—Specifies a comment describing this event. (Length: 0–127 characters)
- **owner name**—Specifies the name of the person who configured this event. (Valid string)

Default Configuration
If the owner name is not specified, it defaults to an empty string.

Command Mode
Global Configuration mode

Example
The following example configures an event identified as index 10, for which the device generates a notification in the log table.

```
Console(config)# rmon event 10 log
```

show rmon events
Use the **show rmon events** EXEC mode command to display the RMON event table.

Syntax
show rmon events

Command Mode
EXEC mode

Example

The following example displays the RMON event table.

```
Console# show rmon events

Index   Descrip      Type     Community   Owner      Last time
        tion                                         sent
-----   --------     ------   --------    ------     --------
1       Errors       Log                  CLI        Jan18 2006
                                                     23:58:17
2       High         Log-     Router      Manager    Jan18 2006
        Broadcast    Trap                            23:59:48
```

The following table describes significant fields shown in the display:

Field	Description
Index	A unique index that identifies this event.
Description	A comment describing this event.
Type	The type of notification that the device generates about this event. Can have the following values: **none**, **log**, **trap**, **log-trap**. In the case of log, an entry is made in the log table for each event. In the case of trap, an SNMP trap is sent to one or more management stations.
Community	If an SNMP trap is to be sent, it is sent to the SNMP community specified by this octet string.
Owner	The entity that configured this event.
Last time sent	The time this entry last generated an event. If this entry has not generated any events, this value is zero.

show rmon log

Use the **show rmon log** EXEC mode command to display the RMON log table.

Syntax
show rmon log [*event*]

Parameters
event—Specifies the event index. (Range: 0–65535)

Command Mode
EXEC mode

Example
The following examples display the RMON log table.

```
Console# show rmon log
Maximum table size: 500 (800 after reset)
Event          Description                    Time
-----          -------------                  ------------------
1              MIB Var.:                      Jan 18 2006 23:48:19
               1.3.6.1.2.1.2.2.1.10.53
               , Delta, Rising, Actual
               Val: 800, Thres.Set:
               100, Interval (sec):1
```

rmon table-size

Use the **rmon table-size** Global Configuration mode command to configure the maximum size of RMON tables. Use the no form of this command to return to the default configuration.

Syntax
rmon table-size *{history entries | log entries}*

no rmon table-size *{history | log}*

Parameters

- **history entries**—Specifies the maximum number of history table entries. (Range: 20–270)

- **log entries**—Specifies the maximum number of log table entries. (Range: 20–100)

Default Configuration
The default history table size is 270 entries.

The default log table size is 200 entries.

Command Mode
Global Configuration mode

User Guidelines
The configured table size takes effect after the device is rebooted.

Example
The following example configures the maximum size of RMON history tables to 100 entries.

```
Console(config)# rmon table-size history 100
```

19

802.1x Commands

aaa authentication dot1x

Use the **aaa authentication dot1x** Global Configuration mode command to specify one or more authentication, authorization, and accounting (AAA) methods for use on interfaces running IEEE 802.1x. Use the **no** form of this command to restore the default configuration.

Syntax

aaa authentication dot1x default *method* [*method2* ...]

no aaa authentication dot1x default

Parameters

method [**method2 ...**]—Specify at least one method from the following list:

Keyword	Description
radius	Uses the list of all RADIUS servers for authentication
none	Uses no authentication

Default Configuration

The default method is Radius.

Command Mode

Global Configuration mode

User Guidelines

Additional methods of authentication are used only if the previous method returns an error and not if the request for authentication is denied. Specify

none as the final method in the command line to ensure that authentication succeeds even if all methods return an error.

Example

The following example uses the **aaa authentication dot1x default** command with no authentication.

```
Console(config)# aaa authentication dot1x default none
```

dot1x system-auth-control

Use the **dot1x system-auth-control** Global Configuration mode command to enable 802.1x globally. Use the **no** form of this command to restore the default configuration.

Syntax

dot1x system-auth-control

no dot1x system-auth-control

Default Configuration

All the ports are in FORCE_AUTHORIZED state.

Command Mode

Global Configuration mode

Example

The following example enables 802.1x globally.

```
Console(config)# dot1x system-auth-control
```

dot1x port-control

Use the **dot1x port-control** Interface Configuration (Ethernet) mode command to enable manual control of the port authorization state. Use the **no** form of this command to restore the default configuration.

Syntax

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

no dot1x port-control

Parameters

- **auto**—Enables 802.1x authentication on the interface and causes the port to transition to the authorized or unauthorized state based on the 802.1x authentication exchange between the device and the client.
- **force-authorized**—Disables 802.1x authentication on the interface and causes the port to transition to the authorized state without any authentication exchange required. The port resends and receives normal traffic without 802.1x-based client authentication.
- **force-unauthorized**—Denies all access through this interface by forcing the port to transition to the unauthorized state and ignoring all attempts by the client to authenticate. The device cannot provide authentication services to the client through the interface.

Default Configuration

The port is in the force-authorized state.

Command Mode

Interface Configuration (Ethernet) mode

User Guidelines

It is recommended to disable spanning tree or to enable spanning-tree PortFast mode on 802.1x edge ports (ports in **auto** state that are connected to end stations), in order to proceed to the forwarding state immediately after successful authentication.

Example

The following example enables 802.1x authentication on gigabitethernet port 1/0/15.

```
Console(config)# interface gigabitethernet 1/0/15
Console(config-if)# dot1x port-control auto
```

dot1x re-authentication

Use the **dot1x reauthentication** Interface Configuration mode command to enable periodic re-authentication of the client. Use the **no** form of this command to return to the default setting.

Syntax

dot1x reauthentication

no dot1x reauthentication

Parameters

This command has no arguments or keywords.

Default

Periodic re-authentication is disabled.

Command Mode

Interface configuration (Ethernet)

Example

```
console(config)# interface gigabitethernet 1/0/1
console(config-if)# dot1x reauthentication
```

dot1x timeout reauth-period

Use the **dot1x timeout reauth-period** Interface Configuration mode command to set the number of seconds between re-authentication attempts. Use the **no** form of this command to return to the default setting.

Syntax

dot1x timeout reauth-period *seconds*

no dot1x timeout reauth-period

Parameters
seconds—Number of seconds between re-authentication attempts. (Range: 30–4294967295)

Default
3600

Command Mode
Interface Configuration (Ethernet) mode

Example

```
console(config)# interface gigabitethernet 1/0/1
console(config-if)# dot1x timeout reauth-period 5000
```

dot1x re-authenticate

The **dot1x re-authenticate** Privileged EXEC mode command manually initiates re-authentication of all 802.1x-enabled ports or the specified 802.1x-enabled port.

Syntax
dot1x re-authenticate *[interface-id]*

Parameters
interface-id—Specifies an interface ID. The interface ID must be an Ethernet port.

Command Mode
Privileged EXEC mode

Example
The following command manually initiates re-authentication of 802.1x-enabled gigabitethernet port 1/0/15.

```
Console# dot1x re-authenticate gigabitethernet 1/0/15
```

dot1x timeout quiet-period

Use the **dot1x timeout quiet-period** Interface Configuration (Ethernet) mode command to set the time interval that the device remains in a quiet state following a failed authentication exchange (for example, the client provided an invalid password). Use the **no** form of this command to restore the default configuration.

Syntax

dot1x timeout quiet-period *seconds*

no dot1x timeout quiet-period

Parameters

seconds—Specifies the time interval in seconds that the device remains in a quiet state following a failed authentication exchange with the client. (Range: 0–65535 seconds)

Default Configuration

The default quiet period is 60 seconds.

Command Mode

Interface Configuration (Ethernet) mode

User Guidelines

During the quiet period, the device does not accept or initiate authentication requests.

The default value of this command should only be changed to adjust to unusual circumstances, such as unreliable links or specific behavioral problems with certain clients and authentication servers.

To provide faster response time to the user, a smaller number than the default value should be entered.

Example

The following example sets the time interval that the device remains in the quiet state following a failed authentication exchange to 3600 seconds.

```
Console(config)# interface gigabitethernet 1/0/15
Console(config-if)# dot1x timeout quiet-period 3600
```

dot1x timeout tx-period

Use the **dot1x timeout tx-period** Interface Configuration (Ethernet) mode command to set the time interval during which the device waits for a response to an Extensible Authentication Protocol (EAP) request/identity frame from the client before resending the request. Use the **no** form of this command to restore the default configuration.

Syntax

dot1x timeout tx-period *seconds*

no dot1x timeout tx-period

Parameters

seconds—Specifies the time interval in seconds during which the device waits for a response to an EAP-request/identity frame from the client before resending the request. (Range: 1–65535 seconds)

Default Configuration

The default timeout period is 30 seconds.

Command Mode

Interface Configuration (Ethernet) mode

User Guidelines

The default value of this command should be changed only to adjust to unusual circumstances, such as unreliable links or specific behavioral problems with certain clients and authentication servers.

Example

The following command sets the time interval during which the device waits for a response to an EAP request/identity frame to 3600 seconds.

```
Console(config)# interface gigabitethernet 1/0/15
Console(config-if)# dot1x timeout tx-period 3600
```

dot1x max-req

Use the **dot1x max-req** Interface Configuration mode command to set the maximum number of times that the device sends an Extensible Authentication Protocol (EAP) request/identity frame (assuming that no response is received) to the client before restarting the authentication process. Use the **no** form of this command to restore the default configuration.

Syntax

dot1x max-req *count*

no dot1x max-req

Parameters

count—Specifies the maximum number of times that the device sends an EAP request/identity frame before restarting the authentication process. (Range: 1–10)

Default Configuration

The default maximum number of attempts is 2.

Command Mode

Interface Configuration (Ethernet) mode

User Guidelines

The default value of this command should be changed only to adjust to unusual circumstances, such as unreliable links or specific behavioral problems with certain clients and authentication servers.

Example

The following example sets the maximum number of times that the device sends an EAP request/identity frame to 6

```
Console(config)# interface gigabitethernet 1/0/15
Console(config-if)# dot1x max-req 6
```

dot1x timeout supp-timeout

Use the **dot1x timeout supp-timeout** Interface Configuration (Ethernet) mode command to set the time interval during which the device waits for a response to an Extensible Authentication Protocol (EAP) request frame from the client before resending the request. Use the **no** form of this command to restore the default configuration.

Syntax

dot1x timeout supp-timeout *seconds*

no dot1x timeout supp-timeout

Parameters

seconds—Specifies the time interval in seconds during which the device waits for a response to an EAP request frame from the client before resending the request. (Range: 1–65535 seconds)

Default Configuration

The default timeout period is 30 seconds.

Command Mode

Interface Configuration (Ethernet) mode

User Guidelines

The default value of this command should be changed only to adjust to unusual circumstances, such as unreliable links or specific behavioral problems with certain clients and authentication servers.

Example

The following example sets the time interval during which the device waits for a response to an EAP request frame from the client before resending the request to 3600 seconds.

```
Console(config)# interface gigabitethernet 1/0/15
Console(config-if)# dot1x timeout supp-timeout 3600
```

dot1x timeout server-timeout

Use the **dot1x timeout server-timeout** Interface Configuration (Ethernet) mode command to set the time interval during which the device waits for a response from the authentication server. Use the **no** form of this command to restore the default configuration.

Syntax

dot1x timeout server-timeout *seconds*

no dot1x timeout server-timeout

Parameters

seconds—Specifies the time interval in seconds during which the device waits for a response from the authentication server. (Range: 1–65535 seconds)

Default Configuration

The default timeout period is 30 seconds.

Command Mode

Interface Configuration (Ethernet) mode

User Guidelines

The actual timeout period can be determined by comparing the value specified by the **dot1x timeout server-timeout** command to the result of multiplying the number of retries specified by the **radius-server retransmit** command by the timeout period specified by the **radius-server timeout** command, and selecting the lower of the two values.

Example

The following example sets the time interval between retransmission of packets to the authentication server to 3600 seconds.

```
Console(config)# interface gigabitethernet 1/0/15
Console(config-if)# dot1x timeout server-timeout 3600
```

show dot1x

Use the **show dot1x** Privileged EXEC mode command to display the 802.1x device or specified interface status.

Syntax

show dot1x *[interface interface-id]*

Parameters

interface-id—Specify an interface ID. The interface ID must be an Ethernet port.

Command Mode

Privileged EXEC mode

Example

The following examples display the status of 802.1x-enabled Ethernet ports.

```
Console# show dot1x
802.1x is enabled

Port       Admin        Oper           Reauth    Reauth   Username
           Mode         Mode           Control   Period
----       ----------   ------------   -------   ------   --------
gi1/0/1    Auto         Authorized     Ena       3600     Bob
gi1/0/2    Auto         Authorized     Ena       3600     John
gi1/0/3    Auto         Unauthorized   Ena       3600     Clark
gi1/0/4    Force-auth   Authorized     Dis       3600     n/a
gi1/0/5    Force-auth   Unauthorized   Dis       3600     n/a

* Port is down or not present.

Console# show dot1x interface gi1/0/3

802.1x is enabled.
```

```
Port       Admin        Oper           Reauth    Reauth   Username
           Mode         Mode           Control   Period
----       ----------   ------------   -------   ------   --------
gi1/0/3    Auto         Unauthorized   Enable    3600     Clark


Quiet period:           60 Seconds
Tx period:              30 Seconds
Max req:                2
Supplicant timeout:     30 Seconds

Server timeout:                         30 Seconds
Session Time (HH:MM:SS):                08:19:17
MAC Address:                            00:08:78:32:98:78
Authentication Method:                  Remote
Termination Cause:                      Supplicant logoff

Authenticator State Machine

State:                                  HELD

Backend State Machine

State:                                  IDLE
Authentication success:                 9
Authentication fails:                   1
```

The following table describes the significant fields shown in the display.

Field	Description
Port	The port number.
Admin mode	The port admin mode. Possible values: Force-auth, Force-unauth, Auto.
Oper mode	The port oper mode. Possible values: Authorized, Unauthorized or Down.
Reauth Control	Reauthentication control.
Reauth Period	Reauthentication period.

Field	Description
Username	The username representing the supplicant identity. This field shows the username if the port control is auto. If the port is Authorized, it displays the username of the current user. If the port is Unauthorized, it displays the last user authenticated successfully.
Quiet period	The number of seconds that the device remains in the quiet state following a failed authentication exchange (for example, the client provided an invalid password).
Tx period	The number of seconds that the device waits for a response to an Extensible Authentication Protocol (EAP) request/identity frame from the client before resending the request.
Max req	The maximum number of times that the device sends an EAP request frame (assuming that no response is received) to the client before restarting the authentication process.
Supplicant timeout	The number of seconds that the device waits for a response to an EAP-request frame from the client before resending the request.
Server timeout	The number of seconds that the device waits for a response from the authentication server before resending the request.
Session Time	The amount of time (HH:MM:SS) that the user is logged in.
MAC address	The supplicant MAC address.
Authentication Method	The authentication method used to establish the session.
Termination Cause	The reason for the session termination.
State	The current value of the Authenticator PAE state machine and of the Backend state machine.
Authentication success	The number of times the state machine received a Success message from the Authentication Server.
Authentication fails	The number of times the state machine received a Failure message from the Authentication Server.

show dot1x users

Use the **show dot1x users** Privileged EXEC mode command to display active 802.1x authenticated users for the device.

Syntax

show dot1x users *[username username*]

Parameters

username—Specifies the supplicant username (Length: 1–160 characters)

Command Mode

Privileged EXEC mode

Example

The following example displays 802.1x users.

```
Switch# show dot1x users
Port    Username     Session        Auth     MAC               VLAN
 Filter
                    Time           Method   Address
------ ----------   ------------- --------  -------------     ----  ----
gi1/0/1 Bob           1d 03:08:58     Remote   0008.3b79.8787    3
gi1/0/2 John          08:19:17        None     0008.3b89.3127    2
OK


Port    Username    Session         Auth     MAC               VLAN
 Filter
                    Time           Method   Address
--------- ----------------------------  -----------  ---- ------
gi1/0/1 Bob        1d 09:07:38        Remote     0008.3b79.8787  3  OK
gi1/0/1 Bernie   03:08:58           Remote      0008.3b79.3232  9  OK
gi1/0/2 John       08:19:17           Remote      0008.3b89.3127   2
gi1/0/3 Paul       02:12:48           Remote      0008.3b89.8237   8
Warning


Switch# show dot1x users username Bob
Port    Username    Session       Auth      MAC               VLAN
Filter
                   Time          Method    Address
--------- ----------------------------  -----------        ---- -----
gi1/0/1 Bob          1d 09:07:38   Remote    0008.3b79.8787     3  OK
Filter ID #1: Supplicant-IPv4
Filter ID #2: Supplicant-IPv6
Switch# show dot1x users username Bernie
Port    Username    Session       Auth      MAC               VLAN
Filter
                   Time          Method    Address
--------- ----------------------------  -----------        ---- -----
gi1/0/1 Bernard     03:08:58     Remote    0008.3b79.3232      9   OK
Filter ID #1: Supplicant-IPv4
```

show dot1x statistics

Use the **show dot1x statistics** Privileged EXEC mode command to display 802.1x statistics for the specified interface.

Syntax

show dot1x statistics interface *interface-id*

Parameters

interface-id—Specifies an interface ID. The interface ID must be an Ethernet port.

Command Mode

Privileged EXEC mode

Example

The following example displays 802.1x statistics for gigabitethernet port 1/0/1.

```
Console# show dot1x statistics interface gigabitethernet 1/0/1

EapolFramesRx: 11
EapolFramesTx: 12
EapolStartFramesRx: 1
EapolLogoffFramesRx: 1
EapolRespIdFramesRx: 3
EapolRespFramesRx: 6
EapolReqIdFramesTx: 3
EapolReqFramesTx: 6
InvalidEapolFramesRx: 0
EapLengthErrorFramesRx: 0
LastEapolFrameVersion: 1
LastEapolFrameSource: 00:08:78:32:98:78
```

The following table describes the significant fields shown in the display:

Field	Description
EapolFramesRx	The number of valid EAPOL frames of any type that have been received by this Authenticator.
EapolFramesTx	The number of EAPOL frames of any type that have been transmitted by this Authenticator.
EapolStartFramesRx	The number of EAPOL Start frames that have been received by this Authenticator.
EapolLogoffFramesRx	The number of EAPOL Logoff frames that have been received by this Authenticator.
EapolRespIdFramesRx	The number of EAP Resp/Id frames that have been received by this Authenticator.
EapolRespFramesRx	The number of valid EAP Response frames (other than Resp/Id frames) that have been received by this Authenticator.
EapolReqIdFramesTx	The number of EAP Req/Id frames that have been transmitted by this Authenticator.
EapolReqFramesTx	The number of EAP Request frames (other than Req/Id frames) that have been transmitted by this Authenticator.
InvalidEapolFramesRx	The number of EAPOL frames that have been received by this Authenticator for which the frame type is not recognized.
EapLengthErrorFramesRx	The number of EAPOL frames that have been received by this Authenticator in which the Packet Body Length field is invalid.
LastEapolFrameVersion	The protocol version number carried in the most recently received EAPOL frame.
LastEapolFrameSource	The source MAC address carried in the most recently received EAPOL frame.

clear dot1x statistics

Use the **clear dot1x statistics** Privileged EXEC mode command to clear 802.1x statistics.

Syntax
clear dot1x statistics [*interface-id*]

Parameters
interface-id—Specify an Ethernet port ID..

Default Configuration
Statistics on all ports are cleared.

Command Mode
Privileged EXEC mode

Example
The following example displays how to clear 802.1x statistics on all ports

```
Console# clear dot1x statistics
```

dot1x auth-not-req

Use the **dot1x auth-not-req** Interface Configuration (VLAN) mode command to enable unauthorized devices access to the VLAN. Use the **no** form of this command to disable access to the VLAN.

Syntax
dot1x auth-not-req

no dot1x auth-not-req

Default Configuration
Access is enabled.

Command Mode
Interface Configuration (VLAN) mode

User Guidelines
An access port cannot be a member in an unauthenticated VLAN.

The native VLAN of a trunk port cannot be an unauthenticated VLAN.

For a general port, the PVID can be an unauthenticated VLAN (although only tagged packets are accepted in the unauthorized state).

Example

The following example enables unauthorized devices access to VLAN 5.

```
Console(config)# interface vlan 5
Console(config-if)# dot1x auth-not-req
```

dot1x host-mode

Use the **dot1x host-mode** Interface Configuration mode command to allow a single host (client) or multiple hosts on an IEEE 802.1x-authorized port. Use the **no** form of this command to return to the default setting.

Syntax

dot1x host-mode *{multi-host | single-host | multi-sessions}*

Parameters

- **multi-host**—Enable multiple-hosts mode.
- **single-host**—Enable single-hosts mode.
- **multi-sessions**—Enable multiple-sessions mode.

Default

Default mode is multi-host.

Command Mode

Interface Configuration (Ethernet) mode

User Guidelines

In multiple hosts mode only one of the attached hosts must be successfully authorized for all hosts to be granted network access. If the port becomes unauthorized, all attached clients are denied access to the network.

In multiple sessions mode each host must be successfully authorized in order to grant network access. Please note that packets are NOT encrypted, and

after success full authentication filtering is based on the source MAC address only.

Port security on a port can't be enabled in single-host mode and in multiple-sessions mode.

It is recommended to enable reauthentication when working in multiple-sessions mode in order to detect User Logout for users that hadn't sent Logoff.

Example

```
console(config)# interface gigabitethernet 1/0/1
console(config-if)# dot1x host-mode multi-host
console(config-if)# dot1x host-mode single-host
console(config-if)# dot1x host-mode multi-sessions
```

dot1x violation-mode

Use the **dot1x violation-mode** Interface Configuration (Ethernet) mode command to configure the action to be taken, when a station whose MAC address is not the supplicant MAC address, attempts to access the interface. Use the **no** form of this command to return to default.

Syntax

dot1x violation-mode *{restrict | protect | shutdown}*

no dot1x violation-mode

Parameters

- **restrict**—Generates a trap when a station whose MAC address is not the supplicant MAC address, attempts to access the interface. The minimum time between the traps is 1 second. Those frames are forwarded but their source address are not learned.
- **protect**—Discard frames with source addresses not the supplicant address.
- **shutdown**—Discard frames with source addresses not the supplicant address and shutdown the port

Default Configuration
Protect

Command Mode
Interface Configuration (Ethernet) mode

User Guidelines
The command is relevant for single-host mode.

The command is not relevant for multiple-hosts mode.

The command is relevant for multiple-sessions mode, but you should note that since PCs are sending traffic prior to successful 802.1X authentication, this command might not be useful in this mode.

BPDU message whose MAC address is not the supplicant MAC address wouldn't be discarded in the protect mode.

BPDU message whose MAC address is not the supplicant MAC address would cause a shutdown in the shutdown mode.

Example

```
console(config)# interface gigabitethernet gi1/0/1
console(config-if)# dot1x violation-mode protect
```

dot1x guest-vlan

Use the **dot1x guest-vlan** Interface Configuration (VLAN) mode command to define a guest VLAN. Use the **no** form of this command to restore the default configuration.

Syntax
dot1x guest-vlan

no dot1x guest-vlan

Default Configuration
No VLAN is defined as a guest VLAN.

Command Mode
Interface Configuration (VLAN) mode

User Guidelines
Use the **dot1x guest-vlan enable** Interface Configuration mode command to enable unauthorized users on an interface to access the guest VLAN.

If the guest VLAN is defined and enabled, the port automatically joins the guest VLAN when the port is unauthorized and leaves it when the port becomes authorized. To be able to join or leave the guest VLAN, the port should not be a static member of the guest VLAN.

Example
The following example defines VLAN 2 as a guest VLAN.

```
Console# configure
Console(config)# interface vlan 2
Console(config-if)# dot1x guest-vlan
```

dot1x guest-vlan timeout
Use the **dot1x guest-vlan timeout** Global Configuration mode command to set the time delay between enabling 802.1x (or port up) and adding a port to the guest VLAN. Use the **no** form of this command to restore the default configuration.

Syntax
dot1x guest-vlan timeout *timeout*

no dot1x guest-vlan timeout

Parameters
timeout—Specifies the time delay in seconds between enabling 802.1x (or port up) and adding the port to the guest VLAN. (Range: 30–180)

Default Configuration
The guest VLAN is applied immediately.

Command Mode
Global Configuration mode

User Guidelines
This command is relevant if the guest VLAN is enabled on the port. Configuring the timeout adds delay from enabling 802.1X (or port up) to the time the device adds the port to the guest VLAN.

Example
The following example sets the delay between enabling 802.1x and adding a port to a guest VLAN to 60 seconds.

```
Console(config)# dot1x guest-vlan timeout 60
```

dot1x guest-vlan enable

Use the **dot1x guest-vlan enable** Interface Configuration (Ethernet) mode command to enable unauthorized users on the interface access to the guest VLAN. Use the **no** form of this command to disable access.

Syntax
dot1x guest-vlan enable

no dot1x guest-vlan enable

Default Configuration
The default configuration is disabled.

Command Mode
Interface Configuration (Ethernet) mode

User Guidelines
A device can have only one global guest VLAN. The guest VLAN is defined using the **dot1x guest-vlan** Interface Configuration mode command.

Example

The following example enables unauthorized users on gigabitethernet port 1/0/1 to access the guest VLAN.

```
Console(config)# interface gigabitethernet 1/0/15
Console(config-if)# dot1x guest-vlan enable
```

dot1x mac-authentication

Use the **dot1x mac-authentication** Interface Configuration (Ethernet) mode command to enable authentication based on the station's MAC address. Use the **no** form of this command to disable access.

Syntax

dot1x mac-authentication {mac-only | mac-and-802.1x}

no dot1x mac-authentication

Parameters

- **mac-only**—Enables authentication based on the station's MAC address only. 802.1X frames are ignored.
- **mac-and-802.1x**—Enables 802.1X authentication and MAC address authentication on the interface.

Default Configuration

Authentication based on the station's MAC address is disabled.

Command Mode

Interface Configuration (Ethernet) mode

User Guidelines

The guest VLAN must be enabled when MAC authentication is enabled.

Static MAC addresses cannot be authorized. Do not change an authenticated MAC address to a static address.

It is not recommended to delete authenticated MAC addresses.

Reauthentication must be enabled when working in this mode.

Example
The following example enables authentication based on the station's MAC address on gigabitethernet port `1/0/1`.

```
Console(config)# interface gi1/0/1
Console(config-if)# dot1x mac-authentication mac-only
```

dot1x traps mac-authentication success

Use the **dot1x traps mac-authentication success** Global Configuration mode command to enable sending traps when a MAC address is successfully authenticated by the 802.1X mac-authentication access control. Use the **no** form of this command to disable the traps.

Syntax
dot1x traps mac-authentication success

no dot1x traps mac-authentication success

Parameters
This command has no arguments or keywords.

Default
Default is disabled.

Command Mode
Global Configuration mode

dot1x traps mac-authentication failure

Use the d**ot1x traps mac-authentication failure** Global Configuration mode command to enable sending traps when MAC address was failed in authentication of the 802.1X MAC authentication access control. Use the **no** form of this command to disable the traps.

Syntax

dot1x traps mac-authentication failure

no dot1x traps mac-authentication failure

Parameters

This command has no arguments or keywords.

Default

Default is disabled.

Command Mode

Global Configuration mode

dot1x radius-attributes vlan

Use the **dot1x radius-attributes vlan** Interface Configuration mode command, to enable user-based VLAN assignment. Use the **no** form of this command to disable user-based VLAN assignment.

Syntax

dot1x radius-attributes vlan

no dot1x radius-attributes vlan

Parameters

This command has no arguments or keywords.

Default

Disabled

Command Mode

Interface Configuration (Ethernet) mode

User Guidelines

The configuration of this command is allowed only when the port is Forced Authorized.

Radius attributes are supported only in the multiple sessions mode (multiple hosts with authentication)

When Radius attributes are enabled and the Radius Accept message does not contain the supplicant's VLAN as an attribute, then the supplicant is rejected.

Packets to the supplicant are sent untagged.

After successful authentication the port remains member in the unauthenticated VLANs and in the Guest VLAN. Other static VLAN configuration is not applied on the port. If the supplicant VLAN does not exist on the switch, the supplicant is rejected.

Example

```
console(config)# interface gi1/0/1
console(config-if)# dot1x radius-attributes vlan
```

dot1x radius-attributes filter-id

Use the **dot1x radius-attributes filter-id** Interface Configuration mode command to enable user-based ACL/Qos-Policy assignment. Use the **no** form of this command to disable user-based ACL/Qos-Policy assignment.

Syntax

dot1x radius-attributes filter-id

no dot1x radius-attributes filter-id

Parameters

This command has no arguments or keywords.

Default

Disabled

Command Mode

Interface Configuration (Ethernet) mode

User Guidelines

User based ACL/Qos-Policy assignment is supported only in 802.1x multiple sessions.

The configuration of the parameter is allowed only when the port is Forced Authorized or Forced Unauthorized.

dot1x radius-attributes errors

Use the **dot1x radius-attributes errors** Global Configuration mode command to specify error handling for the Radius attributes feature. Use the **no** form of this command to return to default.

Syntax

dot1x radius-attributes errors *filter-id resources {accept | reject}*

no dot1x radius-attributes errors *filter-id resources*

Parameters

accept—If the Filter-ID cannot be allocated for resource allocation reasons, the user is accepted. If the Filter-ID canot be allocated for other reasons, the user is rejected.

reject—If the Filter-ID cannot be assigned, the user is rejected.

Default

Reject

Command Mode

Global Configuration mode

dot1x legacy-supp-mode

Use the **dot1x legacy-supp-mode** Interface Configuration mode command in multiple session mode to enable 802.1x switch to send a periodic EAPOL request identity frame according to tx timeout period in order to verify authentication in multiple session mode of clients that do not follow 802.1x standard behavior. Use the **no** form of this command to return to the default setting.

Syntax
dot1x legacy-supp-mode

no dot1x legacy-supp-mode

Parameters
This command has no arguments or keywords.

Default
Legacy support is disabled.

Command Mode
Interface Configuration (Ethernet) mode

User Guidelines
The command causes 802.1x switch to send an Extensible Authentication Protocol (EAP)-request/identity frame from the authenticator (switch) each tx-period automatically, when in multiple session mode. The command should be activated onlywhen all devices connected to that port do not follow 802.1x standard behavior to send EAPOL start packets when the client link goes up (for example, some Windows OS with pre Service Pack 3).

show dot1x advanced

Use the **show dot1x advanced** Privileged EXEC mode command to display 802.1x advanced features for the device or specified interface.

Syntax
show dot1x advanced *[interface-id]*

Parameters
nterface-id—Specify an interface ID. The interface ID must be an Ethernet port.

Command Mode
Privileged EXEC mode

Example

The following example displays 802.1x advanced features for the device.

```
console# show dot1x advanced
Guest VLAN: 3978
Unauthenticated VLANs: 91, 92
Interface Multiple Guest   MAC              VLAN        Legacy-  Policy
          Hosts    VLAN    Authentication  Assignment  supp
                                                       Mode  Assignment
----------------- ---------------------- -----------  --------- ------
gi1/0/1    Disabled Enabled MAC-and-802.1X  Enabled     Enable      Disabled
gi1/0/2    Enabled  Disabled Disabled       Enabled     Enable      Disabled


Switch# show dot1x advanced gigabitethernet 1/0/1

Interface Multiple Guest   MAC              VLAN        Legacy-  Policy
          Hosts    VLAN    Authentication   Assignment sup Mode Assignment
----------------- ---------------------- -----------  ------  -------
gi1/0/1   Disabled Enabled  MAC-and-802.1X  Enabled     Enable
Legacy-Supp mode is disabled
Policy assignment resource err handling: Accept
Single host parameters
Violation action: Discard
Trap: Enabledx
Status: Single-host locked
Violations since last trap: 9
```

dot1x system-auth-control monitor

Use the **dot1x system-auth-control monitor** Global Configuration command to enable 802.1x globally the 802.1x Monitoring mode and define the Monitor VLAN. Use the **no** format of the command to return to default.

Syntax

dot1x system-auth-control monitor *[vlan vlan-id]*

no dot1x system-auth-control monitor

Parameters
vlan vlan-id—Specifies the 802.1x Monitoring VLAN. If the parameter is omitted, the Default VLAN is used as the 802.1x Monitoring VLAN.(Range: Any manually created VLAN or the Default VLAN)

Default
Disabled

Command Mode
Global Configuration mode

User Guidelines
The 802.1x Monitoring VLAN cannot be deleted manually.

show dot1x monitoring result

Use the **show dot1x monitoring result** Privileged EXEC mode command to display the captured information of each interface/host on the switch/stack.

Syntax
show dot1x monitoring result *[username username]*

Parameters
username username—Specifies supplicant username (Range: 1–80 characters)

Command Mode
Privileged EXEC mode

User Guidelines
The following table describes the significant fields shown in the display:

Field	Description
Usernamr	Supplicant Username
VLAN	VLAN assigned to Supplicant
MAC address	Supplicant MAC address

Port	Ethernet port or port-channel
Reject reason	Reason in the case of failure. The following table describes the reasons.
Time	Supplicant Session time

Table 1: Reject Reason Description

Abbreviation	Description
ACL-DEL	ACL was deleted by a user
ACL-NOTEXST	ACL sent by radius Server does not exist on the device
ACL-OVRFL	ACL sent by radius server can not be applied because of TCAM overflow
AUTH-ERR	Rejected by Radius due wrong user name or password in Radius server
FLTR-ERR	Radius accept message contains more than 2 filter-id
FRS-MTH-DENY	First method is "deny"
IPv6WithMAC	Radius accept message contains filter with IPv6 DIP and MAC addresses
IPV6WithNotIP	Radius accept message contains IPv6 and not IP simultaneously
POL-BasicMode	Policy Map is not supported in the QoS basic mode
POL-DEL	Policy Map was deleted by a user
POL-OVRFL	Policy Map sent by radius server can not be applied because of TCAM overflow
RAD-APIERR	RADIUS API returned error (e.g. No RADIUS server is configured).
RAD_INVLRES	RADIUS server returned invalid packet (e.g. EAP Attribute is missing)
RAD-NORESP	RADIUS server is not responding
VLAN-DFLT	VLAN sent by radius server can not be applied because it is the Default VLAN

Table 1: Reject Reason Description

VLAN-DYNAM	VLAN sent by radius server can not be applied because it is a Dynamic VLAN
VLAN-GUEST	VLAN sent by radius server can not be applied because it is the Guest VLAN

Examples

```
Example 1
Switch# show dot1x monitoring results
Monitoring VLAN: 100

Port VLAN  UsernameMAC      Reject Time
             Address     Reason
--------- ---------------------------    ----------  ---------
gi1/0/1  100 Bob     0008.3b79.8787   VLAN-NOTEX08:19:17
gi1/0/2  15  John    0008.3b89.3128   SERV-ERR 09:20:11
gi1/0/2  5   John    0008.3b89.3129   SERV-ERR 09:20:11
```

```
Example 2
Switch# show dot1x monitoring Bob
Username: Bob
Port             gi1/0/1
Quiet period: 60 Seconds
Tx period:   30 Seconds
Max req:     2
Supplicant timeout: 30 Seconds
Server timeout: 30 Seconds
Session Time (HH:MM:SS): 08:19:17
MAC Address: 00:08:78:32:98:78
Authentication Method: Remote
Assigned VLAN:   207
Reason for Failure: Radius server rejected authentication because
username/password mismatch
```

```
Example 3
```

```
Switch# show dot1x monitoring Tom
Username: Tom
Port             gi1/0/1
Quiet period: 60 Seconds
Tx period:   30 Seconds
Max req:     2
Supplicant timeout: 30 Seconds
Server timeout: 30 Seconds
Session Time (HH:MM:SS): 08:19:17
MAC Address: 00:08:78:32:98:78
Authentication Method: Remote
Assigned VLAN:   207
Reason for Failure:VLAN was not defined on Switch
```

20

Ethernet Configuration Commands

interface

Use the **interface** Global Configuration mode command to configure an interface and enter interface configuration mode.

Syntax

interface interface-id

Parameters

interface-id—Specifies an interface ID. The interface ID can be one of the following types: Ethernet port or Port-channel.

interface range

Use the **interface range** command to execute a command on multiple ports at the same time.

Syntax

interface range *interface-id-list*

Parameters

interface-id-list—Specify list of interface IDs. The interface ID can be one of the following types: Ethernet port or Port-channel

User Guidelines

Commands under the interface range context are executed independently on each interface in the range: If the command returns an error on one of the interfaces, it does not stop the execution of the command on other interfaces.

Example

```
console(config)# interface range gi1/0/1-20
```

description

Use the **description** Interface Configuration (Ethernet, Port-channel) mode command to add a description to an interface. Use the **no** form of this command to remove the description.

Syntax

description *string*

no description

Parameters

string—Specifies a comment or a description of the port to assist the user. (Length: 1–64 characters)

Default Configuration

The interface does not have a description.

Command Mode

Interface Configuration (Ethernet, Port-channel) mode

Example

The following example adds the description 'SW#3' to gigabitethernet port 1/0/5.

```
Console(config)# interface gigabitethernet 1/0/5
Console(config-if)# description SW#3
```

speed

Use the **speed** Interface Configuration (Ethernet, Port-channel) mode command to configure the speed of a given Ethernet interface when not

using auto-negotiation. Use the **no** form of this command to restore the default configuration.

Syntax

speed *{10 | 100 | 1000 | 10000}*

no speed

Parameters

- **10**—Forces10 Mbps operation.
- **100**—Forces 100 Mbps operation.
- **1000**—Forces 1000 Mbps operation.
- **10000**—Forces 10000 Mbps operation.

Default Configuration

The port operates at its maximum speed capability.

Command Mode

Interface Configuration (Ethernet, Port-channel) mode

User Guidelines

The **no speed** command in a Port-channel context returns each port in the Port-channel to its maximum capability.

Example

The following example configures the speed of gigabitethernet port `1/0/5` to 100 Mbps operation.

```
Console(config)# interface gigabitethernet 1/0/5
Console(config-if)# speed 100
```

duplex

Use the **duplex** Interface Configuration (Ethernet, Port-channel) mode command to configure the full/half duplex operation of a given Ethernet interface when not using auto-negotiation. Use the **no** form of this command to restore the default configuration.

Syntax

duplex *{half | full}*

no duplex

Parameters

- **half**—Forces half-duplex operation.
- **full**—Forces full-duplex operation.

Default Configuration

The interface operates in full duplex mode.

Command Mode

Interface Configuration (Port-channel) mode

Example

The following example configures gigabitethernet port `1/0/5` to operate in full duplex mode.

```
Console(config)# interface gigabitethernet 1/0/5
Console(config-if)# duplex full
Console(config-if)#
```

negotiation

Use the **negotiation** Interface Configuration (Ethernet, Port-channel) mode command to enable auto-negotiation operation for the speed and duplex parameters and master-slave mode of a given interface, where the preferred default mode is master mode. Use the **no** form of this command to disable auto-negotiation.

Syntax

negotiation [*capability* [*capability2 ... capability5*]] [preferred {master | slave}]

no negotiation

Parameters

- **capability**—Specifies the capabilities to advertise. (Possible values: 10h, 10f, 100h,100f, 1000f). If unspecified, defaults to list of all the capabilities of the port.
- **Preferred**—Specifies the master-slave preference:
  - Master—Advertise master preference
  - Slave—Advertise slave preference

Default Configuration
Auto-negotiation is enabled and preferred default mode is master mode.

Command Mode
Interface Configuration (Ethernet, Port-channel) mode

Example
The following example enables auto-negotiation on gigabitethernet port 1/0/5.

```
Console(config)# interface gigabitethernet 1/0/5
Console(config-if)# negotiation
Console(config-if)#
```

flowcontrol

Use the **flowcontrol** Interface Configuration (Ethernet, Port-channel) mode command to configure the Flow Control on a given interface. Use the **no** form of this command to disable Flow Control.

Syntax
flowcontrol *{auto | on | off}*

no flowcontrol

Parameters

- **aut**—Specifies auto-negotiation.
- **on**—Enables Flow Control.

- **off**—Disables Flow Control.

Default Configuration
Flow control is enabled.

Command Mode
Interface Configuration (Ethernet, Port-channel) mode

User Guidelines
Use the **negotiation** command to enable **flow control auto**.

Example
The following example enables Flow Control on port `gi1/0/1`

```
Console(config)# interface gigabitethernet 1/0/1
Console(config-if)# flowcontrol on
```

flowcontrol (Global)

Use the flowcontrol Global Configuration mode command to configure the Flow Control global mode.

Syntax
flowcontrol {*receive-only* | *send-receive*}

Parameters

- **receive-only**—The interfaces with enabled Flow Control will receive pause frames, but will not send Flow Control pause frames.
- **send-receive**—The interfaces with enabled Flow Control will receive and send pause frames.

Default Configuration
receive-only.

Command Mode
Global Configuration mode

User Guidelines
This command only determines the global mode and does not enable/disable Flow Control on any interface. Flowcontrol must also be enabled on the specific interfaces required (they are enabled by default).

Example
The following example enables Flow Control in the mode of only receiving pause frames and not sending them.

```
Console(config)# flowcontrol receive-only
```

show flowcontrol
Use the **show flowcontrol** Exec mode command to display the Flow Control global mode.

Syntax
show flowcontrol

Parameters
N/A

Default Configuration
N/A

Command Mode
Exec mode

Example
The following example displays the global Flow Control mode when it is receive-only.

```
Console# show flowcontrol
Global Flow Control mode is receive-only.
```

mdix

Use the **mdix** Interface Configuration (Ethernet) mode command to enable cable crossover on a given interface. Use the **no** form of this command to disable cable crossover.

Syntax

mdix *{on | auto}*

no mdix

Parameters

- **on**—Enables manual MDIX.
- **auto**—Enables automatic MDI/MDIX.

Default Configuration

The default setting is On.

Command Mode

Interface Configuration (Ethernet) mode

Example

The following example enables automatic crossover on port 1/5.

```
Console(config)# interface gi1/0/1/5
Console(config-if)# mdix auto.
```

The following example enables automatic crossover on port gigabitethernet 1/0/1.

```
Console(config)# interface gigabitethernet 1/0/5
Console(config-if)# mdix auto
```

back-pressure

Use the **back-pressure** Interface Configuration (Ethernet) mode command to enable back pressure on a specific interface. Use the **no** form of this command to disable back pressure.

Syntax

back-pressure

no back-pressure

Default Configuration

Back pressure is enabled.

Command Mode

Interface Configuration (Ethernet) mode

Example

The following example enables back pressure on port `gi1/0/5`.

```
Console(config)# interface gigabitethernet 1/0/5
Console(config-if)# back-pressure
```

port jumbo-frame

Use the **port jumbo-frame** Global Configuration mode command to enable jumbo frames on the device. Use the **no** form of this command to disable jumbo frames.

Syntax

port jumbo-frame

no port jumbo-frame

Default Configuration

Jumbo frames are disabled on the device.

Command Mode
Global Configuration mode

User Guidelines
This command takes effect only after resetting the device.

Example
The following example enables jumbo frames on the device.

```
Console(config)# port jumbo-frame
```

clear counters

Use the **show interfaces counters** EXEC mode command to display traffic seen by all the physical interfaces or by a specific interface.

Syntax
show interfaces counters *[interface-id] [**detailed**]*

Parameters
interface-id—Specifies an interface ID. The interface ID can be one of the following types: Ethernet port or Port-channel.

detailed—Displays information for non-present ports in addition to present ports.

Command Mode
EXEC mode

Example
The following example clears the statistics counters for gigabitethernet port 1/0/5.

```
Console# clear counters gigabitethernet 1/0/5.
```

set interface active

Use the **set interface active** EXEC mode command to reactivate an interface that was shut down.

Syntax

set interface active *{ interface-id }*

Parameters

interface-id—Specifies an interface ID. The interface ID can be one of the following types: Ethernet port or Port-channel.

Command Mode

EXEC mode

User Guidelines

This command is used to activate interfaces that were configured to be active, but were shut down by the system.

Example

The following example reactivates `gigabitethernet` port `1/0/1`.

```
Console# set interface active gigabitethernet 1/0/1
```

show interfaces configuration

Use the **show interfaces configuration** EXEC mode command to display the configuration for all configured interfaces or for a specific interface.

Syntax

show interfaces configuration *[interface-id]*

Parameters

interface-id—Specifies an interface ID. The interface ID can be one of the following types: Ethernet port or Port-channel.

Command Mode
EXEC mode

Example
The following example displays the configuration of all configured interfaces:

```
console# show interfaces configuration

                                        Flow     Admin  Back     Mdix
Port   Type      Duplex  Speed  Neg     control  State  Pressure Mode
------ --------- ------  -----  -------- -------  -----  -------- -
gi1/0/1 1G-Copper Full    10000  Disabled Off      Up     Disabled Off
gi1/0/2 1G-Copper Full    1000   Disabled Off      Up     Disabled Off
                                    Flow    Admin
Ch      Type   Speed  Neg         Control State
------  ------ -----  -------- -------   -----
Po1                   Disabled Off      Up
```

show interfaces status

Use the **show interfaces status** EXEC mode command to display the status of all configured interfaces or of a specific interface.

Syntax
show interfaces status *[interface-id][**detailed**]*

Parameters
interface-id—Specifies an interface ID. The interface ID can be one of the following types: Ethernet port or Port-channel.

detailed—Displays information for non-present ports in addition to present ports.

Command Mode
EXEC mode

Example
The following example displays the status of all configured interfaces.

```
console# show interfaces status
                                        Flow Link   Back     Mdix
Port   Type      Duplex Speed Neg       ctrl State  Pressure Mode
------ --------- ------ ----- -------- ---- ------ -------- --
gi1/0/1 1G-Copper Full   1000  Disabled Off  Up     Disabled Off
gi1/0/2 1G-Copper --     --     --       --   Down   --       --
                                        Flow  Link
Ch     Type      Duplex Speed  Neg      ctrl  State
-----  -------   ------ -----  -------  ----  ------
Po1    1G        Full   10000  Disabled Off  Up
```

show interfaces advertise

Use the **show interfaces advertise** EXEC mode command to display auto-negotiation advertisement information for all configured interfaces or for a specific interface.

Syntax
show interfaces advertise *[interface-id]*

Parameters
interface-id—Specifies an interface ID. The interface ID can be one of the following types: Ethernet port or Port-channel.

Command Mode
EXEC mode

Examples

The following examples display auto-negotiation information.

```
Console# show interfaces advertise

Port      Type          Neg      Operational Link Advertisement
----      ----------    ------   ------------------------------
gi1/0/1   1G-Copper     Enable   1000f, 100f, 10f, 10h
gi1/0/2   1G-Copper     Enable   1000f

Console# show interfaces advertise gigabitethernet 1/0/1
Port:gi1/0/1
Type: 1G-Copper
Link state: Up
Auto Negotiation: enabled

                                 10h    10f    100    100f   1000f
                                 ---    ---    h      ----   -----
Admin Local link Advertisement   yes    yes    ---    yes    yes
Oper Local link Advertisement    yes    yes    -      yes    yes
Remote Local link                no     no     yes    yes    yes
Advertisement                    -      -      yes    -      yes
Priority Resolution                             yes
                                                -

Console# show interfaces advertise gigabitethernet 1/0/1
Port: gi1/0/1
Type: 1G-Copper
Link state: Up
Auto negotiation: disabled.
```

show interfaces description

Use the **show interfaces description** EXEC mode command to display the description for all configured interfaces or for a specific interface.

Syntax

show interfaces description *[interface-id]*

Parameters

interface-id—Specifies an interface ID. The interface ID can be one of the following types: Ethernet port or Port-channel.

Command Mode
EXEC mode

Example
The following example displays the description of all configured interfaces.

```
Console# show interfaces description

Port        Descriptions
gi1/0/1     ----------------------------------------
gi1/0/1     Port that should be used for management only
gi1/0/2
gi1/0/1
gi1/0/1
gi1/0/2


Ch          Description
----        -----------
Po1         Output
```

show interfaces counters

Use the **show interfaces counters** EXEC mode command to display traffic seen by all the physical interfaces or by a specific interface.

Syntax
show interfaces counters *[interface-id]*

Parameters
interface-id—Specifies an interface ID. The interface ID can be one of the following types: Ethernet port or Port-channel.

Command Mode
EXEC mode

Example

The following example displays traffic seen by all the physical interfaces.

```
console# show interfaces counters gigabitethernet 1/0/
Port       InUcastPkts  InMcastPkts  InBcastPkts    InOctets
---------- ------------ ------------ ------------ ------------
gi1/0/1           0            0            0            0
Port       OutUcastPkts OutMcastPkts OutBcastPkts  OutOctets
---------- ------------ ------------ ------------ ------------
     gi1/0/1      0            1            35          7051
Alignment Errors: 0
FCS Errors: 0
Single Collision Frames: 0
Multiple Collision Frames: 0
SQE Test Errors: 0
Deferred Transmissions: 0
Late Collisions: 0
Excessive Collisions: 0
Carrier Sense Errors: 0
Oversize Packets: 0
Internal MAC Rx Errors: 0
Symbol Errors: 0
Received Pause Frames: 0
Transmitted Pause Frames: 0
```

The following table describes the fields shown in the display.

Field	Description
InOctets	The number of received octets.
InUcastPkts	The number of received unicast packets.
InMcastPkts	The number of received multicast packets.
InBcastPkts	The number of received broadcast packets.
OutOctets	The number of transmitted octets.
OutUcastPkts	The number of transmitted unicast packets.
OutMcastPkts	The number of transmitted multicast packets.
OutBcastPkts	The number of transmitted broadcast packets.
FCS Errors	The number of frames received that are an integral number of octets in length but do not pass the FCS check.
Single Collision Frames	The number of frames that are involved in a single collision, and are subsequently transmitted successfully.
Multiple Collision Frames	The number of frames that are involved in more than one collision and are subsequently transmitted successfully.
SQE Test Errors	The number of times that the SQE TEST ERROR is received. The SQE TEST ERROR is set in accordance with the rules for verification of the SQE detection mechanism in the PLS Carrier Sense Function as described in IEEE Std. 802.3, 2000 Edition, section 7.2.4.6.
Deferred Transmissions	The number of frames for which the first transmission attempt is delayed because the medium is busy.
Late Collisions	The number of times that a collision is detected later than one slotTime into the transmission of a packet.
Excessive Collisions	The number of frames for which transmission fails due to excessive collisions.
Oversize Packets	The number of frames received that exceed the maximum permitted frame size.

Field	Description
Internal MAC Rx Errors	The number of frames for which reception fails due to an internal MAC sublayer receive error.
Received Pause Frames	The number of MAC Control frames received with an opcode indicating the PAUSE operation.
Transmitted Pause Frames	The number of MAC Control frames transmitted on this interface with an opcode indicating the PAUSE operation.

show port jumbo-frame

Use the **show port jumbo-frame** EXEC mode command to display the configuration of jumbo frames.

Syntax

show port jumbo-frame

Command Mode

EXEC mode

Example

The following example displays the configuration of jumbo frames on the device.

```
Console# show port jumbo-frame

Jumbo frames are disabled
Jumbo frames will be enabled after reset
```

show errdisable interfaces

Use the **show errdisable interfaces** EXEC mode command to display the Err-Disable state of all interfaces or of a specific interface.

Syntax
show errdisable interfaces

Parameters

- Interface - Interface number
- port-channel-number - Port channel index.

Command Mode
EXEC mode

Example
The following example displays the Err-Disable state of all interfaces.

```
Console# show errdisable interfaces
Interface Reason
--------- --------------
gi1/1/50 stp-bpdu-guard
```

storm-control broadcast enable

Use the **storm-control broadcast enable** Interface Configuration mode command to enable storm control. Use the **no** form of this command to disable storm control.

Syntax
storm-control broadcast enable

no storm-control broadcast enable

Parameters
This command has no arguments or keywords.

Default Configuration
Disabled

Command Mode
Interface Configuration mode(Ethernet)

User Guidelines

- Use the **storm-control broadcast level** Interface Configuration command to set the maximum rate.
- Use the **storm-control include-multicast** Interface Configuration command to also count multicast packets and optionally unknown unicast packets in the storm control calculation.
-

Example

```
console(config)# interface gigabitethernet 1/0/1
console(config-if)# storm-control broadcast enable
```

storm-control broadcast level kbps

Use the **storm-control broadcast level**Interface Configuration mode command to configure the maximum rate of broadcast. Use the **no** form of this command to return to default.

Syntax
storm-control broadcast level kbps *kbps*

no storm-control broadcast level

Parameters
kbps—Maximum of kilo bits per second of broadcast traffic on a port. (Range: GE: 3.5M–1G, 10GE: 8.5M–10G)

Default Configuration
1000

Command Mode
Interface Configuration mode (Ethernet)

User Guidelines

Use the **storm-control broadcast enable** Interface Configuration command to enable storm control.

The calculated rate includes the 20 bytes of Ethernet framing overhead (preamble+SFD+IPG).

Example

```
console(config)# interface gigabitethernet 1/0/1
console(config-if)# storm-control broadcast level kbps 12345
```

storm-control include-multicast

Use the **storm-control include-multicast** Interface Configuration mode command to count multicast packets in the broadcast storm control. Use the **no** form of this command to disable counting of multicast packets in the broadcast storm control.

Syntax

storm-control include-multicast

no storm-control include-multicast

Parameters

Default Configuration

Disabled

Command Mode

Interface Configuration mode (Ethernet)

User Guidelines

Example

```
console(config)# interface gigabitethernet 1/0/1
console(config-if)# storm-control include-multicast
```

show storm-control

Use the **show storm-control** EXEC mode command to display the configuration of storm control.

Syntax

show storm-control *[interface-id]*

Parameters

interface-id—Specifies the interface.

Command Mode

EXEC mode

Example

```
console# show storm-control
Port   State    Rate [Kbits/Sec] Included
------ -------- --------------- ------------------------
gi1/0/1 Enabled  12345           Broadcast, Multicast,
                                  Unknown unicast
gi1/0/2 Disabled 100000          Broadcast
```

User Guidelines

Use the **storm-control broadcast enable** Interface Configuration command to enable storm control.

The calculated rate includes the 20 bytes of Ethernet framing overhead (preamble+SFD+IPG).

If the suppression level in percentage is translated (for the current port's speed) to a rate that is lower then the minimum rate, the minimum rate would be set.

Example

```
console(config)# interface gi1/0/1
console(config-if)# storm-control broadcast level kbps 12345
```

21

PHY Diagnostics Commands

test cable-diagnostics tdr

Use the **test cable-diagnostics tdr** Privileged EXEC mode command to use Time Domain Reflectometry (TDR) technology to diagnose the quality and characteristics of a copper cable attached to a port.

Syntax

test cable-diagnostics tdr interface *interface-id*

Parameters

interface-id—Specifies an interface ID. The interface ID must be an Ethernet port.

Command Mode

Privileged EXEC mode

User Guidelines

The port to be tested should be shut down during the test, unless it is a combination port with fiber port active.

The maximum length of cable for the TDR test is 120 meters.

Example

The following examples test the copper cables attached to ports 7 and 8.

```
Console# test cable-diagnostics tdr interface gi1/0/7
Cable is open at 64 meters

Console# test cable-diagnostics tdr interface gi1/0/8
```

```
Can't perform the test on fiber ports
```

show cable-diagnostics tdr

Use the **show cable-diagnostics tdr** EXEC mode command to display information on the last Time Domain Reflectometry (TDR) test performed on all copper ports or on a specific copper port.

Syntax

show cable-diagnostics tdr [*interface interface-id*]

Parameters

interface-id—Specifies an interface ID. The interface ID must be an Ethernet port.

Command Mode

EXEC mode

User Guidelines

The maximum length of cable for the TDR test is 120 meters.

Example

The following example displays information on the last TDR test performed on all copper ports.

```
Console> show cable-diagnostics tdr
Port        Result       Length [meters]     Date
----        ---------    -------------       --------------------
gi1/0/1     OK
gi1/0/2     Short        50                  13:32:00 23 July 2010
gi1/0/3     Test has not been performed
gi1/0/4     Open         64                  13:32:00 23 July 2010
gi1/0/5     Fiber        -                   -
```

show cable-diagnostics cable-length

Use the **show cable-diagnostics cable-length** EXEC mode command to display the estimated copper cable length attached to all ports or to a specific port.

Syntax

show cable-diagnostics cable-length [*interface interface-id*]

Parameters

interface-id—Specify an interface ID. The interface ID must be an Ethernet port.

Command Mode

EXEC mode

User Guidelines

The port must be active and working at 100 M or 1000 M.

Example

The following example displays the estimated copper cable length attached to all ports.

```
Console> show cable-diagnostics cable-length
Port        Length [meters]
----        -----------------
gi1/0/1     < 50
gi1/0/2     Copper not active
gi1/0/3     110-140
gi1/0/4     Fiber
```

show fiber-ports optical-transceiver

Use the **show fiber-ports optical-transceiver** EXEC mode command to display the optical transceiver diagnostics.

Syntax

show fiber-ports optical-transceiver [*interface interface-id] [detailed*]

Parameters

- **interface-id**—Specifies an interface ID. The interface ID must be an Ethernet port.
- **detailed**—Displays detailed diagnostics.

Command Mode

EXEC mode

Example

The following examples display the optical transceiver diagnostics results.

```
console# show fiber-ports optical-transceiver

   Port      Temp  Voltage Current Output Input LOS
                                   Power  Power
----------- ------ ------- ------- ------ ----- ---
   gi1/0/1    W       OK      OK     OK     OK   OK
   gi1/0/2    OK      OK      OK     E      OK   OK

 Temp         - Internally measured transceiver temperature
 Voltage      - Internally measured supply voltage
 Current      - Measured TX bias current
 Output Power - Measured TX output power in milliWatts
 Input Power  - Measured RX received power in milliWatts
 LOS          - Loss of signal
 N/A - Not Available, N/S - Not Supported,
 W - Warning, E - Error
```

```
console# show fiber-ports optical-transceiver detailed

   Port      Temp  Voltage Current Output  Input   LOS
             [C]   [Volt]  [mA]    Power   Power
                                   [mWatt] [mWatt]
----------- ------ ------- ------- ------- ------- ---
   gi0/1    Copper
  gi0/26    Copper
  gi0/27      28    3.32    7.26    3.53    3.68   No
  gi0/28      29    3.33    6.50    3.53    3.71   No
 Temp         - Internally measured transceiver temperature
 Voltage      - Internally measured supply voltage
 Current      - Measured TX bias current
 Output Power - Measured TX output power in milliWatts
 Input Power  - Measured RX received power in milliWatts
 LOS          - Loss of signal
 N/A - Not Available, N/S - Not Supported, W - Warning, E - Error
```

22

Power over Ethernet (PoE) Commands

power inline

Use the **power inline** Interface Configuration mode command to configure the inline power administrative mode on an interface.

Syntax

power inline *{auto | never}*

Parameters

- **auto**—Turns on the device discovery protocol and applies power to the device.
- **never**—Turns off the device discovery protocol and stops supplying power to the device.

Default Configuration

The default configuration is set to auto.

Command Mode

Interface Configuration (Ethernet) mode

Example

The following example turns on the device discovery protocol on port 4.

```
Console(config)# interface gigabitethernet 1/0/4
Console(config-if)# power inline auto
```

power inline powered-device

Use the **power inline powered-device** Interface Configuration mode command to add a description of the powered device type. Use the **no** form of this command to remove the description.

Syntax

power inline powered-device *pd-type*

no power inline powered-device

Parameters

pd-type—Enters a comment or a description to assist in recognizing the type of the powered device attached to this interface. (Length: 1–24 characters)

Default Configuration

There is no description.

Command Mode

Interface Configuration (Ethernet) mode

Example

The following example adds the description 'ip phone' of the device connected to port 4.

```
Console(config)# interfacegigabitethernet 1/0/4
Console(config-if)# power inline powered-device ip phone
```

power inline priority

Use the **power inline priority** Interface Configuration (Ethernet) mode command to configure the interface inline power management priority. Use the **no** form of this command to restore the default configuration.

Syntax

power inline priority *{critical | high | low}*

no power inline priority

Parameters

- **critical**—Specifies that the powered device operation is critical.
- **high**—Specifies that the powered device operation is high priority.
- **low**—Specifies that the powered device operation is low priority.

Default Configuration
The default configuration is set to low priority.

Command Mode
Interface Configuration (Ethernet) mode

Example
The following example sets the inline power management priority of `gigabitethernet` port 4 to High.

```
Console(config)# interfacegigabitethernet 1/0/4
Console(config-if)# power inline priority high
```

power inline usage-threshold

Use the **power inline usage-threshold** Global Configuration mode command to configure the threshold for initiating inline power usage alarms. Use the **no** form of this command to restore the default configuration.

Syntax
power inline usage-threshold *percent*

no power inline usage-threshold

Parameters
percent—Specifies the threshold in percent to compare to the measured power. (Range: 1–99)

Default Configuration
The default threshold is 95 percent.

Command Mode
Global Configuration mode

Example
The following example configures the threshold for initiating inline power usage alarms to 90 percent.

```
Console(config)# power inline usage-threshold 90
```

power inline traps enable

Use the **power inline traps enable** Global Configuration mode command to enable inline power traps. Use the **no** form of this command to disable traps.

Syntax
power inline traps enable

no power inline traps enable

Default Configuration
Inline power traps are disabled.

Command Mode
Global Configuration mode

Example
The following example enables inline power traps.

```
Console(config)# power inline traps enable
```

power inline limit

Use the **power inline limit** Interface Configuration mode command to configure the power limit per port on an interface. Use the **no** form of the command to return to default.

Syntax

power inline limit *power*

no power inline limit

Parameters

power—States the port power consumption limit in Milliwatts (Range: 0-15400

Default Configuration

The default value is the maximum power allowed in the specific working mode:

- 15.4W

Command Mode

Interface Configuration (Ethernet) mode

Example

The following example sets inline power on a port.

```
console(config)# interface gi1/0/1
console(config-if)# power inline limit 2222
```

show power inline

Use the **show power inline** EXEC mode command to display information about the inline power for all interfaces or for a specific interface.

Syntax

show power inline [*interface-id* | *module stack-member-number*]

Parameters

interface-id—Specifies an interface ID. The interface ID must be an Ethernet port.

stack-member-number—Specifies the switch member in a stack.

Default Configuration

There is no default configuration for this command.

Command Mode

EXEC mode

Example 1:

The following example displays information about the inline power.

```
console(config)# show power inline
Port based power-limit mode
Unit  Power  Nominal    Consumed      Usage       Traps
             Power      Power         Threshold
---- ------- -------    -------       ------      --------
 1     On  500 Watts  100 Watts (20%) 95         Disable
 2     Off   1 Watts    0 Watts (0%)   95         Disable
 3     Off   1 Watts    0 Watts (0%)   95         Disable
 4     Off   1 Watts    0 Watts (0%)   95         Disable
 5     Off   1 Watts    0 Watts (0%)   95         Disable
 6     Off   1 Watts    0 Watts (0%)   95         Disable
 7     Off   1 Watts    0 Watts (0%)   95         Disable
 8     Off   1 Watts    0 Watts (0%)   95         Disable

Port    Powered Device        State      Status    Priority  Class
-----   --------------      -----------  --------  --------  -------
gi1/0/1 IP Phone Model A     Auto        On        High      Class0
gi1/0/2 Wireless AP Model A  Auto        On        Low       Class1
gi1/0/3                      Auto        Off       Low       N/A
...
```

Example 2:

The following example displays information about the inline power for a specific port.

```
console(config)# show power inline gi1/1/1
Port    Powered Device     State    Status  Priority  Class
-----   --------------     -------  ------  --------  -------
gi1/1/1 IP Phone Model A   Auto     On      High      Class0

Power limit (for port power-limit mode): 15.4W
Overload Counter: 0
Short Counter: 0
Denied Counter: 0
Absent Counter: 0
Invalid Signature Counter: 0
```

The following table describes the fields shown in the display:

Field	Description
Power	The inline power sourcing equipment operational status.
Nominal Power	The inline power sourcing equipment nominal power in Watts.
Consumed Power	The measured usage power in Watts.
Usage Threshold	The usage threshold expressed in percent for comparing the measured power and initiating an alarm if threshold is exceeded.
Traps	Indicates if inline power traps are enabled.
Port	The Ethernet port number.
Powered device	A description of the powered device type.
Admin State	Indicates if the port is enabled to provide power. The possible values are Auto or Never.
Priority	The port inline power management priority. The possible values are Critical, High or Low.
Oper State	Describes the port inline power operational state. The possible values are On, Off, Test-Fail, Testing, Searching or Fault.

Field	Description
Classification	The power consumption classification of the powered device.
Overload Counter	Counts the number of overload conditions detected.
Short Counter	Counts the number of short conditions detected.
Denied Counter	Counts the number of times power was denied.
Absent Counter	Counts the number of times power was removed because powered device dropout was detected.
Invalid Signature Counter	Counts the number of times an invalid signature of a powered device was detected.

The following table describes the fields shown in the display:

Following is a list of port status values:

Port is on - valid capacitor detected

Port is on - valid resistor detected

Port is off - main supply voltage is high

Port is off - main supply voltage is low

Port is off -‘disable all ports’ pin is active

Port is off - non-existing port number Fewer ports are available than the max.

Port is off - Port is yet undefined

Port is off - internal hardware fault

Port is off - user setting

Port is off - detection is in process

Port is off - non-802.3af powered device

Port is off - Overload & Underload states

Port is off – Underload state

Port is off – Overload state

Port is off - power budget exceeded

Port is off - internal hardware fault

Port is off – voltage injection into the port

Port is off - improper Capacitor Detection results

Port is off - discharged load Port fails Capacitor

Port is on – detection regardless (Force On)

```
Undefined error during Force On
Supply voltage higher than settings
Supply voltage lower than settings
Disable_PDU flag raised during Force On
Port is forced on, then disabled
Port is off – forced power error due to Overload
Port is off - “out of power budget” during Force On
Communication error with PoE devices after Force On
Port is off – short condition
Port is off – over temperature at the port
Port is off – device is too hot
Unknown device port status
Force Power Error Short Circuit
Force Power Error Channel Over Temperature
Force Power Error Chip Over Temperature
Power Management-Static
Power Management-Static -ovl
Force Power Error Management Static
Force Power Error Management Static -ovl
High power port is ON
Chip Over Power
Force Power Error Chip Over Power
```

show power inline consumption

Use the **show power inline consumption** EXEC mode command to display information about the inline power consumption for all interfaces or for a specific interface.

Syntax

show power inline consumption *[interface-id | module stack-member-number]*

Parameters

Interface-id—Specifies an interface ID. The interface ID must be an Ethernet port.

stack-member-number—Specifies the switch member in a stack.

Default Configuration
There is no default configuration for this command.

Command Mode
EXEC mode

Example
The following example displays information about the inline power consumption.

```
Console# show power inline consumption

Port      Power          Power (W)     Voltage (V)  Current
----      Limit (W)      ----------    ---------    (mA)
gi1/0/1   ----------     4.115         50.8         ---------
gi1/0/1   15.4           4.157         50.7         81
gi1/0/1   15.4           4.021         50.9         82
          15.4                                      79
```

show power inline version

Use the **show power inline version** EXEC mode command to display the power inline microcontroller's software version for all the stacking units or for a specific unit.

Syntax
show power inline version *[unit unit]*

Parameters
unit unit — Specifies the stacking unit number.

Default Configuration
There is no default configuration for this command.

Command Mode
EXEC mode

Example
The following example displays information about the inline power consumption.

```
Console# show power inline version

Unit             Software version
----             ----------------
1                1.12
2                1.12
```

23

EEE Commands

eee enable (global)

Use the **eee enable** Global Configuration command to enable the EEE mode globally. Use the **no** format of the command to disable the mode.

Syntax

eee enable

no eee enable

Default Configuration

EEE is enabled.

Command Mode

Global Configuration mide

User Guidelines

Since EEE uses the Auto-Negotiation to negotiate the EEE support on both sides of the link, if Auto-Negotiation is not enabled on the port, the EEE Operational status is disabled.

eee enable (interface)

Use the **eee enable** Interface Configuration command to enable the EEE mode on an Ethernet port. Use the **no** format of the command to disable the mode.

Syntax

eee enable

no eee enable

Default Configuration
EEE is enabled.

Command Mode
Interface Configuration mode (Ethernet)

User Guidelines
Since EEE uses the Auto-Negotiation to negotiate the EEE support on both sides of the link, if Auto-Negotiation is not enabled on the port, the EEE Operational status is disabled.

eee lldp enable

Use the **eee lldp enable** Interface Configuration command to enable EEE support by LLDP on an Ethernet port. Use the **no** format of the command to disable the support.

Syntax
eee lldp enable

no eee lldp enable

Default Configuration
Enabled

Command Mode
Interface Configuration mode (Ethernet)

User Guidelines
Enabling EEE LLDP advertisement allows devices to choose and change system wake-up times in order to get the optimal energy saving mode.

show eee

Use the **show eee** EXEC command to display EEE information.

Syntax

show eee *[interface-id]*

Parameters

interface-id—Specify an interface ID. The interface ID must be an Ethernet port.

Command Mode

EXEC

Examples

```
Example 1. Brief Information about all ports
Switch>show eee
EEE globally enabled
EEE Administrate status is enabled on ports: gi1/0/1-6,gi1/0/12
EEE Operational status is enabled on ports: gi1/0/1,gi1/0/3-
6,gi1/0/12,gi1/0/15
EEE LLDP Administrate status is enabled on ports: gi1/0/1-10
EEE LLDP Operational status is enabled on ports: gi1/0/3-5
```

```
Example 2.  Port in state notPresent, no information if port
supports EEE
Switch> show eee gi1/0/10
Port Status: notPresent
EEE Administrate status: enabled
EEE LLDP Administrate status: enabled
EEE LLDP Administrate status: enabled
```

```
Example 3. Port in status DOWN
Switch>show eee gi1/0/10
Port Status: DOWN
EEE capabilities:
  Speed 10M: EEE not supported
```

```
  Speed 100M: EEE supported
  Speed 1G: EEE supported
  Speed 10G: EEE not supported
EEE Administrate status: enabled
EEE LLDP Administrate status: enabled
```

```
Example 4. Port in status UP and does not support EEE
Switch>show eee gi1/0/20
Port Status: UP
EEE capabilities:
  Speed 10M: EEE not supported
  Speed 100M: EEE supported
  Speed 1G: EEE supported
  Speed 10G: EEE not supported
Current port speed: 1Gbps
EEE Administrate status: enabled
EEE LLDP Administrate status: enabled
```

```
Example 5. Neighbor does not support EEE
Switch>show eee gi1/0/15
Port Status: UP
EEE capabilities:
  Speed 10M: EEE not supported
  Speed 100M: EEE supported
  Speed 1G: EEE supported
  Speed 10G: EEE not supported
Current port speed: 1Gbps
EEE Remote status: disabled
EEE Administrate status: enabled
EEE Operational status: disabled (neighbor does not support)
EEE LLDP Administrate status: enabled
```

```
EEE LLDP Operational status: disabled
```

```
Example 6. EEE is disabled on the port
Switch>show eee gi1/0/10
Port Status: UP
EEE capabilities:
  Speed 10M: EEE not supported
  Speed 100M: EEE supported
  Speed 1G: EEE supported
  Speed 10G: EEE not supported
Current port speed: 1Gbps
EEE Administrate status: disabled
EEE Operational status: disabled
EEE LLDP Administrate status: enabled
EEE LLDP Operational status: disabled
```

```
Example 7. EEE is running on the port, EEE LLDP is disabled
Switch>show eee gi1/0/12
Port Status: UP
EEE capabilities:
  Speed 10M: EEE not supported
  Speed 100M: EEE supported
  Speed 1G: EEE supported
  Speed 10G: EEE not supported
Current port speed: 1Gbps
EEE Remote status: enabled
EEE Administrate status: enabled
EEE Operational status: enabled
EEE LLDP Administrate status: disabled
EEE LLDP Operational status: disabled
Resolved Tx Timer: 10usec
```

```
Local Tx Timer: 10 usec
Resolved Timer: 25 usec
Local Rx Timer: 20 usec
```

Example 8. EEE and EEE LLDP are running on the port

```
Switch>show eee gi1/0/3
Port Status: UP
EEE capabilities:
  Speed 10M: EEE not supported
  Speed 100M: EEE supported
  Speed 1G: EEE supported
  Speed 10G: EEE not supported
Current port speed: 1Gbps
EEE Remote status: enabled
EEE Administrate status: enabled
EEE Operational status: enabled
EEE LLDP Administrate status: enabled
EEE LLDP Operational status: enabled
Resolved Tx Timer: 10usec
Local Tx Timer: 10 usec
Remote Rx Timer: 5 usec
Resolved Timer: 25 usec
Local Rx Timer: 20 usec
Remote Tx Timer: 25 usec
```

Example 9. EEE is running on the port, EEE LLDP enabled but not synchronized with remote link partner

```
Switch>show eee gi1/0/9
Port Status: up
EEE capabilities:
  Speed 10M: EEE not supported
  Speed 100M: EEE supported
```

```
  Speed 1G: EEE supported
  Speed 10G: EEE not supported
Current port speed: 1Gbps
EEE Remote status: enabled
EEE Administrate status: enabled
EEE Operational status: enabled
EEE LLDP Administrate status: enabled
EEE LLDP Operational status:  disabled
Resolved Tx Timer: 64
Local Tx Timer: 64
Resolved Rx Timer: 16
Local Rx Timer: 16
```

```
Example 10. EEE and EEE LLDP are running on the port
Switch>show eee gi1/0/3
Port Status: UP
EEE capabilities:
  Speed 10M: EEE not supported
  Speed 100M: EEE supported
  Speed 1G: EEE supported
  Speed 10G: EEE not supported
Current port speed: 1Gbps
EEE Remote status: enabled
EEE Administrate status: enabled
EEE Operational status: enabled
EEE LLDP Administrate status: enabled
EEE LLDP Operational status: enabled
Resolved Tx Timer: 10usec
Local Tx Timer: 10 usec
Remote Rx Timer: 5 usec
Resolved Timer: 25 usec
```

```
Local Rx Timer: 20 usec
Remote Tx Timer: 25 usec
```

24

Green Ethernet

show green-ethernet

Use the **show green-ethernet** Privileged EXEC mode command to show green-ethernet configuration and information.

Syntax

show green-ethernet *[interface-id]*

Parameters

interface-id—Specifies an interface ID. The interface ID must be an Ethernet port.

Parameters Range

Default. When no interface is specified, this command shows information for all interfaces.

Command Mode

Privileged EXEC mode

User Guidelines

The following describes all possible reasons the **show** command displays, and their descriptions.

If there are a several reasons for non-operation, then only the highest priority reason is displayed.

Energy-detect Non-operational Reasons		
priority	Reason	Description

1	NP	Port is not present
2	LT	Link Type is not supported (fiber, auto media select)
3	LU	Port Link is up – NA

Short-Reach Non-operational Reasons		
Priority	**Reason**	**Description**
1	NP	Port is not present
2	LT	Link Type is not supported (fiber)
3	LS	Link Speed Is not Supported (100M,10M,10G)
4	LL	Link Length received from VCT Test exceed threshold
6	LD	Port Link is Down – NA

Example

```
console# show green-ethernet
Energy-Detect mode: Enabled
Short-Reach mode: Disabled
Power Consumption: 76% (3.31W out of maximum 4.33W)
Cumulative Energy Saved: 33 [Watt*Hour]
Short-Reach cable length threshold: 50m

Port     Energy-Detect       Short-Reach           VCT Cable
      Admin Oper Reason   Admin Force Oper Reason   Length
----  ----- ---- -------  ----- ----- ---- -------  ------
gi1/0/1  on   on             off  off   off
gi1/0/2  on   off  LU         on   off   off           < 50
gi1/0/3  on   off  LU         off  off   off
```

green-ethernet short-reach (global)

Use the **green-ethernet short-reach** Global Configuration mode command to enable green-ethernet short-reach mode globally. Use the **no** form of this command to disabled it.

Syntax

green-ethernet short-reach

no green-ethernet short-reach

Parameters

This command has no arguments or keywords.

Default Configuration

EEE is enabled.

Command Mode

Global Configuration mode

Example

```
console(config)# green-ethernet short-reach
```

green-ethernet short-reach (interface)

Use the **green-ethernet short-reach** Interface Configuration mode command to enable green-ethernet short-reach mode on an interface. Use the **no** form of this command to disable it on an interface.

Syntax

green-ethernet short-reach

no green-ethernet short-reach

Parameters

This command has no arguments or keywords.

Default Configuration
EEE is enabled.

Command Mode
Interface Configuration mode (Ethernet)

User Guidelines
When **short-reach Mode** is enabled and is not forced, the VCT (Virtual Cable Tester) length check must be performed. The VCT length check can be performed only on a copper port operating at a speed of 1000 Mbps. If the media is not copper or the link speed is not 1000 Mbps and short-reach mode is not forced (by **green-ethernet short-reach force**), short-reach mode is not applied.

When the interface is set to enhanced mode, after the VCT length check has completed and set the power to low, an active monitoring for errors is done continuously. In the case of errors crossing a certain threshold, the PHY will be reverted to long reach.

Example

```
console(config)# interface gi1/0/1
console(config-if)# green-ethernet short-reach
```

green-ethernet short-reach force

Use the **green-ethernet short-reach force** Interface Configuration mode command to force short-reach mode on an interface. Use the **no** form of this command to return to default.

Syntax
green-ethernet short-reach force

no green-ethernet short-reach force

Parameters
This command has no arguments or keywords.

Default Configuration
Short-reach mode is not forced.

Command Mode
Interface Configuration mode(Ethernet)

Example

```
console(config)# interface gi1/0/1
console(config-if)# green-ethernet short-reach force
```

green-ethernet short-reach threshold

Use the **green-ethernet short-reach threshold** Global Configuration mode command to set the maximum cable length for applying short-reach. Use the **no** form of this command to return to default.

Syntax
green-ethernet short-reach threshold *cable-length*

no green-ethernet short-reach threshold

Parameters
cable-length—Specifies the maximum cable length (in meters) measured by VCT that allows applying short-reach mode (cable-length 0–70 meters)

Default Configuration
The default length is 40 meters.

Command Mode
Global Configuration mode

User Guidelines
Note that the automatic cable length measurement accuracy is +-10 meters. i.e. a cable with a real length of 30 m may be evaluated in the range of 20m–40m. Length performance depends on the link partner signal quality, cable quality and whether link partner also operates in short-reach mode.

The recommended default is 50m, as recommended by Marvell PHY team for any cable type. see appendix

However, Marvell tests show that link partner can operate error free with an up to 80 m cable (cat 5e).

The user may choose to change the threshold parameter under certain circumstances.

Setting the threshold to 0 meters basically results in the short reach feature always being disabled, because the threshold will always be exceeded.

green-ethernet power-meter reset

Use the **green-ethernet power meter reset** Privileged EXEC mode command to reset the power save meter.

Syntax

green-ethernet power-meter reset

Command Mode

Privileged EXEC mode.

25

Port Channel Commands

Use the **channel-group** Interface Configuration (Ethernet) mode command to associate a port with a port-channel. Use the **no** form of this command to remove a port from a port-channel.

Syntax

channel-group *port-channel mode {on | auto}*

no channel-group

Parameters

- **port-channel**—Specifies the port channel number for the current port to join.
- **mode {on | auto}**—Specifies the mode of joining the port channel. The possible values are:
  - **on**—Forces the port to join a channel without an LACP operation.
  - **auto**—Forces the port to join a channel as a result of an LACP operation.

Default Configuration

The port is not assigned to a port-channel.

Command Mode

Interface Configuration (Ethernet) mode

Example

The following example forces port `gi1/0/1` to join port-channel 1 without an LACP operation.

```
Console(config)# interface gigabitethernet 1/0/1
```

```
Console(config-if)# channel-group 1 mode on
```

port-channel load-balance

Use the **port-channel load-balance** Global Configuration mode command to configure the load balancing policy of the port channeling. Use the **no** form of this command to reset to default.

Syntax

port-channel load-balance *{src-dst-mac | src-dst-ip | src-dst-mac-ip | }*

no port-channel load-balance

Parameters

- **src-dst-mac**—Port channel load balancing is based on the source and destination MAC address.
- **src-dst-ip**—Port channel load balancing is based on the source and destination IP address.
- **src-dst-mac-ip**—Port channel load balancing is based on the source and destination of MAC and IP addresses.

Default Configuration

src-dst-mac is the default option.

Command Mode

Global Configuration mode

User Guidelines

In **src-dst-mac-ip-port l**oad balancing policy, fragmented packets might be reordered.

Example

```
console#
console# configure
console(config)# port-channel load-balance src-dst-mac
console(config)# port-channel load-balance src-dst-ip
```

```
console(config)# port-channel load-balance src-dst-mac-ip
console(config)# port-channel load-balance src-dst-mac-ip-port
console(config)#
```

show interfaces port-channel

Use the **show interfaces port-channel** EXEC mode command to display port-channel information for all port channels or for a specific port channel.

Syntax

show interfaces port-channel *[interface-id]*

Parameters

interface-id—Specify an interface ID. The interface ID must be a Port Channel.

Command Mode

EXEC mode

Example

The following example displays information on all port-channels.

```
console#
console# show interfaces port-channel
Load balancing: src-dst-mac.
Gathering information...
Channel  Ports
-------  -----
Po1      Active: gi1/0/1,Inactive: gi1/0/2-3
Po2      Active: gi1/0/25 Inactive: gi1/0/24
Po3
console# show interfaces switchport gi1/0/10
Gathering information...

Name: gi1/0/10
Switchport: enable
```

```
Administrative Mode: access
Operational Mode: down
Access Mode VLAN: 1
Access Multicast TV VLAN: none
Trunking Native Mode VLAN: 1
Trunking VLANs Enabled: 1
                        2-4094 (Inactive)
General PVID: 1
General VLANs Enabled: none
General Egress Tagged VLANs Enabled: none
General Forbidden VLANs: none
General Ingress Filtering: enabled
General Acceptable Frame Type: all
General GVRP status: disabled
Customer Mode VLAN: none
Private-vlan promiscuous-association primary VLAN: none
Private-vlan promiscuous-association Secondary VLANs Enabled: none
Private-vlan host-association primary VLAN: none
Private-vlan host-association Secondary VLAN Enabled: none
DVA: disable
```

26

Address Table Commands

bridge multicast filtering

Use the **bridge multicast filtering** Global Configuration mode command to enable the filtering of multicast addresses. Use the **no** form of this command to disable multicast address filtering.

Syntax

bridge multicast filtering

no bridge multicast filtering

Default Configuration

Multicast address filtering is disabled. All multicast addresses are flooded to all ports.

Command Mode

Global Configuration mode

User Guidelines

If multicast devices exist on the VLAN, do not change the unregistered multicast addresses' states to drop on the device ports.

If multicast devices exist on the VLAN and IGMP-snooping is not enabled, the **bridge multicast forward-all** command should be used to enable forwarding all multicast packets to the multicast switches.

Example

The following example enables bridge multicast filtering.

```
Console(config)# bridge multicast filtering
```

bridge multicast address

Use the **bridge multicast address** Interface Configuration (VLAN) mode command to register a MAC-layer multicast address in the bridge table and statically add or remove ports to or from the group. Use the **no** form of this command to unregister the MAC address.

Syntax

bridge multicast address {*mac-multicast-address*} *[[add | remove] {ethernet interface-list* |
port-channel *port-channel-list*}]

no bridge multicast address {*mac-multicast-address*}

Parameters

- **mac-multicast-address**—Specifies the group MAC multicast address.
- **add**—Adds ports to the group.
- **remove**—Removes ports from the group.
- **ethernet interface-list**—Specifies a list of Ethernet ports. Separate nonconsecutive Ethernet ports with a comma and no spaces. Use a hyphen to designate a range of ports.
- **port-channel port-channel-list**—Specifies a list of port channels. Separate nonconsecutive port-channels with a comma and no spaces; use a hyphen to designate a range of port channels.

Default Configuration

No multicast addresses are defined.

If **ethernet interface-list** or **port-channel port-channel-list** is specified without specifying **add** or **remove**, the default option is **add**.

Command Mode

Interface Configuration (VLAN) mode

User Guidelines

To register the group in the bridge database without adding or removing ports or port channels, specify the **mac-multicast-address** parameter only.

Static multicast addresses can be defined on static VLANs only.

You can execute the command before the VLAN is created.

Example

The following example registers the MAC address to the bridge table:

```
Console(config)# interface vlan 8
Console(config-if)# bridge multicast address 01:00:5e:02:02:03
```

The following example registers the MAC address and adds ports statically.

```
Console(config)# interface vlan 8
Console(config-if)# bridge multicast address 01:00:5e:02:02:03
add  gi1/0/1-2
```

bridge multicast forbidden address

Use the **bridge multicast forbidden address** Interface Configuration (VLAN) mode command to forbid adding or removing a specific multicast address to or from specific ports. Use the **no** form of this command to restore the default configuration.

Syntax

bridge multicast forbidden address {*mac-multicast-address*} *{add | remove}* *{ethernet interface-list | port-channel port-channel-list}*

no bridge multicast forbidden address {*mac-multicast-address*}

Parameters

- **mac-multicast-address**—Specifies the group MAC multicast address.
- **add**—Forbids adding ports to the group.
- **remove**—Forbids removing ports from the group.
- **ethernet interface-list**—Specifies a list of Ethernet ports. Separate nonconsecutive Ethernet ports with a comma and no spaces. Use a hyphen to designate a range of ports.

- **port-channel port-channel-list**—Specifies a list of port channels. Separate nonconsecutive port-channels with a comma and no spaces. Use a hyphen to designate a range of port channels.

Default Configuration
No forbidden addresses are defined.

Command Mode
Interface Configuration (VLAN) mode

User Guidelines
Before defining forbidden ports, the multicast group should be registered.

You can execute the command before the VLAN is created.

Example
The following example forbids MAC address 0100.5e02.0203 on port 2/9 within VLAN 8.

```
Console(config)# interface vlan 8
Console(config-if)# bridge multicast address 0100.5e.02.0203
Console(config-if)# bridge multicast forbidden address
0100.5e02.0203 add gi1/0/9
```

bridge multicast unregistered

Use the **bridge multicast unregistered** Interface Configuration (Ethernet, Port-Channel) mode command to configure the forwarding state of unregistered multicast addresses. Use the **no** form of this command to restore the default configuration.

Syntax
bridge multicast unregistered *{forwarding | filtering}*

no bridge multicast unregistered

Parameters

- **forwarding**—Forwards unregistered multicast packets.

- **filtering**—Filters unregistered multicast packets.

Default Configuration
Unregistered multicast addresses are forwarded.

Command Mode
Interface Configuration (Ethernet, Port-Channel) mode

User Guidelines
Do not enable unregistered multicast filtering on ports that are connected to routers, because the 224.0.0.x address range should not be filtered. Note that routers do not necessarily send IGMP reports for the 224.0.0.x range.

You can execute the command before the VLAN is created.

Example
The following example specifies that unregistered multicast packets are filtered on gigabitethernet port `1/0/1`:

```
Console(config)# interface gi1/0/1
Console(config-if)# bridge multicast unregistered filtering
```

bridge multicast forward-all

Use the **bridge multicast forward-all** Interface Configuration (VLAN) mode command to enable forwarding all multicast packets for a range of ports or port channels. Use the **no** form of this command to restore the default configuration.

Syntax
bridge multicast forward-all *{add | remove} {ethernet interface-list | port-channel port-channel-list}*

no bridge multicast forward-all

Parameters
- **add**—Forces forwarding of all multicast packets.
- **remove**—Does not force forwarding of all multicast packets.

- **ethernet interface-list**—Specifies a list of Ethernet ports. Separate nonconsecutive Ethernet ports with a comma and no spaces. Use a hyphen to designate a range of ports.
- **port-channel port-channel-list**—Specifies a list of port channels. Separate nonconsecutive port-channels with a comma and no spaces. Use a hyphen to designate a range of port channels.

Default Configuration
Forwarding of all multicast packets is disabled.

Command Mode
Interface Configuration (VLAN) mode

Example
The following example enables all multicast packets on port gi1/0/8 to be forwarded.

```
Console(config)# interface vlan 2
Console(config-if)# bridge multicast forward-all add gi1/0/8
```

bridge multicast forbidden forward-all
Use the **bridge multicast forbidden forward-all** Interface Configuration (VLAN) mode command to forbid a port to dynamically join multicast groups. Use the no form of this command to restore the default configuration.

Syntax
bridge multicast forbidden forward-all *{add | remove} {ethernet interface-list | port-channel port-channel-list}*

no bridge multicast forbidden forward-all

Parameters
- **add**—Forbids forwarding of all multicast packets.
- **remove**—Does not forbid forwarding of all multicast packets.

- **ethernet interface-list**—Specifies a list of Ethernet ports. Separate nonconsecutive Ethernet ports with a comma and no spaces. Use a hyphen to designate a range of ports.
- **port-channel port-channel-list**—Specifies a list of port channels. Separate nonconsecutive port-channels with a comma and no spaces; use a hyphen to designate a range of port channels.

Default Configuration
Ports are not forbidden to dynamically join multicast groups.

Command Mode
Interface Configuration (VLAN) mode

User Guidelines
Use this command to forbid a port to dynamically join (by IGMP, for example) a multicast group.

The port can still be a multicast router port.

Example
The following example forbids forwarding of all multicast packets to gi1/0/1 within VLAN 2.

```
Console(config)# interface vlan 2
Console(config-if)# bridge multicast forbidden forward-all add ethernet gi1/0/1
```

mac address-table static

Use the **mac address-table static** Global Configuration mode command to add MAC-layer station source address to the MAC address table. Use the **no** form of this command to delete the MAC address.

Syntax
mac address-table static *mac-address vlan vlan-id interface interface-id [permanent | delete-on-reset | delete-on-timeout | secure]*

no mac address-table static [*mac-address] vlan vlan-id*

Parameters

mac-address—AC address (Range: Valid MAC address)

vlan-id—Specify the VLAN

interface-id—Specify an interface ID. The interface ID can be one of the following types: Ethernet port or port-channel (Range: Valid Ethernet port, Valid Port-channel number)

permanent—The address can only deleted by the no bridge address command.

delete-on-reset—The address is deleted after reset.

delete-on-timeout—The address is deleted after aged out.

secure—The address is deleted after the port changes mode to unlock learning (no port security command). Available only when the port is in learning locked mode.

Default Configuration

No static addresses are defined. The default mode for an added address is permanent.

Command Mode

Global Configuration mode

Example

```
console(config)# mac address-table static 00:3f:bd:45:5a:b1 vlan 1
gi1/0/1
```

clear mac address-table

Use the **clear mac address-table** Privileged EXEC command to remove learned or secure entries from the forwarding database.

Syntax

clear mac address-table *dynamic [interface interface-id]*

clear mac address-table *secure interface interface-id*

Parameters
interface interface-id—Delete all dynamic address on the specified interface.The interface ID can be one of the following types: Ethernet port or port-channel.

Command Mode
Privileged EXEC mode

Example

```
console# clear mac address-table dynamic
```

mac address-table aging-time

Use the **mac address-table aging-time** global configuration command to set the aging time of the address table. Use the **no** form of this command to restore the default.

Syntax
mac address-table aging-time *seconds*

no mac address-table aging-time

Parameters
seconds—Time is number of seconds. (Range:10–300)

Default Configuration
300

Command Mode
Global Configuration mode

Example

```
console(config)# mac address-table aging-time 600
```

port security

Use the **port security** Interface Configuration (Ethernet, Port-channel) mode command to enable port security on an interface. Use the **no** form of this command to disable port security on an interface.

Syntax

port security [*forward* | *discard* | *discard-shutdown*] *[trap seconds]*

no port security

Parameters

- **forward**—Forwards packets with unlearned source addresses, but does not learn the address.
- **discard**—Discards packets with unlearned source addresses.
- **discard-shutdown**—Discards packets with unlearned source addresses and shuts down the port.
- **trap seconds**—Sends SNMP traps and specifies the minimum time interval in seconds between consecutive traps. (Range: 1–1000000)

Default Configuration

The feature is disabled

The default mode is discard.

Command Mode

Interface Configuration (Ethernet, port-channel) mode

Example

The following example forwards all packets to port gi1/0/1 without learning addresses of packets from unknown sources and sends traps every 100 seconds if a packet with an unknown source address is received.

```
console(config)# gigabitethernet 1/0/1
Console(config-if)# port security forward trap 100
```

port security mode

Use the **port security mode** Interface Configuration (Ethernet, port-channel) mode command configures the port security learning mode. Use the no form of this command to restore the default configuration.

Syntax

port security mode {lock | max-addresses }

no port security mode

Parameters

- **lock**—Saves the current dynamic MAC addresses associated with the port and disables learning, relearning and aging.
- **max-addresses**—Deletes the current dynamic MAC addresses associated with the port and learns up to the maximum number of addresses allowed on the port. Relearning and aging are enabled.

Default Configuration

The default port security mode is lock.

Command Mode

Interface Configuration (Ethernet, port-channel) mode

Example

The following example sets the port security mode to dynamic for gigabitethernet interface 1/0/7.

```
Console(config)# interface gigabitethernet 1/0/7
Console(config-if)# port security mode dynamic
```

port security max

Use the **port security mode** Interface Configuration (Ethernet, Port-channel) mode command to configure the maximum number of addresses that can be learned on the port while the port is in port security max-addresses mode. Use the **no** form of this command to restore the default configuration.

Syntax

port security max {*max-addr*}

no port security max

Parameters

max-addr—Specifies the maximum number of addresses that can be learned on the port. (Range: 0–128)

Default Configuration

This default maximum number of addresses is 1.

Command Mode

Interface Configuration (Ethernet, Port-channel) mode

User Guidelines

This command is relevant in port security max-addresses mode only.

Example

```
Console(config)# interface gigabitethernet 1/0/1
Console(config-if)# port security max 20
```

port security routed secure-address

Use the **port security routed secure-address** Interface Configuration (Ethernet, Port-channel) mode command to add a MAC-layer secure address to a routed port. Use the no form of this command to delete a MAC address from a routed port.

Syntax

port security routed secure-address *mac-address*

no port security routed secure-address [*mac-address*]

Parameters

mac-address—Specifies the MAC address.

Default Configuration
No addresses are defined.

Command Mode
Interface Configuration (Ethernet, port-channel) mode. It cannot be configured for a range of interfaces (range context).

User Guidelines
This command enables adding secure MAC addresses to a routed port in port security mode. The command is available when the port is a routed port and in port security mode. The address is deleted if the port exits the security mode or is not a routed port.

This command is required because the **bridge address** command cannot be executed on internal VLANs.

Example
The following example adds the MAC-layer address 66:66:66:66:66:66 to gigabitethernet port 1/0/1.

```
Console(config)# interface gigabitethernet 1/0/1
Console(config-if)# port security routed secure-address
66:66:66:66:66:66
```

show mac address-table

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

Syntax
show mac address-table *[dynamic | static| secure] [vlan vlan] [interface interface-id] [address mac-address]*

Parameters
- **dynamic**—Displays only dynamic MAC address table entries.
- **static**—Displays only static MAC address table entries.
- **secure**—Displays only secure MAC address table entries.

- **vlan**—Specifies VLAN, such as VLAN 1.
- **interface-id**—Specifies an interface ID. The interface ID can be one of the following types: Ethernet port or port-channel.
- **mac-address**—MAC address.

Default

Command Mode
EXEC mode

User Guidelines
Internal usage VLANs (VLANs that are automatically allocated on routed ports) are presented in the VLAN column by a port number and not by a VLAN ID.

Example

```
Console# show mac address-table
Aging time is 300 sec
 VLAN        MAC Address         Port       Type
-------- ------------------- ---------- ----------
   1       00:00:26:08:13:23       0         self
   1       00:3f:bd:45:5a:b1     gi1/0/1      static
   1       00:a1:b0:69:63:f3     gi1/0/24    dynamic
   2       00:a1:b0:69:63:f3     gi1/0/24    dynamic

Console# show mac address-table 00:3f:bd:45:5a:b1
Aging time is 300 sec

VLAN        MAC Address         Port       Type
-------- ------------------- ---------- ----------
1         00:3f:bd:45:5a:b1    static      gi1/0/9
```

show mac address-table count

Use the **show mac address-table count** EXEC mode command to display the number of addresses present in the Forwarding Database.

Syntax

show mac address-table count *[vlan vlan | interface interface-id]*

Parameters

- vlan—Specifies VLAN.
- **interface-id**—Specifies an interface ID. The interface ID can be one of the following types: Ethernet port or port-channel.

Command Mode

EXEC mode

Example

```
Console# show mac address-table count

Capacity: 8192
Free: 8083
Used: 109

Static addresses: 2
Secure addresses: 1
Dynamic addresses: 97
Internal addresses: 9
```

show bridge multicast address-table

Use the **show bridge multicast address-table** EXEC mode command to display multicast MAC address or IP address table information.

Syntax

show bridge multicast address-table *[vlan vlan-id] [address {mac-multicast-address | ipv4-multicast-address | ipv6-multicast-address}] [format {ip | mac}]*

Parameters

- **vlan vlan-id**—Specifies the VLAN ID.
- **address {mac-multicast-address | ipv4-multicast-address | ipv6-multicast-address}**—Specifies the multicast address. The possible values are:
  - **mac-multicast-address**—Specifies the MAC multicast address.
  - **ipv4-multicast-address**—Specifies the IPv4 multicast address.
  - **ipv6-multicast-address**—Specifies the IPv6 multicast address.
- **format {ip | mac}**—Specifies the multicast address format. The possible values are:
  - **ip**—Specifies that the multicast address is an IP address.
  - **mac**—Specifies that the multicast address is a MAC address.

Default Configuration

If the format is not specified, it defaults to mac.

Command Mode

EXEC mode

User Guidelines

A MAC address can be displayed in IP format only if it is within the range 0100.5e00.0000 through 0100.5e7f.ffff.

Multicast Router ports (defined statically or discovered dynamically) are members in all MC groups.

Ports that were defined via **bridge multicast forbidden forward-all** command are displayed in all forbidden MC entries.

Example

The following example displays bridge multicast address information.

```
Console# show bridge multicast address-table
```

```
Multicast address table for VLANs in MAC-GROUP bridging mode:

Vlan    MAC Address         Type           Ports
---- -----------------    --------------   -----
8    01:00:5e:02:02:03     Static          1-2


Forbidden ports for multicast addresses:

Vlan    MAC Address         Ports
---- -----------------      -----
8    01:00:5e:02:02:03      gi1/0/9


Multicast address table for VLANs in IPv4-GROUP bridging mode:

Vlan    MAC Address         Type             Ports
---- -----------------    --------------     -----
1      224.0.0.251         Dynamic           gi1/0/12


Forbidden ports for multicast addresses:

Vlan    MAC Address         Ports
---- -----------------      -----
1      232.5.6.5
1      233.22.2.6


Multicast address table for VLANs in IPv4-SRC-GROUP bridging mode:

Vlan  Group Address  Source address  Type        Ports
---- --------------- --------------- --------    -----
1     224.2.2.251     11.2.2.3       Dynamic     gi1/0/11
Forbidden ports for multicast addresses:
```

```
Vlan  Group Address  Source Address   Ports
---- --------------- --------------- -------
8    239.2.2.2       *               gi1/0/9
8    239.2.2.2       1.1.1.11        gi1/0/9


Multicast address table for VLANs in IPv6-GROUP bridging mode:

VLAN  IP/MAC Address   Type      Ports
---- ----------------- --------- --------------------
8    ff02::4:4:4       Static    gi1/0/1-2,gi1/0/7,Po1

Forbidden ports for multicast addresses:

VLAN  IP/MAC Address   Ports
---- ----------------- -----------
8    ff02::4:4:4       gi1/0/9

Multicast address table for VLANs in IPv6-SRC-GROUP bridging mode:

Vlan  Group Address  Source address  Type     Ports
---- --------------- --------------- -------- ------------------
8    ff02::4:4:4     *               Static   gi1/0/1-2,gi1/0/7,Po1
8    ff02::4:4:4     fe80::200:7ff:  Static
                     fe00:200
Forbidden ports for multicast addresses:

Vlan  Group Address  Source address  Ports
---- --------------- --------------- ----------
8    ff02::4:4:4     *               gi1/0/9
8    ff02::4:4:4     fe80::200:7ff:f    gi1/0/9
                     e00:200
```

show bridge multicast address-table static

Use the **show bridge multicast address-table static** EXEC mode command to display the statically configured multicast addresses.

Syntax

show bridge multicast address-table static *[vlan vlan-id] [address mac-multicast-address | ipv4-multicast-address | ipv6-multicast-address] [source ipv4-source-address | ipv6-source-address] [all | mac | ip*]

Parameters

- **vlan vlan-id**—Specifies the VLAN ID.
- **address {mac-multicast-address | ipv4-multicast-address | ipv6-multicast-address}**—Specifies the multicast address. The possible values are:
  - **mac-multicast-address**—Specifies the MAC multicast address.
  - **ipv4-multicast-address**—Specifies the IPv4 multicast address.
  - **ipv6-multicast-address**—Specifies the IPv6 multicast address.
- **source {ipv4-source-address | ipv6-source-address}**—Specifies the source address. The possible values are:
  - *i***pv4-address**—Specifies the source IPv4 address.
  - **ipv6-address**—Specifies the source IPv6 address.

Default Configuration

When all/mac/ip is not specified, all entries (mac and ip) will be displayed.

Command Mode

EXEC mode

User Guidelines

A MAC address can be displayed in IP format only if it is within the range 0100.5e00.0000–- 0100.5e7f.ffff.

Example

The following example displays the statically configured multicast addresses.

```
Console# show bridge multicast address-table static

MAC-GROUP table

Vlan          MAC Address            Ports
----          --------------         --------
1             0100.9923.8787         gi1/0/1, gi1/0/2

Forbidden ports for multicast addresses:

Vlan          MAC Address            Ports
----          --------------         --------
IPv4-GROUP Table

Vlan          IP Address             Ports
----          ----------             --------
1             231.2.2.3              gi1/0/1, gi1/0/2
19            231.2.2.8              gi1/0/1-8
19            231.2.2.8              gi1/0/9-11

Forbidden ports for multicast addresses:

Vlan          IP Address             Ports
----          ----------             --------
1             231.2.2.3              gi1/0/8
19            231.2.2.8              gi1/0/8

IPv4-SRC-GROUP Table:
```

```
Vlan          Group Address          Source                    Ports
----          ---------------        address                   ------
                                     ---------------

Forbidden ports for multicast addresses:

Vlan          Group Address          Source                    Ports
----          ---------------        address                   ------
                                     ---------------

IPv6-GROUP Table

Vlan          IP Address             Ports
----          -----------------      ---------
191           FF12::8                gi1/0/1-8

Forbidden ports for multicast addresses:

Vlan          IP Address             Ports
----          -----------------      ---------
11            FF12::3                gi1/0/8
191           FF12::8                gi1/0/8

IPv6-SRC-GROUP Table:

Vlan          Group Address          Source                    Ports
----          ---------------        address                   ------
192           FF12::8                ---------------           gi1/0/1-
                                     FE80::201:C9A9:FE40:8988  8
```

```
Forbidden ports for multicast addresses:

Vlan        Group Address      Source                Ports
----        --------------     address               ------
192         FF12::3            ---------------       gi1/0/8
                               FE80::201:C9A9:FE40
                               :8988
```

show bridge multicast filtering

Use the **show bridge multicast filtering** EXEC mode command to display the multicast filtering configuration.

Syntax

show bridge multicast filtering *vlan-id*

Parameters

vlan-id—Specifies the VLAN ID. (Range: Valid VLAN)

Command Mode

EXEC mode

Example

The following example displays the multicast configuration for VLAN 1.

```
Console# show bridge multicast filtering 1

Filtering: Enabled

VLAN: 1

Port            Forward-All
-----           Static          Status
gi1/0/1         ---------       ------
gi1/0/2         Forbidden       Filter
gi1/0/3         Forward         Forward(s)
                -               Forward(d)
```

show bridge multicast unregistered

Use the **show bridge multicast unregistered** EXEC mode command to display the unregistered multicast filtering configuration.

Syntax

show bridge multicast unregistered *[interface-id]*

Parameters

interface-id—Specifies an interface ID. The interface ID can be one of the following types: Ethernet port or Port-channel.

Command Mode

EXEC mode

Example
The following example displays the unregistered multicast configuration.

```
Console# show bridge multicast unregistered


Port          Unregistered
-------       -------------
gi1/0/1       Forward
gi1/0/2       Filter
gi1/0/3       Filter
```

show ports security

Use the **show ports security** Privileged EXEC mode command to display the port-lock status.

Syntax
show ports security *[interface-id]*

Parameters
interface-id—Specifies an interface ID. The interface ID can be one of the following types: Ethernet port or Port-channel.

Command Mode
Privileged EXEC mode

Example
The following example displays the port-lock status of all ports.

```
console# show ports security

Port   Status   Learning   Action    Max  Trap     Frequency
------- -------- --------- ------    ---  -------  --------
gi1/0/1  Enabled  Max-       Discard   3     Enabled 100
               Addresses
gi1/0/2  Disabled Max-       -         28    -        -
```

```
                Addresses
gi1/0/3  Enabled  Lock        Discard, 8     Disabled -
                                    Shutdown
```

The following table describes the fields shown above.

Field	Description
Port	The port number.
Status	The port security status. The possible values are: Enabled or Disabled.
Mode	The port security mode.
Action	The action taken on violation.
Maximum	The maximum number of addresses that can be associated on this port in the Max-Addresses mode.
Trap	The status of SNMP traps. The possible values are: Enable or Disable.
Frequency	The minimum time interval between consecutive traps.

show ports security addresses

Use the **show ports security addresses** Privileged EXEC mode command to display the current dynamic addresses in locked ports.

Syntax

show ports security addresses [*interface-id*

Parameters

interface-id—Specifies an interface ID. The interface ID can be one of the following types: Ethernet port or Port-channel.

Command Mode

Privileged EXEC mode

Example

The following example displays dynamic addresses in all currently locked ports.

```
Console# show ports security addresses

Port        Status      Learning          Current     Maximum
----        --------    -------------     -------     -------
gi1/0/1     Enabled     Max-addresses     2           3
gi1/0/2     Disabled    Max-addresses     -           128
gi1/0/3     Enabled     Lock              NA          NA
```

27

Port Monitor Commands

port monitor

Use the **port monitor** Interface Configuration (Ethernet) mode command to start a port monitoring session. Use the **no** form of this command to stop a port monitoring session.

Syntax

port monitor *src-interface-id [rx | tx]*

no port monitor *src-interface-id*

Parameters

- **rx**—Monitors received packets only. If no option is specified, it monitors both rx and tx.
- **tx**—Monitors transmitted packets only. If no option is specified, it monitors both rx and tx.
- **src-interface-id**—Specifies an interface ID. The interface ID must be and Ethernet port.

Default Configuration

Monitors both received and transmitted packets.

Command Mode

Interface Configuration (Ethernet) mode. It cannot be configured for a range of interfaces (range context).

User Guidelines

This command enables port copy between Source Port (src-interface) to a Destination Port (The port in context).

The analyzer port for port ingress traffic mirroring should be the same port for all mirrored ports.

The analyzer port for port egress traffic mirroring should be the same port for all mirrored ports.

Following are restrictions apply for ports that are configured to be source ports:

- The port cannot be a destination port.

The following restrictions apply to ports that are configured to be monitor ports:

- The port can't be source port.
- The port isn't member in port-channel.
- IP interface is not configured on the port.
- GVRP is not enabled on the port.
- The port is not a member in any VLAN, except for the default VLAN (will be automatically removed from the default VLAN).
- L2 protocols are not active on the copy dest. Port: LLDP, LBD, STP, LACP.

The following restrictions apply to ports that are configured to be monitor ports:

- The port cannot be source port.
- The port is not a member in port-channel.

Notes:

1. In this mode some traffic duplication on the analyzer port may be observed. For example:
   - Port 2 is being egress monitored by port 4.
   - Port 2 & 4 are members in VLAN 3.
   - Unknown Unicast packet sent to VLAN 3 will egress from port 4 twice, one instance as normal forward and another instance as mirrored from port 2.

- Moreover, if port 2 is an untagged member in VLAN 3 and port 4 is a tagged member then both instances will look different (one tagged and the other is not).

2) When the port is configured to 802.1X auto mode it will forward any mirrored traffic regardless of the .1X state. However, it will operate as a normal network port (forward traffic) only after authorization is done.

3) Mirrored traffic is exposed to STP state, i.e. if the port is in STP blocking, it will not egress any mirrored traffic.

Example
The following example copies traffic for both directions (Tx and Rx) from the source port 1/8 to destination port 1/1.

```
Console(config)# interface gi1/0/1
Console(config-if)# port monitor gi1/0/8
Console(config)# interface gigabitethernet 1/0/1
Console(config-if)# port monitor 1/8
```

show ports monitor

Use the **show ports monitor** EXEC mode command to display the port monitoring status.

Syntax
show ports monitor

Command Mode
EXEC mode

Example
The following example displays the port monitoring status.

```
Console# show ports monitor
Source port     Destination Port   Type      Status
-----------   ----------------    --------  --------
gi1/0/8           gi1/0/1        RX,TX     Active
```

```
gi1/0/2           gi1/0/1         RX,TX     Active
gi1/0/18          gi1/0/1         Rx        Active
gi1/0/
```

28

sFlow Commands

sflow receiver

Use the **sflow receiver** Global Configuration mode command to define sFlow collector. Use the **no** form of this command to remove the definition of the collector.

Syntax

sflow receiver *index {ipv4-address | ipv6-address | hostname} [port port] [max-datagram-size bytes]*

no sflow receiver *index*

Parameters

- **index**—The index of the receiver. (Range: 1–8)
- **ipv4-address**—Pv4 address of the host to be used as an sFlow Collector.
- **ipv6-address**—IPv6 address of the host to be used as an sFlow Collector. When the IPv6 address is a Link Local address (IPv6Z address), the outgoing interface name must be specified. Refer to the User Guidelines for the interface name syntax.
- **hostname**—Hostname of the host to be used as an sFlow Collector. Only translation to IPv4 addresses is supported.
- **port**—Port number for syslog messages. If unspecified, the port number defaults to 6343. The range is 1-65535.
- **bytes**—Specifies the maximum number of bytes that can be sent in a single sample datagram. If unspecified, it defaults to 1400.

Default

No receiver is defined.

Command Mode
Global Configuration mode

User Guidelines

If the IP address of the sFlow receiver is set to 0.0.0.0, no sFlow datagrams are sent.

sflow flow-sampling

Use the **sflow flow-sampling** Interface Configuration mode command to enable sFlow Flow sampling and configure the average sampling rate of a specific port. Use the **no** form of this command to disable Flow sampling.

Syntax
sflow flow-sampling *rate receiver-index [max-header-size bytes]*

no sflow flow-sampling

Parameters
- **rate**—Specifies the average sampling rate (Range: 1, 1024–1073741823.)
- **receiver-index**—Index of the receiver/collector (Range: 1–8.)
- **bytes**—Specifies the maximum number of bytes that would be copied from the sampled packet. If unspecified, defaults to 128. (Range: 20–256.)

Default
Disabled

Command Mode
Interface Configuration (Ethernet) mode

User Guidelines

A new sampling rate configuration is not immediately loaded to the hardware. It will be loaded to the hardware only after the next packet is sampled (based on the current sampling rate).

sflow counters-sampling

Use the **sflow counters-sampling** Interface Configuration mode command to enable sFlow Counters sampling and to configure the maximum interval of a specific port. Use the **no** form of this command to disable sFlow Counters sampling.

Syntax

sflow counters-sampling *interval receiver-index*

no sflow counters-sampling

Parameters

- **interval**—Specifies the maximum number of seconds between successive samples of the interface counters. (Range: 1, 15–86400.)
- **receiver-index**—Index of the receiver/collector. (Range: 1–8.)

Default

Disabled

Command Mode

Interface Configuration (Ethernet) mode

clear sflow statistics

Use the **clear sFlow statistics** EXEC mode command to clear sFlow statistics.

Syntax

clear sflow statistics *[interface-id]*

Parameters

interface-id—Specifies an interface ID. The interface ID must be an Ethernet port.

Command Mode

EXEC mode

User Guidelines

If no interface is specified by the user, the command clears all the sFlow statistics counters (including datagrams sent). If an interface is specified by the user, the command clears only the counter of the specific interface.

show sflow configuration

Use the **show sflow configuration** EXEC mode command to display the sFlow configuration for ports that are enabled for Flow sampling or Counters sampling.

Syntax

show sflow configuration *[interface-id]*

Parameters

interface-id—Specifies an interface ID. The interface ID must be an Ethernet port.

Command Mode

EXEC mode

Example

```
Console # show sflow configuration
Receivers
Index      IP Address        Port   Max Datagram Size
----- ------------------- -------- ----------------
  1         0.0.0.0          6343         1400
  2         172.16.1.2       6343         1400
  3         0.0.0.0          6343         1400
  4         0.0.0.0          6343         1400
  5         0.0.0.0          6343         1400
  6         0.0.0.0          6343         1400
  7         0.0.0.0          6343         1400
  8         0.0.0.0          6343         1400
Interfaces
```

```
Inter-  Flow       Counters  Max Header Flow      Counters Collector
face    Sampling   Sampling  Size       Collector Index    Index
----- ----------- --------- ---------   ---------- -----   ------------
gi1/0/1   1/2048     60 sec    128        1                  1
gi1/0/2   1/4096     Disabled  128        0                  2
```

show sflow statistics

Use the **show sflow statistics** EXEC mode command to display the sFlow statistics for ports that are enabled for Flow sampling or Counters sampling.

Syntax

show sflow statistics *[interface-id]*

Parameters

interface-id—Specifies an interface ID. The interface ID must be an Ethernet port.

Command Mode

EXEC mode

Example

```
Console # show sflow statistics
Total sFlow datagrams sent to collectors: 100
```

Interface	Packets sampled	datagrams sent to collector
1/1	30	50
1/2	10	10

1/1	0	10
1/2	0	0

29

LLDP Commands

lldp run

Use the **lldp run** Global Configuration mode command to enable Link Layer Discovery Protocol (LLDP). To disable LLDP, use the **no** form of this command.

Syntax

lldp run

no lldp run

Parameters

This command has no arguments or keywords.

Default

Enabled

Command Mode

Global Configuration mode

Example

```
console(config)# lldp run
```

lldp transmit

Use the **lldp transmit** Interface Configuration mode command to enable transmitting Link Layer Discovery Protocol (LLDP) on an interface. Use the **no** form of this command to stop transmitting LLDP on an interface.

Syntax

lldp transmit

no lldp transmit

Parameters

This command has no arguments or keywords.

Default

Enabled

Command Mode

Interface Configuration (Ethernet) mode

User Guidelines

LLDP manages LAG ports individually. LLDP sends separate advertisements on each port in a LAG.

LLDP operation on a port is not dependent on the STP state of a port. I.e. LLDP frames are sent on blocked ports.

If a port is controlled by 802.1X, LLDP would operate only if the port is authorized.

Example

```
console(config)# interface gigabitethernet 1/0/1
console(config-if)# lldp transmit
```

lldp receive

Use the **lldp receive** Interface Configuration mode command to enable receiving Link Layer Discovery Protocol (LLDP) on an interface. Use the **no** form of this command to stop receiving LLDP on an interface.

Syntax

lldp receive

no lldp receive

Parameters
This command has no arguments or keywords.

Default
Enabled

Command Mode
Interface Configuration (Ethernet) mode

User Guidelines
LLDP manages LAG ports individually. LLDP data received through LAG ports is stored individually per port.

LLDP operation on a port is not dependent on the STP state of a port. I.e. LLDP frames are received on blocked ports.

If a port is controlled by 802.1X, LLDP would operate only if the port is authorized.

Example

```
console(config)# interface gigabitethernet 1/0/1
console(config-if)# lldp receive
```

lldp timer

Use the **lldp timer** Global Configuration mode command to specify how often the software sends Link Layer Discovery Protocol (LLDP) updates. Use the **no** form of this command to restore the default configuration.

Syntax
lldp timer *seconds*

no lldp timer

Parameters
seconds—Specifies, in seconds, how often the software sends LLDP updates. (Range: 5?32768 seconds)

Default Configuration
The default update interval is 30 seconds.

Command Mode
Global Configuration mode

Example
The following example sets the interval for sending LLDP updates to 60 seconds.

```
Console(config)# lldp timer 60
```

lldp hold-multiplier

Use the **lldp hold-multiplier** Global Configuration mode command to set the time interval during which the receiving device holds a Link Layer Discovery Protocol (LLDP) packet before discarding it. Use the **no** form of this command to restore the default configuration.

Syntax
lldp hold-multiplier *number*

no lldp hold-multiplier

Parameters
number—Specifies the LLDP packet hold time interval as a multiple of the LLDP timer value. (Range: 2use the **no** form of this command10)

Default Configuration
The default LLDP hold multiplier is 4.

Command Mode
Global Configuration mode

User Guidelines
The actual Time-To-Live (TTL) value of LLDP frames is expressed by the following formula:

TTL = min(65535, LLDP-Timer * LLDP-HoldMultiplier)

For example, if the value of the LLDP timer is 30 seconds, and the value of the LLDP hold multiplier is 4, then the value 120 is encoded in the TTL field of the LLDP header.

Example

The following example sets the LLDP packet hold time interval to 90 seconds.

```
Console(config)# lldp timer 30
Console(config)# lldp hold-multiplier 3
```

lldp reinit

Use the **lldp reinit** Global Configuration mode command to specify the minimum time an LLDP port waits before reinitializing LLDP transmission. Use the **no** form of this command to revert to the default setting.

Syntax

lldp reinit seconds

no lldp reinit

Parameters

seconds—Specifies the minimum time in seconds an LLDP port waits before reinitializing LLDP transmission.(Range: 1–10)

Default

2 seconds

Command Mode

Global Configuration mode

Example

```
console(config)# lldp reinit 4
```

lldp tx-delay

Use the **lldp tx-delay** Global Configuration mode command to set the delay between successive LLDP frame transmissions initiated by value/status changes in the LLDP local systems MIB. Use the **no** form of this command to restore the default configuration.

Syntax

lldp tx-delay *seconds*

no lldp tx-delay

Parameters

seconds—Specifies the delay in seconds between successive LLDP frame transmissions initiated by value/status changes in the LLDP local systems MIB. (Range: 1?8192 seconds)

Default Configuration

The default LLDP frame transmission delay is 2 seconds.

Command Mode

Global Configuration mode

User Guidelines

It is recommended that the tx-delay be less than 0.25 of the LLDP timer interval.

Example

The following example sets the LLDP transmission delay to 10 seconds.

```
Console(config)# lldp tx-delay 10
```

lldp optional-tlv

Use the **lldp optional-tlv** Interface Configuration (Ethernet) mode command to specify which optional TLVs from the basic set are transmitted. Use the **no** form of this command to restore the default configuration.

Syntax

lldp optional-tlv *tlv* [*tlv2* … *tlv5*]

no lldp optional-tlv

Parameters

tlv—Specifies TLV that should be included. Available optional TLVs are: port-desc, sys-name, sys-desc, sys-cap, 802.3-mac-phy, 802.3-lag, 802.3-max-frame-size.

Default Configuration

No optional TLV is transmitted.

Command Mode

Interface Configuration (Ethernet) mode

Example

The following example specifies that the port description TLV is transmitted on gigabitethernet port 1/0/2.

```
Console(config)# interface gigabitethernet 1/0/2
Console(config-if)# lldp optional-tlv port-desc
```

lldp management-address

Use the **lldp management-address** Interface Configuration (Ethernet) mode command to specify the management address advertised from an interface. Use the **no** form of this command to stop advertising management address information.

Syntax

lldp management-address *{ip-address | none | automatic [interface-id] }*

no lldp management-address

Parameters

- **ip-address**—Specifies the static management address to advertise.
- **none**—Specifies that no address is advertised.

- **automatic**—Specifies that the software would automatically choose a management address to advertise from all the IP addresses of the product. In case of multiple IP addresses the software chooses the lowest IP address among the dynamic IP addresses. If there are no dynamic addresses, the software chooses the lowest IP address among the static IP addresses.
- **automatic interface-id**—Specifies that the software automatically chooses a management address to advertise from the IP ddresses that are configured (associated) for the interface ID. In case of multiple IP addresses, the software chooses the lowest IP address among the dynamic IP addresses of the interface. If there are no dynamic addresses, the software chooses the lowest IP address among the static IP addresses of the interface. The interface ID can be one of the following types: Ethernet port, Port-channel or VLAN. Note that if the port or port- channel are members in a VLAN that has an IP address, that address is not included because the address is associated with the VLAN.

Default Configuration

No IP address is advertised.

The default advertisement is **automatic**.

Command Mode

Interface Configuration (Ethernet) mode

User Guidelines

Each port can advertise one IP address.

Example

The following example sets the LLDP management address advertisement mode to **automatic** on gigabitethernet port `1/0/2`.

```
Console(config)# interface gigabitethernet 1/0/2
Console(config)# lldp management-address automatic
```

lldp notifications

Use the **lldp notifications** Interface Configuration (Ethernet) mode command to enable or disable sending Link Layer Discovery Protocol (LLDP)

notifications on an interface. Use the **no** form of this command to restore the default configuration.

Syntax

lldp notifications *{enable | disable}*

no lldp notifications

Parameters

- **enable**—Enables sending LLDP notifications.
- **disable**—Disables sending LLDP notifications.

Default Configuration

Sending LLDP notifications is disabled.

Command Mode

Interface Configuration (Ethernet) mode

Example

The following example enables sending LLDP notifications on gigabitethernet port `1/0/5`.

```
Console(config)# interface gigabitethernet 1/0/5
Console(config)# lldp notifications 10
```

lldp notifications interval

Use the **lldp notifications interval** Global Configuration mode command to configure the maximum transmission rate of LLDP notifications. Use the **no** form of this command to return to the default.

Syntax

lldp notifications interval *seconds*

no lldp notifications interval

Parameters

seconds—The device should not send more than one notification in the indicated period. (Range: 5–3600)

Default

5 seconds

Command Mode

Global Configuration mode

Example

```
console(config)# lldp notification interval 10
```

lldp optional-tlv 802.1

Use the **lldp optional-tlv** Interface Configuration mode command to specify which optional TLVs from the basic set to transmit. Use the **no** form of this command revert to the default setting.

Syntax

lldp optional-tlv 802.1 *pvid*

no lldp optional-tlv 802.1 *pvid*

lldp optional-tlv 802.1 **ppvid add** *ppvid*

lldp optional-tlv 802.1 **ppvid remove** *ppvid*

lldp optional-tlv 802.1 **vlan-name add** *vlan-id*

lldp optional-tlv 802.1 **vlan-name remove** *vlan-id*

lldp optional-tlv 802.1 **protocol add** *{stp | rstp | mstp | pause | 802.1x | lacp | gvrp}*

lldp optional-tlv 802.1 **protocol remove** *{stp | rstp | mstp | pause | 802.1x | lacp | gvrp}*

Parameters

- *pvid*—Advertises the PVID of the port.

- ppvid—Adds/removes PPVID for advertising. PPVID 0 can be used to advertise the PPVIDs capabilities of the interface.(Range: 0–4094)
- vlan—Adds/removse VLAN ID for advertising. (Range: 1–4094)

Default
No optional TLV is transmitted.

Command Mode
Interface Configuration (Ethernet) mode

lldp med enable

Use the **lldp med enable** Interface Configuration (Ethernet) mode command to enable Link Layer Discovery Protocol (LLDP) Media Endpoint Discovery (MED) on an interface. Use the **no** form of this command to disable LLDP MED on an interface.

Syntax
lldp med enable [*tlv* … *tlv4*]

no lldp med enable

Parameters
tlv—Specifies the TLV that should be included. Available TLVs are: network-policy, location, and poe-pse, inventory. The capabilities TLV is always included if LLDP-MED is enabled.

Default Configuration
LLDP MED is disabled.

Command Mode
Interface Configuration (Ethernet) mode

Example
The following example enables LLDP MED with the **location** TLV on gigabitethernet port `1/0/`3.

```
Console(config)# interface gigabitethernet 1/0/3
Console(config)# lldp med enable location
```

lldp med notifications topology-change

Use the **lldp med notifications topology-change** Interface Configuration (Ethernet) mode command to enable sending LLDP MED topology change notifications. Use the **no** form of this command to restore the default configuration.

Syntax

lldp med notifications topology-change *{enable | disable}*

no lldp med notifications topology-change

Parameters

- **enable**—Enables sending LLDP MED topology change notifications.
- **disable**—Disables sending LLDP MED topology change notifications.

Default Configuration

Disable is the default.

Command Mode

Interface Configuration (Ethernet) mode

Example

The following example enables sending LLDP MED topology change notifications on gigabitethernet port 1/0/2.

```
Console(config)# interface gigabitethernet 1/0/2
Console(config)# lldp med notifications topology-change enable
```

lldp med fast-start repeat-count

Use the **lldp med fast-start repeat-count** Global Configuration mode command to configure the number of times the fast start LLDPDU is being sent during the activation of the fast start mechanism defined by LLDP-MED. Use the **no** form of this command return to default.

Syntax

lldp med fast-start repeat-count *number*

no lldp med fast-start repeat-count

Parameters

number—Specifies the number of times the fast start LLDPDU is being sent during the activation of the fast start mechanism.

Default

3

Command Mode

Global Configuration mode

Example

```
console(config)# lldp med fast-start repeat-count 4
```

lldp med network-policy (global)

Use the **lldp med network-policy** Global Configuration mode command to define LLDP MED network policy. Use the **no** form of this command to remove LLDP MED network policy.

Syntax

lldp med network-policy *number application [vlan id] [vlan-type {tagged | untagged}] [up priority] [dscp value]*

no lldp med network-policy *number*

Parameters

- **number**—Network policy sequential number.
- **application**—The name or the number of the primary function of the application defined for this network policy. Available application names are: voice, voice-signaling, guest-voice, guest-voice-signaling, softphone-voice, video-conferencing, streaming-video, video-signaling.
- **vlan id**—VLAN identifier for the application.
- **vlan-type**—Specifies if the application is using a Tagged or an Untagged VLAN.
- **up priority**—User Priority (Layer 2 priority) to be used for the specified application.
- **dscp value**—DSCP value to be used for the specified application.

Default

No Network policy is defined.

Command Mode

Global Configuration mode

User Guidelines

Use the **lldp med network-policy** Interface Configuration command to attach a network policy to a port.

Up to 32 network policies can be defined.

Example

```
console(config)# lldp med network-policy 1 voice-signaling vlan 1
```

lldp med network-policy (interface)

Use the **lldp med network-policy** Interface Configuration (Ethernet) mode command to attach or remove an LLDP MED network policy on an interface. Use the **no** form of this command to remove all the LLDP MED network policies from the interface.

Syntax

lldp med network-policy *{add | remove} number*

no lldp med network-policy *number*

Parameters

- **number**—Specifies the network policy sequential number.
- **add**—Attaches the specified network policy to the interface.
- **remove**—Removes the specified network policy from the interface.

Default Configuration

No network policy is attached to the interface.

Command Mode

Interface Configuration (Ethernet) mode

User Guidelines

For each port, only one network policy per application (voice, voice-signaling, etc.) can be defined.

Example

The following example attaches LLDP MED network policy 1 to `gigabitethernet` port `1/0/1`.

```
Console(config)# interface gigabitethernet 1/0/1
Console(config-if)# lldp med network-policy add 1
```

clear lldp table

Use the **clear lldp table** command in Privileged EXEC mode to restart the LLDP RX state machine and clear the neighbors table.

Syntax

clear lldp table *[interface-id]*

Parameters

interface-id—Specifies an interface ID. The interface ID must be an Ethernet port.

Command Mode

Privileged EXEC mode

Example

```
console# clear lldp table gigabitethernet 1/0/1
```

lldp med location

Use the **lldp med location** Interface Configuration (Ethernet) mode command to configure the location information for the Link Layer Discovery Protocol (LLDP) Media Endpoint Discovery (MED) for an interface. Use the **no** form of this command to delete location information for an interface.

Syntax

lldp med location *{{coordinate data} | {civic-address data} | {ecs-elin data}}*

no lldp med location *{coordinate | civic-address | ecs-elin}*

Parameters

- **coordinate**—Specifies the location data as coordinates.
- **civic-address**—Specifies the location data as a civic address.
- **ecs-elin**—Specifies the location data as an Emergency Call Service Emergency Location Identification Number (ECS ELIN).
- **data**—Specifies the location data in the format defined in ANSI/TIA 1057: dotted hexadecimal data: Each byte in a hexadecimal character string is two hexadecimal digits. Bytes are separated by a period or colon. (Length: coordinate: 16 bytes. Civic-address: 6-160 bytes. Ecs-elin: 10-25 bytes)

Default Configuration

The location is not configured.

Command Mode
Interface Configuration (Ethernet) mode

Example
The following example configures the LLDP MED location information on gigabitethernet port 1/0/2 as a civic address.

```
console(config)# interface gi1/0/2
console(config-if)# lldp med location civic-address 616263646566
```

show lldp configuration

Use the **show lldp configuration** Privileged EXEC mode command to display the Link Layer Discovery Protocol (LLDP) configuration for all interfaces or for a specific interface.

Syntax
show lldp configuration *[interface-id]*

Parameters
interface-id—Specifies an interface ID. The interface ID must be an Ethernet port.

Command Mode
Privileged EXEC mode

Example
The following example sets the LLDP re-initialization delay to 10 seconds.

```
Switch# show lldp configuration
State: Enabled
Timer: 30 Seconds
Hold multiplier: 4
Reinit delay: 2 Seconds
Tx delay: 2 Seconds
Notifications interval: 5 seconds
```

```
LLDP packets handling: Filtering

Port    State  Optional TLVs      Address       Notifications
----    ----- --------------      -------       ------------
gi1/0/1  RX,TX PD, SN, SD, SC       172.16.1.1    Disabled
gi1/0/2  TX    PD, SN               172.16.1.1    Disabled
gi1/0/3  RX,TX PD, SN, SD, SC       None          Disabled
gi1/0/5  RX,TX D, SN, SD, SC        automatic     Disabled
gi1/0/6  RX,TX PD, SN, SD, SC       auto vlan 1   Disabled
gi1/0/7  RX,TX PD, SN, SD, SC       auto g1       Disabled
gi1/0/8   RX,TX PD, SN, SD, SC     auto ch1      Disabled
Switch# show lldp configuration gi1/0/1
State: Enabled
Timer: 30 Seconds
Hold multiplier: 4
Reinit delay: 2 Seconds
Tx delay: 2 Seconds
Notifications interval: 5 seconds
LLDP packets handling: Filtering

Port State    Optional TLVs     Address      Notifications
------------- -------------- ------------------------
gi1/0/1  RX, TX   PD, SN, SD, SC    72.16.1.1    Disabled

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

802.1 optional TLVs
PVID: Enabled
PPVIDs: 0, 1, 92
VLANs: 1, 92
Protocols: 802.1x
```

The following table describes the significant fields shown in the display:

Field	Description
Timer	The time interval between LLDP updates.
Hold multiplier	The amount of time (as a multiple of the timer interval) that the receiving device holds a Link Layer Discovery Protocol (LLDP) packet before discarding it.
Reinit timer	The minimum time interval an LLDP port waits before re-initializing an LLDP transmission.
Tx delay	The delay between successive LLDP frame transmissions initiated by value/status changes in the LLDP local systems MIB.
Port	The port number.
State	The port's LLDP state.
Optional TLVs	Optional TLVs that are advertised. Possible values are: PD - Port description SN - System name SD - System description SC - System capabilities
Address	The management address that is advertised.
Notifications	Indicates whether LLDP notifications are enabled or disabled.

show lldp med configuration

Use the **show lldp med configuration** Privileged EXEC mode command to display the Link Layer Discovery Protocol (LLDP) Media Endpoint Discovery (MED) configuration for all interfaces or for a specific interface.

Syntax

show lldp med configuration *[interface-id]*

Parameters

interface-id—Specifies an interface ID. The interface ID must be an Ethernet port.

Command Mode
Privileged EXEC mode

Example
The following examples display the LLDP MED configuration for all interfaces and for gigabitethernet port 1/0/1.

```
console# show lldp med configuration

Fast Start Repeat Count: 4.
Network policy 1
-------------------
Application type: voiceSignaling
VLAN ID: 1  untagged
Layer 2 priority: 0
DSCP: 0

Port   Capabilities Network    Location  Notifications  Inventory
                    policy
------ -----------  ---------- ---------- ------------  --------
gi1/0/1   Yes          Yes        Yes       Enabled        Yes
gi1/0/2   Yes          Yes        No        Enabled        No
gi1/0/3   No           No         No        Enabled        No

console# show lldp med configuration gigabitethernet 1/0/1


Port   Capabilities Network policy Location Notifications Inventory
------------------- -------------- -------- ----------    --------
gi1/0/1   Yes          Yes            Yes      Enabled       Yes

Network policies:
Location:
Civic-address: 61:62:63:64:65:66
```

show lldp local tlvs-overloading

Use the **show lldp local tlvs-overloading** EXEC mode command to display the status of TLVs overloading of the Link Layer Discovery Protocol (LLDP).

Syntax

show lldp local tlvs-overloading *[interface-id]*

Parameters

interface-id—Specifies an interface ID. The interface ID must be an Ethernet port.

Command Mode

EXEC mode

User Guidelines

The command calculates the overloading status of the current LLDP configuration, and not for the last LLDP packet that was sent.

Example

```
Switch# show lldp local tlvs-overloading
Ports with LLDP TLV overloading are: gi1/0/1, gi1/0/9
Switch# show lldp local tlvs-overloading
No LLDP TLV overloading.
Switch# show lldp local tlvs-overloading gi1/0/1
TLVs Group             Bytes       Status
------------           ------      --------------
Mandatory               31         Transmitted
LLDP-MED Capabilities   9          Transmitted
LLDP-MED Location       200        Transmitted
802.1 1360          Overloading

Total: 1600 bytes
Left: 100 bytes
```

show lldp local

Use the **show lldp local** Privileged EXEC mode command to display the Link Layer Discovery Protocol (LLDP) information that is advertised from a specific port.

Syntax

show lldp local *interface-id*

Parameters

Interface-id—Specifies an interface ID. The interface ID must be an Ethernet port.

Command Mode

Privileged EXEC mode

Example

The following examples display LLDP information that is advertised from gigabitethernet ports `1/0/`1 and `1/0/`2.

```
Switch# show lldp local gi1/0/1
Device ID: 0060.704C.73FF
Port ID: gi1/0/1
Capabilities: Bridge
System Name: ts-7800-1
System description:
Port description:
Management address: 172.16.1.8
802.3 MAC/PHY Configuration/Status
Auto-negotiation support: Supported
Auto-negotiation status: Enabled
Auto-negotiation Advertised Capabilities: 100BASE-TX full duplex,
1000BASE-T full duplex
Operational MAU type: 1000BaseTFD
802.3 Link Aggregation
Aggregation capability: Capable of being aggregated
Aggregation status: Not currently in aggregation
```

```
Aggregation port ID: 1
802.3 Maximum Frame Size: 1522

802.3 EEE
Local Tx: 30 usec
Local Rx: 25 usec
Remote Tx Echo: 30 usec
Remote Rx Echo: 25 usec


802.1 PVID: 1
802.1 PPVID: 2 supported, enabled
802.1 VLAN: 2 (VLAN2)
802.1 Protocol: 88 8E 01

LLDP-MED capabilities: Network Policy, Location Identification
LLDP-MED Device type: Network Connectivity
LLDP-MED Network policy
Application type: Voice
Flags: Tagged VLAN
VLAN ID: 2
Layer 2 priority: 0
DSCP: 0

LLDP-MED Power over Ethernet
Device Type: Power Sourcing Entity
Power source: Primary Power Source
Power priority: High
Power value: 9.6 Watts

LLDP-MED Location
Coordinates: 54:53:c1:f7:51:57:50:ba:5b:97:27:80:00:00:67:01


LLDP-MED Inventory
Hardware Revision: B1
Firmware Revision: A1
```

```
Software Revision: 3.8
Serial number: 7978399
Manufacturer name: Manufacturer
Model name: Model 1
Asset ID: Asset 123

Switch# show lldp local gi1/0/2

LLDP is disabled.
```

show lldp neighbors

Use the **show lldp neighbors** Privileged EXEC mode command to display information about neighboring devices discovered using Link Layer Discovery Protocol (LLDP). The information can be displayed for all interfaces or for a specific interface.

Syntax

show lldp neighbors *[interface-id]*

Parameters

interface-id—Specifies an interface ID. The interface ID must be an Ethernet port.

Command Mode

Privileged EXEC mode

User Guidelines

There are no guidelines for this command.

A TLV value that cannot be displayed as an ASCII string is displayed as an hexadecimal string.

Example

The following examples display information about neighboring devices discovered using LLDP.

Location information, if it exists, is also displayed.

```
Switch# show lldp neighbors

Port  Device ID            Port ID  System Name Capabilities TTL
----- ------------------   -------- ----------  -----------  ----
gi1/0/1 00:00:00:11:11:11    gi1/0/1    ts-7800-2   B            90
gi1/0/1 00:00:00:11:11:11 D  gi1/0/1    ts-7800-2   B            90
gi1/0/2 00:00:26:08:13:24    gi1/0/3    ts-7900-1   B, R         90
gi1/0/3 00:00:26:08:13:24    gi1/0/2    ts-7900-2   W            90

Switch# show lldp neighbors gi1/0/1

Device ID: 00:00:00:11:11:11
Port ID: gi1/0/
System Name: ts-7800-2
Capabilities: B
System description:
Port description:
Management address: 172.16.1.1
Time To Live: 90 seconds

802.3 MAC/PHY Configuration/Status
Auto-negotiation support: Supported.
Auto-negotiation status: Enabled.
Auto-negotiation Advertised Capabilities: 100BASE-TX full duplex,
1000BASE-T full duplex.
Operational MAU type: 1000BaseTFD

802.3 Power via MDI
MDI Power support Port Class: PD
PSE MDI Power Support: Not Supported
PSE MDI Power State: Not Enabled
PSE power pair control ability: Not supported.
PSE Power Pair: Signal
PSE Power class: 1

802.3 Link Aggregation
```

```
Aggregation capability: Capable of being aggregated
Aggregation status: Not currently in aggregation
Aggregation port ID: 1

802.3 Maximum Frame Size: 1522

802.3 EEE
Remote Tx: 25 usec
Remote Rx: 30 usec
Local Tx Echo: 30 usec
Local Rx Echo: 25 usec

802.1 PVID: 1
802.1 PPVID: 2 supported, enabled
802.1 VLAN: 2(VLAN2)
802.1 Protocol: 88 8E 01

LLDP-MED capabilities: Network Policy.
LLDP-MED Device type: Endpoint class 2.

LLDP-MED Network policy
Application type: Voice
Flags: Unknown policy
VLAN ID: 0
Layer 2 priority: 0
DSCP: 0

LLDP-MED Power over Ethernet
Device Type: Power Device
Power source: Primary power
Power priority: High
Power value: 9.6 Watts

LLDP-MED Inventory
Hardware revision: 2.1
Firmware revision: 2.3
```

```
Software revision: 2.7.1
Serial number: LM759846587
Manufacturer name: VP
Model name: TR12
Asset ID: 9

LLDP-MED Location
Coordinates: 54:53:c1:f7:51:57:50:ba:5b:97:27:80:00:00:67:01
```

The following table describes significant LLDP fields shown in the display:

Field	Description
Port	The port number.
Device ID	The neighbor device's configured ID (name) or MAC address.
Port ID	The neighbor device's port ID.
System name	The neighbor device's administratively assigned name.
Capabilities	The capabilities discovered on the neighbor device. Possible values are: B - Bridge R - Router W - WLAN Access Point T - Telephone D - DOCSIS cable device H - Host r - Repeater O - Other
System description	The neighbor device's system description.
Port description	The neighbor device's port description.
Management address	The neighbor device's management address.
Auto-negotiation support	The auto-negotiation support status on the port. (Supported or Not Supported)
Auto-negotiation status	The active status of auto-negotiation on the port. (Enabled or Disabled)

Auto-negotiation Advertised Capabilities	The port speed/duplex/flow-control capabilities advertised by the auto-negotiation.
Operational MAU type	The port MAU type.
LLDP MED	
Capabilities	The sender's LLDP-MED capabilities.
Device type	The device type. Indicates whether the sender is a Network Connectivity Device or Endpoint Device, and if an Endpoint, to which Endpoint Class it belongs.
LLDP MED - Network Policy	
Application type	The primary function of the application defined for this network policy.
Flags	Flags. The possible values are: Unknown policy: Policy is required by the device, but is currently unknown. Tagged VLAN: The specified application type is using a Tagged VLAN. Untagged VLAN: The specified application type is using an Untagged VLAN.
VLAN ID	The VLAN identifier for the application.
Layer 2 priority	The Layer 2 priority used for the specified application.
DSCP	The DSCP value used for the specified application.
LLDP MED - Power Over Ethernet	
Power type	The device power type. The possible values are: Power Sourcing Entity (PSE) or Power Device (PD).
Power Source	The power source utilized by a PSE or PD device. A PSE device advertises its power capability. The possible values are: Primary power source and Backup power source. A PD device advertises its power source. The possible values are: Primary power, Local power, Primary and Local power.
Power priority	The PD device priority. A PSE device advertises the power priority configured for the port. A PD device advertises the power priority configured for the device. The possible values are: Critical, High and Low.

Power value	The total power in watts required by a PD device from a PSE device, or the total power a PSE device is capable of sourcing over a maximum length cable based on its current configuration.
LLDP MED - Location	
Coordinates, Civic address, ECS ELIN.	The location information raw data.

show lldp statistics

Use the show **lldp statistics** EXEC mode command to display the Link Layer Discovery Protocol (LLDP) statistics.

Syntax

show lldp statistics *[interface-id]*

Parameters

interface-id—Specifies an interface ID. The interface ID must be an Ethernet port.

Command Mode

EXEC mode

Example

```
Switch# show lldp statistics
```

Contax(config-if)# do show lldp statistics

Tables Last Change Time: 14-Oct-2010 32:08:18

Tables Inserts: 26

Tables Deletes: 2

Tables Dropped: 0

Tables Ageouts: 1

	TX Frames	RX Frames			RX TLVs		RX Ageouts
Port	Total	Total	Discarded	Errors	Discarded	Unrecognized	Total
gi1/0/1	730	850	0	0	0	0	0
gi1/0/2	0	0	0	0	0	0	0
gi1/0/3	730	0	0	0	0	0	0
gi1/0/4	0	0	0	0	0	0	0
gi1/0/5	0	0	0	0	0	0	0
gi1/0/6	8	7	0	0	0	0	1
gi1/0//7	0	0	0	0	0	0	0
gi1/0/8	0	0	0	0	0	0	0
gi1/0/9	730	0	0	0	0	0	0
gi1/0/10	0	0	0	0	0	0	0

30

Spanning-Tree Commands

spanning-tree

Use the **spanning-tree** Global Configuration mode command to enable spanning-tree functionality. Use the **no** form of this command to disable the spanning-tree functionality.

Syntax

spanning-tree

no spanning-tree

Default Configuration

Spanning-tree is enabled.

Command Mode

Global Configuration mode

Example

The following example enables spanning-tree functionality.

```
Console(config)# spanning-tree
```

spanning-tree mode

Use the **spanning-tree mode** Global Configuration mode command to configure the spanning-tree protocol currently running. Use the **no** form of this command to restore the default configuration.

Syntax

spanning-tree mode *{stp | rstp | mst}*

no spanning-tree mode

Parameters

- **stp**—Specifies that the Spanning Tree Protocol (STP) is enabled.
- **rstp**—Specifies that the Rapid Spanning Tree Protocol (RSTP) is enabled.
- **mst**—Specifies that the Multiple Spanning Tree Protocol (MSTP) is enabled.

Default Configuration

The default is RSTP.

Command Mode

Global Configuration mode

User Guidelines

In RSTP mode, the device uses STP when the neighbor device uses STP.

In MSTP mode, the device uses RSTP when the neighbor device uses RSTP, and uses STP when the neighbor device uses STP.

Example

The following example configures the spanning-tree protocol as RSTP.

```
console(config)# spanning-tree mode mstp
```

spanning-tree forward-time

Use the **spanning-tree forward-time** Global Configuration mode command to configure the spanning-tree bridge forward time, which is the amount of time a port remains in the listening and learning states before entering the forwarding state. Use the **no** form of this command to restore the default configuration.

Syntax

spanning-tree forward-time *seconds*

no spanning-tree forward-time

Parameters

seconds—Specifies the spanning-tree forward time in seconds. (Range: 4–30)

Default Configuration

The default forwarding time for the IEEE Spanning Tree Protocol (STP) is 15 seconds.

Command Mode

Global Configuration mode

User Guidelines

When configuring the forwarding time, the following relationship should be maintained:

```
2*(Forward-Time - 1) >= Max-Age
```

Example

The following example configures the spanning tree bridge forwarding time to 25 seconds.

```
Console(config)# spanning-tree forward-time 25
```

spanning-tree hello-time

Use the **spanning-tree hello-time** Global Configuration mode command to configure the spanning tree bridge Hello time, which is how often the device broadcasts Hello messages to other devices. Use the **no** form of this command to restore the default configuration.

Syntax

spanning-tree hello-time *seconds*

no spanning-tree hello-time

Parameters

seconds—Specifies the spanning-tree Hello time in seconds. (Range: 1–10)

Default Configuration

The default Hello time for IEEE Spanning Tree Protocol (STP) is 2 seconds.

Command Mode

Global Configuration mode

User Guidelines

When configuring the Hello time, the following relationship should be maintained:

```
Max-Age >= 2*(Hello-Time + 1)
```

Example

The following example configures the spanning-tree bridge hello time to 5 seconds.

```
Console(config)# spanning-tree hello-time 5
```

spanning-tree max-age

Use the **spanning-tree max-age** Global Configuration mode command to configure the spanning-tree bridge maximum age. Use the **no** form of this command to restore the default configuration.

Syntax

spanning-tree max-age *seconds*

no spanning-tree max-age

Parameters

seconds—Specifies the spanning-tree bridge maximum age in seconds. (Range: 6–40)

Default Configuration
The default maximum age for IEEE Spanning Tree Protocol (STP) is 20 seconds.

Command Mode
Global Configuration mode

User Guidelines
When configuring the maximum age, the following relationships should be maintained:

2*(Forward-Time - 1) >= Max-Age

Max-Age >= 2*(Hello-Time + 1)

Example
The following example configures the spanning-tree bridge maximum age to 10 seconds.

```
Console(config)# spanning-tree max-age 10
```

spanning-tree priority
Use the **spanning-tree priority** Global Configuration mode command to configure the device spanning-tree priority, which is used to determine which bridge is selected as the root bridge. Use the **no** form of this command to restore the default device spanning-tree priority.

Syntax
spanning-tree priority *priority*

no spanning-tree priority

Parameters
priority—Specifies the bridge priority. (Range: 0–61440)

Default Configuration
The default bridge priority for IEEE Spanning Tree Protocol (STP) is 32768.

Command Mode
Global Configuration mode

User Guidelines
The priority value must be a multiple of 4096.

The switch with the lowest priority is the root of the spanning tree.

Example
The following example configures the spanning-tree priority to 12288.

```
Console(config)# spanning-tree priority 12288
```

spanning-tree disable

Use the **spanning-tree disable** Interface Configuration (Ethernet, port-channel) mode command to disable the spanning tree on a specific port. Use the **no** form of this command to enable the spanning tree on a port.

Syntax
spanning-tree disable

no spanning-tree disable

Default Configuration
Spanning tree is enabled on all ports.

Command Mode
Interface Configuration (Ethernet, port-channel) mode

Example
The following example disables the spanning tree on gigabitethernet port 1/0/5

```
Console(config)# interface gigabitethernet 1/0/5
Console(config-if)# spanning-tree disable
```

spanning-tree cost

Use the **spanning-tree cost** Interface Configuration (Ethernet, port-channel) mode command to configure the spanning-tree path cost for a port. Use the **no** form of this command to restore the default configuration.

Syntax

spanning-tree cost *cost*

no spanning-tree cost

Parameters

cost—Specifies the port path cost. (Range: 1–200000000)

Default Configuration

Default path cost is determined by port speed and path cost method (long or short) as shown below:

Interface	Long	Short
Port-channel	20,000	4
Gigabit Ethernet (1000 Mbps)	20,000	4
Fast Ethernet (100 Mbps)	200,000	19
Ethernet (10 Mbps)	2,000,000	100

Command Mode

Interface Configuration (Ethernet, port-channel) mode

Example

The following example configures the spanning-tree cost on gigabitethernet port `1/0/`15 to 35000.

```
Console(config)# interface gigabitethernet 1/0/15
Console(config-if)# spanning-tree cost 35000
```

spanning-tree port-priority

Use the **spanning-tree port-priority** Interface Configuration (Ethernet, port-channel) mode command to configure the port priority. Use the **no** form of this command to restore the default configuration.

Syntax

spanning-tree port-priority *priority*

no spanning-tree port-priority

Parameters

priority—Specifies the port priority. (Range: 0–240)

Default Configuration

The default port priority for IEEE Spanning Tree Protocol (STP) is 128.

Command Mode

Interface Configuration (Ethernet, port-channel) mode

User Guidelines

The priority value must be a multiple of 16.

Example

The following example configures the spanning priority on gigabitethernet port 1/0/15 to 96

```
Console(config)# interface gigabitethernet 1/0/15
Console(config-if)# spanning-tree port-priority 96
```

spanning-tree portfast

Use the **spanning-tree portfast** Interface Configuration (Ethernet, port-channel) mode command to enable the PortFast mode. In PortFast mode, the interface is immediately put into the forwarding state upon linkup, without waiting for the standard forward time delay. Use the **no** form of this command to disable the PortFast mode.

Syntax

spanning-tree portfast [**auto**]

no spanning-tree portfast

Parameters

auto—Specifies that the software waits for 3 seconds (with no BPDUs received on the interface) before putting the interface into the PortFast mode.

Default Configuration

PortFast mode is disabled.

Command Mode

Interface Configuration (Ethernet, port-channel) mode

Example

The following example enables the PortFast mode on gigabitethernet port 1/0/15.

```
Console(config)# interface gigabitethernet 1/0/15
Console(config-if)# spanning-tree portfast
```

spanning-tree link-type

Use the **spanning-tree link-type** Interface Configuration (Ethernet, port-channel) mode command to override the default link-type setting determined by the port duplex mode, and enable Rapid Spanning Tree Protocol (RSTP) transitions to the forwarding state. Use the **no** form of this command to restore the default configuration.

Syntax

spanning-tree link-type *{point-to-point | shared}*

no spanning-tree spanning-tree link-type

Parameters

- **point-to-point**—Specifies that the port link type is point-to-point.

- **shared**—Specifies that the port link type is shared.

Default Configuration
The device derives the port link type from the duplex mode. A full-duplex port is considered a point-to-point link and a half-duplex port is considered a shared link.

Command Mode
Interface Configuration (Ethernet, port-channel) mode

Example
The following example enables shared spanning-tree on gigabitethernet port 1/0/15.

```
Console(config)# interface gigabitethernet 1/0/15
Console(config-if)# spanning-tree link-type shared
```

spanning-tree pathcost method

Use the **spanning-tree pathcost method** Global Configuration mode command to set the default path cost method. Use the **no** form of this command to return to the default configuration.

Syntax
spanning-tree pathcost method *{long | short}*

no spanning-tree pathcost method

Parameters
- **long**—Specifies that the default port path costs are within the range: 1–200,000,000.
- **short**—Specifies that the default port path costs are within the range: 1–65,535.

Default Configuration
Short path cost method.

Command Mode
Global Configuration mode

User Guidelines
This command applies to all the spanning tree instances on the switch.

- If the short method is chosen, the switch use for the default cost values in the range 1 through 65,535.
- If the long method is chosen, the switch use for the default cost values in the range 1 through 200,000,000.

Example
The following example sets the default path cost method to Long.

```
Console(config)# spanning-tree pathcost method long
```

spanning-tree bpdu (Global)

Use the **spanning-tree bpdu** Global Configuration mode command to define BPDU handling when the spanning tree is disabled globally or on a single interface. Use the **no** form of this command to restore the default configuration.

Syntax
spanning-tree bpdu *{filtering | flooding}*

no spanning-tree bpdu

Parameters

- **filtering**—Specifies that BPDU packets are filtered when the spanning tree is disabled on an interface.
- **flooding**—Specifies that untagged BPDU packets are flooded unconditionally (without applying VLAN rules) to all ports with the spanning tree disabled and BPDU handling mode of flooding. Tagged BPDU packets are filtered.

Default Configuration
The default setting is **flooding**.

Command Mode
Global Configuration mode

User Guidelines
The **filtering** and **flooding** modes are relevant when the spanning tree is disabled globally or on a single interface.

Example
The following example defines the BPDU packet handling mode as **flooding** when the spanning tree is disabled on an interface**.**

```
Console(config)# spanning-tree bpdu flooding
```

spanning-tree bpdu (Interface)
Use the **spanning-tree bpdu** Interface Configuration (Ethernet, Port-channel) mode command to define BPDU handling when the spanning tree is disabled on a single interface. Use the **no** form of this command to restore the default configuration.

Syntax
spanning-tree bpdu *{filtering | flooding}*

no spanning-tree bpdu

Parameters
- **filtering**—Specifies that BPDU packets are filtered when the spanning tree is disabled on an interface.
- **flooding**—Specifies that untagged BPDU packets are flooded unconditionally (without applying VLAN rules) to ports with the spanning tree disabled and BPDU handling mode of flooding. Tagged BPDU packets are filtered.

Default Configuration
The **spanning-tree bpdu (Global)** command determines the default configuration.

Command Mode
Interface Configuration (Ethernet, Port-channel) mode

Example
The following example defines the BPDU packet as **flooding** when the spanning tree is disabled on gigabitethernet port `1/0/3`.

```
Console(config)# interface gigabitethernet 1/0/3
Console(config-if)# spanning-tree bpdu flooding
```

spanning-tree guard root

use the **spanning-tree guard root** Interface Configuration (Ethernet, Port-channel) mode command to enable root guard on all spanning-tree instances on the interface. Root guard prevents the interface from becoming the root port of the device. Use the **no** form of this command to disable the root guard on the interface.

Syntax
spanning-tree guard root

no spanning-tree guard root

Default Configuration
Root guard is disabled.

Command Mode
Interface Configuration (Ethernet, Port-channel) mode

User Guidelines
Root guard can be enabled when the device operates in STP, RSTP and MSTP modes.

When root guard is enabled, the port changes to the alternate state if the spanning-tree calculations select the port as the root port.

Example

The following example prevents gigabitethernet port `1/0/`1 from being the root port of the device..

```
Console(config)# interface gigabitethernet 1/0/1
Console(config-if)# spanning-tree guard root
```

spanning-tree bpduguard

Use the **spanning-tree bpduguard** Interface Configuration (Ethernet, port-channel) mode command to shut down an interface when it receives a bridge protocol data unit (BPDU). Use the **no** form of this command to restore the default configuration.

Syntax

spanning-tree bpduguard *{enable | disable}*

no spanning-tree bpduguard

Parameters

enable—Enables BPDU Guard.

disable—Disables BPDU Guard.

Default Configuration

BPDU Guard is disabled.

Command Mode

Interface Configuration (Ethernet, Port-channel) mode

User Guidelines

The command can be enabled when the spanning tree is enabled (useful when the port is in the PortFast mode) or disabled.

Example
The following example shuts down Ethernet port `1/0/5` when it receives a BPDU.

```
Console(config)# interface gigabitethernet 1/0/5
Console(config-if)# spanning-tree bpduguard enable
```

clear spanning-tree detected-protocols

Use the **clear spanning-tree detected-protocols** Privileged EXEC command to restart the protocol migration process (force the renegotiation with neighboring switches) on all interfaces or on the specified interface

Syntax
clear spanning-tree detected-protocols *[interface interface-id]*

Parameters
interface-id—Specifies an interface ID. The interface ID can be one of the following types: Ethernet port or Port-channel.

Command Mode
Privileged EXEC mode

User Guidelines
This feature should be used only when working in RSTP or MSTP mode.

Example

```
console# clear spanning-tree detected-protocols
```

spanning-tree mst priority

Use the **spanning-tree mst priority** Global Configuration mode command to configure the device priority for the specified spanning-tree instance. Use the **no** form of this command to restore the default configuration.

Syntax

spanning-tree mst *instance-id priority priority*

no spanning-tree mst *instance-id priority*

Parameters

- **instance-id**—Specifies the spanning-tree instance ID. (Range:1–15)
- **priority**—Specifies the device priority for the specified spanning-tree instance. This setting affects the likelihood that the switch is selected as the root switch. A lower value increases the probability that the switch is selected as the root switch. (Range: 0–61440)

Default Configuration

The default bridge priority for IEEE Spanning Tree Protocol (STP) is 32768.

Command Mode

Global Configuration mode

User Guidelines

The priority value must be a multiple of 4096.

The switch with the lowest priority is the root of the spanning tree.

Example

The following example configures the spanning tree priority of instance 1 to 4096.

```
Console(config)# spanning-tree mst 1 priority 4096
```

spanning-tree mst max-hops

Use the **spanning-tree mst max-hops** Global Configuration mode command to configure the number of hops in an MST region before the BDPU is discarded and the port information is aged out. Use the **no** form of this command to restore the default configuration.

Syntax

spanning-tree mst max-hops *hop-count*

no spanning-tree mst max-hops

Parameters
hop-count—Specifies the number of hops in an MST region before the BDPU is discarded. (Range: 1–40)

Default Configuration
The default number of hops is 20.

Command Mode
Global Configuration mode

Example
The following example configures the maximum number of hops that a packet travels in an MST region before it is discarded to 10.

```
Console(config)# spanning-tree mst max-hops 10
```

spanning-tree mst port-priority
Use the **spanning-tree mst port-priority** Interface Configuration (Ethernet, port-channel) mode command to configure the priority of a port. Use the **no** form of this command to restore the default configuration.

Syntax
spanning-tree mst *instance-id* **port-priority** *priority*

no spanning-tree mst *instance-id* **port-priority**

Parameters
- **instance-id**—Specifies the spanning tree instance ID. (Range: 1–15)
- **priority**—Specifies the port priority. (Range: 0–240 in multiples of 16)

Default Configuration
The default port priority for IEEE Spanning Tree Protocol (STP) is 128.

Command Mode
Interface Configuration (Ethernet, port-channel) mode

User Guidelines
The priority value must be a multiple of 16.

Example
The following example configures the port priority of port gi1/0/1 to 144.

```
Console(config)# interface gigabitethernet 1/0/1
Console(config-if)# spanning-tree mst 1 port-priority 144
```

spanning-tree mst cost
Use the **spanning-tree mst cost** Interface Configuration (Ethernet, Port-channel) mode command to configure the path cost for multiple spanning-tree (MST) calculations. If a loop occurs, the spanning tree considers path cost when selecting an interface to put in the forwarding state. Use the **no** form of this command to restore the default configuration.

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

no spanning-tree mst *instance-id* **cost**

Parameters
- **instance-id**—Specifies the spanning-tree instance ID. (Range: 1–15)
- **cost**—Specifies the port path cost. (Range: 1–200000000)

Default Configuration
Default path cost is determined by the port speed and path cost method (long or short) as shown below:

Interface	Long	Short
Port-channel	20,000	4
Gigabit Ethernet (1000 Mbps)	20,000	4

Fast Ethernet (100 Mbps)	200,000	19
Ethernet (10 Mbps)	2,000,000	100

Command Mode
Interface Configuration (Ethernet, port-channel) mode

Example
The following example configures the MSTP instance 1 path cost for gigabitethernet port `1/0/9` to 4.

```
Console(config)# interface gigabitethernet 1/0/9
Console(config-if)# spanning-tree mst 1 cost 4
```

spanning-tree mst configuration

Use the **spanning-tree mst configuration** Global Configuration mode command to enable configuring an MST region by entering the Multiple Spanning Tree (MST) mode.

Syntax
spanning-tree mst configuration

Command Mode
Global Configuration mode

User Guidelines
For two or more switches to be in the same MST region, they need to contain the same VLAN mapping, the same configuration revision number, and the same name.

Example
The following example configures an MST region.

```
Console(config)# spanning-tree mst configuration
Console(config-mst)# instance 1 vlan 10-20
Console(config-mst)# name region1
```

```
Console(config-mst)# revision 1
```

instance (MST)

Use **instance** MST Configuration mode command to map VLANs to an MST instance. Use the **no** form of this command to restore default mapping.

Syntax

instance *instance-id* ***vlan*** *vlan-range*

no instance *instance-id* ***vlan*** *vlan-range*

Parameters

- **instance-id**—MST instance (Range: 1–15)
- **vlan-range**—The specified range of VLANs is added to the existing ones. To specify a range, use a hyphen. To specify a series, use a comma. (Range: 1–4094)

Default Configuration

All VLANs are mapped to the common and internal spanning tree (CIST) instance (instance 0).

Command Mode

MST Configuration mode

User Guidelines

All VLANs that are not explicitly mapped to an MST instance are mapped to the common and internal spanning tree (CIST) instance (instance 0) and cannot be unmapped from the CIST.

For two or more devices to be in the same MST region, they must have the same VLAN mapping, the same configuration revision number, and the same name.

Example

The following example maps VLANs 10-20 to MST instance 1.

```
Console(config)# spanning-tree mst configuration
```

```
Console(config-mst)# instance 1 vlan 10-20
```

name (MST)

Use the **name** MST Configuration mode command to define the MST configuration name. Use the **no** form of this command to restore the default setting.

Syntax

name *string*

no name

Parameters

string—Specifies the MST configuration name. (Length: 1–32 characters)

Default Configuration

The default name is the bridge address.

Command Mode

MST Configuration mode

Example

The following example defines the configuration name as Region1.

```
Console(config)# spanning-tree mst configuration
Console(config-mst)# name region1
```

revision (MST)

Use the **revision** MST Configuration mode command to define the MST configuration revision number. Use the **no** form of this command to restore the default configuration.

Syntax

revision *value*

no revision

Parameters
value—Specifies the MST configuration revision number. (Range: 0–65535)

Default Configuration
The default configuration revision number is 0.

Command Mode
MST Configuration mode

Example
The following example sets the configuration revision to 1.

```
Console(config) # spanning-tree mst configuration
Console(config-mst) # revision 1
```

show (MST)

Use the **show** MST Configuration mode command to displays the current or pending MST region configuration.

Syntax
show *{current | pending}*

Parameters

- **current**—Displays the current MST region configuration.
- **pending**—Displays the pending MST region configuration.

Command Mode
MST Configuration mode

Example
The following example displays a pending MST region configuration.

```
Console(config-mst)# show pending

Pending MST configuration
Name: Region1
Revision: 1
Instance   Vlans Mapped    State
--------   ------------    -------
0          1-9,21-4094     Enabled
1          10-20           Enabled
```

exit (MST)

Use the **exit** MST Configuration mode command to exit the MST region Configuration mode and appy all configuration changes.

Syntax
exit

Command Mode
MST Configuration mode

Example
The following example exits the MST Configuration mode and saves changes.

```
Console(config)# spanning-tree mst configuration
Console(config-mst)# exit
Console(config)#
```

abort (MST)

Use the **abort** MST Configuration mode command to exit the MST Configuration mode without applying the configuration changes.

Syntax

abort

Command Mode

MST Configuration mode

Example

The following example exits the MST Configuration mode without saving changes.

```
Console(config)# spanning-tree mst configuration
Console(config-mst)# abort
```

show spanning-tree

Use the **show spanning-tree** Privileged EXEC mode command to display the spanning-tree configuration.

Syntax

show spanning-tree *[interface-id] [instance instance-id]*

show spanning-tree *[detail] [active | blockedports] [instance instance-id]*

show spanning-tree *mst-configuration*

Parameters

- **instance instance-id**—Specifies the spanning tree instance ID. (Range: 0–15)
- **detail**—Displays detailed information.
- **active**—Displays active ports only.
- **blockedports**—Displays blocked ports only.

- **mst-configuration**—Displays the MST configuration identifier.
- **interface-id**—Specifies an interface ID. The interface ID can be one of the following types: Ethernet port or Port-channel.

Command Mode
Privileged EXEC mode

Example
The following examples display spanning-tree information.

```
Console# show spanning-tree
Spanning tree enabled mode RSTP
Default port cost method: long
Loopback guard: Disabled

Root ID     Priority         32768
            Address          00:01:42:97:e0:00
            Path Cost        20000
            Root Port        gi1/0/1

            Hello Time 2 sec         Max Age 20 sec Forward Delay 15 sec


Bridge ID   Priority         36864
            Address          00:02:4b:29:7a:00

            Hello Time 2 sec         Max Age 20 sec Forward Delay 15 sec
```

```
Interfaces
Name       State    Prio.    Cost     Sts     Role    PortFast Type
---------  ------   Nbr      -----    ---     ----    -------------------
                    ------
gi1/0/1    Enabled  128.1    20000    FWD     Root    No       P2p (RSTP)
gi1/0/2    Enabled  128.2    20000    FWD     Desg    No       Shared (STP)
gi1/0/3    Disabled 128.3    20000    -       -       -        -
gi1/0/4    Enabled  128.4    20000    BLK     Altn    No       Shared (STP)
gi1/0/5    Enabled  128.5    20000    DIS     -       -        -


Console# show spanning-tree

Spanning tree enabled mode RSTP
Default port cost method: long


Root ID    Priority         36864
           Address          00:02:4b:29:7a:00

           This switch is the Root.

           Hello Time 2 sec         Max Age 20 sec Forward Delay 15 sec

Interfaces
```

```
Name       State    Prio.Nbr Cost    Sts    Role   PortFast Type
--------   -------- -------- ------  ---    ----   -------- --------------------
gi1/0/1    Enabled  128.1    20000   FWD    Desg   No       P2p (RSTP)
gi1/0/2    Enabled  128.2    20000   FWD    Desg   No       Shared (STP)
gi1/0/3    Disabled 128.3    20000   -      -      -        -
gi1/0/4    Enabled  128.4    20000   FWD    Desg   No       Shared (STP)
gi1/0/5    Enabled  128.5    20000   DIS    -      -        -


Console# show spanning-tree

Spanning tree disabled (BPDU filtering) mode RSTP
Default port cost method: long

Root ID    Priority         N/A
           Address          N/A
           Path Cost        N/A
           Root Port        N/A
           Hello Time       N/A      Max Age N/A    Forward Delay N/A


Bridge ID  Priority         36864
           Address          00:02:4b:29:7a:00
           Hello Time 2 sec         Max Age 20 sec Forward Delay 15 sec

Interfaces
```

```
Name       State    Prio.Nbr Cost    Sts    Role   PortFast Type
---------  ---------------  -----   ---    ----   -------------
gi1/0/1    Enabled  128.1   20000   -      -      -        -
gi1/0/2    Enabled  128.2   20000   -      -      -        -
gi1/0/3    Disabled 128.3   20000   -      -      -        -
gi1/0/4    Enabled  128.4   20000   -      -      -        -
gi1/0/5    Enabled  128.5   20000   -      -      -        -


Console# show spanning-tree active

Spanning tree enabled mode RSTP
Default port cost method: long


Root ID    Priority         32768
           Address          00:01:42:97:e0:00
           Path Cost        20000
           Root Port        gi1/0/1
           Hello Time 2 sec         Max Age 20 sec Forward Delay 15 sec


Bridge ID  Priority         36864
           Address          00:02:4b:29:7a:00
           Hello Time 2 sec         Max Age 20 sec Forward Delay 15 sec

Interfaces
```

```
Name       State    Prio.Nbr Cost    Sts    Role   PortFast Type
---------  -------- -------- ------  ---    ----   -------------------
gi1/0/1    -        -        20000   FWD    Root   No       P2p (RSTP)
gi1/0/2    Enabled  128.1    20000   FWD    Desg   No       Shared (STP)
gi1/0/4    Enabled  128.2    20000   BLK    Altn   No       Shared (STP)
           Enabled  128.4
```

```
Console# show spanning-tree blockedports

Spanning tree enabled mode RSTP
Default port cost method: long

Root ID    Priority         32768
           Address          00:01:42:97:e0:00
           Path Cost        20000
           Root Port        gi1/0/1
           Hello Time 2 sec         Max Age 20 sec Forward Delay 15 sec

Bridge ID  Priority         36864
           Address          00:02:4b:29:7a:00
           Hello Time 2 sec         Max Age 20 sec Forward Delay 15 sec

Interfaces
```

```
Name        State    Prio.Nbr Cost     Sts     Role    PortFast Type
---------   ---------------- -----    ---     ----    -------------------
gi1/0/4     -        -        19       BLK     Altn    No       Shared (STP)
            Enabled  128.4

Console# show spanning-tree detail

Spanning tree enabled mode RSTP
Default port cost method: long

Root ID     Priority         32768
            Address          00:01:42:97:e0:00
            Path Cost        20000
            Root Port        gi1/0/1

            Hello Time 2 sec         Max Age 20 sec Forward Delay 15 sec


Bridge ID   Priority         36864
            Address          00:02:4b:29:7a:00

            Hello Time 2 sec         Max Age 20 sec Forward Delay 15 sec


Number of topology changes 2 last change occurred 2d18h ago

Times:      hold 1, topology change 35, notification 2
            hello 2, max age 20, forward delay 15


Port 1 (gi1/0/1) enabled
State: Forwarding                    Role: Root
Port id: 128.1                       Port cost: 20000
Type: P2p (configured: auto) RSTP    Port Fast: No (configured:no)
Designated bridge Priority: 32768    Address: 00:01:42:97:e0:00
Designated port id: 128.25           Designated path cost: 0
Guard root: Disabled                 BPDU guard: Disabled

Number of transitions to forwarding state: 1
BPDU: sent 2, received 120638
```

```
Port 2 (gi1/0/2) enabled
State: Forwarding                    Role: Designated
Port id: 128.2                       Port cost: 20000
Type: Shared (configured: auto) STP  Port Fast: No (configured:no)
Designated bridge Priority: 32768    Address: 00:02:4b:29:7a:00
Designated port id: 128.2            Designated path cost: 20000
Guard root: Disabled                 BPDU guard: Disabled

Number of transitions to forwarding state: 1
BPDU: sent 2, received 170638


Port 3 (gi1/0/3) disabled
State: N/A                           Role: N/A
Port id: 128.3                       Port cost: 20000
Type: N/A (configured: auto)         Port Fast: N/A (configured:no)
Designated bridge Priority: N/A      Address: N/A
Designated port id: N/A              Designated path cost: N/A
Guard root: Disabled                 BPDU guard: Disabled

Number of transitions to forwarding state: N/A
BPDU: sent N/A, received N/A


Port 4 (gi1/0/4) enabled
State: Blocking                      Role: Alternate
Port id: 128.4                       Port cost: 20000
Type: Shared (configured:auto) STP   Port Fast: No (configured:no)
Designated bridge Priority: 28672    Address: 00:30:94:41:62:c8
Designated port id: 128.25           Designated path cost: 20000
Guard root: Disabled                 BPDU guard: Disabled

Number of transitions to forwarding state: 1
BPDU: sent 2, received 120638


Port 5 (gi1/0/5) enabled
State: Disabled                      Role: N/A
Port id: 128.5                       Port cost: 20000
Type: N/A (configured: auto)         Port Fast: N/A (configured:no)
Designated bridge Priority: N/A      Address: N/A
Designated port id: N/A              Designated path cost: N/A
Guard root: Disabled                 BPDU guard: Disabled
```

```
Number of transitions to forwarding state: N/A
BPDU: sent N/A, received N/A


Console# show spanning-tree ethernet gi1/0/1


Port 1 (gi1/0/1) enabled
State: Forwarding                    Role: Root
Port id: 128.1                       Port cost: 20000
Type: P2p (configured: auto) RSTP    Port Fast: No (configured:no)
Designated bridge Priority: 32768    Address: 00:01:42:97:e0:00
Designated port id: 128.25           Designated path cost: 0
Guard root: Disabled                 BPDU guard: Disabled

Number of transitions to forwarding state: 1
BPDU: sent 2, received 120638


Console# show spanning-tree mst-configuration

Name: Region1
Revision: 1

Instance            Vlans mapped     State
--------            ------------     ---------
0                   1-9, 21-4094     Enabled
1                   10-20            Enabled
```

```
Console# show spanning-tree

Spanning tree enabled mode MSTP
Default port cost method: long

###### MST 0 Vlans Mapped: 1-9

CST Root ID         Priority 32768
                    Address  00:01:42:97:e0:00
                    Path     20000
                    Cost      gi1/0/1
                    Root
                    Port

                    Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec


IST Master ID       Priority 32768
                    Address  00:02:4b:29:7a:00

                    This switch is the IST master.

                    Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

                    Max hops 20

Interfaces
Name        State    Prio.Nbr Cost     Sts     Role    PortFast Type
----        -------  -------- -----    ---     ----    -------- ---------------
gi1/0/1     Enabled  128.1    20000    FWD     Root    No       P2p Bound
gi1/0/2     Enabled  128.2    20000    FWD     Desg    No       (RSTP)
gi1/0/3     Enabled  128.3    20000    FWD     Desg    No       Shared Bound
gi1/0/4     Enabled  128.4    20000    FWD     Desg    No       (STP)
                                                               P2p
                                                               P2p
```

```
###### MST 1 Vlans Mapped: 10-20

Root ID             Priority 24576
                    Address  00:02:4b:29:89:76
                    Path     20000
                    Cost      gi1/0/4
                    Root     19
                    Port
                    Rem hops


Bridge ID           Priority 32768
                    Address  00:02:4b:29:7a:00


Interfaces

Name        State    Prio.Nbr Cost     Sts     Role    PortFast Type
----        -------  -------- -----    ---     ----    -------- ---------------
gi1/0/1     Enabled  128.1    20000    FWD     Boun    No       P2p Bound
gi1/0/2     Enabled  128.2    20000    FWD     Boun    No       (RSTP)
gi1/0/3     Enabled  128.3    20000    BLK     Altn    No       Shared Bound
gi1/0/4     Enabled  128.4    20000    FWD     Root    No       (STP)
                                                               P2p
                                                               P2p


Console# show spanning-tree detail

Spanning tree enabled mode MSTP
Default port cost method: long

###### MST 0 Vlans Mapped: 1-9

CST Root ID         Priority 32768
                    Address  00:01:42:97:e0:00
                    Path     20000
                    Cost      gi1/0/1
                    Root
                    Port

                    Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
```

```
IST Master ID      Priority 32768
                   Address  00:02:4b:29:7a:00

                   This switch is the IST master.

                   Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

                   Max hops 20
                   Number of topology changes 2 last change occurred 2d18h
                   ago
                   Times:  hold 1, topology change 35, notification 2
                   hello 2, max age 20, forward delay 15


Port 1 (gi1/0/1) enabled
State: Forwarding                          Role: Root
Port id: 128.1                             Port cost: 20000
Type: P2p (configured: auto) Boundary RSTP Port Fast: No (configured:no)
Designated bridge Priority: 32768          Address: 00:01:42:97:e0:00
Designated port id: 128.25                 Designated path cost: 0
Number of transitions to forwarding state: 1
BPDU: sent 2, received 120638


Port 2 (gi1/0/2) enabled
State: Forwarding                          Role: Designated
Port id: 128.2                             Port cost: 20000
Type: Shared (configured: auto) Boundary STPPort Fast: No (configured:no)
Designated bridge Priority: 32768          Address: 00:02:4b:29:7a:00
Designated port id: 128.2                  Designated path cost: 20000
Number of transitions to forwarding state: 1
BPDU: sent 2, received 170638
```

```
Port 3 (gi1/0/3) enabled
State: Forwarding                              Role: Designated
Port id: 128.3                                 Port cost: 20000
Type: Shared (configured: auto) Internal       Port Fast: No (configured:no)
Designated bridge Priority: 32768              Address: 00:02:4b:29:7a:00
Designated port id: 128.3                      Designated path cost: 20000
Number of transitions to forwarding state: 1
BPDU: sent 2, received 170638


Port 4 (gi1/0/4) enabled
State: Forwarding                              Role: Designated
Port id: 128.4                                 Port cost: 20000
Type: Shared (configured: auto) Internal       Port Fast: No (configured:no)
Designated bridge Priority: 32768              Address: 00:02:4b:29:7a:00
Designated port id: 128.2                      Designated path cost: 20000
Number of transitions to forwarding state: 1
BPDU: sent 2, received 170638


###### MST 1 Vlans Mapped: 10-20

Root ID             Priority 24576
                    Address  00:02:4b:29:89:76
                    Path Cost20000
                    Root Port gi1/0/4

                    Rem hops 19


Bridge ID           Priority 32768
                    Address  00:02:4b:29:7a:00

                    Number of topology changes 2 last change occurred 1d9h
                    ago

                    Times:  hold 1, topology change 2, notification 2
                    hello 2, max age 20, forward delay 15
```

```
Port 1 (gi1/0/1) enabled
State: Forwarding                          Role: Boundary
Port id: 128.1                             Port cost: 20000
Type: P2p (configured: auto) Boundary RSTP  Port Fast: No (configured:no)
Designated bridge Priority: 32768          Address: 00:02:4b:29:7a:00
Designated port id: 128.1                  Designated path cost: 20000
Number of transitions to forwarding state: 1
BPDU: sent 2, received 120638


Port 2 (gi1/0/2) enabled
State: Forwarding                          Role: Designated
Port id: 128.2                             Port cost: 20000
Type: Shared (configured: auto) Boundary STPPort Fast: No (configured:no)
Designated bridge Priority: 32768          Address: 00:02:4b:29:7a:00
Designated port id: 128.2                  Designated path cost: 20000
Number of transitions to forwarding state: 1
BPDU: sent 2, received 170638


Port 3 (gi1/0/3) disabled
State: Blocking                            Role: Alternate
Port id: 128.3                             Port cost: 20000
Type: Shared (configured: auto) Internal   Port Fast: No (configured:no)
Designated bridge Priority: 32768          Address: 00:02:4b:29:1a:19
Designated port id: 128.78                 Designated path cost: 20000
Number of transitions to forwarding state: 1
BPDU: sent 2, received 170638


Port 4 (gi1/0/4) enabled
State: Forwarding                          Role: Designated
Port id: 128.4                             Port cost: 20000
Type: Shared (configured: auto) Internal   Port Fast: No (configured:no)
Designated bridge Priority: 32768          Address: 00:02:4b:29:7a:00
Designated port id: 128.2                  Designated path cost: 20000
Number of transitions to forwarding state: 1
BPDU: sent 2, received 170638
```

```
Console# show spanning-tree

Spanning tree enabled mode MSTP
Default port cost method: long

###### MST 0 Vlans Mapped: 1-9

CST Root ID         Priority 32768
                    Address  00:01:42:97:e0:00
                    Path Cost20000
                    Root     gi1/0/1
                    Port

                    Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec


IST Master ID       Priority 32768
                    Address  00:02:4b:19:7a:00
                    Path Cost10000
                    Rem hops 19


Bridge ID           Priority 32768
                    Address  00:02:4b:29:7a:00

                    Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

                    Max hops 20


Console# show spanning-tree

Spanning tree enabled mode MSTP
Default port cost method: long

###### MST 0 Vlans Mapped: 1-9

CST Root ID         Priority 32768
                    Address  00:01:42:97:e0:00

                    This switch is root for CST and IST master.
```

```
Root      gi1/0/1
Port

Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Max hops 20
```

show spanning-tree bpdu

Use the **show spanning-tree bpdu** EXEC mode command to display the BPDU handling when spanning-tree is disabled.

Syntax

show spanning-tree bpdu *[interface-id]*

Parameters

interface-id—Specifies an interface ID. The interface ID can be one of the following types: Ethernet port or Port-channel.

Command Mode

EXEC mode

Example

The following examples display spanning-tree information.

```
Console# show spanning-tree bpdu



Global: Flooding

Interface          Admin Mode        Oper Mode
---------          ----------        ---------
gi1/0/1            Global            Flooding
gi1/0/2            Global            STP
gi1/0/3            Flooding          STP
```

31

VLAN Commands

vlan database

Use the **vlan database** Global Configuration mode command to enter the VLAN Configuration mode.

Syntax
vlan database

Command Mode
Global Configuration mode

Example
The following example enters the VLAN database mode.

```
Console(config)# vlan database
Console(config-vlan)#
```

vlan

Use the **vlan** VLAN Configuration mode command to create a VLAN. Use the **no** form of this command to restore the default configuration or delete a VLAN.

Syntax
vlan *vlan-range [name vlan-name]*

no vlan *vlan-range*

The device accepts also the following syntax:

vlan *vlan-range [name vlan-name] [media ethernet] [state active]*

no vlan *vlan-range*

Parameters

- **vlan-range**—Specifies a list of VLAN IDs to add. Separate nonconsecutive VLAN IDs with a comma and no spaces. Use a hyphen to designate a range of IDs.
- **name**—Specifies the VLAN name. The option is only valid in cass where only one VLAN is configured by the command (Range: 1–32 characters)

Command Mode
VLAN Configuration mode

Example
The following example creates VLAN number 1972.

```
Console(config)# vlan database
Console(config-vlan)# vlan 1972
```

interface vlan

Use the **interface vlan** Global Configuration mode command to enter the Interface Configuration (VLAN) mode and enable configuration of the specified VLAN ID.

Syntax
interface vlan *vlan-id*

Parameters
vlan-id—Specifies an existing VLAN ID.

Command Mode
Global Configuration mode

User Guidelines

If the VLAN does not exist (ghost VLAN), not all of the commands are available under the interface VLAN context.

The commands that are supported for VLANs that do not exist are:

- IGMP snooping control commands
- Bridge multicast configuration commands

Example

The following example configures VLAN 1 with IP address 131.108.1.27 and subnet mask 255.255.255.0.

```
Console (config)# interface vlan 1
Console (config-if)# ip address 131.108.1.27 255.255.255.0
```

interface range vlan

Use the **interface range vlan** Global Configuration mode command to enable configuring multiple VLANs simultaneously.

Syntax

interface range vlan *vlan-range*

Parameters

vlan-range—Specifies a list of VLAN IDs. Separate nonconsecutive VLAN IDs with a comma and no spaces. Use a hyphen to designate a range of IDs.

Command Mode

Global Configuration mode

User Guidelines

Commands under the interface range context are executed independently on each interface in the range. If the command returns an error on one of the interfaces, an error message is displayed and command execution continues on the other interfaces.

Example
The following example groups VLANs 221 through 228 and 889 to receive the same command.

```
Console(config)# interface range vlan 221-228, vlan 889
Console(config-if)#
```

name

Use the **name** Interface Configuration (VLAN) mode command to add a name to a VLAN. Use the **no** form of this command to remove the VLAN name.

Syntax
name *string*

no name

Parameters
string—Specifies a unique name associated with this VLAN. (Length: 1–32 characters)

Default Configuration
No name is defined.

Command Mode
Interface Configuration (VLAN) mode. It cannot be configured for a range of interfaces (range context).

User Guidelines
The VLAN name must be unique.

Example
The following example gives VLAN number 19 the name Marketing.

```
Console(config)# interface vlan 19
Console(config-if)# name Marketing
```

switchport protected-port

Use the **switchport protected-port** Interface Configuration mode command to isolate unicast, multicast, and broadcast traffic at Layer 2 from other protected ports on the same switch. Use the **no** form of this command to disable protection on the port.

Syntax

switchport protected-port

no switchport protected-port

Parameters

This command has no arguments or keywords.

Default Configuration

Unprotected

Command Mode

Interface configuration (Ethernet, port-channel)

User Guidelines

Use this command to isolate unicast, multicast, and broadcast traffic at Layer 2 from other protected ports (that are not associated with the same community as the ingress interface) on the same switch. Please note that the packet is still subject to FDB decision and to all filtering rules. Use the **switchport community** Interface Configuration command to associate the interface with a community.

Example

```
console(config)# interface gi1/0/1
console(config-if)# switchport protected-port
```

switchport community

Use the **switchport community** Interface Configuration mode command to associate a protected port with a community. Use the **no** form of this command to return to default.

Syntax

switchport community *community*

no switchport community

Parameters

community—Specifies the community number. (Range:1 - 30)

Default Configuration

The port is not associated with any community.

Command Mode

Interface Configuration (Ethernet, port-channel) mode

User Guidelines

The command is relevant only when the port is defined as a protected port. Use the **switchport protected-port** Interface Configuration command to define a port as a protected port.

Example

```
console(config)# interface gigabitethernet 1/0/1
console(config-if)# switchport community 1
```

show interfaces protected-ports

Use the **show interfaces protected-ports** EXEC mode command to show protected ports configuration.

Syntax

show interfaces protected-ports [*interface-id*]

Parameters

interface-id—Specifies an interface ID. The interface ID can be one of the following types: Ehernet port or Port-channel.

Command Mode

EXEC mode

Example

```
console# show interfaces protected-ports

Interface     State      Community
--------- -------------  ---------
  gi1/0/1     Protected       1
  gi1/0/2     Protected   Isolated
  gi1/0/3    Unprotected     20
  gi1/0/4    Unprotected  Isolated
```

Note: The Community column for unprotected ports is relevant only when the port state is changed to Protected.

switchport

Use the **switchport** Interface Configuration mode command with no keywords to put an interface that is in Layer 3 mode into Layer 2 mode for Layer 2 configuration. Use the **no** form of this command to put an interface in Layer 3 mode.

Syntax

switchport

no switchport

Default Configuration

Layer 2 mode

Command Mode
Interface Configuration (Ethernet, port-channel) mode

switchport mode

Use the **switchport mode** Interface Configuration (Ethernet, port-channel) mode command to configure the VLAN membership mode of a port. Use the **no** form of this command to restore the default configuration.

Syntax
switchport mode *{ access | trunk | general | private-vlan {promiscuous | host} | customer }*

no switchport mode

Parameters

- **access**—Specifies an untagged layer 2 VLAN port.
- **trunk**—Specifies a trunking layer 2 VLAN port.
- **general**—Specifies a full 802-1q supported VLAN port.
- **customer**—Specifies that the port is connected to customer equipment. Used when the switch is in a provider network.
- **private-vlan promiscous**—Private-VLAN promiscous port.
- **private-vlan host**—Private-VLAN host port.

Default Configuration

Command Mode
Interface Configuration (Ethernet, port-channel) mode

User Guidelines

- When the port mode is changed, it receives the configuration corresponding to the mode.
- If the port mode is changed to access and the access VLAN does not exist, then the port will not belongs to any VLAN.

Example

The following example configures gigabitethernet port `1/0/1` as an untagged layer 2 VLAN port.

```
Console(config)# interface gigabitethernet 1/0/1
Console(config-if)# switchport mode access
```

switchport access vlan

Use the **switchport access vlan** Interface Configuration (Ethernet, port-channel) mode command to configure the VLAN ID when the interface is in access mode. Use the **no** form of this command to restore the default configuration.

Syntax

switchport access vlan *{ vlan-id | none }*

no switchport access vlan

Parameters

vlan-id—Specifies the VLAN ID to which the port is configured.

none—Specifies the access port cannot belong to any VLAN.

Default Configuration

If the default VLAN is enabled, the VLAN ID is 1. Otherwise, it is not a member of any VLAN.

Command Mode

Interface Configuration (Ethernet, port-channel) mode

User Guidelines

The command automatically removes the port from the previous VLAN and adds it to the new VLAN.

Example
The following example configures a VLAN ID of 23 to the untagged layer 2 VLAN gigabitethernet port `1/0/1`.

```
Console(config)# interface gigabitethernet 1/0/1
Console(config-if)# switchport access vlan 23
```

switchport access multicast-tv vlan

Use the **switchport access multicast-tv vlan** Interface Configuration (Ethernet, Port-channel) mode command to enable receiving multicast transmissions from a VLAN that is not the Access port VLAN, while keeping the L2 segregation with subscribers on different Access port VLANs. Use the **no** form of this command to disable receiving multicast transmissions.

Syntax
switchport access multicast-tv vlan *vlan-id*

no switchport access multicast-tv vlan

Parameters
vlan-id—Specifies the Multicast TV VLAN ID.

Default Configuration
Receiving multicast transmissions is disabled.

Command Mode
Interface Configuration (Ethernet, Port-channel) mode

User Guidelines
The user cannot transmit multicast transmissions on the multicast TV VLAN.

A multicast TV VLAN cannot be enabled if a Guest VLAN is enabled on the interface.

Example

The following example enables gigabitethernet port 1/0/5 to receive multicast transmissions from VLAN 11.

```
Console(config)# interface gigabitethernet 1/0/5
Console(config-if)# switchport access multicast-tv vlan 11
```

switchport trunk allowed vlan

Use the **switchport trunk allowed vlan** Interface Configuration mode command to set the trunk characteristics when the interface is in trunking mode. Use the **no** form of this command to reset a trunking characteristic to the default.

Syntax

switchport trunk allowed vlan *{ all | none | add vlan-list | remove vlan-list | except vlan-list }*

no switchport trunk allowed vlan

Parameters

all—Specifies all VLANs from 1 to 4094. At any time, the port belongs to all VLANs exiting at the time. (Range: 1–4094)

none—Specifies an empty VLAN list The port does not belong to any VLAN.

add vlan-list—List of VLAN IDs to add. Separate nonconsecutive VLAN IDs with a comma and no spaces. Use a hyphen to designate a range of IDs.

remove vlan-list—List of VLAN IDs to remove. Separate nonconsecutive VLAN IDs with a comma and no spaces. Use a hyphen to designate a range of IDs.

except vlan-list—List of VLAN IDs is calculated by inverting the defined list of VLANs (the calculated list will include all VLANs from interval 1..4094 except VLANs from the defined list.

Default Configuration
The Default VLAN is its Native VLAN and the port belongs to either all VLANs or only to the Default VLAN depending on a value of parameter Trunk Port Default Configuration.

Command Mode
Interface Configuration (Ethernet, port-channel) mode

User Guidelines
The RS port model behavior allows only the following options: Add and Remove.

Inside **except vlan-list** is saved as **add ~ vlan-list**, where **~ vlan-list** is a list of all VLANs from 1 to 4094 minus the VLANs from **vlan-list**. Command **show running/startup** always uses the latter format.

The port must be in trunk mode before the command can take effect.

Example

```
console(config)# interface gigabitethernet 1/0/1
console(config-if)# switchport mode trunk
console(config-if)# switchport trunk allowed vlan all
```

switchport trunk native vlan
Use the **switchport trunk native vlan** Interface Configuration (Ethernet, port-channel) mode command to define the native VLAN when the interface is in trunk mode. Use the **no** form of this command to restore the default configuration.

Syntax
switchport trunk native vlan *{ vlan-id | none }*

no switchport trunk native vlan

Parameters
- **vlan-id**—Specifies the native VLAN ID.
- **none**—Specifies the access port cannot belong to any VLAN.

Default Configuration
If the default VLAN is enabled, the VLAN ID is 1. Otherwise, the VLAN ID is 4095.

Command Mode
Interface Configuration (Ethernet, port-channel) mode

User Guidelines
The command adds the port as a member of the VLAN. If the port is already a member of the VLAN (not a native), it must first be removed from the VLAN.

Example
The following example configures VLAN number 123 as the native VLAN when the port is in trunk mode.

```
Console# interface gi1/0/1
Console(config-if)# switchport trunk native vlan 123
```

switchport general allowed vlan
Use the **switchport general allowed vlan** Interface Configuration mode command to set the general characteristics when the interface is in general mode. Use the **no** form of this command to reset a general characteristic to the default.

Syntax
switchport general allowed vlan *{***add** */* **remove***}* *vlan-list [***tagged**|**untagged***]*

no switchport general allowed vlan

Parameters
- **add vlan-list**—List of VLAN IDs to add. Separate nonconsecutive VLAN IDs with a comma and no spaces. Use a hyphen to designate a range of IDs. (Range: 1–4094)

- **remove vlan-list**—List of VLAN IDs to remove. Separate nonconsecutive VLAN IDs with a comma and no spaces. Use a hyphen to designate a range of IDs.
- **tagged** - Specify that packets would be transmitted tagged for the configured VLANs
- **untagged** - Specify that packets would be transmitted untagged for the configured VLANs (this is the default)

Default Configuration
The port's PVID equals to the Default VLAN ID and belongs to the Default VLAN as untagged one.

Command Mode
Interface Configuration mode

Example

```
console(config-if)# interface gigabitethernet 1/0/1
console(config-if)# switchport mode general
console(config-if)# switchport general allowed vlan add 2-3 tagged
```

switchport general pvid

Use the **switchport general pvid** Interface Configuration (Ethernet, Port-channel) mode command to configure the Port VLAN ID (PVID) when the interface is in general mode. Use the **no** form of this command to restore the default configuration.

Syntax
switchport general pvid *vlan-id*

no switchport general pvid

Parameters
vlan-id—Specifies the Port VLAN ID (PVID).

Default Configuration
If the default VLAN is enabled, PVID is 1. Otherwise, PVID is =4095.

Command Mode
Interface Configuration (Ethernet, Port-channel) mode

Example
The following example configures PVID 234 for gigabitethernet port 1/0/2, when the interface is in general mode.

```
Console(config)# interface gigabitethernet 1/0/2
Console(config-if)# switchport mode general
Console(config-if)# switchport general pvid 234
```

switchport general ingress-filtering disable

Use the **switchport general ingress-filtering disable** Interface Configuration (Ethernet, Port-channel) mode command to disable port ingress filtering. Use the no form of this command to restore the default configuration.

Syntax
switchport general ingress-filtering disable

no switchport general ingress-filtering disable

Default Configuration
Ingress filtering is enabled.

Command Mode
Interface Configuration (Ethernet, port-channel) mode

Example
The following example disables port ingress filtering on gigabitethernet port 1/0/1.

```
Console(config)# interface gigabitethernet 1/0/1
Console(config-if)# switchport mode general
```

```
Console(config-if)# switchport general ingress-filtering disable
```

switchport general acceptable-frame-type

Use the **switchport general acceptable-frame-type** Interface Configuration mode command to configure ingress filtering based on packet type tagged/untagged. Use the **no** form of this command to return to default.

Syntax

switchport general acceptable-frame-type *{tagged-only | untagged-only | all}*

no switchport general acceptable-frame-type

Parameters

- **tagged-only**—Discard untagged packets and priority tagged packets.
- **untagged-only**—Discard VLAN tagged packets (not including Priority tagged packets)
- **all**—Do not discard packets based on whether the packet is VLAN tagged or not.

Default Configuration

All frame types are accepted at ingress.

Command Mode

Interface Configuration (Ethernet, port-channel) mode

Example

The following example configures gigabitethernet port `1/0/3` to discard untagged frames at ingress.

```
Console(config)# interface gigabitethernet 1/0/3
Console(config-if)# switchport mode general
Console(config-if)# switchport general acceptable-frame-type
tagged-only
```

switchport customer vlan

Use the **switchport customer vlan** Interface Configuration (Ethernet, Port-channel) mode command to set the port's VLAN when the interface is in customer mode. Use the no form of this command to restore the default configuration.

Syntax

switchport customer vlan *vlan-id*

no switchport customer vlan

Parameters

vlan-id—Specifies the customer VLAN ID.

Default Configuration

No VLAN is configured.

Command Mode

Interface Configuration (Ethernet, Port-channel) mode

Example

The following example defines gigabitethernet port 1/0/5 as a member of customer VLAN 5.

```
Console(config)# interface gigabitethernet 1/0/5
Console(config-if)# switchport mode custmer
Console(config-if)# switchport customer vlan isolated 5
```

switchport general forbidden vlan

Use the **switchport general forbidden vlan** Interface Configuration (Ethernet, Port-channel) mode command to forbid adding or removing specific VLANs to or from a port. Use the no form of this command to restore the default configuration.

Syntax

switchport general forbidden vlan *{add vlan-list | remove vlan-list}*

no switchport general forbidden vlan *{add vlan-list | remove vlan-list}*

Parameters

- **add vlan-list**—Specifies a list of VLAN IDs to add. Separate nonconsecutive VLAN IDs with a comma and no spaces. Use a hyphen to designate a range of IDs.
- **remove vlan-list**—Specifies a list of VLAN IDs to remove. Separate nonconsecutive VLAN IDs with a comma and no spaces. Use a hyphen designate a range of IDs.

Default Configuration

All VLANs are allowed.

Command Mode

Interface Configuration (Ethernet, Port-channel) mode

Example

The following example forbids adding VLAN IDs 234 to 256 to gigabitethernet port `1/0/7`.

```
Console(config)# interface gigabitethernet 1/0/7
Console(config-if)# switchport mode general
Console(config-if)# switchport general forbidden vlan add 234-
256
```

map protocol protocols-group

Use the **map protocol protocols-group** VLAN Configuration mode command to map a protocol to a group of protocols. Use the **no** form of this command to delete a protocol from a group.

Syntax

map protocol *protocol* [*encapsulation*] **protocols-group** *group*

no map protocol *protocol* [*encapsulation*]

Parameters

- **protocol**—Specifies a 16-bit protocol number or one of the reserved names listed in the User Guidelines. (Range: 0x0600–0xFFFF)
- **encapsulation**—Specifies one of the following values: Ethernet, rfc1042, llcOther. If no option is indicated, the default is Ethernet.
- **protocols-group group**—Specifies the group number of the group of protocols associated together. (Range: 1–2147483647)

Default Configuration

The default encapsulation is Ethernet.

Command Mode

VLAN Configuration mode

User Guidelines

The value 0x8100 is not valid as the protocol number for Ethernet encapsulation.

The following protocol names are reserved for Ethernet Encapsulation:

- ip
- arp
- ipv6
- ipx

Example

The following example maps protocol ip to protocol group number 213.

```
Console(config)# vlan database
Console(config-vlan)# map protocol ip protocols-group 213
```

switchport general map protocols-group vlan

Use the **switchport general map protocols-group vlan** Interface Configuration (Ethernet, Port-channel) mode command to set a protocol-based classification rule. Use the no form of this command to delete a classification.

Syntax

switchport general map protocols-group *group* **vlan** *vlan-id*

no switchport general map protocols-group *group*

Parameters

- **group**—Specifies the group number as defined in the **map protocol protocols-group** command. (Range: 1–65535)
- **vlan-id**—Defines the VLAN ID in the classifying rule.

Command Mode

Interface Configuration (Ethernet, port-channel) mode

Default Configuration

No classification is defined.

User Guidelines

The VLAN classification rule priorities are:

1. MAC-based VLAN (Best match among the rules)
2. Subnet-based VLAN (Best match among the rules)
3. Protocol-based VLAN
4. PVID

Example

The following example sets a protocol-based classification rule.

```
Console(config-if)# switchport general map protocols-group 1
vlan 8
```

private-vlan

Use the **private-vlan** Interface VLAN Configuration mode command to configure a private VLAN. Use the **no** form of this command to return the VLAN to normal VLAN configuration.

Syntax

private-vlan *{primary | isolated}*

no private-vlan

Parameters

- **Primary**—Designate the VLAN as Primary VLAN.
- **Isolated**—Designate the VLAN as Isolated VLAN.

Default Configuration

No private VLANs are configured.

Command Mode

Interface Configuration (VLAN) mode

User Guidelines

- The VLAN type cannot be changed if there is a private-VLAN port that is a member in the VLAN.
- The VLAN type cannot be changed if it is associated with other private VLANs.
- The VLAN type is not kept as a property of the VLAN when it is deleted.

private-vlan association

Use the **private-vlan association** Interface VLAN Configuration mode command to configure the association between the primary VLAN and the secondary VLANs.. Use the **no** form of this command to remove the association.

Syntax

private-vlan association *[add | remove] secondary-vlan-list*

no private-vlan association

Parameters

- **add**—Associates a secondary VLAN to a primary VLAN. This is the default action.

- **remove**—Clears the association between a secondary VLAN and a primary VLAN.
- **secondary-vlan-list**—Specifies one or more secondary VLANs to be associated with a primary VLAN in a private VLAN.

Default Configuration
No private VLANs are configured.

Command Mode
Interface Configuration (VLAN) mode

User Guidelines
- The command can only be executed in the context of the primary VLAN.
- Private VLAN cannot be removed or change its type if it is associated with other private VLANs.
- Primary VLAN can be associated with only single isolated VLAN.
- A secondary VLAN can be associated with only one primary VLAN.
- The association of secondary VLANs with a primary VLAN cannot be removed if there are private VLAN ports that are members in the secondary VLAN.
- In MSTP mode, all the VLANs that are associated with a private VLAN should be mapped to the same instance.

switchport private-vlan mapping

Use the **switchport private-vlan mapping** Interface Configuration mode command to configure the VLANs of the private-vlan promiscuous port. Use the **no** form of this command to reset to default.

Syntax
switchport private-vlan mapping *primary-vlan-id [add | remove] secondary-vlan-list*

no switchport private-vlan mapping

Parameters

- **primary-vlan-id**—The VLAN ID of the primary VLAN.
- **secondary-vlan-list**—Specifies one or more secondary VLANs.

Default Configuration
No VLAN is configured.

Command Mode
Interface Configuration (Ethernet, port-channel) mode

User Guidelines
The secondary VLANs should be associated with the primary VLANs, otherwise the configuration is not accepted. See the command **private-vlan** association.

switchport private-vlan host-association

Use the **switchport private-vlan host-association** Interface Configuration mode command to configure the VLANs of the private-vlan host port. Use the **no** form of this command to reset to default.

Syntax
switchport private-vlan host-association *primary-vlan-id secondary-vlan-id*

no switchport private-vlan host-association

Parameters

- **primary-vlan-id**—The VLAN ID of the primary VLAN.
- **secondary-vlan-list**—Specifies the secondary VLANs. The secondary VLAN is an isolated port.

Default Configuration
No VLAN is configured.

Command Mode
Interface Configuration (Ethernet, port-channel) mode

User Guidelines
The secondary VLAN should be associated with the primary VLANs, otherwise the configuration is not accepted. See the command **private-vlan association**.

show vlan private-vlan

Use the **show vlan private-vlan** EXEC mode command to show the private VLANs information.

Syntax
show vlan private-vlan *[tag vlan-id]*

Parameters
vlan-id—VLAN ID

Command Mode
EXEC mode

User Guidelines
The **show** command does not include non-private-vlan ports that are members in private VLANs.

Example
```
Console# show vlan private-vlan

  Primary    Secondary     Type             Ports
----------- ----------- ----------- ----------------------
    150                   primary          gi1/0/15
    150         151      isolated          gi1/0/15
```

ip internal-usage-vlan

Use the **ip internal-usage-vlan** Interface Configuration (Ethernet, Port-channel) mode command to reserve a VLAN as the internal usage VLAN of

an interface. Use the **no** form of this command to restore the default configuration.

Syntax

ip internal-usage-vlan *vlan-id*

no ip internal-usage-vlan

Parameters

vlan-id—Specifies the internal usage VLAN ID.

Command Mode

Interface Configuration (Ethernet, Port-channel) mode. It cannot be configured for a range of interfaces (range context).

User Guidelines

An internal usage VLAN is required when an IP interface is defined on an Ethernet port or Port-channel.

Use this command to define the internal usage VLAN of a port.

If an internal usage VLAN is not defined for a port, the software chooses one of the unused VLANs.

If a VLAN ID was chosen by the software for internal usage, but it is desired to use that VLAN ID for a static or dynamic VLAN, do one of the following:

- Remove the IP interface, create the VLAN, and recreate the IP interface.
- Use this command to explicitly define the internal usage VLAN.

Example

The following example reserves unused VLAN 200 as the internal usage VLAN of Ethernet port 1/3gigabitethernet port 1/0/3.

```
Console(config)# interface gigabitethernet 1/0/3
Console(config-if)# ip internal-usage-vlan 200
```

show vlan

Use the **show vlan** Privileged EXEC mode command to display VLAN information for all VLANs or for a specific VLAN.

Syntax

show vlan [*tag vlan-id* / *name vlan-name*]

Parameters

- **tag vlan-id**—Specifies a VLAN ID.
- **name vlan-name**—Specifies a VLAN name string. (Length: 1–32 characters)

Command Mode

Privileged EXEC mode

Example

The following example displays information for all VLANs.

```
Console# show vlan

VLAN    Name          Ports          Type        Authorization
----    ----------    --------       -------     -------------
1       default       gi1/0/1-2      Other       Required
10      VLAN0010      gi1/0/3-4      dynamic     Required
11      VLAN0011      gi1/0/1-2      static      Required
20      VLAN0020      gi1/0/3-4      static      Required
21      VLAN0021                     static      Required
30      VLAN0030                     static      Required
31      VLAN0031                     static      Required
91      VLAN0091      gi1/0/1-2      static      Not Required
3978    Guest VLAN    gi1/0/17       static      Guest
```

show vlan multicast-tv

Use the **show vlan multicast-tv** EXEC mode command to display information on the source ports and receiver ports of multicast-TV VLAN.

Syntax

show vlan multicast-tv vlan *vlan-id*

Parameters

vlan-id—Specifies the VLAN ID.

Command Mode

EXEC mode

Example

The following example displays information on the source and receiver ports of multicast-TV VLAN ID 1000.

```
Console # show vlan multicast-tv vlan 1000


Source ports  Receiver Ports
------------  ---------------------
gi1/0/8,      gi1/0/1-18, gi1/0/1-18, gi1/0/1-18
gi1/0/9
```

The following table describes the significant fields shown in the display:

Field	Description
Source ports	Ports that can transmit and receive traffic to and from the VLAN.
Receiver ports	Ports that can only receive traffic from the VLAN.

show vlan protocols-groups

Use the **show vlan protocols-groups** EXEC mode command to display protocols-groups information.

Syntax
show vlan protocols-groups

Command Mode
EXEC mode

Example
The following example displays protocols-groups information.

```
Console> show vlan protocols-groups

Protocol              Encapsulation         Group
------------          -------------         --------
0x800 (IP)            Ethernet              1
0x806 (ARP)           Ethernet              1
0x86dd (IPv6)         Ethernet              2
0x8898                Ethernet              3
```

show vlan internal usage

Use the **show vlan internal usage** Privileged EXEC mode command to display a list of VLANs used internally by the device.

Syntax
show vlan internal usage

Command Mode
Privileged EXEC mode

Example
The following example displays VLANs used internally by the device.

```
Console# show vlan internal usage

VLAN        Usage           IP address   Reserved
--------    --------        ----------   ----------
1007        Eth 1/21        Active       No
1008        Eth 1/22        Inactive     Yes
1009        Eth 1/23        Active       Yes
```

show interfaces switchport

Use the **show interfaces switchport** Privileged EXEC command to display the administrative and operational status of all interfaces or a specific interface.

Syntax
show interfaces switchport *[interface-id]*

Parameters
Interface-id—Specifies an interface ID. The interface ID can be one of the following types: Ehernet port or Port-channel.

Example

```
console# show interfaces switchport gi2/0/1
Gathering information...

Name: gi1/0/1
Switchport: enable
Administrative Mode: access
Operational Mode: down
Access Mode VLAN: 1
Access Multicast TV VLAN: none
```

```
Trunking Native Mode VLAN: 1
Trunking VLANs Enabled: 1
                        2-4094 (Inactive)
General PVID: 1
General VLANs Enabled: none
General Egress Tagged VLANs Enabled: none
General Forbidden VLANs: none
General Ingress Filtering: enabled
General Acceptable Frame Type: all
General GVRP status: disabled
General GVRP VLANs: none
Customer Mode VLAN: none
Private-vlan promiscuous-association primary VLAN: none
Private-vlan promiscuous-association Secondary VLANs Enabled: none
Private-vlan host-association primary VLAN: none
Private-vlan host-association Secondary VLAN Enabled: none
DVA: disable
Protected: Enabled, Uplink is gi1/0/1

Classification rules:

Classification type   Group ID   VLAN ID
-------------------   --------   -------
Protocol                   1        19
Protocol                   1        20
Protocol                   2        72
Subnet                     1        15
MAC                        6        11
```

32

IGMP Snooping Commands

ip igmp snooping (Global)

Use the **ip igmp snooping** Global Configuration mode command to enable Internet Group Management Protocol (IGMP) snooping. Use the **no** form of this command to disable IGMP snooping.

Syntax

ip igmp snooping

no ip igmp snooping

Default Configuration

IGMP snooping is disabled.

Command Mode

Global Configuration mode

Example

The following example enables IGMP snooping.

```
Console(config)# ip igmp snooping
```

ip igmp snooping vlan

Use the **ip igmp snooping vlan** Global Configuration mode command to enable Internet Group Management Protocol (IGMP) snooping on a specific VLAN. Use the **no** form of this command to disable IGMP snooping on a VLAN interface.

Syntax

ip igmp snooping vlan *vlan-id*

no ip igmp snooping vlan *vlan-id*

Parameters

vlan-id—Specifies the VLAN.

Default

Disabled

Command Mode

Global Configuration mode

User Guidelines

IGMP snooping can be enabled only on static VLANs.

IGMPv1, IGMPv2 and IGMPv3 are supported.

To activate IGMP snooping, the **bridge multicast filtering** should be enabled.

The User Guidelines of the bridge multicast mode Interface VLAN Configuration command describes the configuration that is written into the FDB as a function of the FDB mode and the IGMP version that is used in the network.

Example

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

ip igmp snooping mrouter

Use the **ip igmp snooping mrouter** Global Configuration mode command to enable automatic learning of multicast router ports. Use the **no** form of this command to remove the configuration.

Syntax

ip igmp snooping *vlan vlan-id* **mrouter** l*earn pim-dvmrp*

no ip igmp snooping *vlan vlan-id* **mrouter** *learn pim-dvmrp*

Parameters
vlan-id—Specifies the VLAN.

Default
Learning pim-dvmrp is enabled.

Command Mode
Global Configuration mode

User Guidelines
Multicast router ports are learned based on:

- Queries received on the port
- PIM/PIMv2 received on the port
- DVMRP received on the port
- MRDISC received on the port
- MOSPF received on the port

You can execute the command before the VLAN is created.

Example

```
console(config)# ip igmp snooping vlan 1 mrouter learn pim-dvmrp
```

ip igmp snooping mrouter interface

Use the **ip igmp snooping mrouter interface** Global Configuration mode command to define a port that is connected to a multicast router port. Use the **no** form of this command to remove the configuration.

Syntax
ip igmp snooping *vlan vlan-id* **mrouter interface** i*nterface-list*

no ip igmp snooping *vlan vlan-id* **mrouter interface** *interface-list*

Parameters

- **vlan-id**—Specifies the VLAN.

- **interface-list**—Specifies the list of interfaces. The interfaces can be one of the following types: Ethernet port or Port-channel.

Default
No ports defined

Command Mode
Global Configuration mode

User Guidelines
A port that is defined as a multicast router port receives all IGMP packets (reports and queries) as well as all multicast data.

You can execute the command before the VLAN is created.

Example

```
console(config)# ip igmp snooping vlan 1 mrouter interface gi1/0/1
```

ip igmp snooping forbidden mrouter interface

Use the **ip igmp snooping forbidden mrouter interface** Global Configuration mode command to forbid a port from being defined as a multicast router port by static configuration or by automatic learning. Use the **no** form of this command to remove the configuration.

Syntax
ip igmp snooping *vlan vlan-id* **forbidden mrouter interface** *interface-list*

no ip igmp snooping vlan vlan-id forbidden mrouter interface interface-list

Parameters

- **vlan-id**—Specifies the VLAN.
- **interface-list**—Specifies a list of interfaces. The interfaces can be from one of the following types: Ethernet port or Port-channel.

Default
No ports defined

Command Mode
Global Configuration mode

User Guidelines
A port that is a forbidden mrouter port cannot be a multicast router port (i.e. cannot be learned dynamically or assigned statically).

You can execute the command before the VLAN is created.

Example

```
console(config)# ip igmp snooping vlan 1 forbidden mrouter interface
gi1/0/1
```

ip igmp snooping static

Use the **ip igmp snooping static** Global Configuration mode command to register an IP-layer multicast address to the bridge table, and to add statically ports to the group. Use the **no** form of this command to remove ports specified as members of a static multicast group.

Syntax
ip igmp snooping *vlan vlan-id* **static** *ip-address [interface interface-list]*

no ip igmp snooping *vlan vlan-id* **static** *ip-address [interface interface-list]*

Parameter

- **vlan-id**—Specifies the VLAN.
- **ip-address**—Specifies the IP multicast address.
- **interface-list**—Specifies a list of interfaces. The interfaces can be from one of the following types: Ethernet port or Port-channel.

Default Configuration
No multicast addresses are defined.

Command Mode
Global Configuration mode

User Guidelines

Static multicast addresses can only be defined on static VLANs.

You can execute the command before the VLAN is created.

You can register an entry without specifying an interface.

Using the **no**. command without a port-list removes the entry.

Example

```
console(config)# ip igmp snooping vlan 1 static 239.2.2.2 gi1/0/
```

ip igmp snooping multicast-tv

Use the **ip igmp snooping multicast-tv** Global Configuration mode command to define the multicast ip-addresses that are associated with a multicast-tv VLAN. Use the **no** form of this command to remove all associations.

Syntax

ip igmp snooping *vlan vlan-id* **multicast-tv** *ip-multicast-address [count number]*

no ip igmp snooping *vlan vlan-id* **multicast-tv** *ip-multicast-address [count number]*

Parameters

- **vlan-id**—Specifies the VLAN
- **number**—Configures multiple contiguous multicast IP addresses. If not specified, the default is 1. (Range: 1–256)

Default

No multicast IP address is associated.

Command Mode

Global Configuration mode

User Guidelines
Use this command to define the multicast transmissions on a multicast-TV VLAN. The configuration is only relevant for an Access port that is a member in the configured VLAN as a multicast-TV VLAN.

If an IGMP message is received on such an Access port, it is associated with the multicast-TV VLAN only if it is for one of the multicast IP addresses that are associated with the multicast-TV VLAN.

Up to 256 VLANs can be configured.

ip igmp snooping querier

Use the **ip igmp snooping querier** Global Configuration mode command to enable the Internet Group Management Protocol (IGMP) querier on a specific VLAN. Use the **no** form of this command to disable the IGMP querier on a VLAN interface.

Syntax
ip igmp snooping *vlan vlan-id* **querier**

no ip igmp snooping *vlan vlan-id* **querier**

Parameters
vlan-id—Specifies the VLAN

Default
Disabled

Command Mode
Global Configuration mode

User Guidelines
The IGMP snooping querier can be enabled on a VLAN only if IGMP snooping is enabled for that VLAN.

No more then one switch can be configured as an IGMP Querier for a VLAN.

When the IGMP snooping querier is enabled, it starts after a host-time-out/2 with no IGMP traffic detected from a multicast router.

The IGMP Snooping Querier disables itself if it detects IGMP traffic from a multicast router. It restarts automatically after host-time-out/2.

Following are the IGMP snooping querier parameters as a function of the IGMP snooping parameters:

- QueryMaxResponseTime: host-time-out/10.
- QueryInterval: host-time-out/ 3.

Example

```
console(config)# ip igmp snooping vlan 1 querier
```

ip igmp snooping querier address

Use the **ip igmp snooping querier address** Global Configuration mode command to define the source IP address that the IGMP snooping querier would use. Use the **no** form of this command to return to default.

Syntax

ip igmp snooping *vlan vlan-id* **querier address** *ip-address*

no ip igmp snooping *vlan vlan-id* **querier address**

Parameters

- **vlan-id**—Specifies the VLAN.
- **ip-addres**—Source IP address.

Default

If an IP address is configured for the VLAN, it is used as the source address of the IGMP snooping querier.

Command Mode

Global Configuration mode

User Guidelines

If an IP address is not configured by this command, and no IP address is configured for the querier's VLAN, the querier is disabled.

Example

```
console(config)# ip igmp snooping vlan 1 querier address 1.2.3.4
```

ip igmp robustness

Use the **ip igmp robustness** Interface Configuration mode command to change a value of the IGMP robustness variable. Use the **no** format of the command to return to default.

Syntax

ip igmp robustness *count*

no ip igmp robustness

Parameters

count—The number of expected packet loss on a link. Parameter range. (Range: 1–7)

Default

2

Command Mode

Interface Configuration (VLAN) mode

User Guidelines

You can execute the command before the VLAN is created.

```
console(config)# interface vlan 1
console(config-if)# ip igmp robustness 3
```

ip igmp query-interval

Use the **ip igmp query-interval** Interface Configuration mode command to configure the Query interval. Use the **no** format of the command to return to default.

Syntax

ip igmp query-interval *seconds*

no ip igmp query-interval

Parameters

seconds—Frequency, in seconds, at which IGMP query messages are sent on the interface. (Range: 30–18000)

Default

125

Command Mode

Interface Configuration (VLAN) mode

User Guidelines

You can execute the command before the VLAN is created.

Example

ip igmp query-max-response-time

Use the **ip igmp query-max-response-time** Interface Configuration mode command to configure the Query Maximum Response time. Use the **no** format of the command to return to default.

Syntax

ip igmp query-max-response-time *seconds*

no ip igmp query-max-response-time

Parameters

seconds—Maximum response time, in seconds, advertised in IGMP queries. (Range: 5–20)

Default

10

Command Mode
Interface Configuration (VLAN) mode

User Guidelines
You can execute the command before the VLAN is created.

Example

ip igmp last-member-query-count

Use the **ip igmp last-member-query-count** Interface Configuration mode command to configure the Last Member Query Counter. Use the **no** format of the command to return to default.

Syntax
ip igmp last-member-query-count *count*

no ip igmp last-member-query-count

Parameter
count—The number of times that group- or group-source-specific queries are sent upon receipt of a message indicating a leave. (Range: 1–7)

Default
A value of Robustness variable

Command Mode
Interface Configuration (VLAN) mode

User Guidelines
You can execute the command before the VLAN is created.

Example

ip igmp last-member-query-interval

Use the **ip igmp last-member-query-interval** Interface Configuration mode command to configure the Last Member Query interval. Use the **no** format of the command to return to default.

Syntax

ip igmp last-member-query-interval *milliseconds*

no ip igmp last-member-query-interval

Parameters

milliseconds—Interval, in milliseconds, at which IGMP group-specific host query messages are sent on the interface. (Range: 100–25500)

Default

1000

Command Mode

Interface Configuration (VLAN) mode

User Guidelines

You can execute the command before the VLAN is created.

Example

ip igmp snooping vlan immediate-leave

Use the **ip igmp snooping vlan immediate-leave** Global Configuration mode command to enable the IGMP Snooping Immediate-Leave processing on a VLAN. Use the **no** format of the command to disable IGMP Snooping Immediate-Leave processing.

Syntax

ip igmp snooping vlan *vlan-id* **immediate-leave**

no ip igmp snooping vlan *vlan-id* **immediate-leave**

Parameters
vlan-id—Specifies the VLAN ID value. (Range: 1–4094)

Default
Disabled

Command Mode
Global Configuration mode

User Guidelines
You can execute the command before the VLAN is created.

Example

show ip igmp snooping mrouter

The **show ip igmp snooping mrouter** EXEC mode command displays information on dynamically learned multicast router interfaces for all VLANs or for a specific VLAN.

Syntax
show ip igmp snooping mrouter *[interface vlan-id]*

Parameters
interface vlan-id—Specifies the VLAN ID.

Command Mode
EXEC mode

Example
The following example displays information on dynamically learned multicast router interfaces for VLAN 1000.

```
Console# show ip igmp snooping mrouter interface 1000


VLAN        Static          Dynamic       Forbidden
----        ------          -------       ---------
1000        gi1/0/1         gi1/0/2       gi1/0/3-gi1/0/23
```

show ip igmp snooping interface

The **show ip igmp snooping interface** EXEC mode command displays the IGMP snooping configuration for a specific VLAN.

Syntax
show ip igmp snooping interface *vlan-id*

Parameters
vlan-id—Specifies the VLAN ID.

Command Mode
EXEC mode

Example
The following example displays the IGMP snooping configuration for VLAN 1000

```
Console # show ip igmp snooping interface 1000
IGMP Snooping is globally enabled
IGMP Snooping admin: Enabled
IGMP Snooping oper: Enabled
Routers IGMP version: 3
Groups that are in IGMP version 2 compatibility mode:
231.2.2.3, 231.2.2.3
Groups that are in IGMP version 1 compatibility mode:
```

```
IGMP snooping querier admin: Enabled
IGMP snooping querier oper: Enabled
IGMP snooping querier address admin:
IGMP snooping querier address oper: 172.16.1.1
IGMP snooping querier version admin: 3

IGMP snooping robustness: admin 2  oper 2
IGMP snooping query interval: admin 125 sec oper 125 sec
IGMP snooping query maximum response: admin 10 sec oper 10
sec
IGMP snooping last member query counter: admin 2 oper 2
IGMP snooping last member query interval: admin 1000 msec
oper 500 msec
IGMP snooping last immediate leave: enable

Automatic learning of multicast router ports is enabled
```

show ip igmp snooping groups

The **show ip igmp snooping groups** EXEC mode command displays the multicast groups learned by the IGMP snooping.

Syntax

show ip igmp snooping groups *[vlan vlan-id] [address ip-multicast-address] [source ip-address]*

Parameters

vlan vlan-id—Specifies the VLAN ID.

address ip-multicast-address—Specifies the IP multicast address.

source ip-address—Specifies the IP source address.

Command Mode

EXEC mode

User Guidelines

To see the full multicast address table (including static addresses), use the **show bridge multicast address-table** command.

The Include list contains the ports which are in forwarding state for this group according to the snooping database. In general, the Exclude list contains the ports that have issued an explicit Exclude for that specific source in a multicast group. The Reporters That Are Forbidden Statically list contains the list of ports which have asked to receive a multicast flow but were defined as forbidden for that multicast group in multicast bridge.

Note: under certain circumstances, the Exclude list may not contain accurate information.For example, in the case when two Exclude reports were received on the same port for the same group but for different sources, the port will not be in the Exclude list but rather in the Include' list.

Example

The following example shows the output for IGMP version 2.

```
Console# show ip igmp snooping groups

Vlan     IP              Querier         Ports
         Address                         --------
----     ---------       ---------
1        231.2.2.2       Yes             gi1/0/1
1        231.2.2.3       No              gi1/0/2
19       231.2.2.4       Yes             gi1/0/9
```

show ip igmp snooping multicast-tv

The **show ip igmp snooping multicast-tv** EXEC mode command displays the IP addresses associated with Multicast TV VLANs.

Syntax

show ip igmp snooping multicast-tv *[vlan vlan-id]*

Parameters

vlan vlan-id—Specifies the VLAN ID.

Command Mode
EXEC mode

Example
The following example displays the IP addresses associated with all Multicast TV VLANs.

```
Console# show ip igmp snooping multicast-tv
VLAN IP Address
---- -----------
1000 239.255.0.0
1000 239.255.0.1
1000 239.255.0.2
1000 239.255.0.3
1000 239.255.0.4
1000 239.255.0.5
1000 239.255.0.6
1000 239.255.0.7
```

33

LACP Commands

lacp system-priority

Use the **lacp system-priority** Global Configuration mode command to set the system priority. Use the **no** form of this command to restore the default configuration.

Syntax

lacp system-priority *value*

no lacp system-priority

Parameters

value—Specifies the system priority value. (Range: 1–65535)

Default Configuration

The default system priority is 1.

Command Mode

Global Configuration mode

Example

The following example sets the system priority to 120.

```
Console(config)# lacp system-priority 120
```

lacp port-priority

Use the **lacp port-priority** Interface Configuration (Ethernet) mode command to set the physical port priority. Use the **no** form of this command to restore the default configuration.

Syntax

lacp port-priority *value*

no lacp port-priority

Parameters

value—Specifies the port priority. (Range: 1use the **no** form of this command65535)

Default Configuration

The default port priority is 1.

Command Mode

Interface Configuration (Ethernet) mode

Example

The following example sets the priority of gigabitethernet port 1/0/6.

```
console(config)# interface gi1/0/6
console(config-if)# lacp port-priority 247
```

lacp timeout

Use the **lacp timeout** Interface Configuration (Ethernet) mode command to assign an administrative LACP timeout to an interface. Use the **no** form of this command to restore the default configuration.

Syntax

lacp timeout *{long | short}*

no lacp timeout

Parameters

- **long**—Specifies the long timeout value.
- **short**—Specifies the short timeout value.

Default Configuration
The default port timeout value is Long.

Command Mode
Interface Configuration (Ethernet) mode

Example
The following example assigns a long administrative LACP timeout to gigabitethernet port 1/0/6.

```
Console(config)# interface gigabitethernet 1/0/6
Console(config-if)# lacp timeout long
```

show lacp

Use the **show lacp** EXEC mode command to display LACP information for all Ethernet ports or for a specific Ethernet port.

Syntax
show lacp *interface-id* [*parameters* | *statistics* | *protocol-state*]

Parameters

- **parameters**—Displays parameters only.
- **statistics**—Displays statistics only.
- **protocol-state**—Displays protocol state only.

Command Mode
EXEC mode

Example

The following example displays LACP information for gigabitethernet port 1/0/1.

```
Console> show lacp ethernet gi1/0/1

Port gi1/0/1 LACP parameters:
      Actor
             system priority:            1
             system mac addr:            00:00:12:34:56:78
             port Admin key:             30
             port Oper key:              30
             port Oper number:           21
             port Admin priority:        1
             port Oper priority:         1
             port Admin timeout:         LONG
             port Oper timeout:          LONG
             LACP Activity:              ACTIVE
             Aggregation:                AGGREGATABLE
             synchronization:            FALSE
             collecting:                 FALSE
             distributing:               FALSE
             expired:                    FALSE
      Partner
```

```
                system priority:            0
                system mac addr:            00:00:00:00:00:00
                port Admin key:             0
                port Oper key:              0
                port Oper number:           0
                port Admin priority:        0
                port Oper priority:         0
                port Admin timeout:         LONG
                port Oper timeout:          LONG
                LACP Activity:              PASSIVE
                Aggregation:                AGGREGATABLE
                synchronization:            FALSE
                collecting:                 FALSE
                distributing:               FALSE
                expired:                    FALSE


Port gi1/0/1 LACP Statistics:
LACP PDUs sent:                             2
LACP PDUs received:                         2


Port gi1/0/1 LACP Protocol State:
      LACP State Machines:

              Receive FSM:                  Port Disabled State
              Mux FSM:                      Detached State

      Control Variables:

              BEGIN:                        FALSE
              LACP_Enabled:                 TRUE
              Ready_N:                      FALSE
              Selected:                     UNSELECTED
              Port_moved:                   FALSE
              NNT:                          FALSE
              Port_enabled:                 FALSE

      Timer counters:

              periodic tx timer:            0
              current while timer:          0
              wait while timer:             0
```

show lacp port-channel

Use the **show lacp port-channel** EXEC mode command to display LACP information for a port-channel.

Syntax

show lacp port-channel *[port_channel_number]*

Parameters

port_channel_number—Specifies the port-channel number.

Command Mode

EXEC mode

Example

The following example displays LACP information about port-channel 1.

```
Console> show lacp port-channel 1

Port-Channel 1:Port Type 1000 Ethernet
      Actor
                System Priority:      1
                MAC Address:          000285:0E1C00
                Admin Key:            29
                Oper Key:             29

      Partner
                System Priority:      0
                MAC Address:          00:00:00:00:00:00
                Oper Key:             14
```

34

GVRP Commands

gvrp enable (Global)

Use the **gvrp enable** Global Configuration mode command to enable the Generic Attribute Registration Protocol (GARP) VLAN Registration Protocol (GVRP) globally. Use the **no** form of this command to disable GVRP on the device.

Syntax

gvrp enable

no gvrp enable

Default Configuration

GVRP is globally disabled.

Command Mode

Global Configuration mode

Example

The following example enables GVRP globally on the device.

```
Console(config)# gvrp enable
```

gvrp enable (Interface)

Use the **gvrp enable** Interface Configuration (Ethernet, Port-channel) mode command to enable GVRP on an interface. Use the **no** form of this command to disable GVRP on an interface.

Syntax

gvrp enable

no gvrp enable

Default Configuration

GVRP is disabled on all interfaces.

Command Mode

Interface Configuration (Ethernet, Port-channel) mode

User Guidelines

An access port does not dynamically join a VLAN because it is always a member of one VLAN only. Membership in an untagged VLAN is propagated in the same way as in a tagged VLAN. That is, the PVID must be manually defined as the untagged VLAN VID.

Example

The following example enables GVRP on gigabitethernet port 1/0/6.

```
Console(config)# interface gigabitethernet 1/0/6
Console(config-if)# gvrp enable
```

garp timer

Use the **garp timer** Interface Configuration (Ethernet, port channel) mode command to adjust the values of the join, leave and leaveall timers of GARP applications, such as GVRP. Use the **no** form of this command to restore the default configuration.

Syntax

garp timer *{join | leave | leaveall} timer-value*

no garp timer

Parameters

- **join | leave | leaveall**—Specifies the type of timer for which the timer value is specified. The possible values are:

- **join**—Specifies the GARP join timer. The GARP join timer value specifies the time interval between the two join messages sent by the GARP application.
- **leave**—Specifies the GARP leave timer. The GARP leave timer value specifies the time interval for a GARP application to wait for a join message after receiving a leave message for a GARP attribute, before it de-registers the GARP attribute.
- **leaveall**—Specifies the GARP leaveall timer. The GARP leaveall timer value specifies the time interval between leaveall messages for a GARP entity, which prompt other GARP entities to re-reregister all attribute information on this entity.

- **timer-value**—Specifies the timer value in milliseconds in multiples of 10. (Range: 10–2147483640)

Default Configuration

The following are the default timer values:

- **Join timer**—200 milliseconds
- **Leave timer**—600 milliseconds
- **Leaveall timer**—10000 milliseconds

Command Mode

Interface Configuration (Ethernet, Port-channel) mode

User Guidelines

The **timer-value** value must be a multiple of 10.

The following relationship must be maintained between the timers:

- The leave time must be greater than or equal to three times the join time.
- The leave-all time must be greater than the leave time.

Set the same GARP timer values on all Layer 2-connected devices to ensure proper operation of the GARP application.

Example
The following example sets the leave timer for gigabitethernet port 1/0/6 to 900 milliseconds.

```
Console(config)# interface gigabitethernet 1/0/6
Console(config-if)# garp timer leave 900
```

gvrp vlan-creation-forbid

Use the **gvrp vlan-creation-forbid** Interface Configuration (Ethernet, Port-channel) mode command to disable dynamic VLAN creation or modification. Use the **no** form of this command to enable dynamic VLAN creation or modification.

Syntax
gvrp vlan-creation-forbid

no gvrp vlan-creation-forbid

Default Configuration
Dynamic VLAN creation or modification is enabled.

Command Mode
Interface Configuration (Ethernet, Port-channel) mode

Example
The following example disables dynamic VLAN creation on gigabitethernet port 1/0/3.

```
Console(config)# interface gigabitethernet 1/0/3
Console(config-if)# gvrp vlan-creation-forbid
```

gvrp registration-forbid

Use the **gvrp registration-forbid** Interface Configuration (Ethernet, Port-channel) mode command to deregister all dynamic VLANs on a port and

prevent VLAN creation or registration on the port. Use the **no** form of this command to allow dynamic registration of VLANs on a port.

Syntax

gvrp registration-forbid

no gvrp registration-forbid

Default Configuration

Dynamic registration of VLANs on the port is allowed.

Command Mode

Interface Configuration (Ethernet, Port-channel) mode

Example

The following example forbids dynamic registration of VLANs on gigabitethernet port 1/0/2.

```
Console(config)# interface gigabitethernet 1/0/2
Console(config-if)# gvrp registration-forbid
```

clear gvrp statistics

Use the **clear gvrp statistics** Privileged EXEC mode command to clear GVRP statistical information for all interfaces or for a specific interface.

Syntax

clear gvrp statistics *[interface-id]*

Parameters

Interface-id—Specifies an interface ID. The interface ID can be one of the following types: Ethernet port or Port-channel.

Command Mode

Privileged EXEC mode

Example
The following example clears all GVRP statistical information on gigabitethernet port 1/0/5.

```
Console# clear gvrp statistics ethernet 1/5
```

show gvrp configuration

Use the **show gvrp configuration** EXEC mode command to display GVRP configuration information, including timer values, whether GVRP and dynamic VLAN creation are enabled, and which ports are running GVRP.

Syntax
show gvrp configuration *[interface-id]*

Parameters
interface-id—Specifies an interface ID. The interface ID can be one of the following types: Ethernet port or Port-channel.

Command Mode
EXEC mode

Example
The following example displays GVRP configuration information.

```
console# show gvrp configuration

GVRP Feature is currently Enabled on the device.
Maximum VLANs: 4094

Port(s) GVRP-Status Regist-  Dynamic   Timers(ms)
                    ration   VLAN                    Leave
                             Creation  Join     Leave All
------- ----------- -------- ---------  ----    ----- ----
gi1/0/1   Enabled     Forbidden Disabled  200     600    10000
gi1/0/2   Enabled     Normal    Enabled   400     1200   20000
```

show gvrp statistics

Use the **show gvrp statistics** EXEC mode command to display GVRP statistics for all interfaces or for a specific interface.

Syntax

show gvrp statistics *[interface-id]*

Parameters

interface-id—Specifies an interface ID. The interface ID can be one of the following types: Ethernet port or Port-channel.

Command Mode

EXEC mode

Example

The following example displays GVRP statistical information.

```
Console# show gvrp statistics

GVRP statistics:
---------------
Legend:
rJE : Join Empty         rJIn: Join In Received
rEmp: Received           rLIn: Leave In Received
rLE : Empty Received     rLA : Leave All Received
sJE : Leave Empty        sJIn: Join In Sent
sEmp: Received           sLIn: Leave In Sent
sLE : Join Empty Sent    sLA : Leave All Sent
      Empty Sent
      Leave Empty Sent
```

```
Port   rJE  rJIn rEmp rLIn rLE  rLA   sJE  sJIn sEmp sLIn sLE  sLA
-----  ---- ---- ---- ---- ---- ----  ---- ---- ---- ---- ---- ---
1/1    0    0    0    0    0    0     0    0    0    0    0    0
1/2    0    0    0    0    0    0     0    0    0    0    0    0
1/3    0    0    0    0    0    0     0    0    0    0    0    0
1/4    0    0    0    0    0    0     0    0    0    0    0    0
1/5    0    0    0    0    0    0     0    0    0    0    0    0
1/6    0    0    0    0    0    0     0    0    0    0    0    0
1/7    0    0    0    0    0    0     0    0    0    0    0    0
1/8    0    0    0    0    0    0     0    0    0    0    0    0
```

show gvrp error-statistics

Use the **show gvrp error-statistics** EXEC mode command to display GVRP error statistics for all interfaces or for a specific interface.

Syntax

show gvrp error-statistics *[interface-id]*

Parameters

interface-id—Specifies an interface ID. The interface ID can be one of the following types: Ethernet port or Port-channel.

Command Mode

EXEC mode

Example

The following example displays GVRP error statistics.

```
console# show gvrp error-statistics

GVRP Error Statistics:
----------------------
Legend:
  INVPROT  : Invalid Protocol Id
  INVATYP  : Invalid Attribute Type  INVALEN : Invalid Attribute Length
  INVAVAL  : Invalid Attribute Value INVEVENT: Invalid Event
```

Port	INVPROT	INVATYP	INVAVAL	INVALEN	INVEVENT
gi1/0/1	0	0	0	0	0
gi1/0/2	0	0	0	0	0
gi1/0/3	0	0	0	0	0
gi1/0/4	0	0	0	0	0
gi1/0/5	0	0	0	0	0
gi1/0/6	0	0	0	0	0
gi1/0/0/7	0	0	0	0	0
gi1/0/0/8	0	0	0	0	0

35

Voice VLAN Commands

The **voice vlan id** Global Configuration mode command specified the Voice VLAN Identified. The **no** format of the command returns the value to default.

Syntax
voice vlan id *vlan-id*

no voice vlan id

Parameters
vlan-id—Specifies the voice VLAN ID.

Parameters Range
vlan-id—1-4094.

Default Configuration
Default VLAN's Identifier.

Command Mode
Global Configuration mode

User Guidelines
If the Voice VLAN does not exist it is created automatically. It will not removed automatically.

Example
The following example enables VLAN 35 as the voice VLAN on the device.

```
Console(config)# voice vlan id 35
```

voice vlan oui-table

Use the **voice vlan oui-table** Global Configuration mode command to configure the voice OUI table. Use the **no** form of this command to restore the default configuration.

Syntax

voice vlan oui-table *{**add** mac-address-prefix | **remove** mac-address-prefix}* [*text*]

no voice vlan oui-table

Parameters

- **add** *mac-address-prefix*—Adds the specified MAC address to the voice VLAN OUI table. (Length: 3 bytes)
- *text*—Adds the specified text as a description of the specified MAC address to the voice VLAN OUI table. (Length: 1–32 characters)
- **remove** *mac-address-prefix*—Removes the specified MAC address from the voice VLAN OUI table. (Length: 3 bytes)

Default Configuration

The default voice VLAN OUI table is:

OUI	Description
00:e0:bb	3COM Phone
00:03:6b	Cisco Phone
00:e0:75	Veritel Polycom Phone
00:d0:1e	Pingtel Phone
00:01:e3	Siemens AG Phone
00:60:b9	NEC/Philips Phone
00:0f:e2	Huawei-3COM Phone
00:09:6e	Avaya Phone

Command Mode

Global Configuration mode

User Guidelines

The classification of a packet to Packets from VoIP Equipment/Phones is based on the packet's OUI of the source Mac Address.

In MAC addresses, the first three bytes contain a manufacturer ID (Organizationally Unique Identifiers - OUI) and the last three bytes contain a unique station ID.

OUIs are globally assigned (administered) by the IEEE.

Since the number of IP phones manufacturers that dominates the market is limited and well known, the known OUI values can be configured (as a default and user configurable) to the switch.

Example

The following example adds an entry to the voice VLAN OUI table.

```
Console(config)# voice vlan oui-table add 00:AA:BB description
experimental
```

voice vlan cos mode

Use the **voice vlan cos mode** Interface Configuration mode command to select the OUI Voice VLAN Class Of Service mode. Use the **no** form of this command. to return to the default.

Syntax

voice vlan cos mode *{src | all}*

no voice vlan cos mode

Parameters

- **src**—QoS attributes are applied only on packets from IP phones. See the User Guidelines.
- **all**—QoS attributes are applied only on all packets that are classified to the Voice VLAN.

Command Mode

Interface Configuration (Ethernet, port-channel) mode

voice vlan cos

Use the **voice vlan cos** Global Configuration mode command to set the OUI Voice VLAN Class of Service (CoS). Use the **no** form of this command to restore the default configuration..

Syntax

voice vlan cos *cos [remark]*

no voice vlan cos

Parameters

- **cos**—Specifies the voice VLAN Class of Service. (Range: 0–7)
- **remark**—Specifies that the L2 User Priority is remarked.

Default Configuration

The default CoS value is 6.

The L2 User Priority is not remarked.

Command Mode

Global Configuration mode

User Guidelines

Example

The following example sets the OUI Voice VLAN CoS to 6.

```
Console(config)# voice vlan cos 7
```

voice vlan aging-timeout

Use the **voice vlan aging-timeout** Global Configuration mode command to set the OUI Voice VLAN aging timeout interval. Use the **no** form of this command to restore the default configuation.

Syntax
voice vlan aging-timeout *minutes*

no voice vlan aging-timeout

Parameters
minutes—Specifies the voice VLAN aging timeout interval in minutes. (Range: 1–43200)

Default Configuration
The default voice VLAN aging timeout interval is 1440 minutes.

Command Mode
Global Configuration mode

Example
The following example sets the OUI Voice VLAN aging timeout interval to 12 hours.

```
Console(config)# voice vlan aging-timeout 720
```

voice vlan enable

Use the **voice vlan enable** Interface Configuration (Ethernet, Port-channel) mode command to enable OUI Voice VLAN configuration on a port. Use the **no** form of this command to disable OUI Voice VLAN configuration on a port.

Syntax
voice vlan enable

no voice vlan enable

Default Configuration
Automatic voice VLAN configuration of a port is disabled.

Command Mode
Interface Configuration (Ethernet, Port-channel) mode

User Guidelines

The port is added to the voice VLAN if a packet with a source MAC address that is a telephony MAC address (defined by the **voice vlan oui-table** Global Configuration mode command) is trapped on the port. Note: The packet VLAN ID can be the voice VLAN ID or any other VLAN ID.

The port joins the voice VLAN as a tagged port.

If the time since the last MAC address with a telephony MAC address aged out exceeds the timeout limit (configured by the **voice vlan aging-timeout** Global Configuration mode command), the port is removed from the voice VLAN.

Example

The following example enables OUI Voice VLAN configuration on gigabitethernet port `1/0/2`.

```
Console(config)# interface gigabitethernet 1/0/2
Console(config-if)# voice vlan enable
```

voice vlan secure

Use the **voice vlan secure** Interface Configuration (Ethernet, Port-channel) mode command to enable the secure mode for the OUI Voice VLAN. Use the **no** form of this command to disable the secure mode.

Syntax

voice vlan secure

no voice vlan secure

Default Configuration

The voice VLAN secure mode is disabled.

Command Mode

Interface Configuration (Ethernet, Port-channel) mode

User Guidelines

Use this command to specify that packets that are classified to the voice VLAN with a source MAC address that is not a telephony MAC address (defined by the **voice vlan oui-table** Global Configuration mode command) are discarded.

This command is relevant only to ports that were added to the voice VLAN automatically

Example

The following example enables the secure mode for the OUI Voice VLAN on gigabitethernet port `1/0/8`.

```
Console(config)# interface gigabitethernet 1/0/8
Console(config-if)# voice vlan secure
```

show voice vlan

Use the **show voice vlan** EXEC mode command to display the voice VLAN status for all interfaces or for a specific interface.

Syntax

show voice vlan [**type** {**oui** | **auto**}] [*interface-id*]

Parameters

type {**oui** | **auto**}—Specifies which information is printed:

oui - common and the OUI Voice VLAN specific parameters are printed

auto - common and the Auto Voice VLAN specific parameters are printed

If the parameter is omitted the current Voice VLAN type is applied.

interface-id—Specifies an interface ID. If the parameter is omitted than information about all interfaces are printed. Applied only for the OUI VLAN type.

Parameters Range

interface-id—Ethernet, Port-channel

Command Mode
EXEC mode

Example

```
Example 1.

switch>show voice vlan
Administrate Voice VLAN state is auto-triggered
Operational Voice VLAN state is auto-enabled
Best Local Voice VLAN-ID is 20
Best Local VPT is 4
Best Local DSCP is 1
Voice VLAN is received from switch 00:01:22:01:ab:87:45
Agreed Voice VLAN priority is 0 (active UC device)
Agreed Voice VLAN-ID is 100
Agreed VPT is 0
Agreed DSCP is 0
Agreed VLAN Last Change is 10-Apr-10 20:01:00

Example 2.
Administrate Voice VLAN state is auto-enabled
Operational Voice VLAN state is auto-enabled
Best Local Voice VLAN-ID is 1 (default)
Best Local VPT is 0 (default)
Best Local DSCP is 0 (default)
Agreed Voice VLAN is received from switch 00:01:22:01:ab:87:45
Agreed Voice VLAN priority is 2 (static)
Agreed Voice VLAN-ID is 20
Agreed VPT is 7
Agreed DSCP is 20
Agreed VLAN Last Change is 10-Apr-10 20:01:00

Example 3.
Administrate Voice VLAN state is auto-triggered
Operational Voice VLAN state is disabled
```

```
Example 4.
Administrate Voice VLAN state is disabled
Operational Voice VLAN state is disabled
Best Local Voice VLAN-ID is 20
Best Local VPT is 0 (default)
Best Local DSCP is 0 (default)
Aging timeout: 1440 minutes
CoS: 6
Remark: Yes

Example 5.
Administrate Voice VLAN state is oui-enabled
Operational Voice VLAN state is oui-enabled
Best Local Voice VLAN-ID is 1 (default)
Best Local VPT is 4
Best Local DSCP is 1
Aging timeout: 1440 minutes
CoS: 6
Remark: Yes

OUI table

MAC Address - Prefix   Description
--------------------   ------------------
00:E0:BB               3COM
00:03:6B               Cisco
00:E0:75               Veritel
00:D0:1E               Pingtel
00:01:E3               Simens
00:60:B9               NEC/Philips
00:0F:E2               Huawei-3COM
00:09:6E               Avaya

Interface          Enabled    Secure    Activated  cos Mode
```

```
-------------      -------    -------   ---------  --------
gi1/0/1              Yes       Yes         Yes      all
gi1/0/2              Yes       Yes         No       src
gi1/0/3              No        No           -       src
```

36

DHCP Snooping and ARP Inspection Commands

ip dhcp snooping

Use the **ip dhcp snooping** Global Configuration mode command to enable Dynamic Host Configuration Protocol (DHCP) Snooping globally. Use the **no** form of this command to restore the default configuration.

Syntax

ip dhcp snooping

no ip dhcp snooping

Default Configuration

DHCP snooping is disabled.

Command Mode

Global Configuration mode

User Guidelines

For any DHCP Snooping configuration to take effect, DHCP Snooping must be enabled globally. DHCP Snooping on a VLAN is not active until DHCP Snooping on a VLAN is enabled by using the **ip dhcp snooping vlan** Global Configuration mode command.

Example

The following example enables DHCP Snooping on the device.

```
Console(config)# ip dhcp snooping
```

ip dhcp snooping vlan

Use the **ip dhcp snooping vlan** Global Configuration mode command to enable DHCP Snooping on a VLAN. Use the **no** form of this command to disable DHCP Snooping on a VLAN.

Syntax

ip dhcp snooping vlan *vlan-id*

no ip dhcp snooping *vlan-id*

Parameters

vlan-id—Specifies the VLAN ID.

Default Configuration

DHCP Snooping on a VLAN is disabled.

Command Mode

Global Configuration mode

User Guidelines

DHCP Snooping must be enabled globally before enabling DHCP Snooping on a VLAN.

Example

The following example enables DHCP Snooping on VLAN 21.

```
Console(config)# ip dhcp snooping vlan 21
```

ip dhcp snooping trust

Use the **ip dhcp snooping trust** Interface Configuration (Ethernet, Port-channel) mode command to configure a port as trusted for DHCP snooping purposes. Use the **no** form of this command to restore the default configuration.

Syntax

ip dhcp snooping trust

no ip dhcp snooping trust

Default Configuration

The interface is untrusted.

Command Mode

Interface Configuration (Ethernet, Port-channel) mode

User Guidelines

Configure as trusted the ports that are connected to a DHCP server or to other switches or routers. Configure the ports that are connected to DHCP clients as untrusted.

Example

The following example configures gigabitethernet port `1/0/5` as trusted for DHCP Snooping.

```
Console(config)# interface gigabitethernet 1/0/5
Console(config-if)# ip dhcp snooping trust
```

ip dhcp snooping information option allowed-untrusted

Use the **ip dhcp snooping information option allowed-untrusted** Global Configuration mode command to allow a device to accept DHCP packets with option-82 information from an untrusted port. Use the **no** form of this command to drop these packets from an untrusted port.

Syntax

ip dhcp snooping information option allowed-untrusted

no ip dhcp snooping information option allowed-untrusted

Default Configuration
DHCP packets with option-82 information from an untrusted port are discarded.

Command Mode
Global Configuration mode

Example
The following example allows a device to accept DHCP packets with option-82 information from an untrusted port.

```
Console(config)# ip dhcp snooping information option allowed-
untrusted
```

ip dhcp snooping verify

Use the **ip dhcp snooping verify** Global Configuration mode command to configure a device to verify that the source MAC address in a DHCP packet received on an untrusted port matches the client hardware address. Use the **no** form of this command to disable MAC address verification in a DHCP packet received on an untrusted port.

Syntax
ip dhcp snooping verify

no ip dhcp snooping verify

Default Configuration
The switch verifies that the source MAC address in a DHCP packet received on an untrusted port matches the client hardware address in the packet.

Command Mode
Global Configuration mode

Example

The following example configures a device to verify that the source MAC address in a DHCP packet received on an untrusted port matches the client hardware address.

```
Console(config)# ip dhcp snooping verify
```

ip dhcp snooping database

Use the **ip dhcp snooping database** Global Configuration mode command to enable the DHCP Snooping binding database file. Use the **no** form of this command to delete the DHCP Snooping binding database file.

Syntax

ip dhcp snooping database

no ip dhcp snooping database

Default Configuration

The DHCP Snooping binding database file is not defined.

Command Mode

Global Configuration mode

User Guidelines

The DHCP Snooping binding database file resides on Flash.

To ensure that the lease time in the database is accurate, the Simple Network Time Protocol (SNTP) must be enabled and configured.

The device writes binding changes to the binding database file only if the device system clock is synchronized with SNTP.

Example

The following example enables the DHCP Snooping binding database file.

```
Console(config)# ip dhcp snooping database
```

ip dhcp snooping database update-freq

Use the **ip dhcp snooping database update-freq** Global Configuration mode command to set the update frequency of the DHCP Snooping binding database file. Use the **no** form of this command to restore the default configuration.

Syntax

ip dhcp snooping database update-freq *seconds*

no ip dhcp snooping database update-freq

Parameters

seconds—Specifies the update frequency in seconds. (Range: 600–86400)

Default Configuration

The default update frequency value is 1200 seconds.

Command Mode

Global Configuration mode

Example

The following example sets the DHCP Snooping binding database file update frequency to 1 hour.

```
Console(config)# ip dhcp snooping database update-freq 3600
```

ip dhcp snooping binding

Use the **ip dhcp snooping binding** Privileged EXEC mode command to configure the DHCP Snooping binding database and add binding entries to the database. Use the **no** form of this command to delete entries from the binding database.

Syntax

ip dhcp snooping binding *mac-address vlan-id ip-address interface-id expiry {seconds | infinite}*

no ip dhcp snooping binding mac-address vlan-id

Parameters

- **mac-address**— pecifies a MAC address.
- **vlan-id**—Specifies a VLAN number.
- **ip-address**—Specifies an IP address.
- **interface-id**—Specifies an interface ID. The interface ID can be one of the following types: Ethernet port or Port-channel.
- **expiry seconds**—Specifies the time interval, in seconds, after which the binding entry is no longer valid. (Range: 10–4294967295)
- **expiry infinite**—Specifies infinite lease time.

Default Configuration
No static binding exists.

Command Mode
Privileged EXEC mode

User Guidelines
After entering this command, an entry is added to the DHCP Snooping database. If the DHCP Snooping binding file exists, the entry is also added to that file.

The entry is displayed in the show commands as a DHCP Snooping entry.

The user cannot delete dynamic temporary entries for which the IP address is 0.0.0.0.

Example
The following example adds a binding entry to the DHCP Snooping binding database.

```
Console# ip dhcp snooping binding 0060.704C.73FF 23 176.10.1.1
ethernet 1/5 expiry 900
```

clear ip dhcp snooping database

Use the **clear ip dhcp snooping database** Privileged EXEC mode command to clear the DHCP Snooping binding database.

Syntax
clear ip dhcp snooping database

Command Mode
Privileged EXEC mode

Example
The following example clears the DHCP Snooping binding database.

```
Console# clear ip dhcp snooping database
```

show ip dhcp snooping

Use the **show ip dhcp snooping** EXEC mode command to display the DHCP snooping configuration for all interfaces or for a specific interface.

Syntax
show ip dhcp snooping *[interface-id]*

Parameters
interface-id—Specifies an interface ID. The interface ID can be one of the following types: Ethernet port or Port-channel.

Command Mode
EXEC mode

Example
The following example displays the DHCP snooping configuration.

```
console# show ip dhcp snooping
DHCP snooping is Enabled
```

```
DHCP snooping is configured on following VLANs: 21
DHCP snooping database is Enabled
Relay agent Information option 82 is Enabled
Option 82 on untrusted port is allowed
Verification of hwaddr field is Enabled
DHCP snooping file update frequency is configured to: 6666 seconds
Interface    Trusted
----------- ------------
gi1/0/1       Yes
gi1/0/2       Yes
```

show ip dhcp snooping binding

Use the **show ip dhcp snooping binding** User EXEC mode command to display the DHCP Snooping binding database and configuration information for all interfaces or for a specific interface.

Syntax

show ip dhcp snooping binding *[mac-address mac-address] [ip-address ip-address] [vlan vlan-id] [interface-id]*

Parameters

- **mac-address mac-address**—Specifies a MAC address.
- **ip-address ip-address**—Specifies an IP address.
- **vlan vlan-id**—Specifies a VLAN ID.
- **interface-id**—Specifies an interface ID. The interface ID can be one of the following types: Ethernet port or Port-channel.

Command Mode

User EXEC mode

Example
The following examples displays the DHCP snooping binding database and configuration information for all interfaces on a device.

```
Console# show ip dhcp snooping binding

Update frequency: 1200
Total number of binding: 2

Mac Address     IP Address   Lease      Type        VLAN    Interface
------------    ----------   (sec)      --------    ----    ---------
0060.704C.73    10.1.8.1     -------    snooping    3       1/21
FF              10.1.8.2     7983       snooping    3       1/22
0060.704C.7B                 92332      (s)
C1
```

ip arp inspection

Use the **ip arp inspection** Global Configuration mode command globally to enable Address Resolution Protocol (ARP) inspection. Use the **no** form of this command to disable ARP inspection.

Syntax
ip arp inspection

no ip arp inspection

Default Configuration
ARP inspection is disabled.

Command Mode
Global Configuration mode

User Guidelines
Note that if a port is configured as an untrusted port, then it should also be configured as an untrusted port for DHCP Snooping, or the IP-address-MAC-address binding for this port should be configured statically. Otherwise, hosts that are attached to this port cannot respond to ARPs.

Example
The following example enables ARP inspection on the device.

```
Console(config)# ip arp inspection
```

ip arp inspection vlan

Use the **ip arp inspection vlan** Global Configuration mode command to enable ARP inspection on a VLAN, based on the DHCP Snooping database. Use the **no** form of this command to disable ARP inspection on a VLAN.

Syntax
ip arp inspection vlan *vlan-id*

no ip arp inspection vlan *vlan-id*

Parameters
vlan-id—Specifies the VLAN ID.

Default Configuration
DHCP Snooping based ARP inspection on a VLAN is disabled.

Command Mode
Global Configuration mode

User Guidelines
This command enables ARP inspection on a VLAN based on the DHCP snooping database. Use the **ip arp inspection list assign** Global Configuration mode command to enable static ARP inspection.

Example
The following example enables DHCP Snooping based ARP inspection on VLAN 23.

```
Console(config)# ip arp inspection vlan 23
```

ip arp inspection trust

Use the **ip arp inspection trust** Interface Configuration (Ethernet, Port-channel) mode command to configure an interface trust state that determines if incoming Address Resolution Protocol (ARP) packets are inspected. Use the **no** form of this command to restore the default configuration.

Syntax

ip arp inspection trust

no ip arp inspection trust

Default Configuration

The interface is untrusted.

Command Mode

Interface Configuration (Ethernet, Port-channel) mode

User Guidelines

The device does not check ARP packets that are received on the trusted interface; it only forwards the packets.

For untrusted interfaces, the device intercepts all ARP requests and responses. It verifies that the intercepted packets have valid IP-to-MAC address bindings before updating the local cache and before forwarding the packet to the appropriate destination. The device drops invalid packets and logs them in the log buffer according to the logging configuration specified with the **ip arp inspection log-buffer vlan** Global Configuration mode command.

Example

The following example configures gigabitethernet port `1/0/3` as a trusted interface.

```
Console(config)# interface gigabitethernet 1/0/3
Console(config-if)# ip arp inspection trust
```

ip arp inspection validate

Use the **ip arp inspection validate** Global Configuration mode command to perform specific checks for dynamic Address Resolution Protocol (ARP) inspection. Use the **no** form of this command to restore the default configuration.

Syntax

ip arp inspection validate

no ip arp inspection validate

Default Configuration

ARP inspection validation is disabled.

Command Mode

Global Configuration mode

User Guidelines

The following checks are performed:

- **Source MAC address**: Compares 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.
- **Destination MAC address**: Compares the destination MAC address in the Ethernet header against the target MAC address in the ARP body. This check is performed for ARP responses.
- **IP addresses**: Compares the ARP body for invalid and unexpected IP addresses. Addresses include 0.0.0.0, 255.255.255.255, and all IP multicast addresses.

Example

The following example executes ARP inspection validation.

```
Console(config)# ip arp inspection validate
```

ip arp inspection list create

Use the **ip arp inspection list create** Global Configuration mode command to create a static ARP binding list and enters the ARP list configuration mode. Use the **no** form of this command to delete the list.

Syntax

ip arp inspection list create *name*

no ip arp inspection list create *name*

Parameters

name—Specifies the static ARP binding list name. (Length: 1–32 characters)

Default Configuration

No static ARP binding list exists.

Command Mode

Global Configuration mode

User Guidelines

Use the **ip arp inspection list assign** command to assign the list to a VLAN.

Example

The following example creates the static ARP binding list 'servers' and enters the ARP list configuration mode.

```
Console(config)# ip arp inspection list create servers
Console(config-ARP-list)#
```

ip mac

Use the **ip mac** ARP-list Configuration mode command to create a static ARP binding. Use the **no** form of this command to delete a static ARP binding.

Syntax

ip *ip-address* **mac** *mac-address*

no ip *ip-address* **mac** *mac-address*

Parameters

- **ip-address**—Specifies the IP address to be entered to the list.
- **mac-address**—Specifies the MAC address associated with the IP address.

Default Configuration
No static ARP binding is defined.

Command Mode
ARP-list Configuration mode

Example
The following example creates a static ARP binding.

```
Console(config)# ip arp inspection list create servers
Console(config-ARP-list)# ip 172.16.1.1 mac 0060.704C.7321
Console(config-ARP-list)# ip 172.16.1.2 mac 0060.704C.7322
```

ip arp inspection list assign

Use the **ip arp inspection list assign** Global Configuration mode command to assign a static ARP binding list to a VLAN. Use the **no** form of this command to delete the assignment.

Syntax
ip arp inspection list assign *vlan-id name*

no ip arp inspection list assign *vlan*

Parameters

- **vlan-id**—Specifies the VLAN ID.
- **name**—Specifies the static ARP binding list name.

Default Configuration
No static ARP binding list assignment exists.

Command Mode
Global Configuration mode

Example
The following example assigns the static ARP binding list Servers to VLAN 37.

```
Console(config)# ip arp inspection list assign 37 servers
```

ip arp inspection logging interval

Use the **ip arp inspection logging interval** Global Configuration mode command to set the minimum time interval between successive ARP SYSLOG messages. Use the **no** form of this command to restore the default configuration.

Syntax
ip arp inspection logging interval {*seconds* | *infinite*}

no ip arp inspection logging interval

Parameters

- **seconds**—Specifies the minimum time interval between successive ARP SYSLOG messages. A 0 value means that a system message is immediately generated. (Range: 0–86400)
- **infinite**—Specifies that SYSLOG messages are not generated.

Default Configuration
The default minimum ARP SYSLOG message logging time interval is 5 seconds.

Command Mode
Global Configuration mode

Example
The following example sets the minimum ARP SYSLOG message logging time interval to 60 seconds.

```
Console(config)# ip arp inspection logging interval 60
```

show ip arp inspection
Use the **show ip arp inspection** EXEC mode command to display the ARP inspection configuration for all interfaces or for a specific interface.

Syntax
show ip arp inspection *[interface-id]*

Parameters
interface-id—Specifies an interface ID. The interface ID can be one of the following types:Ethernet port or Port-channel.

Command Mode
EXEC mode

Example
The following example displays the ARP inspection configuration.

```
console# show ip arp inspection
IP ARP inspection is Enabled
IP ARP inspection is configured on following VLANs: 1
Verification of packet header is Enabled
IP ARP inspection logging interval is: 222  seconds

 Interface    Trusted
----------- -----------
gi1/0/1       Yes
gi1/0/2       Yes
```

show ip arp inspection list

Use the **show ip arp inspection list** Privileged EXEC mode command to display the static ARP binding list.

Syntax
show ip arp inspection list

Command Mode
Privileged EXEC mode

Example
The following example displays the static ARP binding list.

```
Console# show ip arp inspection list

List name: servers
Assigned to VLANs: 1,2

IP                    ARP
---------             --------------
172.16.1.1            0060.704C.7322
172.16.1.2            0060.704C.7322
```

show ip arp inspection statistics

Use the **show ip arp inspection statistics** EXEC command to display Statistics For The Following Types Of Packets That Have Been Processed By This Feature: Forwarded, Dropped, IP/MAC Validation Failure.

Syntax
show ip arp inspection statistics *[vlan vlan-id]*

Parameters
vlan-id—Specifies VLAN ID.

Command Mode
EXEC mode

User Guidelines
To clear ARP Inspection counters use the **clear ip arp inspection statistics** CLI command. Counters values are kept when disabling the ARP Inspection feature.

Example

```
console# show ip arp inspection statistics

Vlan    Forwarded Packets Dropped Packets IP/MAC Failures
----    ------------------------------------------------
2       1500100     80
```

clear ip arp inspection statistics

Use the **clear ip arp inspection statistics** Privileged EXEC mode command to clear statistics ARP Inspection statistics globally.

Syntax
clear ip arp inspection statistics *[vlan vlan-id]*

Parameters
vlan-id—Specifies VLAN ID

Command Mode
Privileged EXEC mode

Example

```
console# clear ip arp inspection statistics
```

ip dhcp information option

Use the **ip dhcp information option** Global Configuration command to enable DHCP option-82 data insertion. Use the **no** form of this command to disable DHCP option-82 data insertion.

Syntax

ip dhcp information option

no ip dhcp information option

Parameters

This command has no arguments or keywords.

Default Configuration

DHCP option-82 data insertion is disabled.

Command Mode

Global Configuration mode

User Guidelines

DHCP option 82 would be enabled only if DHCP snooping or DHCP relay are enabled.

Example

```
console(config)# ip dhcp information option
```

show ip dhcp information option

The **show ip dhcp information option** EXEC mode command displays the DHCP Option 82 configuration.

Syntax

show ip dhcp information option

Command Mode
EXEC mode

Example
The following example displays the DHCP Option 82 configuration.

```
console# show ip dhcp information option
Relay agent Information option is Enabled
```

37

iSCSI Commands

iscsi enable

Use the iscsi enable Global Configuration mode command to globally enable Internet Small Computer System Interface (iSCSI) awareness. This command changes the Flow Control global mode to receive-only, enables Flow Control on all interfaces, and enables jumbo frames.

Use the no form of this command to globally disable iSCSI awareness. This version of the command does not affect the Flow Control global mode, does not disable Flow Control on all interfaces, and does not disable jumbo frames.

Syntax

iscsi enable

no iscsi enable

Default Configuration

Disabled.

Command Mode

Global Configuration mode

User Guidelines

An iSCSI VLAN must be configured by using the **iscsi vlan** command before the device can assign a specific VLAN to iSCSI flows.

When executing the **no iscsi enable** command, iSCSI resources (TCAM) are released.

Example

The following example enables iSCSI awareness globally.

```
Console(config)# iscsi enable
```

iscsi target port

Use the **iscsi target port** Global Configuration mode command to configures iSCSI target ports. Use the **no** form of this command to delete the iSCSI target ports.

Syntax

iscsi target port *tcp-port-1 [tcp-port-2.... tcp-port-8] [address ip-address] [name targetname]*

no iscsi target port *tcp-port-1 [tcp-port-2.... tcp-port-8] [address ip-address]*

Parameters

- **tcp-port**—Specifies the TCP port number or list of TCP port numbers on which iSCSI targets listen to requests. Up to 8 TCP ports can be defined in the system, in one command or by using multiple commands. (Range: 1–65536)
- **address ip-address**—Specifies the iSCSI target IP address. If the **no** form is used and the TCP port to be deleted is one that was bound to a specific IP address, the IP address field must be present.
- **name targetname**—Specifies the iSCSI target name. The name can be statically configured, but it can also be obtained from iSNS or from the sendTargets response. The initiator must present both its iSCSI Initiator Name and the iSCSI Target Name to which it wishes to connect in the first login request of a new session or connection. The name must comprise valid characters, as specified by RFC 3722. (Length: 1–223 characters)

Default Configuration

iSCSI well-known ports 3260 and 860 are configured as the default target ports, but they can be removed just as any other configured target.

Command Mode
Global Configuration mode

User Guidelines
When working with private iSCSI ports (not IANA assigned iSCSI ports 3260 and 860), it is recommended that the target IP address also be specified, so that the device snoops only frames for which its TCP destination port is one of the configured TCP ports and their destination IP is the target's IP address. In this way, the CPU is not falsely loaded by non-iSCSI flows if other applications choose to use these un-reserved ports.

It is the user's responsibility to not define as iSCSI ports any ports that are well-known or are configured on the product for other uses, such as Telnet, SSH, HTTP, HTTPS, SNMP, or DHCP.

To bind a port to an IP address, and the port is already defined but not bound to an IP address, first remove the port by using the **no** form of the command and then add it again with the relevant IP address.

Target names are displayed only when using the **show iscsi** command. These names are not used to match (or to perform any sanity check on) the iSCSI session information acquired by snooping.

A maximum of 16 TCP ports can be configured either bound to IP or not. This number can be changed by using the **iscsi max target ports** command. However, the change takes effect only after reset.

Example
The following example configures an iSCSI target port.

```
Console(config)# iscsi target port 30001 address 176.16.1.1
name iqn.1993-11.com.disk-
vendor:diskarrays.sn.45678.tape:sys1.xyz
```

iscsi cos

Use the **iscsi cos** Global Configuration mode command to set the quality of service profile to apply to iSCSI flows. Use the **no** form of this command to restore the default configuration.

Syntax

iscsi cos enable

iscsi cos disable

iscsi cos {***vpt*** *vpt* | ***dscp*** *dscp*} [***remark***]

Parameters

- **enable – enables iSCSI CoS**
- **vpt** —Specifies the VLAN Priority Tag (VPT) that iSCSI frames are assigned. (Range: 0–7)
- **dscp** —Specifies the Differentiated Services Code Point (DSCP) that iSCSI frames are assigned. (Range: 0–63)
- **remark**—Marks the iSCSI frames with the configured VPT or DSCP when egressing the switch.

Default Configuration

iSCSI COS is disabled by default, the default profile is VPT 5.

Command Mode

Global Configuration mode

User Guidelines

The **iscsi cos enable** command is used to enable an iSCSI CoS profile (whether the default profile or one configured by using the **iscsi cos vpt/dscp** command).

When executing the **iscsi cos disable** command, iSCSI CoS configuration is not deleted.

Use the Remark option to prioritize iSCSI traffic in the next hop switch, which might be iSCSI-unaware.

iSCSI flows are assigned by default with a VPT/DSCP that is mapped to the highest queue not used for stack management or voice VLAN (if the mapping was not changed by the user). The user should also configure the relevant (vpt to queue/dscp to queue) table to complete the setting.

Setting the VPT/DSCP sets the QoS profile that determines the egress queue to which the frame is mapped. The switch default setting for egress queues

scheduling is strict priority. The downside of strict priority queuing is that in certain circumstances (heavy high priority traffic), lower priority traffic may become bandwidth-starved. In WRR, the queue to which the flow is assigned can be set to get the required percentage. The user may want to complete the QoS setting by configuring the relevant ports to work in WRR mode with adequate weights.

Example

The following example sets the QoS profile to apply to iSCSI flows by assigning iSCSI frames with DSCP 31.

```
Console(config)# iscsi cos enable
Console(config)# iscsi cos dscp 31
```

iscsi aging-time

Use the **iscsi aging-time** Global Configuration mode command to set the idle time interval for iSCSI sessions. Use the **no** form of this command. to cancel iSCSI session aging.

Syntax

iscsi aging-time *minutes*

no iscsi aging-time

Parameters

minutes—Specifies the iSCSI session idle time interval in minutes before the session is terminated. (Minimum: 1 minute)

Default Configuration

The default idle time interval for iSCSI sessions is 120 minutes.

Command Mode

Global Configuration mode

User Guidelines

iSCSI session aging time may be longer than the defined aging time. This is due to a lack of ASIC counters used by the application for aging.

When changing the iSCSI session aging time, the following occurs:

- If the aging time is increased, the aging time for the current session is recalculated and increased by the difference between the new aging time and the current aging time.
- If the aging time is decreased, the aging time for the current session is recalculated and decreased by the difference between the new aging time and the current aging time. If, after recalculation, it is determined that the current session idle time is greater than the new aging time, the session is immediately terminated.

Example
The following example sets the aging time for iSCSI sessions to 10 minutes.

```
Console(config)# iscsi aging-time 10
```

iscsi max-tcp-connections

To set the maximum number of iSCSI sessions that can be supported use the **iscsi max-tcp-connections** command in global configuration mode. To return to default, use the no form of this command.

Syntax
iscsi max-tcp-connections *max-connections*

no iscsi max-tcp-connections

Parameters
max-connections—Specifies the maximum number of iSCSI connections that can be supported. (5-1024)

Default Configuration
256 TCP connections

Command Mode
Global Configuration mode

User Guidelines
The new setting will take affect only after reset.

This command enables the user to define the number of iSCSI connections supported in the system.

The amount of iSCSI sessions has effect on the system memory consumption. The memory consumption is ~500 bytes per session and 20 bytes per connection (256 sessions each with 4 connections consumes ~145KB). In the current implementation, if more than 1024 connections exist, you will still get QoS, but only 1024 connections will be displayed

show iscsi

Use the **show iscsi** Privileged EXEC mode command to display the iSCSI configuration.

Syntax
show iscsi

Command Mode
Privileged EXEC mode

User Guidelines
The iSCSI targets displayed are the statically configured targets only.

To display all iSCSI entities (targets and initiators), whether statically configured or dynamically discovered, use the **show iscsi sessions** command.

Example
The following example display the iSCSI configuration.

```
Console# show iscsi
iSCSI disabled
iSCSI COS disabled
iSCSI vpt is 5, Remark
iSCSI aging time: 5 min.

Maximum number of connections: 256

iSCSI targets and TCP ports:
----------------------------
  TCP         Target IP              Name
  Port        Address
--------- ----------------- --------------------
   860         0.0.0.0
  3260         0.0.0.0
  9876         0.0.0.0
  20002        0.0.0.0
  20003        0.0.0.0
  25555        0.0.0.0
```

show iscsi sessions

Use the **show iscsi sessions** Privileged EXEC mode command to display the iSCSI sessions.

Syntax
show iscsi sessions *[detailed]*

Parameters
detailed—Specifies that the displayed list is detailed.

Command Mode
Privileged EXEC mode

User Guidelines

The target list is not sorted alphabetically.

The aging mechanism checks session activity in a group of N TCP iSCSI connections. In the worst case, if all 256 sessions are monitored and are not terminated gracefully, the existing mechanism causes inaccuracies; the last group of monitored iSCSI sessions are aged out after (256/N)*aging-time.

In general, the higher the number of ungraceful terminated iSCSI TCP connections, the higher the aging-time inaccuracy.

Example

The following example displays the iSCSI sessions

```
Console# show iscsi sessions

Target: iqn.1993-11.com.disk-vendor:diskarrays.sn.45678
-------------------------------------------------------
Initiator: iqn.1992-04.com.os-vendor.plan9:cdrom.12
ISID: 11
Initiator: iqn.1995-05.com.os-vendor.plan9:cdrom.10
ISID: 222
-------------------------------------------------------
Target: iqn.103-1.com.storage-
vendor:sn.43338.storage.tape:sys1.xyz
-------------------------------------------------------
Initiator: iqn.1992-04.com.os-vendor.plan9:cdrom.12
ISID: 44
Initiator: iqn.1995-05.com.os-vendor.plan9:cdrom.10
ISID: 65
-------------------------------------------------------
Console# show iscsi sessions detailed
Target: iqn.1993-11.com.disk-vendor:diskarrays.sn.45678
-------------------------------------------------------
Session 1:
---------
```

```
Initiator: iqn.1992-04.com.os-
vendor.plan9:cdrom.12.storage:sys1.xyz
UP Time: 02:10:45 (DD:HH:MM)
Time for aging out: 10 min
ISID: 11


 Initiator          Initiator     Target             Target
 IP Address         TCP Port      IP Address         IP Port
 ----------         ---------     -----------        -------
 172.16.1.3         49154         172.16.1.20        30001
 172.16.1.4         49155         172.16.1.21        30001
 172.16.1.5         49156         172.16.1.22        30001
 Session 2:
 ---------
 Initiator: iqn.1995-05.com.os-vendor.plan9:cdrom.10
 Status: Active
 UP Time: 00:04:50 (DD:HH:MM)
 Time for aging out: 2 min
 ISID: 22
 Initiator          Initiator     Target             Target
 IP Address         TCP Port      IP Address         IP Port
 ----------         ---------     ----------         -------
 172.16.1.30        49200         172.16.1.20        30001
 172.16.1.40        49201         172.16.1.21        30001
```

38

IP Addressing Commands

address

Use the **ip address** Interface Configuration (Ethernet, VLAN, Port-channel) mode command to define an IP address for an interface. Use the **no** form of this command to remove an IP address definition.

Syntax

If the product is a switch router.

ip address *ip-address* {*mask* | *prefix-length*}

no ip address [*ip-address*]

If the product is a switch only.

ip address *ip-address* {*mask* | *prefix-length*} [**default-gateway** *ip-address*]

no ip address [*ip-address*]

If the product is switch only and supports a single IP address:

ip address *ip-address* {*mask* | *prefix-length*} [**default-gateway** *ip-address*]

no ip address

Parameters

- **ip-address**—Specifies the IP address.
- **mask**—Specifies the network mask of the IP address.
- **prefix-length**—Specifies the number of bits that comprise the IP address prefix.The prefix length must be preceded by a forward slash (/). (Range: 8–30)
- **default-gateway ip-address**—Specifies the default gateway IP address.

Default Configuration
No IP address is defined for interfaces.

Command Mode
Interface Configuration (Ethernet, VLAN, Port-channel) mode. It cannot be configured for a range of interfaces (range context).

User Guidelines
Defining a static IP address on an interface implicitly removes the DHCP client configuration on the interface.

If the product supports multiple IP addresses:

> The product supports up to x IP addresses. The IP addresses should be from different IP subnets. When adding an IP address from a subnet that already exists in the list, the new IP address replaces the existing IP address from that subnet.

If the product is switch only and supports a single IP address.

> If the IP address configured in global context then it would be bound to the currently defined management interface. If the management interface is Default VLAN and the VID of the default VLAN is changed then when new setting is applied, the IP address will be automatically redefined on the new Default VLAN.

If the IP address is configured in Interface context then the IP address is bound to the interface in context.

If a static IP address is already defined, the user must do **no IP address** in the relevant interface context before changing the IP address.

If a dynamic IP address is already defined, the user must do **no ip address** in the relevant interface context before configuring another dynamic IP address.

The Interface context could be a port, LAG or VLAN, depending on support that is defined for the product.

Example
The following example configures VLAN 1 with IP address 131.108.1.27 and subnet mask 255.255.255.0.

```
Console(config)# interface vlan 1
```

```
Console(config-if)# ip address 131.108.1.27 255.255.255.0
```

ip address dhcp

Use the **ip address dhcp** Interface Configuration (Ethernet, VLAN, Port-channel) mode command to acquire an IP address for an Ethernet interface from the Dynamic Host Configuration Protocol (DHCP) server. Use the **no** form of this command to release an acquired IP address.

Syntax

ip address dhcp

no ip address dhcp

Parameters

No parameters

Command Mode

Interface Configuration (Ethernet, VLAN, Port-channel) mode. It cannot be configured for a range of interfaces (range context).

User Guidelines

The **ip address dhcp** command allows any interface to dynamically learn its IP address by using the DHCP protocol.

DHCP client configuration on an interface implicitly removes the static IP address configuration on the interface.

If the device is configured to obtain its IP address from a DHCP server, it sends a DHCPDISCOVER message to provide information about itself to the DHCP server on the network.

If the **ip address dhcp** command is used with or without the optional keyword, the DHCP option 12 field (host name option) is included in the DISCOVER message. By default, the host name specified in the option 12 field is the globally configured device host name.

The **no ip address dhcp** command releases any IP address that was acquired, and sends a DHCPRELEASE message.

Example
The following example acquires an IP address for gigabitethernet port `1/0/16` from DHCP.

```
Console(config)# interface gigabitethernet 1/0/16
Console(config-if)# ip address dhcp
```

renew dhcp

Use the **renew dhcp** Privileged EXEC mode command to renew an IP address that was acquired from a DHCP server for a specific interface.

Syntax
renew dhcp *{ interface-id}* [**force-autoconfig**]

Parameters
interface-id—Specifies an interface ID. The interface ID can be one of the following types: Ethernet port, Port-channel or VLAN.

force-autoconfig - In the case the DHCP server holds a DHCP option 67 record for the assigned IP address, the file would overwrite the existing device configuration

Command Mode
Privileged EXEC mode

User Guidelines
Note that this command does not enable DHCP on an interface. If DHCP is not enabled on the requested interface, the command returns an error message.

If DHCP is enabled on the interface and an IP address was already acquired, the command tries to renew that IP address.

If DHCP is enabled on the interface and an IP address has not yet been acquired, the command initiates a DHCP request.

Example
The following example renews an IP address that was acquired from a DHCP server for VLAN 19.

```
Console# renew dhcp vlan 19
```

ip default-gateway

The **ip default-gateway** Global Configuration mode command defines a default gateway (device). Use the **no** form of this command to restore the default configuration.

Syntax
ip default-gateway *ip-address*

no ip default-gateway

Parameters
ip-address—Specifies the default gateway IP address.

Command Mode
Global Configuration mode

Default Configuration
No default gateway is defined.

Example
The following example defines default gateway 192.168.1.1.

```
Console(config)# ip default-gateway 192.168.1.1
```

show ip interface

Use the **show ip interface** EXEC mode command to display the usability status of configured IP interfaces.

Syntax
show ip interface *[interface-id]*

Parameters
interface-id—Specifies an interface ID. The interface ID can be one of the following types: Ethernet port, Port-channel or VLAN.

Command Mode
EXEC mode

Example
The following example displays the configured IP interfaces and their types.

```
console# show ip interface
IP Address       I/F     Type    Directed   Precedence Status
                                 Broadcast
-------------    ------  ------- --------   ---------- -------
10.5.234.232/24  vlan 1  Static  disable    No         Valid
```

arp

Use the **arp** Global Configuration mode command to add a permanent entry to the Address Resolution Protocol (ARP) cache. Use the **no** form of this command to remove an entry from the ARP cache.

Syntax
arp *ip-address mac-address [interface-id]]*

no arp *ip-address*

Parameters

- **ip-address**—IP address or IP alias to map to the specified MAC address.
- **mac-address**—MAC address to map to the specified IP address or IP alias.
- **interface-id**—interface ID. Can be Ethernet port, Port-channel or VLAN.

Command Mode
Global Configuration mode

Default Configuration
No permanent entry is defined.

User Guidelines
The software uses ARP cache entries to translate 32-bit IP addresses into 48-bit hardware (MAC) addresses. Because most hosts support dynamic address resolution, static ARP cache entries generally do not need to be specified.

Example
The following example adds IP address 198.133.219.232 and MAC address 00:00:0c:40:0f:bc to the ARP table.

```
Console(config)# arp 198.133.219.232 00:00:0c:40:0f:bc
ethernet 1/6
```

arp timeout (Global)

Use the **arp timeout** Global Configuration mode command to set the time interval during which an entry remains in the ARP cache. Use the **no** form of this command to restore the default configuration.

Syntax
arp timeout *seconds*

no arp timeout

Parameters
seconds—Specifies the time interval (in seconds) during which an entry remains in the ARP cache.
(Range: 1–40000000)

Default Configuration
The default ARP timeout is 60000 seconds in Router mode, and 300 seconds in Switch mode.

Command Mode
Global Configuration mode

Example
The following example configures the ARP timeout to 12000 seconds.

```
Console(config)# arp timeout 12000
```

arp timeout

Use the **arp timeout** inTerface Configuration command to configure how long an entry remains in the ARP cache for specific interface. Use the **no** form of this command restore the default value.

Syntax
arp timeout *seconds*

no arp timeout

Parameters
seconds—Time (in seconds) that an entry remains in the ARP cache. It is recommended not to set it to less than 3600. (Range: 1–40000000)

Default
Defined by the **arp timeout** Global Configuration command

Command Mode
Interface Configuration (Ethernet, VLAN, Port-channel) mode. It cannot be configured for a range of interfaces (range context).

User Guidelines
This configuration can be applied only if at least one IP address defined on specific interface.

Example

```
Console (config)# interface vlan 1
Console(config-if)# arp timeout 12000
```

ip arp proxy disable

Use the **ip arp proxy disable** Global Configuration mode command to globally disable proxy Address Resolution Protocol (ARP). Use the **no** form of this command reenable proxy ARP.

Syntax

ip arp proxy disable

no ip arp proxy disable

Parameters

This command has no arguments or key words.

Default

Enabled by default.

Command Mode

Global Configuration mode

User Guidelines

The **ip arp proxy disable** command overrides any proxy ARP interface configuration.

ip proxy-arp

Use the **ip proxy-arp** Interface Configuration mode command to enable an ARP proxy on specific interfaces. Use the **no** form of this command disable it.

Syntax

ip proxy-arp

no ip proxy-arp

Default Configuration

ARP Proxy is disabled.

Command Mode
Interface Configuration (Ethernet, VLAN, Port-channel) mode. It cannot be configured for a range of interfaces (range context).

User Guidelines
This configuration can be applied only if at least one IP address is defined on a specific interface.

Example
The following example enables the ARP proxy.

```
Console(config-if)# ip proxy-arp
```

clear arp-cache

Use the **clear arp-cache** Privileged EXEC mode command to delete all dynamic entries from the ARP cache.

Syntax
clear arp-cache

Command Mode
Privileged EXEC mode

Example
The following example deletes all dynamic entries from the ARP cache.

```
Console# clear arp-cache
```

show arp

Use the **show arp** Privileged EXEC mode command to display entries in the ARP table.

Syntax
show arp *[ip-address ip-address] [mac-address mac-address] [interface-id]*

Parameters

- **ip-address ip-address**—Specifies the IP address.
- **mac-address** *mac-address*—Specifies the MAC address.
- interface-id_Specifies an interface ID. The interface ID can be one of the following types: Ethernet port or Port-channel.

Command Mode
Privileged EXEC mode

User Guidelines
Since the associated interface of a MAC address can be aged out from the FDB table, the Interface field can be empty.

If an ARP entry is associated with an IP interface that is defined on a port or port-channel, the VLAN field is empty.

Example
The following example displays entries in the ARP table.

```
Console# show arp

ARP timeout: 80000 Seconds

VLAN      Interface   IP Address    HW Address          Status
-------   ---------   ----------    -------------       -------
VLAN 1    gi1/0/1     10.7.1.102    00:10:B5:04:DB:4B   Dynamic
VLAN 1    gi1/0/2     10.7.1.135    00:50:22:00:2A:A4   Static
```

show arp configuration

Use the **show arp configuration** privileged EXEC command to display the global and interface configuration of the ARP protocol.

Syntax
show arp configuration

Parameters
This command has no arguments or key words.

Command Mode
Privileged EXEC mode

Example

```
Console# show arp configuration

Global configuration:
    ARP Proxy: enabled
ARP timeout:    80000 Seconds

Interface configuration:
g2:
    ARP Proxy: disabled
ARP timeout:60000 Seconds
VLAN 1:
    ARP Proxy: enabled
ARP timeout:70000 Seconds
VLAN 2:
    ARP Proxy: enabled
ARP timeout:80000 Second (Global)
```

interface ip

Use the **interface ip** Global Configuration mode command to enter the IP Interface Configuration mode.

Syntax
interface ip *ip-address*

Parameters
ip-address—Specifies one of the IP addresses of the device.

Command Mode
Global Configuration mode

Example
The following example enters the IP interface configuration mode.

```
Console (config)# interface ip 192.168.1.1
Console (config-ip)#
```

directed-broadcast

Use the **directed-broadcast** IP Interface Configuration mode command to enable the translation of a directed broadcast to physical broadcasts. Use the **no** form of this command to disable this function.

Syntax
directed-broadcast

no directed-broadcast

Default Configuration
Translation of a directed broadcast to physical broadcasts is disabled. All IP directed broadcasts are dropped.

Command Mode
IP Interface Configuration mode

Example
The following example enables the translation of a directed broadcast to physical broadcasts.

```
Console (config)# interface ip 192.168.1.1
Console (config-ip)# directed-broadcast
```

broadcast-address

Use the **broadcast-address** IP Interface Configuration mode command to define a broadcast address for an interface. Use the **no** form of this command to restore the default IP broadcast address.

Syntax

broadcast-address *{255.255.255.255 | 0.0.0.0}*

no broadcast-address

Parameters

- **255.255.255.255**—Specifies 255.255.255.255 as the broadcast address.
- **0.0.0.0**—Specifies 0.0.0.0 as the broadcast address.

Default Configuration

The default broadcast address is 255.255.255.255.

Command Mode

IP Interface Configuration mode

Example

The following example enables the translation of a directed broadcast to physical broadcasts.

```
Console(config)# interface ip 192.168.1.1
Console(config-ip)# broadcast-address 255.255.255.255
```

ip helper-address

Use the **ip helper-address** Global Configuration mode command to enable the forwarding of User Datagram Protocol (UDP) broadcast packets received on an interface to a specific (helper) address. Use the **no** form of this command to disable the forwarding of broadcast packets to a specific (helper) address.

Syntax

ip helper-address {*ip-interface* / *all*} *address* [*udp-port-list*]

no ip helper-address {*ip-interface* / *all*} *address*

Parameters

- **ip-interface**—Specifies the IP interface.
- **all**—Specifies all IP interfaces.
- **address**—Specifies the destination broadcast or host address to which to forward UDP broadcast packets. A value of 0.0.0.0 specifies that UDP broadcast packets are not forwarded to any host.
- **udp-port-list**—Specifies the destination UDP port number to which to forward broadcast packets. (Range: 1–65535)

Default Configuration

Forwarding of User Datagram Protocol (UDP) broadcast packets received on an interface to a specific (helper) address is disabled.

If **udp-port-list** is not specified, packets for the default services are forwarded to the helper address.

Command Mode

Global Configuration mode

User Guidelines

The **ip helper-address** command forwards specific UDP broadcast packets from one interface to another.

Many helper addresses may be defined. However, the total number of address-port pairs is limited to 128 for the device.

The setting of a helper address for a specific interface has precedence over the setting of a helper address for all the interfaces.

Forwarding of BOOTP/DHCP (ports 67, 68) cannot be enabled with this command. Use the DHCP relay commands to relay BOOTP/DHCP packets.

The **ip helper-address** command specifies a UDP port number to which UDP broadcast packets with that destination port number are forwarded. By

default, if no UDP port number is specified, the device forwards UDP broadcast packets for the following six services:

- IEN-116 Name Service (port 42)
- DNS (port 53)
- NetBIOS Name Server (port 137)
- NetBIOS Datagram Server (port 138)
- TACACS Server (port 49)
- Time Service (port 37)

Example
The following example enables the forwarding of User Datagram Protocol (UDP) broadcasts received on all interfaces to specific UDP ports of a destination IP address.

```
Console (config)# ip helper-address all 172.16.9.9 49 53
```

show ip helper-address

Use the **show ip helper-address** Privileged EXEC mode command to display the IP helper addresses configuration on the system.

Syntax
show ip helper-address

Parameters
This command has no arguments or key words.

Command Mode
Privileged EXEC mode

Example

The following example displays the IP helper addresses configuration on the system.

```
Console# show ip helper-address

Interface        Helper Address     Udp ports
------------     --------------     -----------------------
192.168.1.1      172.16.8.8         37, 42, 49, 53, 137, 138
192.168.2.1      172.16.9.9         37, 49
```

source-precedence

Use the **source-precedence** IP Interface Configuration mode command to define a preference for an IP address as a source IP address for DHCP relayed messages on an interface. Use the **no** form of this command to restore the default configuration.

Syntax

source-precedence

no source-precedence

Default Configuration

Source precedence is not defined for the address.

Command Mode

IP Interface Configuration mode

User Guidelines

For relayed DHCP messages, the source IP address selected is:

1. The lowest of the IP addresses defined as source-precedence IP addresses.
2. The lowest of the IP addresses if there are no source-precedence IP addresses.

Example
The following example defines a preference for an IP address as a source IP address for DHCP relayed messages on an interface.

```
Console (config-ip)# source-precedence
```

ip domain lookup

Use the **ip domain lookup** Global Configuration mode command to enable the IP Domain Name System (DNS)-based host name-to-address translation. Use the **no** form of this command to disable DNS-based host name-to-address translation.

Syntax
ip domain lookup

no ip domain lookup

Default Configuration
IP Domain Name System (DNS)-based host name-to-address translation is enabled.

Command Mode
Global Configuration mode

Example
The following example enables IP Domain Name System (DNS)-based host name-to-address translation.

```
Console(config)# ip domain lookup
```

ip domain name

Use the **ip domain name** Global Configuration mode command to define a default domain name used by the software to complete unqualified host names (names without a dotted-decimal domain name). Use the **no** form of this command to remove the default domain name.

Syntax

ip domain name *name*

no ip domain name

Parameters

name—Specifies the default domain name used to complete unqualified host names. Do not include the initial period that separates an unqualified name from the domain name. (Length: 1–158 characters. Maximum label length: 63 characters)

Default Configuration

A default domain name is not defined.

Command Mode

Global Configuration mode

User Guidelines

Domain names and host names are restricted to the ASCII letters A through Z (case-insensitive), the digits 0 through 9, the underscore and the hyphen. A period (.) is used to separate labels.

The maximum size of a label is 63 characters. The maximum name size is 158 bytes.

Example

The following example defines the default domain name as 'www.website.com'.

```
Console(config)# ip domain name www.website.com
```

ip name-server

Use the **ip name-server** Global Configuration mode command to define the available name servers. Use the **no** form of this command to remove a name server.

Syntax

ip name-server *{ server1-ipv4-address | server1-ipv6-address} [server-address2 … server-address8]*

no ip name-server [*server-address … server-address8*]

Parameters

server-address—IP addresses of the name server. Up to 8 servers can be defined in one command or by using multiple commands. The IP address can be IPv4 address or IPv6 address. When the IPv6 address is a Link Local address (IPv6Z address), the outgoing interface name must be specified. Refer to the User Guidelines for the interface name syntax.

Default Configuration

No name server IP addresses are defined.

Command Mode

Global Configuration mode

User Guidelines

The preference of the servers is determined by the order in which they were entered.

Up to 8 servers can be defined using one command or using multiple commands.

The format of an **IPv6Z address** is: <ipv6-link-local-address>%<interface-name>

interface-name = vlan<integer> | ch<integer> | isatap<integer> | <physical-port-name> | 0

integer = <decimal-number> | <integer><decimal-number>

decimal-number = 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9

physical-port-name= Designated port number, for example 1/0/16.

If the egress interface is not specified, the default interface is selected. Specifying interface zone=0 is equal to not defining an egress interface.

Example
The following example defines the available name server.

```
Console(config)# ip name-server 176.16.1.18
```

ip host
Use the **ip host** Global Configuration mode command to define the static host name-to-address mapping in the host cache. Use the **no** form of this command to remove the static host name-to-address mapping.

Syntax
ip host *name address* [*address2 address3 address4*]

no ip host *name*

Parameters
- **name**—Specifies the host name. (Length: 1–158 characters. Maximum label length: 63 characters)
- **address**—Specifies the associated IP address. Up to 4 addresses can be defined.

Default Configuration
No host is defined.

Command Mode
Global Configuration mode

User Guidelines
Host names are restricted to the ASCII letters A through Z (case-insensitive), the digits 0 through 9, the underscore and the hyphen. A period (.) is used to separate labels.

Example
The following example defines a static host name-to-address mapping in the host cache.

```
Console(config)# ip host accounting.website.com 176.10.23.1
```

clear host

Use the **clear host** Privileged EXEC mode command to delete entries from the host name-to-address cache.

Syntax

clear host *{name | *}*

Parameters

- **name**—Specifies the host entry to remove. (Length: 1–158 characters. Maximum label length: 63 characters)
- * —Removes all entries.

Command Mode

Privileged EXEC mode

Example

The following example deletes all entries from the host name-to-address cache.

```
Console# clear host *
```

clear host dhcp

Use the **clear host dhcp** Privileged EXEC mode command to delete entries from the host name-to-address mapping received from Dynamic Host Configuration Protocol (DHCP).

Syntax

clear host dhcp *{name | *}*

Parameters

- **name** —Specifies the host entry to remove. (Length: 1–158 characters. Maximum label length: 63 characters)

- *—Removes all entries.

Command Mode
Privileged EXEC mode

User Guidelines
This command deletes the host name-to-address mapping temporarily until the next refresh of the IP addresses.

Example
The following example deletes all entries from the host name-to-address mapping received from DHCP.

```
Console# clear host dhcp *
```

show hosts

Use the **show hosts** EXEC mode command to display the default domain name, the list of name server hosts, the static and the cached list of host names and addresses.

Syntax
show hosts *[name]*

Parameters
name—Specifies the host name. (Length: 1–158 characters. Maximum label length: 63 characters)

Command Mode
EXEC mode

Example

The following example displays host information.

```
Console> show hosts

System name: Device
Default domain is gm.com, sales.gm.com, usa.sales.gm.com(DHCP)
Name/address lookup is enabled
Name servers (Preference order): 176.16.1.18 176.16.1.19

Configured host name-to-address mapping:
Host                            Addresses
-----------------               ----------------------------
accounting.gm.com               176.16.8.8 176.16.8.9 (DHCP)
                                2002:0:130F::0A0:1504:0BB4


Host              Tota   Elapse  Type     Addresses
----------------  l      d       ----     -------------
www.stanford.edu  ----   ------  IP       171.64.14.203
                  -      -
                  72     3
```

39

IPv6 Addressing Commands

ipv6 enable

Use the **ipv6 enable** Interface Configuration (Ethernet, VLAN, Port-channel) mode command to enable the IPv6 addressing mode on an interface. Use the **no** form of this command to disable the IPv6 addressing mode on an interface.

Syntax

ipv6 enable *[no-autoconfig]*

no ipv6 enable

Parameters

no-autoconfig—EnableS processing of IPv6 on an interface without stateless address autoconfiguration procedure

Default Configuration

IPv6 addressing is disabled.

Unless you are using the no-autoconfig parameter, when the interface is enabled stateless address autoconfiguration procedure is enabled.

Command Mode

Interface Configuration (Ethernet, VLAN, Port-channel) mode. It cannot be configured for a range of interfaces (range context).

User Guidelines

The **ipv6 enable** command automatically configures an IPv6 link-local unicast address on the interface, while also enabling the interface for IPv6

processing. The **no ipv6 enable** command removes the entire IPv6 interface configuration.

To enable stateless address autoconfiguration on an enabled IPv6 interface, use the IPv6 address autoconfig command.

Example
The following example enables VLAN 1 for the IPv6 addressing mode.

```
Console(config)# interface vlan 1
Console(config-if)# ipv6 enable
```

ipv6 address autoconfig

Use the **ipv6 address autoconfig** Interface Configuration mode command to enable automatic configuration of IPv6 addresses, using stateless autoconfiguration on an interface. Addresses are configured depending on the prefixes received in Router Advertisement messages. Use the **no** form of this command to disable address autoconfiguration on the interface.

Syntax
ipv6 address *autoconfig*

no ipv6 address *autoconfig*

Parameters
Thiis command has no arguments or keywords.

Default Configuration
Address autoconfiguration is enabled on the interface, no addresses are assigned by default.

Command Mode
Interface Configuration (Ethernet, VLAN, Port-channel) mode.

User Guidelines

When **address autoconfig** is enabled, router solicitation ND procedure is initiated to discover a router and assign IP addresses to the interface, based on the advertised on-link prefixes.

When disabling address autoconfig, automatically generated addresses that are assigned to the interface are removed.

The default state of the address autoconfig is enabled. Use the **enable ipv6 no-autoconfig** command to enable an IPv6 interface without address autoconfig.

Example

```
console(config)# interface vlan 1
console(config-if)# ipv6 address autoconfig
```

ipv6 icmp error-interval

Use the **ipv6 icmp error-interval** Global Configuration mode command to configure the rate limit interval and bucket size parameters for IPv6 Internet Control Message Protocol (ICMP) error messages. Use the **no** form of this command to return the interval to its default setting.

Syntax

ipv6 icmp error-interval *milliseconds [bucketsize]*

no ipv6 icmp error-interval

Parameters

- **milliseconds**—The time interval between tokens being placed in the bucket. Each token represents a single ICMP error message. The acceptable range is from 0–2147483647 with a default of 100 milliseconds. Setting milliseconds to 0 disables rate limiting. (Range: 0– 2147483647)
- **bucketsize**—(Optional) The maximum number of tokens stored in the bucket. The acceptable range is from 1–200 with a default of 10 tokens.

Default Configuration
The default interval is 100ms and the default bucketsize is 10 i.e. 100 ICMP error messages per second

Command Mode
Global Configuration mode

User Guidelines
To set the average ICMP error rate limit, calculate the interval with the following formula:

Average Packets Per Second = (1/ interval) * bucket size

Example

```
console(config)# ipv6 icmp error-interval 123 45
```

show ipv6 icmp error-interval

Use the **show ipv6 error-interval** command in the EXEC mode to display the IPv6 ICMP error interval.

Syntax
show ipv6 icmp error-interval

Command Mode
EXEC mode

Example

```
Console> show ipv6 icmp error-interval
Rate limit interval: 100 ms
Bucket size: 10 tokens
```

ipv6 address

Use the **ipv6 address** Interface Configuration mode command to configure an IPv6 address for an interface. Use the **no** form of this command To remove the address from the interface.

Syntax

ipv6 address *ipv6-address/prefix-length [eui-64] [anycast]*

no ipv6 address *[ipv6-address/prefix-length] [eui-64]*

Parameters

- **ipv6-address**—Specifies the IPv6 network assigned to the interface. This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.
- **prefix-length**—Specifies the length of the IPv6 prefix. A decimal value that indicates how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address). A slash mark (/) must precede the decimal.
- **eui-64**—(Optional) Builds an interface ID in the low order 64 bits of the IPv6 address based on the interface MAC address.
- **anycast**—(Optional) Indicates that this address is an anycast address.
- **prefix-length**—3–128 (64 when the **eui-64** parameter is used.

Default Configuration

No IP address is defined for the interface.

Command Mode

Interface configuration (Ethernet, VLAN, Port-channel) mode. It cannot be configured for a range of interfaces (range context).

User Guidelines

If the value specified for the /prefix-length argument is greater than 64 bits, the prefix bits have precedence over the interface ID.

Using the no IPv6 address command without arguments removes all manually configured IPv6 addresses from an interface, including link local manually configured addresses.

Example

```
console(config)# interface vlan 1
console(config-if)# ipv6 address 3000::123/64 eui-64 anycast
```

ipv6 address link-local

Use the **ipv6 address link-local** command to configure an IPv6 link-local address for an interface. Use the **no** form of this command to return to the default link local address on the interface.

Syntax

ipv6 address *ipv6-address/prefix-length* **link-local**

no ipv6 address [i*pv6-address/prefix-length* **link-local**]

Parameters

- **ipv6-address**—Specifies the IPv6 network assigned to the interface.This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimals using 16-bit values between colons.
- **prefix-length**—Specifies the length of the IPv6 prefix. A decimal value indicates how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address). A slash mark (/) must precede the decimal. Only 64-bit length is supported, according to IPv6 over Ethernet's well-known practice

Default Configuration

IPv6 is enabled on the interface, link local address of the interface is FE80::EUI64 (interface MAC address).

Command Mode

Interface Configuration (Ethernet, VLAN, Port-channel) mode. It cannot be configured for a range of interfaces (range context).

User Guidelines

Using the **no ipv6 link-local address** command removes the manually configured link local IPv6 address from an interface. Multiple IPv6 addresses can be configured per interface, but only one link-local address. When the **no ipv6 link-local address** command is used, the interface is reconfigured with the standard link local address (the same IPv6 link-local address that is set automatically when the **enable ipv6** command is used). The system automatically generates a link-local address for an interface when IPv6 processing is enabled on the interface. To manually specify a link-local address to be used by an interface, use the **ipv6** link-local address command. The system supports only 64 bits prefix length for link-local addresses.

Example

```
console(config)# interface vlan 1
console(config-if)# ipv6 address fe80::123/64 link-local
```

ipv6 unreachables

Use the **ipv6 unreachables** Interface Configuration mode command to enable the generation of Internet Control Message Protocol for IPv6 (ICMPv6) unreachable messages for any packets arriving on a specified interface. Use the **no** form of this command To prevent the generation of unreachable messages.

Syntax

ipv6 unreachables

no ipv6 unreachables

Parameters

This command has no arguments or keywords.

Default Configuration

ICMP unreachable messages are sent by default.

Command Mode

Interface Configuration (Ethernet, VLAN, Port-channel) mode.

User Guidelines

When ICMP unreachable messages are enabled, when receiving a packet addressed to one of the interface's IP address with TCP/UDP port not assigned, the device sends ICMP unreachable messages. Use the **no ipv6 unreachables** command to disable sending ICMP unreachable messages on the interface.

Example

```
console(config)# interface gi1/0/1
console(config-if)# ipv6 unreachables
```

ipv6 default-gateway

Use the **ipv6 default-gateway** Global Configuration mode command to define an IPv6 default gateway. Use the **no** form of this command To remove the default gateway.

Syntax

ipv6 default-gateway *ipv6-address*

no ipv6 default-gateway

Parameters

ipv6-address—Specifies the IPv6 address of the next hop that can be used to reach that network. When the IPv6 address is a Link Local address (IPv6Z address), the outgoing interface name must be specified. Refer to the user guidelines for the interface name syntax.

Default Configuration

No default gateway is defined.

Command Mode

Global Configuration mode

User Guidelines

The format of an IPv6Z address is: <ipv6-link-local-address>%<interface-name>

interface-name = vlan<integer> | ch<integer> | <physical-port-name> | 0

integer = <decimal-number> | <integer><decimal-number>

decimal-number = 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9

physical-port-name = Designated port number, for example `1/0/`16.

Configuring a new default GW without deleting the previous configured information overwrites the previous configuration. A configured default GW has a higher precedence over automatically advertised (via router advertisement message). Precedence takes effect once the configured default GW is reachable. Reachability state is not verified automatically by the neighbor discovery protocol. Router reachability can be confirmed by either receiving Router Advertisement message containing router's MAC address or manually configured by user using the IPv6 neighbor CLI command. Another option to force reachability confirmation is to ping the router link-local address (this will initiate the neighbor discovery process).

If the egress interface is not specified, the default interface is selected. Specifying interface zone=0 is equal to not defining an egress interface.

Example

```
console(config)# ipv6 default-gateway fe80::abcd
```

show ipv6 interface

Use the **show ipv6 interface** EXEC command mode to display the usability status of interfaces configured for IPv6.

Syntax

show ipv6 interface *[interface-id]*

Parameters

interface-id—Specifies an interface ID. The interface ID can be one of the following types: Ethernet port, Port-channel or VLAN.

Default Configuration

Displays all IPv6 interfaces.

Command Mode
EXEC mode

User Guidelines
Use the s**how ipv6 neighbors** command in the privileged EXEC mode to display IPv6 neighbor discovery cache information.

Example

```
Console# show ipv6 interface
Interface    IP addresses                                Type
-----------  ----------------------------------------  ------------
VLAN 1       4004::55/64 [ANY]                         manual
VLAN 1       fe80::200:b0ff:fe00:0                     linklayer
VLAN 1       ff02::1                                   linklayer
VLAN 1       ff02::77                                  manual
VLAN 1       ff02::1:ff00:0                            manual
VLAN 1       ff02::1:ff00:1                            manual
VLAN 1       ff02::1:ff00:55                           manual

Default Gateway IP address     Type     Interface   State
---------------------------   -------- ---------   -----
fe80::77                      Static   VLAN 1     unreachable
fe80::200:cff:fe4a:dfa8       Dynamic  VLAN 1     stale

Console# show ipv6 interface Vlan 15
IPv6 is disabled

Console# show ipv6 interface Vlan 1
Number of ND DAD attempts: 1
MTU size: 1500
Stateless Address Autoconfiguration state: enabled
ICMP unreachable message state: enabled
MLD version: 2

IP addresses                            Type        DAD State
```

```
-----------------------------------  ---------   -----------
4004::55/64 [ANY]                    manual      Active
fe80::200:b0ff:fe00:0                linklayer   Active
ff02::1                              linklayer   ------
ff02::77                             manual      ------
ff02::1:ff00:0                       manual      ------
ff02::1:ff00:1                       manual      ------
ff02::1:ff00:55                      manual      ------
```

show IPv6 route

Use the **show ipv6 route** command to display the current state of the IPv6 routing table.

Syntax

show ipv6 route

Command Mode

EXEC mode

Example

```
Console> show ipv6 route
Codes: L - Local, S - Static, I - ICMP, ND - Router Advertisment
The number in the brackets is the metric.

S  ::/0 via fe80::77 [0] VLAN 1 Lifetime Infinite
ND ::/0 via fe80::200:cff:fe4a:dfa8 [0] VLAN 1 Lifetime 1784 sec
L  2001::/64 is directly connected, g2 Lifetime Infinite
L  2002:1:1:1::/64 is directly connected, VLAN 1 Lifetime 2147467 sec
L  3001::/64 is directly connected, VLAN 1 Lifetime Infinite
L  4004::/64 is directly connected, VLAN 1 Lifetime Infinite
L  6001::/64 is directly connected, g2 Lifetime Infinite
```

ipv6 nd dad attempts

Use the **ipv6 nd dad attempts** Interface Configuration (Ethernet, VLAN, Port-channel) mode command to configure the number of consecutive neighbor solicitation messages that are sent on an interface while Duplicate Address Detection (DAD) is performed on the unicast IPv6 addresses of the interface. Use the **no** form of this command to restore the number of messages to the default value.

Syntax

ipv6 nd dad attempts *attempts*

Parameters

attempts—Specifies the number of neighbor solicitation messages. A value of 0 disables DAD processing on the specified interface. A value of 1 configures a single transmission without follow-up transmissions. (Range: 0–600)

Default Configuration

Duplicate Address Detection on unicast IPv6 addresses with the sending of one neighbor solicitation message is enabled.

Command Mode

Interface Configuration (Ethernet, VLAN, Port-channel) mode. It cannot be configured for a range of interfaces (range context).

User Guidelines

Duplicate Address Detection (DAD) verifies the uniqueness of new unicast IPv6 addresses before the addresses are assigned to interfaces (the new addresses remain in a tentative state while DAD is performed). DAD uses neighbor solicitation messages to verify the uniqueness of unicast IPv6 addresses.

An interface returning to the administrative Up state restarts DAD for all of the unicast IPv6 addresses on the interface. While DAD is performed on the Link Local address of an interface, the state of the other IPv6 addresses is still set to TENTATIVE. When DAD is completed on the Link Local address, DAD is performed on the remaining IPv6 addresses.

When DAD identifies a duplicate address, the address state is set to DUPLICATE and the address is not used. If the duplicate address is the Link Local address of the interface, the processing of IPv6 packets is disabled on the interface and an error message is displayed.

All configuration commands associated with the duplicate address remain as configured while the address state is set to DUPLICATE.

If the Link Local address for an interface changes, DAD is performed on the new Link Local address and all of the other IPv6 address associated with the interface are regenerated (DAD is performed only on the new Link Local address).

Configuring a value of 0 with the **ipv6 nd dad attempts** Interface Configuration mode command disables duplicate address detection processing on the specified interface. A value of 1 configures a single transmission without follow-up transmissions. The default is 1 message.

Until the DAD process is completed, an IPv6 address is in the tentative state and cannot be used for data transfer. It is recommended to limit the configured value.

Example

The following example configures the number of consecutive neighbor solicitation messages sent during DAD processing to 2 on gigabitethernet port 1/0/9.

```
Console (config)# interface gigabitethernet 1/0/9
Console (config-if)# ipv6 nd dad attempts 2
```

ipv6 host

Use the **ipv6 host** Global Configuration mode command to define a static host name-to-address mapping in the host name cache. Use the **no** form of this command to remove the host name-to-address mapping.

Syntax

ipv6 host name *ipv6-address1 [ipv6-address2...ipv6-address4]*

no ipv6 host name

Parameters

nameName of the host. (Range: 1–158 characters)

- **ipv6-address1**—Associated IPv6 address. This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons. When the IPv6 address is a Link Local address (IPv6Z address), the outgoing interface name must be specified. Refer to the user guidelines for the interface name syntax.
- **ipv6-address2-4**—(Optional) Additional IPv6 addresses that may be associated with the host's name

Default Configuration

No host is defined.

Command Mode

Global Configuration mode

User Guidelines

The format of an IPv6Z address is: <ipv6-link-local-address>%<interface-name>

interface-name = vlan<integer> | ch<integer> | isatap<integer> | <physical-port-name>

integer = <decimal-number> | <integer><decimal-number>

decimal-number = 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9

physical-port-name = Designated port number, for example `1/0/16`.

Example

```
console(config)# ipv6 host server 3000::a31b
```

ipv6 neighbor

Use the **ipv6 neighbor** command to configure a static entry in the IPv6 neighbor discovery cache. Use the **no** form of this command to remove a static IPv6 entry from the IPv6 neighbor discovery cache.

Syntax

ipv6 neighbor *ipv6_addr interface-id hw_addr*

no ipv6 neighbor *ipv6_addr interface-id*

Parameters

- **Ipv6_addr**—Specifies the Pv6 address to map to the specified MAC address.
- **interface-id**—Specifies the interface that is associated with the IPv6 address
- **hw_addr**—Specifies the MAC address to map to the specified IPv6 address.

Command Mode

Global Configuration mode

User Guidelines

The **IPv6 neighbor** command is similar to the **ARP** (global) command.

If an entry for the specified IPv6 address already exists in the neighbor discovery cache—learned through the IPv6 neighbor discovery process—the entry is automatically converted to a static entry.

A new static neighbor entry with a global address can be configured only if a manually configured subnet already exists in the device.

Use the show **IPv6 neighbors** command to view static entries in the IPv6 neighbor discovery cache.

Example

```
console(config)# ipv6 neighbor 3000::a31b vlan 1 001b.3f9c.84ea
```

ipv6 set mtu

Use the **ipv6 mtu** Interface Configuration mode command to set the maximum transmission unit (MTU) size of IPv6 packets sent on an interface. Use the default parameter to restore the default MTU size.

Syntax

ipv6 set mtu *{ interface-id } { bytes | default}*

Parameters

- **interface-id**—Specifies an interface ID. The interface ID can be one of the following types: Ethernet port or Port-channel.
- **bytes**—Specifies the MTU in bytes.
- **default**—Sets the default MTU size 1500 bytes. Minimum is 1280 bytes

Default Configuration

1500 bytes

Command Mode

Privileged EXEC mode

User Guidelines

This command is intended for debugging and testing purposes and should be used only by technical support personnel.

Example

```
console# ipv6 set mtu gi1/0/1 default
```

ipv6 mld version

Use the **ipv6 mld version** Interface Configuration mode command to change the version of the Multicast Listener Discovery Protocol (MLD). Use the **no** form of this command to change to the default version.

Syntax

ipv6 mld version *{1 | 2}*

no ipv6 mld version

Parameters

1—Specifies MLD version 1.

2—Specifies MLD version 2.

Default Configuration
MLD version 1.

Command Mode
Interface Configuration (Ethernet, VLAN, Port-channel) mode

```
console(config)# interface vlan 1
console(config-if)# ipv6 mld version 2
```

ipv6 mld join-group

Use the **ipv6 mld join-group** Interface Configuration mode command to configure Multicast Listener Discovery (MLD) reporting for a specified group. Use the **no** form of this command to cancel reporting and leave the group.

Syntax
ipv6 mld join-group *group-address*

no ipv6 mld join-group *group-address*

Parameters
group-address—Specifies the IPv6 address of the multicast group.

Default Configuration

Command Mode
Interface Configuration (Ethernet, VLAN, Port-channel) mode

User Guidelines
The ipv6 mld join-group command configures MLD reporting for a specified group. The packets that are addressed to a specified group address will be passed up to the client process in the device.

Example
The following example configures MLD reporting for specific groups:

```
ipv6 mld join-group ff02::10
```

show ipv6 neighbors

Use the **show ipv6 neighbors** Privileged EXEC mode command to display IPv6 neighbor discovery cache information.

Syntax
show ipv6 neighbors *{static | dynamic}[ipv6-address ipv6-address] [mac-address mac-address] [interface-id]*

Parameters

- **static**—Shows static neighbor discovery cash entries.
- **dynamic**—Shows dynamic neighbor discovery cash entries.
- **ipv6-address**—Shows the neighbor discovery cache information entry of a specific IPv6 address.
- **mac-address**—Shows the neighbor discovery cache information entry of a specific MAC address.
- **interface-id**—Specifies an interface ID. The interface ID can be one of the following types: Ethernet port, Port-channel or VLAN.

Command Mode
Privileged EXEC mode

User Guidelines
Since the associated interface of a MAC address can be aged out from the FDB table, the Interface field can be empty.

When an ARP entry is associated with an IP interface that is defined on a port or port-channel, the VLAN field is empty.

The possible neighbor cash states are:

- INCMP (Incomplete)—Address resolution is being performed on the entry. Specifically, a Neighbor Solicitation has been sent to the solicited-node multicast address of the target, but the corresponding Neighbor Advertisement has not yet been received.
- REACH (Reachable)—Positive confirmation was received within the last ReachableTime milliseconds that the forward path to the neighbor was functioning properly. While REACHABLE, no special action takes place as packets are sent.
- STALE—More than ReachableTime milliseconds have elapsed since the last positive confirmation was received that the forward path was functioning properly. While stale, no action takes place until a packet is sent.
- DELAY—More than ReachableTime milliseconds have elapsed since the last positive confirmation was received that the forward path was functioning properly, and a packet was sent within the last DELAY_FIRST_PROBE_TIME seconds. If no reachability confirmation is received within DELAY_FIRST_PROBE_TIME seconds of entering the DELAY state, send a Neighbor Solicitation and change the state to PROBE.
- PROBE—A reachability confirmation is actively sought by retransmitting Neighbor Solicitations every RetransTimer milliseconds until a reachability confirmation is received.

Example

```
Console# show ipv6 neighbors dynamic

Interface     IPv6 address             HW address         State  Router
----------    -----------------------  ----------------   ------ ------
  VLAN 1      fe80::200:cff:fe4a:dfa8  00:00:0c:4a:df:a8  stale  yes
  VLAN 1      fe80::2d0:b7ff:fea1:264d 00:d0:b7:a1:26:4d  stale  no
```

clear ipv6 neighbors

Use the **clear ipv6 neighbors** Privileged EXEC mode command to delete all entries in the IPv6 neighbor discovery cache, except for static entries.

Syntax
clear ipv6 neighbors

Parameters
This command has no keywords or arguments.

Command Mode
Privileged EXEC mode

Example

```
console# clear ipv6 neighbors
```

40

Tunnel Commands

interface tunnel

Use the **interface tunnel** Global Configuration mode command to enter the Interface Configuration (Tunnel) mode.

Syntax
interface tunnel *number*

Parameters
number—Specifies the tunnel index.

Command Mode
Global Configuration mode

Example
The following example enters the Interface Configuration (Tunnel) mode.

```
Console(config)# interface tunnel 1
Console(config-tunnel)#
```

tunnel mode ipv6ip

Use the **tunnel mode ipv6ip** Interface Configuration (Tunnel) mode command to configure an IPv6 transition-mechanism global support mode. Use the **no** form of this command to remove an IPv6 transition mechanism.

Syntax
tunnel mode ipv6ip *{isatap}*

no tunnel mode *ipv6ip*

Parameters
isatap—Enables an automatic IPv6 over IPv4 Intra-Site Automatic Tunnel Addressing Protocol (ISATAP) tunnel.

Default Configuration
The IPv6 transition-mechanism global support mode is disabled.

Command Mode
Interface Configuration (Tunnel) mode

User Guidelines
The system can be enabled to ISATAP tunnel. When enabled, an automatic tunnel interface is created on each interface that is assigned an IPv4 address.

Note that on a specific interface (for example, port or VLAN), both native IPV6 and transition-mechanisms can coexist. The host implementation chooses the egress interface according to the scope of the destination IP address (such as ISATAP or native IPv6).

Example
The following example configures an IPv6 transition mechanism global support mode.

```
Console(config)# interface tunnel 1
Console(config-tunnel)# tunnel mode ipv6ip isatap
```

tunnel isatap router

Use the **tunnel isatap router** Interface Configuration (Tunnel) mode command to configure a global string that represents a specific automatic tunnel router domain name. Use the **no** form of this command to remove the string associated with the router domain name and restore the default configuration.

Syntax
tunnel isatap router *router-name*

no tunnel isatap router

Parameters
router-name—Specifies the router's domain name.

Default Configuration
The automatic tunnel router's default domain name is ISATAP.

Command Mode
Interface Configuration (Tunnel) mode

User Guidelines
The **ipv6 tunnel routers-dns** command determines the string that the host uses for automatic tunnel router lookup in the IPv4 DNS procedure. By default, the string ISATAP is used for the corresponding automatic tunnel types.

Only one string can represent the automatic tunnel router name per tunnel. Using this command, therefore, overwrites the existing entry.

Example
The following example configures the global string ISATAP2 as the automatic tunnel router domain name.

```
Console(config)# tunnel 1
Console(config-tunnel)# tunnel isatap router ISATAP2
```

tunnel source

Use the **tunnel source** Interface Configuration (Tunnel) mode command to set the local (source) IPv4 address of a tunnel interface. The **no** form deletes the tunnel local address.

Syntax
tunnel source *{ auto | ipv4-address }*

no tunnel source

Parameters

- **auto**—The system minimum IPv4 address is used as the source address for packets sent on the tunnel interface. If the IPv4 address is changed, then the local address of the tunnel interface is changed too.
- **ip4-address**—Specifies the IPv4 address to use as the source address for packets sent on the tunnel interface. The local address of the tunnel interface is not changed when the IPv4 address is moved to another interface (only if StackTable is changed).

Default
No source address is defined.

Command Mode
Interface Configuration (Tunnel) mode

User Guidelines
The configured source IPv4 address is used for forming the tunnel interface identifier. The interface identifier is set to the 8 least significant bytes of the SIP field of the encapsulated IPv6 tunneled packets.

Example

```
console(config)# interface tunnel 1
console(config-tunnel)# tunnel source auto
```

tunnel isatap query-interval

Use the **tunnel isatap query-interval** Global Configuration mode command to set the time interval between Domain Name System (DNS) queries (before the ISATAP router IP address is known) for the automatic tunnel router domain name. Use the **no** form of this command to restore the default configuration.

Syntax
tunnel isatap query-interval *seconds*

no tunnel isatap query-interval

Parameters
seconds—Specifies the time interval in seconds between DNS queries. (Range: 10–3600)

Default Configuration
The default time interval between DNS queries is 10 seconds.

Command Mode
Global Configuration mode

User Guidelines
This command determines the time interval between DNS queries before the ISATAP router IP address is known. If the IP address is known, the robustness level that is set by the **tunnel isatap robustness** Global Configuration mode command determines the refresh rate.

Example
The following example sets the time interval between DNS queries to 30 seconds.

```
Console(config)# tunnel isatap query-interval 30
```

tunnel isatap solicitation-interval
Use the **tunnel isatap solicitation-interval** Global Configuration mode command to set the time interval between ISATAP router solicitation messages. Use the **no** form of this command to restore the default configuration.

Syntax
tunnel isatap solicitation-interval *seconds*

no tunnel isatap solicitation-interval

Parameters
seconds—Specifies the time interval in seconds between ISATAP router solicitation messages. (Range: 10–3600)

Default Configuration
The default time interval between ISATAP router solicitation messages is 10 seconds.

Command Mode
Global Configuration mode

User Guidelines
This command determines the interval between router solicitation messages when there is no active ISATAP router. If there is an active ISATAP router, the robustness level set by the **tunnel isatap robustness** Global Configuration mode command determines the refresh rate.

Example
The following example sets the time interval between ISATAP router solicitation messages to 30 seconds.

```
Console(config)# tunnel isatap solicitation-interval 30
```

tunnel isatap robustness

Use the **tunnel isatap robustness** Global Configuration mode command to configure the number of DNS query/router solicitation refresh messages that the device sends. Use the **no** form of this command to restore the default configuration.

Syntax
tunnel isatap robustness *number*

no tunnel isatap robustness

Parameters
number—Specifies the number of DNS query/router solicitation refresh messages that the device sends. (Range: 1–20)

Default Configuration
The default number of DNS query/router solicitation refresh messages that the device sends is 3.

Command Mode
Global Configuration mode

User Guidelines
The DNS query interval (after the ISATAP router IP address is known) is the Time-To-Live (TTL) that is received from the DNS, divided by (Robustness + 1).

The router solicitation interval (when there is an active ISATAP router) is the minimum-router-lifetime that is received from the ISATAP router, divided by (Robustness + 1).

Example
The following example sets the number of DNS query/router solicitation refresh messages that the device sends to 5.

```
Console(config)# tunnel isatap robustness 5
```

show ipv6 tunnel

Use the **show ïpv6 tunnel** EXEC mode command to display information on the ISATAP tunnel.

Syntax
show ïpv6 tunnel

Command Mode
EXEC mode

Example
The following example displays information on the ISATAP tunnel.

```
Console> show ipv6 tunnel
Tunnel 1
--------

Tunnel status                    : DOWN
```

```
Tunnel protocol                  : NONE
Tunnel Local address type        : auto
Tunnel Local Ipv4 address        : 0.0.0.0
Router DNS name                  : ISATAP
Router IPv4 address              : 0.0.0.0
DNS Query interval               : 300 seconds
Min DNS Query interval           : 0 seconds
Router Solicitation interval     : 10 seconds
Min Router Solicitation interval : 0 seconds
Robustness                       : 2
```

41

DHCP Relay Commands

ip dhcp relay enable (Global)

Use the **ip dhcp relay enable** Global Configuration mode command to enable Dynamic Host Configuration Protocol (DHCP) relay features on the device. Use the **no** form of this command to disable the DHCP relay agent.

Syntax

ip dhcp relay enable

no ip dhcp relay enable

Default Configuration

DHCP relay features are disabled.

Command Mode

Global Configuration mode

Example

The following example enables DHCP features on the device.

```
Console(config)# ip dhcp relay enable
```

ip dhcp relay enable (Interface)

Use the **ip dhcp relay enable** Interface Configuration (VLAN, Ethernet, Port-channel) mode command to enable Dynamic Host Configuration Protocol (DHCP) relay features on the router. Use the **no** form of this command To disable the DHCP relay agent features.

Syntax

ip dhcp relay enable

no ip dhcp relay enable

Default Configuration

Disabled

Command Mode

Interface Configuration (VLAN) mode

Interface Configuration (VLAN, Ethernet, Port-channel) mode

User Guidelines

Enable DHCP relay globally before enabling DHCP relay on an interface.

Example

The following example enables DHCP features on VLAN 21.

```
Console(config)# interface vlan 21
Console(config-if)# ip dhcp relay enable
```

ip dhcp relay address (Global)

Use the **ip dhcp relay address** Global Configuration mode command to define the DHCP servers available for the DHCP relay. Use the **no** form of this command to remove servers from the list.

Syntax

ip dhcp relay address *ip-address*

no ip dhcp relay address [*ip-address*]

Parameters

ip-address—Specifies the DHCP server IP address. Up to 8 servers can be defined.

Default Configuration

No server is defined.

Command Mode
Global Configuration mode

Example
The following example defines the DHCP server on the device.

```
Console(config)# ip dhcp relay address 176.16.1.1
```

ip dhcp relay address (Interface)

Use the **ip dhcp relay address** Interface Configuration (VLAN, Ethernet, Port-channel) command to define the DHCP servers available by the DHCP relay for DHCP clients connected to the interface. Use the **no** form of this command to remove the server from the list.

Syntax
ip dhcp relay address *ip-address*

no ip dhcp relay address [*ip-address*]

Parameters
ip-address—Specifies the DHCP server IP address. Up to 8 servers can be defined.

Default Configuration
No server is defined.

Command Mode
Interface Configuration (VLAN, Ethernet, Port-channel) mode

User Guidelines
Use the i**p dhcp relay address** command to define a DHCP Server IP address per the interface. To define a few DHCP Servers, use the command a few times.

To remove a DHCP Server, use the **no** form of the command with the ip-address argument. The no form of the command without the ip-address argument deletes all DHCP servers defined per the interface.

You can use the command regardless if DHCP Relay is enabled on the interface.

Example
The following example defines the DHCP server on VLAN 21.

```
Console(config)# interface vlan 21
Console(config-if)# ip dhcp relay address 176.16.1.1
```

show ip dhcp relay

Use the **show ip dhcp relay** EXEC mode command to display the server addresses on the DHCP relay.

Syntax
show ip dhcp relay

Command Mode
EXEC mode

Example
The following example displays the server addresses on the DHCP relay.

```
Console> show ip dhcp relay

DHCP relay is globally enabled.

DHCP relay is enabled on VLANs: 1, 2
DHCP relay is enabled on ports: 1/1
DHCP relay is enabled on port-channels:

Servers: 172.16.1.11, 172.16.8.11
```

```
Console> show ip dhcp relay
```

```
DHCP relay is globally enabled.

DHCP relay is enabled on VLANs: 1, 2

Servers: 172.16.1.11, 172.16.8.11
```

ip dhcp information option

Use the **ip dhcp information option** Global Configuration command to enable DHCP option-82 data insertion. Use the **no** form of this command to disable DHCP option-82 data insertion.

Syntax

ip dhcp information option

no ip dhcp information option

Parameters

N/A

Default Configuration

DHCP option-82 data insertion is disabled.

Command Mode

Global Configuration mode

User Guidelines

DHCP option 82 would be enabled only if DHCP snooping or DHCP relay are enabled.

Example

The following example enable DHCP option-82 data insertion.

```
Console(config)# ip dhcp information option
```

show ip dhcp information option

The **show ip dhcp information option** EXEC mode command displays the DHCP Option 82 configuration.

Syntax

show ip dhcp information option

Command Mode

EXEC mode

Example

The following example displays the DHCP Option 82 configuration.

```
Console> show ip dhcp information option
Relay agent Information option is Enabled
```

42

DHCP Server Commands

ip dhcp server

Use the **ip dhcp server** Global Configuration mode command to enable the Dynamic Host Configuration Protocol (DHCP) server features on the device. Use the **no** form of this command to disable the DHCP server.

Syntax

ip dhcp server

no ip dhcp server

Default Configuration

The DHCP server is disabled.

Command Mode

Global Configuration mode

Example

The following example enables the DHCP server on the device:

```
Console(config)# ip dhcp server
```

ip dhcp pool host

Use the **ip dhcp pool host** Global Configuration mode command to configure a Dynamic Host Configuration Protocol (DHCP) static address on a DHCP Server and enter the DHCP Pool Host Configuration mode. Use the **no** form of this command to remove the address pool.

Syntax
ip dhcp pool host *name*

no ip dhcp pool host *name*

Parameters
name—Specifies the DHCP address pool name. It can be either a symbolic string (such as Engineering) or an integer (such as 8). (Length: 1–32 characters)

Default Configuration
DHCP hosts are not configured.

Command Mode
Global Configuration mode

User Guidelines
During execution of this command, the configuration mode changes to the DHCP Pool Configuration mode, which is identified by the (config-dhcp)# prompt. In this mode, the administrator can configure host parameters, such as the IP subnet number and default router list.

Example
The following example configures Station as the DHCP address pool:

```
Console(config)# ip dhcp pool host station
Console(config-dhcp)#
```

ip dhcp pool network

Use the **ip dhcp pool network** Global Configuration mode command to configure a Dynamic Host Configuration Protocol (DHCP) address pool on a DHCP Server and enter DHCP Pool Configuration mode. Use the **no** form of this command to remove the address pool.

Syntax
ip dhcp pool network *name*

no ip dhcp pool network *name*

Parameters
name—Specifies the DHCP address pool name. It can be either a symbolic string (such as 'engineering') or an integer (such as 8). (Length: 1–32 characters)

Default Configuration
DHCP address pools are not configured.

Command Mode
Global Configuration mode

User Guidelines
During execution of this command, the configuration mode changes to DHCP Pool Network Configuration mode, which is identified by the (config-dhcp)# prompt. In this mode, the administrator can configure pool parameters, such as the IP subnet number and default router list.

Example
The following example configures Pool1 as the DHCP address pool.

```
Console(config)# ip dhcp pool network pool1
Console(config-dhcp)#
```

address (DHCP Host)

Use the **address** DHCP Pool Host Configuration mode command to manually bind an IP address to a Dynamic Host Configuration Protocol (DHCP) client. Use the **no** form of this command to remove the IP address binding to the client.

Syntax
address *ip-address* {*mask* | *prefix-length*} *{client-identifier unique-identifier | hardware-address mac-address}*

no address

Parameters

- **address**—Specifies the client IP address.
- **mask**—Specifies the client network mask.
- **prefix-length**—Specifies the number of bits that comprise the address prefix. The prefix is an alternative way of specifying the client network mask. The prefix length must be preceded by a forward slash (/).
- **unique-identifier**—Specifies the distinct client identification in dotted hexadecimal notation: Each byte in a hexadecimal character string is two hexadecimal digits. Bytes are separated by a period or colon. For example, 01b7.0813.8811.66.
- **hardware-address**—Specifies the MAC address.

Default Configuration
DHCP hosts are not configured.

Command Mode
DHCP Pool Host Configuration mode

Example
The following example manually binds an IP address to a Dynamic Host Configuration Protocol (DHCP) client.

```
Console(config-dhcp)# address 10.12.1.99 255.255.255.0
01b7.0813.8811.66
```

address (DHCP Network)

Use the **address** DHCP Pool Network Configuration mode command to configure the subnet number and mask for a Dynamic Host Configuration Protocol (DHCP) address pool on DHCP Server. Use the **no** form of this command to remove the subnet number and mask.

Syntax
address *{network-number | low low-address high high-address} {mask | prefix-length}*
no address

Parameters

- **network-number**—Specifies the IP address of the DHCP address pool.
- **mask**—Specifies the pool network mask.
- **prefix-length**—Specifies the number of bits that comprise the address prefix. The prefix is an alternative way of specifying the client network mask. The prefix length must be preceded by a forward slash (/).
- **low** *l***ow-address**—Specifies the first IP address to use in the address range.
- **high high-address**—Specifies the last IP address to use in the address range.

Default Configuration

DHCP address pools are not configured.

If the low address is not specified, it defaults to the first IP address in the network.

If the high address is not specified, it defaults to the last IP address in the network.

Command Mode

DHCP Pool Network Configuration mode

Example

The following example configures the subnet number and mask for a Dynamic Host Configuration Protocol (DHCP) address pool on DHCP Server.

```
Console(config-dhcp)# address 10.12.1.0 255.255.255.0
```

lease

Use the **lease** DHCP Pool Network Configuration mode command to configure the time duration of the lease for an IP address that is assigned from a Dynamic Host Configuration Protocol (DHCP) Server to a DHCP client. Use the **no** form of this command to restore the default value.

Syntax

lease {*days* [{*hours*} [*minutes*]] / *infinite*}

no lease

Parameters

- **days**—Specifies the number of days in the lease.
- **hours**—Specifies the number of hours in the lease. A **days** value must be supplied before configuring an ***hours*** value.
- **minutes**—Specifies the number of minutes in the lease. A **days** value and an **hours** value must be supplied before configuring a **minutes** value.
- **infinite**—Specifies that the duration of the lease is unlimited.

Default Configuration

The default lease duration is 1 day.

Command Mode

DHCP Pool Network Configuration mode

Examples

The following example shows a 1-day lease.

```
Console(config-dhcp)# lease 1
```

The following example shows a one-hour lease.

```
Console(config-dhcp)# lease 0 1
```

The following example shows a one-minute lease.

```
Console(config-dhcp)# lease 0 0 1
```

The following example shows an infinite (unlimited) lease.

```
Console(config-dhcp)# lease infinite
```

client-name

Use the **client-name** DHCP Pool Host Configuration mode command to define the name of a DHCP client. The client name should not include the domain name. Use the **no** form of this command to remove the client name.

Syntax

client-name *name*

no client-name

Parameters

name—Specifies the client name, using standard ASCII characters. The client name should not include the domain name. For example, the name Mars should not be specified as mars.yahoo.com. (Length: 1–32 characters)

Command Mode

DHCP Pool Host Configuration mode

Default Coniguration

No client name is defined.

Example

The following example defines the string Client1 as the client name.

```
Console(config-dhcp)# client-name client1
```

default-router

Use the **default-router** DHCP Pool Configuration mode command to configure the default router list for a Dynamic Host Configuration Protocol (DHCP) client. Use the **no** form of this command to remove the default router list.

Syntax

default-router *ip-address* [*ip-address2 ... ip-address8*]

no default-router

Parameters
ip-address—Specifies the IP address of a router. One IP address is required, although up to eight addresses can be specified in one command line.

Command Mode
DHCP Pool Host Configuration mode

DHCP Pool Network Configuration mode

Default Configuration
No default router is defined.

User Guidelines
The router IP address should be on the same subnet as the client subnet.

Example
The following example specifies 10.12.1.99 as the default router IP address.

```
Console(config-dhcp)# default-router 10.12.1.99
```

dns-server

Use the **dns-server** DHCP Pool Configuration mode command to configure the Domain Name System (DNS) IP servers available to a Dynamic Host Configuration Protocol (DHCP) client. Use the **no** form of this command to remove the DNS server list.

Syntax
dns-server *ip-address* [*ip-address2 ... ip-address8*]

no dns-server

Parameters
ip-address—Specifies a DNS Server IP address. One IP address is required, although up to eight addresses can be specified in one command line.

Command Mode
DHCP Pool Host Configuration mode

DHCP Pool Network Configuration mode

Default Configuration
No DNS server is defined.

User Guidelines
If DNS IP servers are not configured for a DHCP client, the client cannot correlate host names to IP addresses.

Example
The following example specifies 10.12.1.99 as the client domain name server IP address.

```
Console(config-dhcp)# dns-server 10.12.1.99
```

domain-name

Use the **domain-name** DHCP Pool Configuration mode command to specify the domain name for a Dynamic Host Configuration Protocol (DHCP) client. Use the **no** form of this command to remove the domain name.

Syntax
domain-name *domain*

no domain-name

Parameters
domain—Specifies the DHCP client domain name string. (Length: 1–32 characters)

Command Mode
DHCP Pool Host Configuration mode

DHCP Pool Network Configuration mode

Default Configuration
No domain name is defined.

Example
The following example specifies yahoo.com as the DHCP client domain name string.

```
Console(config-dhcp)# domain-name yahoo.com
```

netbios-name-server

Use the **netbios-name-server** DHCP Pool Configuration mode command to configure the NetBIOS Windows Internet Naming Service (WINS) servers that are available to Microsoft Dynamic Host Configuration Protocol (DHCP) clients. Use the **no** form of this command to remove the NetBIOS name server list.

Syntax
netbios-name-server *ip-address* [*ip-address2 ... ip-address8*]

no netbios-name-server

Parameters
ip-address—Specifies the NetBIOS WINS name server IP address. One IP address is required, although up to eight addresses can be specified in one command line.

Command Mode
DHCP Pool Host Configuration mode

DHCP Pool Network Configuration mode

Default Configuration
No bios server is defined.

Example
The following example specifies the IP address of a NetBIOS name server available to the DHCP client.

```
Console(config-dhcp)# netbios-name-server 10.12.1.90
```

netbios-node-type

Use the **netbios-node-type** DHCP Pool Configuration mode command to configure the NetBIOS node type for Microsoft Dynamic Host Configuration Protocol (DHCP) clients. Use the **no** form of this command to remove the NetBIOS node type.

Syntax

netbios-node-type *{b-node | p-node | m-node | h-node}*

no netbios-node-type

Parameters

- **b-node**—Specifies the Broadcast NetBIOS node type.
- **p-node**—Specifies the Peer-to-peer NetBIOS node type.
- **m-node**—Specifies the Mixed NetBIOS node type.
- **h-node**—Specifies the Hybrid NetBIOS node type.

Command Mode

DHCP Pool Host Configuration mode

DHCP Pool Network Configuration mode

Default Configuration

No bios node type is defined.

Example

The following example specifies the client's NetBIOS type as hybrid.

```
Console(config-dhcp)# netbios node-type h-node
```

next-server

Use the **next-server** DHCP Pool Configuration mode command to configure the next server in the boot process of a Dynamic Host Configuration Protocol (DHCP) client. Use the **no** form of this command to remove the boot server.

Syntax

next-server *ip-address*

no next-server

Parameters

ip-address—Specifies the IP address of the next server in the boot process, which is typically a Trivial File Transfer Protocol (TFTP) server.

Default Configuration

If the **next-server** command is not used to configure a boot server list, the DHCP Server uses inbound interface helper addresses as boot servers.

Command Mode

DHCP Pool Host Configuration mode

DHCP Pool Network Configuration mode

Example

The following example specifies 10.12.1.99 as the IP address of the next server in the boot process.

```
Console(config-dhcp)# next-server 10.12.1.99
```

next-server-name

Use the **next-server-name** DHCP Pool Configuration mode command to configure the next server name in the boot process of a Dynamic Host Configuration Protocol (DHCP) client. Use the **no** form of this command to remove the boot server name.

Syntax

next-server-name *name*

no next-server-name

Parameters

name—Specifies the name of the next server in the boot process. (Length: 1–64 characters)

Command Mode
DHCP Pool Host Configuration mode

DHCP Pool Network Configuration mode

Default Configuration
No next server name is defined.

Example
The following example specifies www.bootserver.com as the name of the next server in the boot process of a DHCP client.

```
Console(config-dhcp)# next-server www.bootserver.com
```

bootfile

Use the **bootfile** DHCP Pool Configuration mode command to specify the default boot image file name for a Dynamic Host Configuration Protocol (DHCP) client. Use the **no** form of this command to delete the boot image file name.

Syntax
bootfile *filename*

no bootfile

Parameters
filename—Specifies the file name used as a boot image. (Length: 1–128 characters)

Command Mode
DHCP Pool Host Configuration mode

DHCP Pool Network Configuration mode

Example
The following example specifies boot_image_file as the default boot image file name for a DHCP client.

```
Console(config-dhcp)# bootfile boot_image_file
```

time-server

Use the **time-server** DHCP Pool Configuration mode command to specify the time servers list for a Dynamic Host Configuration Protocol (DHCP) client. Use the **no** form of this command to remove the time servers list.

Syntax
time-server *ip-address* [*ip-address2 ... ip-address8*]

no time-server

Parameters
ip-address—Specifies the IP address of a time server. One IP address is required, although up to eight addresses can be specified in one command line.

Command Mode
DHCP Pool Host Configuration mode

DHCP Pool Network Configuration mode

Default Configuration
No time server name is defined.

User Guidelines
The router IP address should be on the same subnet as the client subnet.

Example
The following example specifies 10.12.1.99 as the time server IP address.

```
Console(config-dhcp)# time-server 10.12.1.99
```

option

Use the **option** DHCP Pool Configuration mode command to configure the Dynamic Host Configuration Protocol (DHCP) Server options. Use the **no** form of this command to remove the options.

Syntax

option *code {ascii ascii-string | hex hex-string | ip ip-address}*

option ip-list *code ip-address1* [*ip-address2* ...]

no option *code*

Parameters

- **code**—Specifies the DHCP option code.
- **ascii ascii-string**—Specifies an NVT ASCII character string. ASCII character strings, which contain white space, must be delimited by quotation marks.
- **hex hex-string**—Specifies dotted hexadecimal data: Each byte in hexadecimal character strings is two hexadecimal digits. Bytes are separated by a period or colon.
- **ip ip-address**—Specifies an IP address.
- **ip-list**—Specifies that a list of IP addresses immediately follows the option code.
- *ip-address1* [*ip-address2* ...]—Specifies a list of one or more IP addresses.

Command Mode

DHCP Pool Host Configuration mode

DHCP Pool Network Configuration mode

User Guidelines

DHCP provides a framework for passing configuration information to hosts on a TCP/IP network. Configuration parameters and other control information are carried in tagged data items that are stored in the DHCP message options field. The data items themselves are also called options. The

current set of DHCP options are documented in RFC 2131, *Dynamic Host Configuration Protocol*.

For options in hexadecimal format, the string parameter should include all the bytes in the option value, including leading zeros.

Examples

The following example configures DHCP option 19, which specifies whether the client should configure its IP layer for packet forwarding. A value of 0 means disable Ip forwarding. A value of 1 means enable IP forwarding. IP forwarding is enabled in the following example.

```
Console(config-dhcp)# option 19 hex 01
```

The following example configures DHCP option 2, which specifies the offset of the client's subnet in seconds from Coordinated Universal Time (UTC). A value of 0xE10 in the following example indicates a location 1 hour east of the meridian.

```
Console(config-dhcp)# option 2 hex 00000E10
```

The following example configures DHCP option 72, which specifies the World Wide Web servers for DHCP clients. World Wide Web servers 172.16.3.252 and 172.16.3.253 are configured in the following example.

```
Console(config-dhcp)# option ip-list 72 172.16.3.252
172.16.3.253
```

ip dhcp excluded-address

Use the **ip dhcp excluded-address** Global Configuration mode command to specify the IP addresses that a Dynamic Host Configuration Protocol (DHCP) Server should not assign to DHCP clients. Use the **no** form of this command to remove the excluded IP addresses.

Syntax

ip dhcp excluded-address *low-address* [*high-address*]

no ip dhcp excluded-address *low-address* [*high-address*]

Parameters

- **low-address**—Specifies the excluded IP address, or first IP address in an excluded address range.
- **high-address**—Specifies the last IP address in the excluded address range.

Default Configuration
All IP pool addresses are assignable.

Command Mode
Global Configuration mode

User Guidelines
The DHCP Server assumes that all pool addresses can be assigned to clients. Use this command to exclude a single IP address or a range of IP addresses.

Example
The following example configures an excluded IP address range from 172.16.1.100 through 172.16.1.199.

```
Console(config)# ip dhcp excluded-address 172.16.1.100
172.16.1.199
```

ip dhcp ping enable

Use the **ip dhcp ping enable** Global Configuration mode command to enable the Dynamic Host Configuration Protocol (DHCP) Server to send ping packets before assigning the address to a requesting client. Use the **no** form of this command to prevent the server from pinging pool addresses.

Syntax
ip dhcp ping enable

no ip dhcp ping enable

Default Configuration
DHCP pinging is disabled.

Command Mode
Global Configuration mode

User Guidelines
The DHCP Server pings a pool address before assigning the address to a requesting client. If the ping is unanswered, the DHCP Server assumes (with a high probability) that the address is not in use and assigns the address to the requesting client.

Example
The following example enables the DHCP Server to send ping packets before assigning the address to a requesting client.

```
Console(config)# ip dhcp ping enable
```

ping enable

Use the **ping enable** DHCP Pool Network Configuration mode command to enable the Dynamic Host Configuration Protocol (DHCP) Server to send ping packets before assigning the address to a requesting client. Use the **no** form of this command to prevent the server from pinging pool addresses.

Syntax
ping enable

no ping enable

Default Configuration
The default configuration is set to enable.

Command Mode
DHCP Pool Network Configuration mode

User Guidelines
The DHCP Server pings a pool address before assigning the address to a requesting client. If the ping is unanswered, the DHCP Server assumes (with a high probability) that the address is not in use and assigns the address to the requesting client.

Example
The following example enables the DHCP Server to send ping packets before assigning the address to a requesting client.

```
Console(config-dhcp)# ping enable
```

ip dhcp ping count

Use the **ip dhcp ping count** Global Configuration mode command to specify the number of packets a Dynamic Host Configuration Protocol (DHCP) Server sends to a pool address as part of a ping operation. Use the **no** form of this command to restore the default configuration.

Syntax
ip dhcp ping count *number*

no ip dhcp ping count

Parameters
number—Specifies the number of ping packets that are sent before assigning the address to a requesting client. (Range: 1-10)

Default Configuration
A Dynamic Host Configuration Protocol (DHCP) Server sends two packets to a pool address as part of a ping operation.

Command Mode
Global Configuration mode

Example
The following example specifies that a DHCP Server sends five packets to a pool address as part of a ping operation.

```
Console(config)# ip dhcp ping count 5
```

ip dhcp ping timeout

The **ip dhcp ping timeout** Global Configuration mode command specifies the time interval during which a Dynamic Host Configuration Protocol (DHCP) Server waits for a ping reply from an address pool. To restore the default timeout, use the **no** form of this command.

Syntax

ip dhcp ping timeout *milliseconds*

no ip dhcp ping timeout

Parameters

milliseconds — Specifies the amount of time (in milliseconds) that the DHCP server waits for a ping reply before it stops attempting to reach a pool address for client assignment. The timeout range is 300-10000 milliseconds.

Default Configuration

The default timeout is 500 milliseconds.

Command Mode

Global Configuration mode

User Guidelines

This command specifies how long to wait for a ping reply (in milliseconds).

Example

The following example specifies that a DHCP Server waits 1 second for a ping reply from an address pool before it stops attempting to reach a pool address for client assignment.

```
Console(config)# ip dhcp ping timeout 1000
```

clear ip dhcp binding

The **clear ip dhcp binding** Privileged EXEC mode command deletes the dynamic address binding from the Dynamic Host Configuration Protocol (DHCP) Server database.

Syntax

clear ip dhcp binding {*address* | *}

Parameters

- *address* — Specifies the binding address to delete from the DHCP database.
- * — Clears all automatic bindings.

Command Mode

Privileged EXEC mode

User Guidelines

Typically, the address denotes the client IP address. If the asterisk (*) character is specified as the address parameter, DHCP clears all dynamic bindings.

Use the **no ip dhcp pool** Global Configuration mode command to delete a manual binding.

Example

The following example deletes the address binding 10.12.1.99 from a DHCP server database:

```
Console# clear ip dhcp binding 10.12.1.99
```

show ip dhcp

The **show ip dhcp** EXEC mode command displays the DHCP configuration.

Syntax

show ip dhcp

Command Mode
EXEC mode

Example
The following example displays the DHCP configuration.

```
Console> show ip dhcp

DHCP server is enabled.
DHCP ping packets is enabled with 2 retries and 500
milliseconds.
```

show ip dhcp excluded-addresses

The **show ip dhcp excluded-addresses** EXEC mode command displays the excluded addresses.

Syntax
show ip dhcp excluded-addresses

Command Mode
EXEC mode

Example
The following example displays the excluded addresses.

```
Console> show ip dhcp excluded-addresses
The number of excluded addresses ranges is 2
Excluded addresses:
10.1.1.212- 10.1.1.219, 10.1.2.212- 10.1.2.219
```

show ip dhcp pool host

The **show ip dhcp pool host** EXEC mode command displays the DHCP pool host configuration.

Syntax

show ip dhcp pool host [*address* | *name*]

Parameters

- *address* — Specifies the client IP address.
- *name* — Specifies the DHCP pool name. (Length: 1-32 characters)

Command Mode

EXEC mode

Example

The following example displays the DHCP pool host configuration.

```
Console> show ip dhcp pool host
The number of host pools is 1

Name           IP Address        Hardware Address    Client Identifier
---------      --------------    -----------------   -----------------
Station        172.16.1.11                           01b7.0813.8811.66

Console> show ip dhcp pool host station

Name           IP Address        Hardware Address    Client Identifier
---------      --------------    -----------------   -----------------
Station        172.16.1.11                           01b7.0813.8811.66
```

```
Mask: 255.255.0.0
Default router: 172.16.1.1
Client name: client1
DNS server: 10.12.1.99
Domain name: yahoo.com
NetBIOS name server: 10.12.1.90
NetBIOS node type: h-node
Next server: 10.12.1.99
Next-server-name: 10.12.1.100
Bootfile: Bootfile
Time server 10.12.1.99
Options:

Code            Value
----            -----
19              Ox01
```

show ip dhcp pool network

The **show ip dhcp pool network** EXEC mode command displays the DHCP network configuration.

Syntax

show ip dhcp pool network [*name*]

Parameters

name — Specifies the DHCP pool name. (Length: 1-32 characters)

Command Mode

EXEC mode

Example

```
Router> show ip dhcp pool network
The number of network pools is 2
Name Address range mask Lease
-------------------------------------------------
```

```
marketing 10.1.1.17-10.1.1.178 255.255.255.0 0d:12h:0m
finance 10.1.2.8-10.1.2.178 255.255.255.0 0d:12h:0m
Router> show ip dhcp pool network marketing
Name Address range mask Lease
-------------------------------- ------------------------
marketing 10.1.1.17-10.1.1.178 255.255.255.0 0d:12h:0m
Statistics:
All-range Available Free Pre-allocated Allocated Expired   Declined
---------- ---------   ----- -------------   --------- --------- --------
162 150 68 50 20        3         9
Default router: 10.1.1.1
Ping packets: enabled
DNS server: 10.12.1.99
Domain name: yahoo.com
NetBIOS name server: 10.12.1.90
NetBIOS node type: h-node
Next server: 10.12.1.99
Next-server-name: 10.12.1.100
Bootfile: Bootfile
Time server 10.12.1.99
Options:
Code Value
------------------
19 Ox01
```

show ip dhcp binding

Use the **show ip dhcp binding** EXEC mode command to display the specific one or all the address bindings on the Dynamic Host Configuration Protocol (DHCP) Server.

Syntax

show ip dhcp binding [*ip-address*]

Parameters

ip-address — Specifies the IP address

Command Mode
EXEC mode

Example
The following example displays the DHCP Server binding address parameters.

```
Router> show ip dhcp binding
DHCP server enabled
The number of used (all types) entries is 5
The number of pre-allocated entries is 1
The number of allocated entries is 1
The number of expired entries is 1
The number of declined entries is 2

IP address Hardware Address Lease Expiration Type    State
---------- ---------------- -------------    ------- ---------
1.16.1.11  00a0.9802.32de    Feb 01 1998     dynamic allocated
1.16.3.23  02c7.f801.0422    12:00AM         dynamic expired
1.16.3.24  02c7.f802.0422                    dynamic declined
1.16.3.25  02c7.f803.0422                    dynamic pre-allocated
1.16.3.26  02c7.f804.0422                    dynamic declined

Router> show ip dhcp binding 1.16.1.11
DHCP server enabled
The number of used (all types) entries is 5
The number of pre-allocated entries is 1
The number of allocated entries is 1
The number of expired entries is 1
The number of declined entries is 2

IP address Hardware Address Lease Expiration  Type    State
---------- ---------------- ----------------- ------- ---------
1.16.1.11  00a0.9802.32de    Feb 01 1998      dynamic allocated
                            12:00 AM
Router> show ip dhcp binding 1.16.3.24
```

```
DHCP server enabled
The number of used (all types) entries is 5
The number of pre-allocated entries is 1
The number of allocated entries is 1
The number of expired entries is 1
The number of declined entries is 2

IP address Hardware Address Lease Expiration   Type    State
---------- ----------------   ---------------  ------- ---------
1.16.3.24  02c7.f802.0422                      dynamic declined
```

The following table describes the significant fields shown in the display.

Field	Description
IP address	The host IP address as recorded on the DHCP Server.
Hardware address	The MAC address or client identifier of the host as recorded on the DHCP Server.
Lease expiration	The lease expiration date of the host IP address.
Type	The manner in which the IP address was assigned to the host.
State	The IP Address state.

show ip dhcp server statistics

Use the **show ip dhcp server statistics** EXEC command to display Dynamic Host Configuration Protocol (DHCP) Server statistics.

Syntax

show ip dhcp server statistics

Command Mode

EXEC mode

Example
The following example displays DHCP Server statistics

```
DHCP server enabled
The number of network pools is 6
The number of excluded pools is 2
The number of used (all types) entries is 7
The number of pre-allocated entries is 1
The number of allocated entries is 3
The number of static entries is 1
The number of dynamic entries is 1
The number of automatic entries is 1
The number of expired entries is 1
The number of declined entries is 2
```

show ip dhcp allocated

Use the **show ip dhcp allocated** EXEC mode command to display the specific one or all the allocated address on the Dynamic Host Configuration Protocol (DHCP) Server.

Syntax
show ip dhcp allocated *[ip-address]*

Parameters
ip-address — Specifies the IP address

Command Mode
EXEC mode

Example
The following example displays the DHCP Server allocated IP addresses.

```
Router> show ip dhcp allocated
DHCP server enabled
```

```
The number of allocated entries is 3
The number of static entries is 1
The number of dynamic entries is 1
The number of automatic entries is 1

IP address   Hardware address Lease expiration      Type
----------   --------------- --------------------  ---------
172.16.1.11  00a0.9802.32de   Feb 01 1998 12:00 AM  Dynamic
172.16.3.253 02c7.f800.0422   Infinite              Automatic
172.16.3.254 02c7.f800.0422   Infinite              Static

Router> show ip dhcp allocated 172.16.1.11
DHCP server enabled
The number of allocated entries is 2
The number of static entries is 0
The number of dynamic entries is 2

IP address   Hardware address Lease expiration      Type
----------   --------------- --------------------  --------
172.16.1.11  00a0.9802.32de   Feb 01 1998 12:00 AM  Dynamic


Router> show ip dhcp allocated 172.16.3.254
DHCP server enabled
The number of allocated entries is 2
The number of static entries is 0
The number of dynamic entries is 2

IP address   Hardware address Lease expiration      Type
----------   --------------- --------------------  -------
172.16.3.254 02c7.f800.0422   Infinite              Static
```

The following table describes the significant fields shown in the display.

Field	Description
IP address	The host IP address as recorded on the DHCP Server.
Hardware address	The MAC address or client identifier of the host as recorded on the DHCP Server.
Lease expiration	The lease expiration date of the host IP address.
Type	The manner in which the IP address was assigned to the host.

show ip dhcp declined

Use the **show ip dhcp declined** EXEC command to display the specific one or all the declined addresses on the Dynamic Host Configuration Protocol (DHCP) server.

Syntax

show ip dhcp declined *[ip-address]*

Parameters

ip-address—Specifies the IP address.

Command Mode

EXEC mode

Example

```
Router> show ip dhcp declined
DHCP server enabled

IP address Hardware address
172.16.1.11 00a0.9802.32de
172.16.3.254 02c7.f800.0422

Router> show ip dhcp declined 172.16.1.11
DHCP server enabled
```

```
IP address Hardware address
172.16.1.1100a0.9802.32de
172.16.1.12
```

show ip dhcp declined Field Descriptions

- **IP address**—The IP address of the host as recorded on the DHCP Server.
- **Hardware address**—The MAC address or client identifier of the host as recorded on the DHCP Server.

show ip dhcp expired

Use the **show ip dhcp expired** EXEC command to display the specific one or all the expired addresses on the Dynamic Host Configuration Protocol (DHCP) server.

Syntax

show ip dhcp expired *[ip-address]*

Parameters

ip-address—Specifies the IP.

Command Mode

EXEC mode

Example

```
Router> show ip dhcp expired
DHCP server enabled

IP address Hardware address
172.16.1.11 00a0.9802.32de
172.16.3.254 02c7.f800.0422

Router> show ip dhcp expired 172.16.1.11
DHCP server enabled
```

```
IP address Hardware address
172.16.1.1300a0.9802.32de
172.16.1.14
```

show ip dhcp expired Field Descriptions

- **IP address**—The IP address of the host as recorded on the DHCP Server.
- **Hardware address**—The MAC address or client identifier of the host as recorded on the DHCP Server.

show ip dhcp pre-allocated

Use the **show ip dhcp pre-allocated** EXEC command to display the specific one or all the pre-allocated addresses on the Dynamic Host Configuration Protocol (DHCP) server.

Syntax

show ip dhcp pre-allocated *[ip-address]*

Parameters

ip-address—Specifies the IP.

Command Mode

EXEC mode

Examples

```
Router> show ip dhcp pre-allocated
DHCP server enabled

IP address Hardware address
172.16.1.11 00a0.9802.32de
172.16.3.254 02c7.f800.0422


Router> show ip dhcp pre-allocated 172.16.1.11
DHCP server enabled
```

```
IP address Hardware address
172.16.1.1500a0.9802.32de
172.16.1.16
```

show ip dhcp declined Field Descriptions

- **IP address**—The IP address of the host as recorded on the DHCP Server.
- **Hardware address**—The MAC address or client identifier of the host as recorded on the DHCP Server.

43

IP Routing Protocol-Independent Commands

ip route

Use the **ip route** Global Configuration mode command to configure static routes. Use the **no** form of this command to remove static routes.

Syntax

ip route *prefix* {*mask* | *prefix-length*} *ip-address [metric distance] [reject-route]*

no ip route *prefix* {*mask* | *prefix-length*} [*ip-address*]

Parameters

- **prefix**—Specifies the IP address that is the IP route prefix for the destination IP.
- **mask**—Specifies the network subnet mask of the IP address prefix.
- **prefix-length**—Specifies the number of bits that comprise the IP address prefix. The prefix length must be preceded by a forward slash (/). (Range: 0–32)
- **ip-address**—Specifies the IP address or IP alias of the next hop that can be used to reach the network.
- **metric distance**—Specifies an administrative distance. (Range: 1–255)
- **reject-route**—Stops routing to the destination network via all gateways.

Default Configuration

The default administrative distance is 1.

Command Mode
Global Configuration mode

Example
The following example configures a static route with prefix 172.16.0.0, prefix length 16, and gateway 131.16.1.1.

```
Console(config)# ip route 172.16.0.0 /16 131.16.1.1
```

ip routing

Use the **ip routing** Global Configuration mode command to enable IPv4 Routing. Use the **no** format of the command to disable IPv4 Routing.

Syntax
ip routing

no ip routing

Default Configuration
Enabled by default.

Command Mode
Global Configuration mode

Default Configuration
No routing is defined

show ip route

Use the **show ip route** EXEC mode command to display the current routing table state.

Syntax
show ip route *[connected | static | {address address [mask | prefix-length] [longer-prefixes]}]*

Parameters

- **connected**—Displays connected routing entries only.
- **static**—Displays static routing entries only.
- **address address**—Specifies the address for which routing information is displayed.
- **mask**—Specifies the network subnet mask of the IP address.
- **prefix-length**—Specifies the number of bits that comprise the IP address prefix. The prefix length must be preceded by a forward slash (/). (Range: 1–32)
- **longer-prefixes**—Specifies that the **address** and **mask** pair becomes a prefix and any routes that match that prefix are displayed.

Command Mode

EXEC mode

Example

The following example displays the current routing table state.

```
Console> show ip route
console# show ip route
Maximum Parallel Paths: 1 (1 after reset)
IP Forwarding:          enabled

Codes: C - connected, S - static, D - DHCP

S  0.0.0.0/0          [1/1] via  10.5.234.254  119:9:27   vlan 1
C  10.5.234.0/24      is directly connected              vlan 1
Console> show ip route address 172.1.1.0 255.255.255.0

Codes: C - connected, S - static, E - OSPF external, * -
candidate default

S 172.1.1.0/24 [5/3] via 10.0.2.1, 17:12:19, Ethernet1
```

```
Console> show ip route address 172.1.1.0 255.255.255.0 longer-
prefixes
Codes: C - connected, S - static, E - OSPF external

S 172.1.1.0/24 [5/3] via 10.0.2.1, 17:12:19, Ethernet1
S 172.1.1.1/32 [5/3] via 10.0.3.1, 19:51:18, Ethernet1
```

The following table describes the significant fields shown in the display:

Field	Description
O	The protocol that derived the route.
10.8.1.0/24	The remote network address.
[30/2000]	The first number in the brackets is the administrative distance of the information source; the second number is the metric for the route.
via 10.0.1.2	The address of the next router to the remote network.
00:39:08	The last time the route was updated, in hours:minutes:seconds.
Ethernet 1	The interface through which the specified network can be reached.

44

ACL Commands

Use the **ip access-list** global configuration mode command to define an IPv4 access list and to place the device in IPv4 access list configuration mode. Use the **no** form of this command to remove the access list.

Syntax

ip access-list extended *access-list-name*

no ip access-list extended *access-list-name*

Parameters

- **access-list-name**—Name of the IPv4 access list.
- **access-list-name**—0–32 characters. (Use "" for empty string)

Default

No IPv4 access list is defined.

Command Mode

Global Configuration mode

User Guidelines

IPv4 ACL is defined by a unique name. IPv4 ACL, IPv6 ACL, MAC ACL or Policy Map cannot have the same name.

Example

```
console(config)# ip access-list extended server
```

permit (IP)

Use the **permit** IP Access-list Configuration mode command to set permit conditions for IPv4 access list.

Syntax

permit *protocol {any | source source-wildcard} {any | destination destination-wildcard} [dscp number | precedence number] [time-range time-range-name]*

permit *icmp {any | source source-wildcard} {any | destination destination-wildcard} [any | icmp-type] [any | icmp-code]] [dscp number | precedence number] [time-range time-range-name]*

permit *igmp {any | source source-wildcard} {any | destination destination-wildcard}[igmp-type] [dscp number | precedence number] [time-range time-range-name]*

permit tcp *{any | source source-wildcard} {any|source-port/port-range}{any | destination destination-wildcard} {any|destination-port/port-range } [dscp number | precedence number] [match-all list-of-flags] [time-range time-range-name]*

permit udp *{any | source source-wildcard} {any|source-port/port-range} {any | destination destination-wildcard} {any|destination-port/port-range } [dscp number | precedence number] [match-all time-range-name] [time-range time-range-name]*

Parameters

- **protocol**—The name or the number of an IP protocol. Available protocol names icmp, igmp, ip, tcp, egp, igp, udp, hmp, rdp, idpr, ipv6, ipv6:rout, ipv6:frag, idrp, rsvp, gre, esp, ah, ipv6:icmp, eigrp, ospf, ipinip, pim, l2tp, isis. To match any protocol use the ip keyword.(Range: 0–255)
- **source**—Source IP address of the packet.
- **source-wildcard**—Wildcard bits to be applied to the source IP address. Use ones in the bit position that you want to be ignored.
- **destination**—Destination IP address of the packet.
- **destination-wildcard**—Wildcard bits to be applied to the destination IP address. Use ones in the bit position that you want to be ignored.

- **dscp number**—Specifies the DSCP value.
- **precedence number**—Specifies the IP precedence value.
- **icmp-type**—Specifies an ICMP message type for filtering ICMP packets. Enter a number or one of the following values: echo-reply, destination-unreachable, source-quench, redirect, alternate-host-address, echo-request, router-advertisement, router-solicitation, time-exceeded, parameter-problem, timestamp, timestamp-reply, information-request, information-reply, address-mask-request, address-mask-reply, traceroute, datagram-conversion-error, mobile-host-redirect, mobile-registration-request, mobile-registration-reply, domain-name-request, domain-name-reply, skip, photuris. (Range: 0–255)
- **icmp-code**—Specifies an ICMP message code for filtering ICMP packets. (Range: 0–255)
- **igmp-type**—IGMP packets can be filtered by IGMP message type. Enter a number or one of the following values: host-query, host-report, dvmrp, pim, cisco-trace, host-report-v2, host-leave-v2, host-report-v3. (Range: 0–255)
- **destination-port**—Specifies the UDP/TCP destination port. You can enter range of ports by using hyphen. E.g. 20 - 21. For TCP enter a number or one of the following values: bgp (179), chargen (19), daytime (13), discard (9), domain (53), drip (3949), echo (7), finger (79), ftp (21), ftp-data (20), gopher (70), hostname (42), irc (194), klogin (543), kshell (544), lpd (515), nntp (119), pop2 (109), pop3 (110), smtp (25), sunrpc (1110, syslog (514), tacacs-ds (49), talk (517), telnet (23), time (37), uucp (117), whois (43), www (80). For UDP enter a number or one of the following values: biff (512), bootpc (68), bootps (67), discard (9), dnsix (90), domain (53), echo (7), mobile-ip (434), nameserver (42), netbios-dgm (138), netbios-ns (137), on500-isakmp (4500), ntp (123), rip (520), snmp (161), snmptrap (162), sunrpc (111), syslog (514), tacacs-ds (49), talk (517), tftp (69), time (37), who (513), xdmcp (177).(Range: 0–65535).
- **source-port**—Specifies the UDP/TCP source port. Predefined port names are defined in the destination-port parameter. (Range: 0–65535)
- **match-all list-of-flags**—List of TCP flags that should occur. If a flag should be set, it is prefixed by "+". If a flag should be unset, it is prefixed by "-". Available options are +urg, +ack, +psh, +rst, +syn, +fin, -urg, -

ack, -psh, -rst, -syn and -fin. The flags are concatenated to a one string. For example: +fin-ack.

- **time-range-name**—Name of the time range that applies to this permit statement. (Range: 1–32)

Default

No IPv4 access list is defined.

Command Mode

IP Access-list Configuration mode

User Guidelines

You enter IP-access list configuration mode by using the IP Access-list Global Configuration command.

After an access control entry (ACE) is added to an access control list, an implied deny any any condition exists at the end of the list. That is, if there are no matches, the packets are denied. However, before the first ACE is added, the list permits all packets.

The number of TCP/UDP ranges that can be defined in ACLs is limited. You can define up to #ASIC-specific ranges for TCP and up to #ASIC-specific ranges for UDP. If a range of ports is used for source port in ACE it would be not be counted again if it is also used for source port in another ACE. If a range of ports is used for destination port in ACE it would be not be counted again if it is also used for destination port in another ACE.

If a range of ports is used for source port it would be counted again if it is also used for destination port.

Example

```
console(config)# ip access-list extended server
console(config-ip-al)# permit ip 1.1.1.0 0.0.0.255 1.1.2.0 0.0.0.0
```

deny (IP)

Use the **deny** IP Access-list Configuration mode command to set deny conditions for IPv4 access list.

Syntax

deny *protocol {any | source source-wildcard} {any | destination destination-wildcard} [dscp number | precedence number] [time-range time-range-name] [disable-port | log-input]*

deny *icmp {any | source source-wildcard} {any | destination destination-wildcard{any|icmp-type} {any|icmp-code} [dscp number | precedence number] [time-range time-range-name] [disable-port | log-input*]

deny *igmp {any | source source-wildcard} {any | destination destination-wildcard}[igmp-type] [dscp number | precedence number] [time-range time-range-name] [disable-port | log-input]*

deny *tcp {any | source source-wildcard} {any|source-port/port-range}{any | destination destination-wildcard} {any|destination-port/port-range } [dscp number | precedence number] [match-all list-of-flags] [time-range time-range-name] [disable-port | log-input]*

deny *udp {any | source source-wildcard} {any|source-port/port-range} {any | destination destination-wildcard} {any|destination-port/port-range } [dscp number | precedence number] [match-all time-range-name] [time-range time-range-name] [disable-port | log-input]*

Parameters

- **protocol**—The name or the number of an IP protocol. Available protocol names: icmp, igmp, ip, tcp, egp, igp, udp, hmp, rdp, idpr, ipv6, ipv6:rout, ipv6:frag, idrp, rsvp, gre, esp, ah, ipv6:icmp, eigrp, ospf, ipinip, pim, l2tp, isis. To match any protocol use the Ip keyword. (Range: 0–255)
- **source**—Source IP address of the packet.
- **source-wildcard**—Wildcard bits to be applied to the source IP address. Use 1s in the bit position that you want to be ignored.
- **destination**—Destination IP address of the packet.
- **destination-wildcard**—Wildcard bits to be applied to the destination IP address. Use 1s in the bit position that you want to be ignored.
- **dscp number**—Specifies the DSCP value.
- **precedence number**—Specifies the IP precedence value.
- **icmp-type**—Specifies an ICMP message type for filtering ICMP packets. Enter a number or one of the following values: echo-reply, destination-unreachable, source-quench, redirect, alternate-host-address, echo-request, router-advertisement, router-solicitation, time-exceeded,

parameter-problem, timestamp, timestamp-reply, information-request, information-reply, address-mask-request, address-mask-reply, traceroute, datagram-conversion-error, mobile-host-redirect, mobile-registration-request, mobile-registration-reply, domain-name-request, domain-name-reply, skip, photuris. (Range: 0–255)

- **icmp-code**—Specifies an ICMP message code for filtering ICMP packets. (Range: 0–255)
- **igmp-type**—IGMP packets can be filtered by IGMP message type. Enter a number or one of the following values: host-query, host-report, dvmrp, pim, cisco-trace, host-report-v2, host-leave-v2, host-report-v3. (Range: 0–255)
- **destination-port**—Specifies the UDP/TCP destination port. You can enter range of ports by using hyphen. E.g. 20 - 21. For TCP enter a number or one of the following values: bgp (179), chargen (19), daytime (13), discard (9), domain (53), drip (3949), echo (7), finger (79), ftp (21), ftp-data (20), gopher (70), hostname (42), irc (194), klogin (543), kshell (544), lpd (515), nntp (119), pop2 (109), pop3 (110), smtp (25), sunrpc (1110, syslog (514), tacacs-ds (49), talk (517), telnet (23), time (37), uucp (117), whois (43), www (80). For UDP enter a number or one of the following values: biff (512), bootpc (68), bootps (67), discard (9), dnsix (90), domain (53), echo (7), mobile-ip (434), nameserver (42), netbios-dgm (138), netbios-ns (137), non500-isakmp (4500), ntp (123), rip (520), snmp 161), snmptrap (162), sunrpc (111), syslog (514), tacacs-ds (49), talk (517), tftp (69), time (37), who (513), xdmcp (177). (Range: 0–65535)
- **source-port**—Specifies the UDP/TCP source port. Predefined port names are defined in the destination-port parameter. (Range: 0–65535)
- **match-all list-of-flags**—List of TCP flags that should occur. If a flag should be set it is prefixed by "+".If a flag should be unset it is prefixed by "-". Available options are +urg, +ack, +psh, +rst, +syn, +fin, -urg, -ack, -psh, -rst, -syn and -fin. The flags are concatenated to a one string. For example: +fin-ack.
- **time-range-name**—Name of the time range that applies to this permit statement. (Range: 1–32)
- **disable-port**—The Ethernet interface is disabled if the condition is matched.

- **log-input**—Specifies sending an informational syslog message about the packet that matches the entry. Because forwarding is done in hardware and logging is done in software, if a large number of packets match a deny ACE containing a log-input keyword, the software might not be able to match the hardware processing rate, and not all packets will be logged.

Default

No IPv4 access list is defined.

Command Mode

IP Access-list Configuration mode

User Guidelines

You enter IP-access list configuration mode by using the IP Access-list Global Configuration command.

After an access control entry (ACE) is added to an access control list, an implied deny any any condition exists at the end of the list. That is, if there are no matches, the packets are denied. However, before the first ACE is added, the list permits all packets.

The number of TCP/UDP ranges that can be defined in ACLs is limited. You can define up to #ASIC-specific ranges for TCP and up to #ASIC-specific ranges for UDP. If a range of ports is used for source port in ACE it would be not be counted again if it is also used for source port in another ACE. If a range of ports is used for destination port in ACE it would be not be counted again if it is also used for destination port in another ACE.

If a range of ports is used for source port, it would be counted again if it is also used for destination port.

Example

```
console(config)# ip access-list extended server
console(config-ip-al)# deny ip 1.1.1.0 0.0.0.255 1.1.2.0 0.0.0.0
```

ipv6 access-list

Use the **ipv6 access-list** global configuration mode command to define an IPv6 access list and to place the device in IPv6 access list configuration mode. Use the **no** form of this command to remove the access list.

Syntax

ipv6 access-list [*access-list-name]*

no ipv6 access-list *[access-list-name]*

Parameters

- **access-list-name**—Name of the IPv6 access list.
- **access-list-name**—0–32 characters (use "" for empty string)

Default

No IPv6 access list is defined.

Command Mode

Global Configuration mode

User Guidelines

IPv6 ACL is defined by a unique name. IPv4 ACL, IPv6 ACL, MAC ACL or Policy Map cannot have the same name.

Every IPv6 ACL has implicit permit icmp any any nd-ns any, permit icmp any any nd-na any, and deny ipv6 any any statements as its last match conditions. (The former two match conditions allow for ICMPv6 neighbor discovery.)

The IPv6 neighbor discovery process makes use of the IPv6 network layer service, therefore, by default, IPv6 ACLs implicitly allow IPv6 neighbor discovery packets to be sent and received on an interface. In IPv4, the Address Resolution Protocol (ARP), which is equivalent to the IPv6 neighbor discovery process, makes use of a separate data link layer protocol; therefore, by default, IPv4 ACLs implicitly allow ARP packets to be sent and received on an interface.

Example

```
Switch (config)# ipv6 access-list acl1
Switch(config-ipv6-acl)# permit tcp 2001:0DB8:0300:0201::/64 any any 80
```

permit (IPv6)

Use the **permit** command in IPv6 Access-list Configuration mode to set permit conditions for IPv6 access list.

Syntax

permit *protocol {any |{source-prefix/length }{any | destination-prefix/length } [dscp number | precedence number] [time-range time-range-name]*

permit *icmp {any | {source-prefix/length }{any | destination- prefix/length } {any|icmp-type} {any|icmp-code} [dscp number | precedence number] [time-range time-range-name]*

permit *tcp {any | {source-prefix/length } {any | source-port/port-range} }{any | destination- prefix/length } {any| destination-port/port-range} [dscp number | precedence number] [match-all list-of-flags] [time-range time-range-name]*

permit *udp {any | {source-prefix/length }} {any | source-port/port-range} }{any | destination- prefix/length } {any| destination-port/port-range} [dscp number | precedence number] [time-range time-range-name]*

Parameters

- **protocol**—The name or the number of an IP protocol. Available protocol names are: icmp (58), tcp (6) and udp (17). To match any protocol, use the ipv6 keyword. (Range: 0–255)
- **source-prefix/length**—The source IPv6 network or class of networks about which to set permit conditions. This argument must be in the form documented in RFC 3513 where the address is specified in hexadecimal using 16-bit values between colons.
- **destination-prefix/length**—The destination IPv6 network or class of networks about which to set permit conditions. This argument must be in the form documented in RFC 3513 where the address is specified in hexadecimal using 16-bit values between colons.
- **dscp number**—Specifies the DSCP value. (Range: 0–63)

- **precedence number**—Specifies the IP precedence value.
- **icmp-type**—Specifies an ICMP message type for filtering ICMP packets. Enter a number or one of the following values: destination-unreachable (1), packet-too-big (2), time-exceeded (3), parameter-problem (4), echo-request (128), echo-reply (129), mld-query (130), mld-report (131), mldv2-report (143), mld-done (132), router-solicitation (133), router-advertisement (134), nd-ns (135), nd-na (136). (Range: 0–255)
- **icmp-code**—Specifies an ICMP message code for filtering ICMP packets. (Range: 0–255)
- **destination-port**—Specifies the UDP/TCP destination port. You can enter a range of ports by using a hyphen. E.g. 20 - 21. For TCP enter a number or one of the following values: bgp (179), chargen (19), daytime (13), discard (9), domain (53), drip (3949), echo (7), finger (79), ftp (21), ftp-data (20), gopher (70), hostname (42), irc (194), klogin (543), kshell (544), lpd (515), nntp (119), pop2 (109), pop3 (110), smtp (25), sunrpc (1110, syslog (514), tacacs-ds (49), talk (517), telnet (23), time (37), uucp (117), whois (43), www (80). For UDP enter a number or one of the following values: biff (512), bootpc (68), bootps (67), discard (9), dnsix (90), domain (53), echo (7), mobile-ip (434), nameserver (42), netbios-dgm (138), netbios-ns (137), non500-isakmp (4500), ntp (123), rip (520), snmp (161), snmptrap (162), sunrpc (111), syslog (514), tacacs (49), talk (517), tftp (69), time (37), who (513), xdmcp (177). (Range: 0–65535)
- **source-port**—Specifies the UDP/TCP source port. Predefined port names are defined in the destination-port parameter. (Range: 0–65535)
- **match-all list-of-flag**—List of TCP flags that should occur. If a flag should be set it is prefixed by "+".If a flag should be unset it is prefixed by "-". Available options are +urg, +ack, +psh, +rst, +syn, +fin, -urg, -ack, -psh, -rst, -syn and -fin. The flags are concatenated to a one string. For example: +fin-ack.
- **time-range-name**—Name of the time range that applies to this permit statement. (Range: 1–32)

Default

No IPv6 access list is defined.

Command Mode
Ipv6 Access-list Configuration mode

User Guidelines
The number of TCP/UDP ranges that can be defined in ACLs is limited. You can define up to #ASIC-specific ranges for TCP and up to #ASIC-specific ranges for UDP. If a range of ports is used for a source port in ACE it would be not be counted again if it is also used for a source port in another ACE. If a range of ports is used for destination port in ACE it would be not be counted again if it is also used for destination port in another ACE.

If a range of ports is used for source port it would be counted again if it is also used for destination port.

Example

```
console(config)# ipv6 access-list server
console(config-ipv6-al)# permit tcp 3001::2/64 any any 80
```

deny (IPv6)

Use the **deny** command in IPv6 access list configuration mode to set permit conditions for IPv6 access list.

Syntax
deny *protocol {any | {source-prefix/length }{any | destination- prefix/length } [dscp number | precedence number] [time-range time-range-name] [disable-port | log-input]*

deny *icmp {any | {source-prefix/length }{any | destination- prefix/length } {any|icmp-type} {any|icmp-code} [dscp number | precedence number] [time-range time-range-name] [disable-port | log-input]*

deny *tcp {any | {source-prefix/length } {any | source-port/port-range} }{any | destination- prefix/length } {any| destination-port/port-range} [dscp number | precedence number] [match-all list-of-flags] [time-range time-range-name] [disable-port | log-input]*

deny *udp {any | {source-prefix/length }} {any | source-port/port-range} }{any | destination- prefix/length } {any| destination-port/port-range} [dscp number | precedence number] [time-range time-range-name] [disable-port | log-input]*

Parameters

- **protocol**—The name or the number of an IP protocol. Available protocol names are: icmp (58), tcp (6) and udp (17). To match any protocol use the ipv6 keyword. (Range: 0–255)
- **source-prefix/length**—The source IPv6 network or class of networks about which to set permit conditions. This argument must be in the form documented in RFC 3513 where the address is specified in hexadecimal using 16-bit values between colons.
- **destination-prefix/length**—The destination IPv6 network or class of networks about which to set permit conditions. This argument must be in the form documented in RFC 3513 where the address is specified in hexadecimal using 16-bit values between colons.
- **dscp number**—Specifies the DSCP value. (Range: 0–63)
- **precedence number**—Specifies the IP precedence value.
- **icmp-type**—Specifies an ICMP message type for filtering ICMP packets. Enter a number or one of the following values: destination-unreachable (1), packet-too-big (2), time-exceeded (3), parameter-problem (4), echo-request (128), echo-reply (129), mld-query (130), mld-report (131), mldv2-report (143), mld-done (132), router-solicitation (133), router-advertisement (134), nd-ns (135), nd-na (136). (Range: 0–255)
- **icmp-code**—Specifies an ICMP message code for filtering ICMP packets. (Range: 0–255)
- **destination-port**—Specifies the UDP/TCP destination port. You can enter a range of ports by using a hyphen. E.g. 20 - 21. For TCP enter a number or one of the following values: bgp (179), chargen (19), daytime (13), discard (9), domain (53), drip (3949), echo (7), finger (79), ftp (21), ftp-data 20), gopher (70), hostname (42), irc (194), klogin (543), kshell (544), lpd (515), nntp (119), pop2 (109), pop3 (110), smtp (25), sunrpc (1110, syslog (514), tacacs-ds (49), talk (517), telnet (23), time (37), uucp (117), whois (43), www (80). For UDP enter a number or one of the following values: biff (512), bootpc (68), bootps (67), discard (9), dnsix (90), domain (53), echo (7), mobile-ip (434), nameserver (42),

netbios-dgm (138), netbios-ns (137), non500-isakmp (4500), ntp (123), rip (520), snmp (161), snmptrap (162), sunrpc (111), syslog (514), tacacs (49), talk (517), tftp (69), time (37), who (513), xdmcp (177). (Range: 0–65535)

- **source-port**—Specifies the UDP/TCP source port. Predefined port names are defined in the destination-port parameter. (Range: 0–65535)
- **match-all list-of-flags**—List of TCP flags that should occur. If a flag should be set it is prefixed by "+".If a flag should be unset it is prefixed by "-". Available options are +urg, +ack, +psh, +rst, +syn, +fin, -urg, -ack, -psh, -rst, -syn and -fin. The flags are concatenated to a one string. For example: +fin-ack.
- time-range-name—Name of the time range that applies to this permit statement. (Range: 1–32)
- **disable-port**—The Ethernet interface would be disabled if the condition is matched.
- **log-input**—Specifies to send an informational syslog message about the packet that matches the entry. Because forwarding is done in hardware and logging is done in software, if a large number of packets match a deny ACE containing a log-input keyword, the software might not be able to match the hardware processing rate, and not all packets will be logged.

Default

No IPv6 access list is defined.

Command Mode

IPv6 Access-list Configuration mode

User Guidelines

The number of TCP/UDP ranges that can be defined in ACLs is limited. You can define up to #ASIC-specific ranges for TCP and up to #ASIC-specific ranges for UDP. If a range of ports is used for source port in ACE it would be not be counted again if it is also used for source port in another ACE. If a range of ports is used for a destination port in ACE it would be not be counted again if it is also used for a destination port in another ACE.

If a range of ports is used for source port it would be counted again if it is also used for destination port.

Example

```
console(config)# ipv6 access-list server
console(config-ipv6-al)# deny tcp 3001::2/64 any any 80
```

mac access-list

Use the **mac access-list** Global Configuration mode command to define a Layer 2 access list and to place the device in MAC access list configuration mode. Use the **no** form of this command to remove the access list.

Syntax

mac access-list extended *access-list-name*

no mac access-list extended *access-list-name*

Parameters

access-list-name—Specifies the name of the MAC access list. (Range: access-list-name0–32 characters - use "" for empty string)

Default

No MAC access list is defined.

Command Mode

Global Configuration mode

User Guidelines

MAC ACL is defined by a unique name. IPv4 ACL, IPv6 ACL, MAC ACL or Policy Map cannot have the same name.

Example

```
console(config)# mac access-list extended server1
```

permit (MAC)

Use the **permit** command in MAC Access List Configuration mode to set permit conditions for an MAC access list,.

Syntax

permit *{any | source source-wildcard}{any | destination destination-wildcard}[eth-type 0| aarp | amber | dec-spanning | decnet-iv | diagnostic | dsm | etype-6000] [vlan vlan-id] [cos cos cos-wildcard] [time-range time-range-name]*

Parameters

- **source**—Source MAC address of the packet.
- **source-wildcard**—Wildcard bits to be applied to the source MAC address. Use 1s in the bit position that you want to be ignored.
- **destination**—Destination MAC address of the packet.
- **destination-wildcard**—Wildcard bits to be applied to the destination MAC address. Use 1s in the bit position that you want to be ignored.
- **eth-type**—The Ethernet type in hexadecimal format of the packet.
- **vlan-id**—The VLAN ID of the packet. (Range: 1–4094)
- **cos**—The Class of Service of the packet. (Range: 0–7)
- **cos-wildcard**—Wildcard bits to be applied to the CoS.
- **time-range-name**—Name of the time range that applies to this permit statement. (Range: 1–32)

Default

No MAC access list is defined.

Command Mode

MAC Access-list Configuration mode

User Guidelines

You enter MAC-access list configuration mode by using the MAC Access-list Global Configuration command.

After an access control entry (ACE) is added to an access control list, an implied deny-any-any condition exists at the end of the list. That is, if there are no matches, the packets are denied. However, before the first ACE is added, the list permits all packets.

Example

```
console(config)# mac access-list extended server1
```

```
console(config-mac-al)# permit 00:00:00:00:00:01 00:00:00:00:00:ff any
```

service-acl input

use the **service-acl input** command in interface configuration mode to control access to an interface. Use the **no** form of this command to remove the access control.

Syntax

service-acl input *acl-name1 [acl-name2]*

no service-acl input

Parameters

acl-name—Specifies an ACL to apply to the interface. See the usage guidelines. (Range: acl-name0–32 characters. Use "" for empty string)

Default

No ACL is assigned.

Command Mode

Interface Configuration (Ethernet, Port-Channel) mode.Interface Configuration (Ethernet, VLAN, Port-Channel) mode.

User Guidelines

IPv4 ACL and IPv6 ACL can be bound together to an interface.

MAC ACL cannot be bound on an interface with IPv4 ACL or IPv6 ACL.

Two ACLs of the same type can't be added to a port.

An ACL cannot be added to a port that is alredy bounded to an ACL, without first removing the current ACL and binding the two ACLs together.

Example

```
console(config)# mac access-list extended server
console(config-mac-al)# permit 00:00:00:00:00:01 00:00:00:00:00:ff any
console(config-mac-al)# exit
console(config)# interface gigabitethernet 1/0/1
```

```
console(config-if)# service-acl input server
```

service-acl output

Use the **service-acl output** command in Interface Configuration mode to control access to an interface on the Egress (transmit path). Use the **no** form of this command to remove the access control..

Syntax

service-acl output *acl-name1 [acl-name2]*

no service-acl output

Parameters

acl-name—Specifies an ACL to apply to the interface. See the Usage Guidelines. Range: acl-name –32 characters. Use "" for empty string

Default

No ACL is assigned.

Command Mode

Interface Configuration (Ethernet, Port-Channel) mode.

Interface Configuration (Ethernet, VLAN, Port-Channel) mode.

User Guidelines

The deny rule actions: log-input and disable-port are not supported. Trying to use these actions will result in an error.

IPv4 ACLs and IPv6 ACLs can be bound together on an interface.

A MAC ACL cannot be bound on an interface together with an IPv4 ACL or IPv6 ACL.

Two ACLs of the same type cannot be added to a port.

An ACL cannot be added to a port that is already bound to an ACL, without first removing the current ACL and binding the two ACLs together

Example

```
console(config)# mac access-list extended server
console(config-mac-al)# permit 00:00:00:00:00:01 00:00:00:00:00:ff any
console(config-mac-al)# exit
console(config)# interface gigabitethernet 1/0/1
console(config-if)# service-acl output server
```

service-acl input block

Use the **service-acl input block** Interface Configuration mode commands to discard packets that are classified to specific protocols. Use the **no** form of those commands to disable discarding of the packets.

Syntax

service-acl input *protocol1 [protocol2 … protocol6*]

no service-acl input

Parameters

protocol—Specifies a protocol to filter. Available values are: blockcdp, blockvtp, blockdtp, blockudld, blockpagp, blocksstp, and blockall.

Default Configuration

No protocol is defined

Command Mode

Interface Configuration ((Ethernet, Port-Channel) mode

User Guidelines

If you want to define multiple protocols on the same interface, those protocols should be defined in the same command.

To change configuration of the protocol filtering for an interface, you should first remove the current assignment of protocol filtering assignment, and then assign the new configuration of the protocol filtering.

If Proprietary Protocol Filtering rules are assigned on an interface, the user is not able to assign ACL or Policy Map or Security suite rules to that interface and to enable 802.1X Dynamic Policy Assignment to that interface.

If ACL or Policy Map or Security suite rules are assigned to an interface or 802.1X Dynamic Policy Assignment is enabled for an interface, the user is not able to assign Proprietary Protocol Filtering rules to that interface.

The following table defines the DA and protocol types of the packets that are subject for discarding per each command:

Command	Destination Address	Protocol Type
blockcdp	0100.0ccc.cccc	0x2000
blockvtp	0100.0ccc.cccc	0x2003
blockdtp	0100.0ccc.cccc	0x2004
blockudld	0100.0ccc.cccc	0x0111
blockpagp	0100.0ccc.cccc	0x0104
blocksstp	0100.0ccc.cccd	-
blockall	0100.0ccc.ccc0 - 0100.0ccc.cccf	-

Example

```
Console (Config-if)# service-acl input blockcdp blockvtp
```

time-range

use the **time-range** global configuration mode command to enable time-range configuration mode and define time ranges for functions (such as access lists). Use the **no** form of this command To remove the time range configuration.

Syntax

time-range *time-range-name*

no time-range *time-range-name*

Parameters

time-range-name—Specifies the name for the time range. (Range: 1–32 characters)

Default

No time range is defined

Command Mode
Global Configuration mode

User Guidelines
After the time-range command, use the periodic time-range configuration command and the absolute time-range configuration command. Multiple periodic commands are allowed in a time range. Only one absolute command is allowed.

If a time-range command has both absolute and periodic values specified, then the periodic items are evaluated only after the absolute start time is reached, and are not further evaluated after the absolute end time is reached.

All time specifications are interpreted as local time.

To ensure that the time range entries take effect at the desired times, the software clock should be set by the user or by SNTP. If the software clock is not set by the user or by SNTP, the time range ACEs are not activated.

The user cannot delete a time-range that is bounded to an ACE or to any other feature.

Example

```
Console (config)# time-range http-allowed
Console (config-time-range)# absolute start 12:00 1 jan 2005 end 12:00 31
dec 2005 Console (config-time-range)# periodic monday 8:00 to friday 20:00
```

absolute

Use the **absolute** Time-range Configuration mode command to specify an absolute time when a time range is in effect. Use the **no** form of this command To remove the time limitation.

Syntax
absolute *start hh:mm day month year*

no absolute *start*

absolute *end hh:mm day month year*

no absolute *end*

Parameters

- **start**—Absolute time and date that the permit or deny statement of the associated access list starts going into effect. If no start time and date are specified, the permit or deny statement is in effect immediately.
- **end**—Absolute time and date that the permit or deny statement of the associated access list is no longer in effect. If no end time and date are specified, the permit or deny statement is in effect indefinitely.
- **hh:mm**—Time in hours (military format) and minutes (Range: 0–23, mm: 0–5)
- **day**—Day (by date) in the month. (Range: 1–31)
- **month**—Month (first three letters by name). (Range: Jan...Dec)
- **year**—Year (no abbreviation) (Range: 2000–2097)

Default

There is no absolute time when the time range is in effect.

Command Mode

Time-range Configuration mode

---

periodic

Use the **periodic** Time-range Configuration mode command to specify a recurring (weekly) time range for functions that support the time-range feature. Use the **no** form of this command To remove the time limitation, .

Syntax

periodic *day-of-the-week hh:mm to day-of-the-week hh:mm*

no periodic *day-of-the-week hh:mm to day-of-the-week hh:mm*

periodic list *hh:mm to hh:mm day-of-the-week1 [day-of-the-week2… day-of-the-week7]*

no periodic list *hh:mm to hh:mm day-of-the-week1 [day-of-the-week2… day-of-the-week7]*

periodic list *hh:mm to hh:mm all*

no periodic list *all hh:mm to hh:mm all*

Parameters

- **day-of-the-week**—The starting day that the associated time range is in effect. The second occurrence is the ending day the associated statement is in effect. The second occurrence can be the following week (see description in the User Guidelines). Possible values are: Monday, Tuesday, Wednesday, Thursday, Friday, Saturday, and Sunday.
- **hh:mm**—The first occurrence of this argument is the starting hours:minutes (military format) that the associated time range is in effect. The second occurrence is the ending hours:minutes (military format) the associated statement is in effect. The second occurrence can be at the following day (see description in the User Guidelines). (Range: 0–23, mm: 0–59)
- **list day-of-the-week1**—Specifies a list of days that the time range is in effect.

Default

There is no periodic time when the time range is in effect.

Command Mode

Time-range Configuration mode

User Guidelines

The second occurrence of the day can be at the following week. E.g. Thursday–Monday means that the time range is effective on Thursday, Friday, Saturday, Sunday, and Monday.

The second occurrence of the time can be at thefollowing day. E.g. “22:00–2:00”.

show time-range

Use the **show time-range** EXEC command To display the time range configuration.

Syntax

show time-range *time-range-name*

Parameters

time-range-name—Specifies the name of the time range. (Range: 1–32)

Command Mode

EXEC mode

Example

```
Console# show time-range
http-allowed
--------------
absolute start 12:00 1 jan 2005
absolute end 12:00 31 dec 2005
periodic monday 8:00 to friday 20:00
```

show access-lists

Use the **show access-lists** Privileged EXEC mode command to display access control lists (ACLs) configured on the switch.

Syntax

show access-lists [*name* | *access-list-number*]

show access-lists *time-range-active [name]*

Parameters

- **name**—Specifies the name of the ACL.
- **access-list-number**—Specifies the number of the IP standard ACL list.
- **time-range-active**—Shows only the Access Control Entries (ACEs) that their time-range is currently active (including those that are not associated with time-range).

Command Mode

Privileged EXEC mode

Example

```
Switch# show access-lists
```

```
Router# show access-lists
Standard IP access list 1
deny   any
Standard IP access list 2
deny   192.168.0.0, wildcard bits 0.0.0.255
permit any
Standard IP access list 3
deny   0.0.0.0
deny   192.168.0.1, wildcard bits 0.0.0.255
permit any
Standard IP access list 4
permit 0.0.0.0
permit 192.168.0.2, wildcard bits 0.0.0.255

Extended IP access list ACL1
permit 234 172.30.40.1 0.0.0.0 any
permit 234 172.30.8.8  0.0.0.0 any

Extended IP access list ACL2
permit 234 172.30.19.1 0.0.0.255 any time-range weekdays
permit 234 172.30.23.8 0.0.0.255 any time-range weekends

Switch# show access-lists time-range-active
Extended IP access list ACL1
permit 234 172.30.40.1 0.0.0.0 any
permit 234 172.30.8.8  0.0.0.0 any

Extended IP access list ACL2
permit 234 172.30.19.1 0.0.0.255 any time-range weekdays

Switch# show access-lists
```

show interfaces access-lists

Use the **show interfaces access-lists** Privileged EXEC mode command to display access lists applied on interfaces.

Syntax

show interfaces access-lists *[interface-id]*

Parameters

interface-id—Specifies an interface ID. The interface ID can be one of the following types: Ethernet port, Port-channel or VLAN.

Command Mode

Privileged EXEC mode

Example

```
Console# show interfaces access-lists
Interface       ACL
----------    ---------
gi1/0/1       Ingress: ip,ipv6
              Egress : mac
gi1/0/4       Egress : mac
gi1/0/5       Ingress: ip
```

clear access-lists counters

Use The **Clear Access-lists Counters** Privileged EXEC mode command to clear access-lists counters.

Syntax

clear access-lists counters *[interface-id]*

Parameters

interface-id—Specifies an interface ID. The interface ID can be one of the following types: Ethernet port or Port-channel.

Command Mode
Privileged EXEC mode

Example

```
console# clear access-lists counters gigabitethernet 1/0/1
```

show interfaces access-lists counters

Use the **show interfaces access-lists counters** Privileged EXEC mode command to display Access List counters.

Syntax
show interfaces access-lists counters *[ethernet interface | port-channel port-channel-number]*

Parameters
interface-id—Specifies an interface ID. The interface ID can be one of the following types: Ethernet port or Port-channel.

Command Mode
Privileged EXEC mode

User Guidelines
The counter of deny ACE hits counts only ACEs with the log-input keyword.

Because forwarding is done in hardware and counting is done in software, if a large number of packets match a deny ACE containing a log-input keyword, the software might not be able to match the hardware processing rate, and not all packets are counted.

Example

```
console# show interfaces access-lists counters
Interface            Deny ACE hits
---------            -------------
gi1/0/1                79
gi1/0/2                9
```

```
gi1/0/3                 0
Number of hits that were counted in global counter (due to lack of
resources) =19
```

45

Quality of Service (QoS) Commands

qos

Use the **qos** Global Configuration mode command to enable Quality of Service (QoS) on the device. Use the **no** form of this command to disable QoS on the device

Syntax

qos [*basic* | *advanced*]

no qos

Parameters

- **basic**—QoS basic mode. If no option is specified, the QoS mode defaults to the basic mode.
- **advanced**—Specifies the QoS advanced mode, which enables the full range of QoS configuration.

Default Configuration

If the **qos** command is entered without any parameters, the QoS **basic** mode is enabled.

Command Mode

Global Configuration mode

Example

The following example enables the QoS basic mode on the device.

```
Console(config)# qos basic
```

show qos

Use the **show qos** EXEC mode command to display the Quality of Service (QoS) mode for the device. The trust mode is displayed for the QoS basic mode.

Syntax

show qos

Parameters

This command has no arguments or keywords.

Default Configuration

Disabled Command Mode

Command Mode

EXEC mode

User Guidelines

Trust mode is displayed if QoS is enabled in basic mode.

Example

The following example displays QoS attributes when QoS is enabled in basic mode on the device and the advanced mode is supported.

```
Console> show qos
Qos: basic
Basic trust: dscp
```

The following example displays QoS attributes when QoS is enabled in basic mode on the device and the advanced mode is not supported.

```
Console> show qos
```

```
Qos: disable
Trust: dscp
```

class-map

Use the **class-map** Global Configuration mode command to create or modify a class map and enters the Class-map Configuration mode. Use the **no** form of this command todelete a class map.

Syntax

class-map *class-map-name [match-all | match-any]*

no class-map *class-map-name*

Parameters

- ***c*lass-map-name**—Specifies the class map name.
- **match-all**—Performs a logical AND of all the matching statements under this class map. All match criteria in this class map must be matched.
- **match-any**—Performs a logical OR of all the matching statements under this class map. One or more match criteria in this class map must be matched.

Default Configuration

If neither **match-all** nor **match-any** is specified, the **match-all** parameter is selected by default.

Command Mode

Global Configuration mode

User Guidelines

The **class-map** Global Configuration mode command specifies the name of the class map for which class-map match criteria are to be created or modified and enters class-map configuration mode. In this mode, up to two match commands can be entered to configure the match criteria for this class. When using two match commands, each has to point to a different type of ACL (one IP and one MAC). The classification is by first match, therefore, the

order is important. The **class-map** command and its subcommands are used to define packet classification, marking, and aggregate policing as part of a globally named service policy applied on a per-interface basis. If there is more than one match statement in a match-all class map and if there is a repetitive classification field in the participating ACLs, an error message is generated.

After entering the Quality of Service (QoS) Class-map Configuration mode, the following configuration commands are available:

exit: Exits the QoS Class-map Configuration mode.

match: Configures classification criteria.

no: Removes a match statement from a class map.

Example

The following example creates a class map called Class1 and configures it to check that packets match all classification criteria in the class map match statement.

```
Console(config)# class-map class1 match-all
Console(config-cmap)#
```

show class-map

The **show class-map** EXEC mode command displays all class maps.

Syntax

show class-map [*class-map-name*]

Parameters

class-map-name—Specifies the name of the class map to be displayed.

Command Mode

EXEC mode

Example

The following example displays the class map for Class1.

```
Console> show class-map class1

Class Map match-any class1 (id4)
Match Ip dscp 11 21
```

match

Use the **match** Class-map Configuration mode command to define the match criteria for classifying traffic. Use the **no** form of this command to delete the match criteria.

Syntax

match access-group *acl-name*

no match access-group *acl-name*

Parameters

acl-name—Specifies the MAC or IP Access Control List (ACL) name.

Default Configuration

No match criterion is supported.

Command Mode

Class-map Configuration mode.

Example

The following example defines the match criterion for classifying traffic as an access group called Enterprise in a class map called Class1.

```
Console(config)# class-map class1
Console(config-cmap)# match access-group enterprise
```

policy-map

Use the **policy-map** Global Configuration mode command to creates a policy map and enter the Policy-map Configuration mode. Use the **no** form of this command to delete a policy map.

Syntax

policy-map *policy-map-name*

no policy-map *policy-map-name*

Parameters

policy-map-name—Specifies the policy map name.

Default Configuration

The default behavior of the policy map is to set the DSCP value to 0 if the packet is an IP packet, and to set the CoS value to 0 if the packet is tagged.

Command Mode

Global Configuration mode

User Guidelines

Use the **policy-map** Global Configuration mode command to specify the name of the policy map to be created, added to, or modified before configuring policies for classes whose match criteria are defined in a class map.

Entering the **policy-map** Global Configuration mode command also enables configuring or modifying the class policies for that policy map. Class policies in a policy map can be configured only if the classes have match criteria defined for them. Use the **class-map** Global Configuration mode and **match** Class-map Configuration mode commands to configure the match criteria for a class.

The match criteria is for a class. Only one policy map per interface per direction is supported. The same policy map can be applied to multiple interfaces and directions.

Example

The following example creates a policy map called Policy1 and enters the Policy-map Configuration mode.

```
Console(config)# policy-map policy1
Console(config-pmap)#
```

class

The **class** Policy-map Configuration mode command defines a traffic classification and enters the Policy-map Class Configuration mode. Use the **no** form of this command to detach a class map from the policy map.

Syntax

class *class-map-name [access-group acl-name*]

no class *class-map-name*

Parameters

- **class-map-name**—Specifies the name of an existing class map. If the class map does not exist, a new class map is created under the specified name.
- **acl-name**—Specifies the name of an IP or MAC Access Control List (ACL).

Default Configuration

No class map is defined for the policy map.

Command Mode

Policy-map Configuration mode

User Guidelines

Use the **policy-map** Global Configuration mode command to identify the policy map and to enter the Policy-map Configuration mode before using the **class** command. After specifying a policy map, a policy for new classes can be configured or a policy for any existing classes in that policy map can be modified.

Use the **service-policy** Interface Configuration (Ethernet, Port-channel) mode command to attach a policy map to an interface. Use an existing class map to attach classification criteria to the specified policy map and use the **access-group** parameter to modify the classification criteria of the class map.

If this command is used to create a new class map, the name of an IP or MAC ACL must also be specified with the **access-group** parameter.

Example
The following example defines a traffic classification called Class1 with an access-group called Enterprise. The class is in a policy map called policy1.

```
Console(config)# policy-map policy1
Console(config-pmap)# class class1 access-group enterprise
```

show policy-map

Use the **show policy-map** EXEC mode command to display all policy maps or a specific policy map.

Syntax
show policy-map [*policy-map-name*]

Parameters
policy-map-name—Specifies the policy map name.

Command Mode
EXEC mode

Example
The following example displays all policy maps.

```
Console> show policy-map
Policy Map policy1
class class1
set Ip dscp 7
Policy Map policy2
class class 2
police 96000 4800 exceed-action drop
class class3
police 124000 96000 exceed-action policed-dscp-transmit
```

trust

Use the **trust** Policy-map Class Configuration mode command to configure the trust state, which selects the value that QoS uses as the source of the internal DSCP value. Use the **no** form of this command to return to the default trust state.

Syntax

trust *cos-dscp*

no trust

Parameters

cos-dscp—Specifies that if the packet is IP, then QoS acts as for **dscp**; otherwise QoS acts as for **cos**.

Default Configuration

The default state is untrusted.

If the **trust** command is specified with no parameters, the default mode is **dscp**.

Command Mode

Policy-map Class Configuration mode

User Guidelines

Use this command to distinguish the Quality of Service (QoS) trust behavior for certain traffic from others. For example, incoming traffic with certain DSCP values can be trusted. A class map can be configured to match and trust the DSCP values in the incoming traffic.

Trust values set with this command supersede trust values set on specific interfaces with the **qos trust** Interface Configuration mode command.

The **trust** command and the **set** Policy-map Class Configuration mode command are mutually exclusive within the same policy map.

Policy maps that contain **set** or **trust** Policy-map Class Configuration mode commands cannot be attached, or that have Access Control List (ACL) classification to an egress interface by using the **service-policy** Interface Configuration mode command.

If specifying **trust cos**, QoS maps a packet to a queue, the received or default port CoS value, and the CoS-to-queue map.

If specifying **trust dscp**, QoS maps the packet using the DSCP value from the ingress packet.

If specifying **tcp-udp-port**, QoS maps the packet to a queue using the TCP\UDP port value from the ingress packet and the tcp-udp-port-to-queue map.

Example

The following example creates an ACL, places it into a class map, places the class map into a policy map and configures the trust state using the DSCP value in the ingress packet.

```
console(config)# mac access-list extended m1
console(config-mac-al)# permit any any
console(config-mac-al)# exit
console(config)# class-map c1
console(config-cmap)# match access-group m1
console(config-cmap)# exit
console(config)# policy-map p1
console(config-pmap)# class c1
console(config-pmap-c)# trust cos-dscp
```

set

Use the **set** Policy-map Class Configuration mode command to set new values in the IP packet.

Syntax

set *{dscp new-dscp | queue queue-id | cos new-cos}*

no set

Parameters

- **dscp new-dscp**—Specifies the new DSCP value for the classified traffic. (Range: 0–63)

- **queue queue-id**—Specifies the explicit queue id to set the egress queue.
- **cos new-cos**—Specifies the new User priority to be marked in the packet. (Range: 0–7)

Command Mode
Policy-map Class Configuration mode

User Guidelines
This command and the **trust** Policy-map Class Configuration mode command are mutually exclusive within the same policy map.

Policy maps that contain **set** or **trust** Policy-map Class Configuration mode commands or that have ACL classifications cannot be attached to an egress interface using the Service-policy Interface Configuration mode command.

To return to the Policy-map Configuration mode, use the **exit** command. To return to the Privileged EXEC mode, use the **end** command.

Example
The following example creates an ACL, places it into a class map, places the class map into a policy map and sets the DSCP value in the packet to 56 for classes in policy map called p1.

```
console(config)# mac access-list extended m1
console(config-mac-al)# permit any any
console(config-mac-al)# exit
console(config)# class-map c1
console(config-cmap)# match access-group m1
console(config-cmap)# exit
console(config)# policy-map p1
console(config-pmap)# class c1
Console(config-pmap-c)# set dscp 56
```

police

Use the **police** Policy-map Class Configuration mode command to define the policer for classified traffic. Use the **no** form of this command to remove a policer.

Syntax

police *committed-rate-kbps committed-burst-byte [exceed-action {drop | policed-dscp-transmit}]*

no police

Parameters

- **committed-rate-kbps**—Specifies the average traffic rate (CIR) in kbits per second (bps). (Range: 3–12582912)
- **committed-burst-byte**—Specifies the normal burst size (CBS) in bytes. (Range: 3000–19173960)
- **exceed-action** {**drop** | **policed-dscp-transmit**}—Specifies the action taken when the rate is exceeded. The possible values are:
  - **drop**—Drops the packet.
  - **policed-dscp-transmit**—Remarks the packet DSCP, according to the policed-DSCP map as configured by the **qos map policed-dscp** Global Configuration mode command.

Command Mode

Policy-map Class Configuration mode

User Guidelines

Policing uses a token bucket algorithm. CIR represents the speed with which the token is removed from the bucket. CBS represents the depth of the bucket.

Example

The following example defines a policer for classified traffic. When the traffic rate exceeds 124,000 kbps or the normal burst size exceeds 9600 bytes, the packet is dropped. The class is called Class1 and is in a policy map called Policy1.

```
Console(config)# policy-map policy1
Console(config-pmap)# class class1
Console(config-pmap-c)# police 124000 9600 exceed-action drop
```

service-policy

Use the **service-policy** Interface Configuration (Ethernet, VLAN, Port-channel) mode command to apply a policy map to the input of a particular interface. Use the **no** form of this command to detach a policy map from an interface.

Syntax

service-policy input *policy-map-name*

no service-policy input

Parameters

policy-map-name—Specifies the policy map name to apply to the input interface. (Length: 1–32 characters)

Command Mode

Interface Configuration (Ethernet, VLAN, Port-channel) mode

User Guidelines

Only one policy map per interface per direction is supported.

Example

The following example attaches a policy map called Policy1 to the input interface.

```
Console(config-if)# service-policy input policy1
```

qos aggregate-policer

Use the **qos aggregate-policer** Global Configuration mode command to define the policer parameters that can be applied to multiple traffic classes. Use the **no** form of this command to remove an existing aggregate policer.

Syntax

qos aggregate-policer *aggregate-policer-name committed-rate-kbps excess-burst-byte* [*exceed-action {drop | policed-dscp-transmit}]*

no qos aggregate-policer *aggregate-policer-name*

Parameters

- **aggregate-policer-name**—Specifies the aggregate policer name.
- **committed-rate-kbps**—Specifies the average traffic rate (CIR) in kbits per second (kbps). (Range: 3–57982058)
- **excess-burst-byte**—Specifies the normal burst size (CBS) in bytes. (Range: 3000–19173960)
- **exceed-action** {**drop** | **policed-dscp-transmit**}—Specifies the action taken when the rate is exceeded. The possible values are:
  - **drop**—Drops the packet.
  - **policed-dscp-transmit**—Remarks the packet DSCP.

Default Configuration

No aggregate policer is defined.

Command Mode

Global Configuration mode

User Guidelines

Define an aggregate policer if the policer is shared with multiple classes.

Policers in one port cannot be shared with other policers in another device. Traffic from two different ports can be aggregated for policing purposes.

An aggregate policer can be applied to multiple classes in the same policy map. An aggregate policer cannot be applied across multiple policy maps.

An aggregate policer cannot be deleted if it is being used in a policy map. The **no police aggregate** Policy-map Class Configuration mode command must first be used to delete the aggregate policer from all policy maps before using the **no mls qos aggregate-policer** command.

Policing uses a token bucket algorithm. CIR represents the speed with which the token is removed from the bucket. CBS represents the depth of the bucket.

Example

The following example defines the parameters of a policer called Policer1 that can be applied to multiple classes in the same policy map. When the average traffic rate exceeds 124,000 kbps or the normal burst size exceeds 9600 bytes, the packet is dropped.

```
Console(config)# qos aggregate-policer policer1 124000 9600
exceed-action drop
```

show qos aggregate-policer

Use the **show qos aggregate-policer** EXEC mode command to display the aggregate policer parameter.

Syntax

show qos aggregate-policer [*aggregate-policer-name*]

Parameters

aggregate-policer-name—Specifies the aggregate policer name.

Command Mode

EXEC mode

Example

The following example displays the parameters of the aggregate policer called Policer1.

```
Console> show qos aggregate-policer policer1
aggregate-policer policer1 96000 4800 exceed-action drop
not used by any policy map
```

police aggregate

Use the **police aggregate** Policy-map Class Configuration mode command to apply an aggregate policer to multiple classes within the same policy map. Use

the **no** form of this command to remove an existing aggregate policer from a policy map.

Syntax

police aggregate *aggregate-policer-name*

no police aggregate *aggregate-policer-name*

Parameters

aggregate-policer-name—Specifies the aggregate policer name.

Command Mode

Policy-map Class Configuration mode

User Guidelines

An aggregate policer can be applied to multiple classes in the same policy map. An aggregate policer cannot be applied across multiple policy maps or interfaces.

Use the **exit** command to return to the Policy-map Configuration mode. Use the **end** command to return to the Privileged EXEC mode.

Example

The following example applies the aggregate policer called Policer1 to a class called Class1 in a policy map called Policy1.

```
Console(config)# policy-map policy1
Console(config-pmap)# class class1
Console(config-pmap-c)# police aggregate policer1
```

wrr-queue cos-map

Use the **wrr-queue cos-map** Global Configuration mode command maps Class of Service (CoS) values to a specific egress queue. Use the **no** form of this command to restore the default configuration.

Syntax

wrr-queue cos-map *queue-id cos0 ... cos7*

no wrr-queue cos-map [*queue-id*]

Parameters

- **queue-id**—Specifies the queue number to which the CoS values are mapped.
- **cos0 ... cos7**—Specifies up to 7 CoS values to map to the specified queue number. (Range: 1–7)

Default Configuration

The default CoS value mapping to 8 queues is as follows:

CoS value 0 is mapped to queue 3.

CoS value 1 is mapped to queue 1.

CoS value 2 is mapped to queue 2.

CoS value 3 is mapped to queue 4.

CoS value 4 is mapped to queue 5.

CoS value 5 is mapped to queue 6.

CoS value 6 is mapped to queue 7.

CoS value 7 is mapped to queue 8.

Command Mode

Global Configuration mode

User Guidelines

Use this command to distribute traffic to different queues, where each queue is configured with different weighted round robin (WRR) and Weighted Random Early Detection (WRED) parameters.

The expedite queues are enabled using the **priority-queue out** Interface Configuration mode commans

Example

The following example maps CoS value 7 to queue 2.

```
Console(config)# wrr-queue cos-map 2 7
```

wrr-queue bandwidth

Use the **wrr-queue bandwidth** global Configuration command to assign Weighted Round Robin (WRR) weights to egress queues. The weight ratio determines the frequency at which the packet scheduler removes packets from each queue. Use the **no** form of this command to restore the default configuration.

Syntax

wrr-queue bandwidth *weight1 weight2 ... weight_n*

no wrr-queue bandwidth

Parameters

weight1 weight2 ... weight_n—Specifies the ratio of the bandwidth assigned by the WRR packet scheduler to the packet queues. Separate values by a space. (Range: 0–255)

Default Configuration

wrr is disabled by default. The default wrr weight is '1' for all queues.

Command Mode

Global Configuration mode

User Guidelines

The ratio for each queue is defined as the queue weight divided by the sum of all queue weights (the normalized weight). This sets the bandwidth allocation of each queue.

A weight of 0 indicates that no bandwidth is allocated for the same queue, and the shared bandwidth is divided among the remaining queues. It is not recommended to set the weight of a queue to a 0 as it might stop transmission of control-protocols packets generated by the device.

All eight queues participate in the WRR, excluding the expedite queues, in which case the corresponding weight is ignored (not used in the ratio calculation). The expedite queue is a priority queue; it is serviced until empty before the other queues are serviced. The expedite queues are enabled by using the **priority-queue out** Interface Configuration mode command.

Example
The followin 7 WRR queues.

```
Console(config)# wrr-queue bandwidth 6 6 6 6 6 6 6 6
```

priority-queue out num-of-queues

Use the **priority-queue out num-of-queues** Global Configuration mode command to configure the number of expedite queues. Use the **no** form of this command to restore the default configuration.

Syntax
priority-queue out num-of-queues *number-of-queues*

no priority-queue out num-of-queues

Parameters
number-of-queues—Specifies the number of expedite queues. Expedite queues have higher indexes. (Range: 0–8). If number-of-queues = 0, all queues are assured forwarding. If number-of-queues = 8, all queues are expedited.

Default Configuration
All queues are expedite queues.

Command Mode
Global Configuration mode

User Guidelines
While configuring the **priority-queue num-of-queues** command, the weighted round robin (WRR) weight ratios are affected because there are fewer queues participating in WRR. This indicates that the corresponding weight in the **wrr-queue bandwidth** Interface Configuration mode command is ignored (not used in the ratio calculation).

Example
The following example configures the number of expedite queues as 2.

```
Console(config)# priority-queue out num-of-queues 2
```

traffic-shape
Use the **traffic-shape** Interface Configuration (Ethernet, Port-channel) mode command to configure the egress port shaper. Use the **no** form of this command to disable the shaper.

Syntax
traffic-shape *committed-rate* [*committed-burst*]

no traffic-shape

Parameters
- **committed-rate**—Specifies the average traffic rate (CIR) in kbits per second (kbps). (Range: GE: 64kbps–maximum port speed; 10GE: 64Kbps–maximum port speed)
- **committed-burst**—Specifies the excess burst size (CBS) in bytes. (Range: 4KB –16MB)

Default Configuration
The shaper is disabled.

Command Mode
Interface Configuration (Ethernet, Port-channel) mode

Example
The following example sets a shaper on gigabitethernet port `1/0/5` on queue 1 when the average traffic rate exceeds 124000 kbps or the normal burst size exceeds 9600 bytes.

```
Console(config)# interface gi1/0/5
Console(config-if)# traffic-shape 1 124000 9600
```

traffic-shape queue

Use the **traffic-shape queue** Interface Configuration (Ethernet, Port-channel) mode command to configure the egress queue shaper. Use the **no** form of this command to disable the shaper.

Syntax

traffic-shape queue *queue-id committed-rate* [*committed-burst*]

no traffic-shape queue *queue-id*

Parameters

- **queue-id**—Specifies the queue number to which the shaper is assigned.
- **committed-rate**—Specifies the average traffic rate (CIR) in kbits per second (kbps). (Range: 64 kbps–maximum port speed)
- **committed-burst**—Specifies the excess burst size (CBS) in bytes. (Range: 4 KB - 16 MB)

Default Configuration

The shaper is disabled.

Command Mode

Interface Configuration (Ethernet, Port-channel) mode

Example

The following example sets a shaper on gigabitethernet port `1/0/5` when the average traffic rate exceeds 124000 kbps or the normal burst size exceeds 9600 bytes.

```
Console(config)# interface gi1/0/5
Console(config-if)# traffic-shape 124000 9600
```

rate-limit (Ethernet)

Use the **rate-limit** Interface Configuration (Ethernet) mode command to limit the incoming traffic rate on a port. Use the **no** form of this command to disable the rate limit.

Syntax

rate-limit *committed-rate-kbps [burst committed-burst-byte]*

no rate-limit

Parameters

- **rate**—Specifies the maximum number of kilobits per second of ingress traffic on a port. The range is 3–10000000.
- **burst bytes**—The burst size in bytes (3000–19173960). If unspecified, defaults to 128K.

Default Configuration

Rate limiting is disabled.

Command Mode

Interface Configuration (Ethernet) mode

User Guidelines

Example

The following example limits the incoming traffic rate on gigabitethernet port 1/0/5 to 150,000 kbps.

```
Console(config)# interface gi1/0/5
Console(config-if)# rate-limit 150000
```

qos wrr-queue wrtd

Use the **qos wrr-queue wrtd** Global Configuration mode command to enable Weighted Random Tail Drop (WRTD). Use the **no** form of this command to disable WRTD.

Syntax

qos wrr-queue wrtd

no qos wrr-queue wrtd

Parameters

This command has no arguments or keywords.

Default

Disabled

Command Mode

Global Configuration mode

User Guidelines

The command is effective after reset.

---

show qos interface

Use the **show qos interface** EXEC mode command to display Quality of Service (QoS) information on the interface.

Syntax

show qos interface [*buffers* / *queueing* / *policers* / *shapers* / *rate-limit*] *[interface-id]*

Parameters

- **buffers**—Displays the buffer settings for the interface's queues. For GE ports, displays the queue depth for each of the 8 queues.
- **queueing**—Displays the queue's strategy (WRR or EF), the weight for WRR queues, the CoS to queue map and the EF priority.
- **policers**—Displays all the policers configured for this interface, their settings, and the number of policers currently unused.
- **shapers**—Displays the shaper of the specified interface and the shaper for the queue on the specified interface.
- **rate-limit**—Displays the rate-limit configuration.

- **interface-id**—Specifies an interface ID. The interface ID can be one of the following types: Ethernet port, or Port-channel.

Default Configuration
There is no default configuration for this command.

Command Mode
EXEC mode

User Guidelines
The **policers** option is relevant for a VLAN interface only.

If no parameter is specified with the **show qos interface** command, the port QoS mode (DSCP trusted, CoS trusted, untrusted, and so on), default CoS value, DSCP-to-DSCP- map (if any) attached to the port, and policy map (if any) attached to the interface are displayed. If a specific interface is not specified, the information for all interfaces is displayed.

Example
This is an example of the output from the **show qos interface buffers** command for 8 queues.

```
Console> show qos interface buffers gi1/0/1
gi1/0/1
Notify Q depth:
buffers gi2/0/1
Ethernet gi2/0/1

qid  thresh0  thresh1  thresh2
1    100      100      80
2    100      100      80
3    100      100      80
4    100      100      80
5    100      100      80
6    100      100      80
7    100      100      80
8    100      100      80
```

This is an example of the output from the **show qos interface shapers** command for 8 queues.

```
Console> show qos interface shapers gi1/0/1
gigabitethernet 1/0/1
Port shaper: enable
Committed rate: 192000 bps
Committed burst: 9600 bytes

                        Target                  Target
QID     Status          Committed               Committed
                        Rate [bps]              Burst [bytes]
1       Enable          100000                  17000
2       Disable         N/A                     N/A
3       Enable          200000                  19000
4       Disable         N/A                     N/A
5       Disable         N/A                     N/A
6       Disable         N/A                     N/A
7       Enable          178000                  8000
8       Enable          23000                   1000
```

This is an example of the output from the **show qos interface policer** command.

```
Console> show qos interface policer gi1/0/1
Ethernet gi1/0/1
Class map: A
Policer type: aggregate
Commited rate: 192000 bps
Commited burst: 9600 bytes
Exceed-action: policed-dscp-transmit

Class map: B
Policer type: single
Commited rate: 192000 bps
Commited burst: 9600 bytes
Exceed-action: drop

Class map: C
Policer type: none
Commited rate: N/A
Commited burst: N/A
Exceed-action: N/A
```

This is an example of the output from the **show qos interface rate-limit** command.

```
Console> show qos interface rate-limit gi1/0/1


Port            rate-limit [kbps]              Burst [KBytes]
-----           -----------------              --------------
gi1/0/1         1000                           512K
```

qos wrr-queue threshold

Use the **qos wrr-queue threshold** Global Configuration mode command to assign queue thresholds globally. Use the **no** form of this command to restore the default configuration.

Syntax

qos wrr-queue threshold ***gigabitethernet*** *queue-id threshold-percentage*

no qos wrr-queue threshold ***gigabitethernet*** *queue-id*

Parameters

- **gigabitethernet**—Specifies that the thresholds are to be applied to Gigabit Ethernet ports.
- **queue-id**—Specifies the queue number to which the tail-drop threshold is assigned.
- **threshold-percentage**—Specifies the queue threshold percentage value.

Default Configuration

The default threshold is 80 percent.

Command Mode

Global Configuration mode

User Guidelines

If the threshold is exceeded, packets with the corresponding DP are dropped until the threshold is no longer exceeded.

Example

The following example assigns a threshold of 80 percent to WRR queue 1.

```
Console(config)# qos wrr-queue threshold gigabitethernet 1 80
```

qos map policed-dscp

Use the **qos map policed-dscp** Global Configuration mode command to configure the policed-DSCP map for remarking purposes. Use the **no** form of this command to restore the default configuration.

Syntax

qos map policed-dscp *dscp-list* ***to*** *dscp-mark-down*

no qos map policed-dscp [*dscp-list*]

Parameters

- **dscp- list**—Specifies up to 8 DSCP values, separated by spaces. (Range: 0–63)
- **dscp-mark-down**—Specifies the DSCP value to mark down. (Range: 0–63)

Default Configuration

The default map is the Null map, which means that each incoming DSCP value is mapped to the same DSCP value.

Command Mode

Global Configuration mode.

Example

The following example marks incoming DSCP value 3 as DSCP value 43 on the policed-DSCP map.

```
Console(config)# qos map policed-dscp 3 to 43
Reserved DSCP. DSCP 3 was not configured.
```

qos map dscp-queue

Use the **qos map dscp-queue** Global Configuration mode command to configure the DSCP to CoS map. Use the **no** form of this command to restore the default configuration.

Syntax

qos map dscp-queue *dscp-list* to *queue-id*

no qos map dscp-queue [*dscp-list*]

Parameters

- **dscp-list**—Specifies up to 8 DSCP values, separated by spaces. (Range: 0–63)
- **queue-id**—Specifies the queue number to which the DSCP values are mapped.

Default Configuration
The default map for 8 queues is as follows.

DSCP value	0-7	8-15	16-23	24-31	32-39	40-47	48-56	57-63
Queue-ID	1	2	3	4	5	6	7	8

Command Mode
Global Configuration mode

Example
The following example maps DSCP values 33, 40 and 41 to queue 1.

```
Console(config)# qos map dscp-queue 33 40 41 to 1
```

qos map dscp-dp

Use the **qos map dscp-dp** Global Configuration mode command to map the DSCP to Drop Precedence. Use the **no** form of this command to restore the default configuration.

Syntax
qos map dscp-dp *dscp-list* to *dp*

no qos map dscp-dp [*dscp-list*]

Parameters

- **dscp-list**—Specifies up to 8 DSCP values, with values separated by a space. (Range: 0–63)
- **dp**—Specifies the Drop Precedence value to which the DSCP values are mapped. (values: 0,2) where 2 is the highest Drop Precedence)

Default Configuration
All the DSCPs are mapped to Drop Precedence 0.

Command Mode
Global Configuration mode.

Example
The following example maps DSCP values 25, 27 and 29 to Drop Precedence 2.

```
Console(config)# qos map dscp-dp 25 27 29 to 2
```

qos trust (Global)

Use the **qos trust** Global Configuration mode command to configure the system to the basic mode and trust state. Use the **no** form of this command to return to the default configuration.

Syntax
qos trust *{cos | dscp }*

no qos trust

Parameters

- **cos**— Specifies that ingress packets are classified with packet CoS values. Untagged packets are classified with the default port CoS value.
- **dscp**—Specifies that ingress packets are classified with packet DSCP values.

Default Configuration
CoS is the default trust mode.

Command Mode
Global Configuration mode

User Guidelines
This command can be used only in QoS basic mode.

Packets entering a quality of service (QoS) domain are classified at the edge of the QoS domain. When the packets are classified at the edge, the switch port within the QoS domain can be configured to one of the trusted states

because there is no need to classify the packets at every switch within the domain.

Use this command to specify whether the port is trusted and which fields of the packet to use to classify traffic.

When the system is configured with trust DSCP, the traffic is mapped to the queue by the DSCP-queue map.

When the system is configured with trust CoS, the traffic is mapped to the queue by the CoS-queue map.

Example
The following example configures the system to the DSCP trust state.

```
Console(config)# qos trust dscp
```

qos trust (Interface)

Use the **qos trust** Interface Configuration (Ethernet, Port-channel) mode command to enable each port trust state while the system is in the basic QoS mode. Use the **no** form of this command to disable the trust state on each port.

Syntax
qos trust

no qos trust

Default Configuration
Each port is enabled while the system is in basic mode.

Command Mode
Interface Configuration (Ethernet, Port-channel) mode

Example
The following example configures gigabitethernet port 1/0/15 to the default trust state.

```
Console(config)# interface gi1/0/15
Console(config-if)# qos trust
```

qos cos

Use the **qos cos** Interface Configuration (Ethernet, Port-channel) mode command to define the default CoS value of a port. Use the **no** form of this command to restore the default configuration.

Syntax

qos cos *default-cos*

no qos cos

Parameters

default-cos—Specifies the default CoS value of the port. If the port is trusted and the packet is untagged, then the default CoS value become the CoS value. (Range: 0–7)

Default Configuration

The default CoS value of a port is 0.

Command Mode

Interface Configuration (Ethernet, Port-channel) mode

User Guidelines

Use the default CoS value to assign a CoS value to all untagged packets entering the port. Use the **qos cos override** command to assign this default CoS value to tagged packets.

Example

The following example defines the port `gi1/0/15` default CoS value as 3 .

```
Console(config)# interface gi1/0/15
Console(config-if)# qos cos 3
```

qos dscp-mutation

Use the **qos dscp-mutation** Global Configuration mode command to apply the DSCP Mutation map to system DSCP trusted ports. Use the **no** form of this command to restore the trusted port with no DSCP mutation.

Syntax

qos dscp-mutation

no qos dscp-mutation

Command Mode

Global Configuration mode.

User Guidelines

Apply the DSCP-to-DSCP-mutation map to a port at the boundary of a Quality of Service (QoS) administrative domain. If two QoS domains have different DSCP definitions, use the DSCP-to-DSCP-mutation map to translate a set of DSCP values to match the definition of another domain. Apply the map to ingress and to DSCP-trusted ports only. Applying this map to a port causes IP packets to be rewritten with newly mapped DSCP values at the ingress ports. If applying the DSCP mutation map to an untrusted port, to class of service (CoS), or to an IP-precedence trusted port, the command has no immediate effect until the port becomes DSCP-trusted.

Example

The following example applies the DSCP Mutation map to system DSCP trusted ports.

```
Console(config)# qos dscp-mutation
```

qos map dscp-mutation

Use the **qos map dscp-mutation** Global Configuration mode command to configure the DSCP to DSCP Mutation table. Use the **no** form of this command to restore the default configuration.

Syntax

qos map dscp-mutation *in-dscp* to *out-dscp*

no qos map dscp-mutation [*in-dscp*]

Parameters

- **in-dscp**—Specifies up to 8 DSCP values to map, separated by spaces. (Range: 0–63)
- **out-dscp**—Specifies up to 8 DSCP mapped values, separated by spaces. (Range: 0–63)

Default Configuration

The default map is the Null map, which means that each incoming DSCP value is mapped to the same DSCP value.

Command Mode

Global Configuration mode.

User Guidelines

This is the only map that is not globally configured. It is possible to have several maps and assign each one to a different port.

Example

The following example changes DSCP values 1, 2, 4, 5 and 6 to DSCP Mutation Map value 63.

```
Console(config)# qos map dscp-mutation 1 2 4 5 6 to 63
```

show qos map

Use the **show qos map** EXEC mode command to display the QoS mapping information.

Syntax

show qos map [**dscp-queue** | **dscp-dp** | **policed-dscp** | **dscp-mutation**]

Parameters

- **dscp-queue**—Displays the DSCP to queue map.
- **dscp-dp**—Displays the DSCP to Drop Precedence map.
- **policed-dscp**—Displays the DSCP to DSCP remark table.
- **dscp-mutation**—Displays the DSCP-DSCP mutation table.

Command Mode
EXEC mode

Example
The following example displays the QoS mapping information.

```
Console> show qos map

Dscp-queue map:
d1    :    d2    0    1    2    3    4    5    6    7    8    9
--    --   --    --   --   --   --   --   --   --   --   --   --
0     :         01   01   01   01   01   01   01   01   02   02
1     :         02   02   02   02   02   02   03   03   03   03
2     :         03   03   03   03   04   04   04   04   04   04
3     :         04   04   05   05   05   05   05   05   05   05
4     :         06   06   06   06   06   06   06   06   07   07
5     :         07   07   07   07   07   07   08   08   08   08
6     :         08   08   08   08
```

The following table appears:.

```
Dscp-DP map:
d1    :    d2    0    1    2    3    4    5    6    7    8    9
--    --   --    --   --   --   --   --   --   --   --   --   --
0     :    00    00   00   00   00   00   00   00   00   00   00
1     :    00    00   00   00   00   00   00   00   00   00   00
2     :    00    00   00   00   00   00   00   00   00   00   00
3     :    00    00   00   00   00   00   00   00   00   00   00
4     :    00    00   00   00   00   00   00   00   00   00   00
5     :    00    00   00   00   00   00   00   00   00   00   00
6     :    00    00   00   00
```

The following table appears:.

```
Policed-dscp map:

d1    :    d2    0    1    2    3    4    5    6    7    8    9
--    --   --    --   --   --   --   --   --   --   --   --   --
0     :         00   01   02   03   04   05   06   07   08   09
1     :         10   11   12   13   14   15   16   17   18   19
2     :         20   21   22   23   24   25   26   27   28   29
3     :         30   31   32   33   34   35   36   37   38   39
4     :         40   41   42   43   44   45   46   47   48   49
5     :         50   51   52   53   54   55   56   57   58   59
6     :         60   61   62   63
```

The following table appears:.

```
Dscp-dscp mutation map:

d1    :    d2    0    1    2    3    4    5    6    7    8    9
--    --   --    --   --   --   --   --   --   --   --   --   --
0     :         00   01   02   03   04   05   06   07   08   09
1     :         10   11   12   13   14   15   16   17   18   19
2     :         20   21   22   23   24   25   26   27   28   29
3     :         30   31   32   33   34   35   36   37   38   39
4     :         40   41   42   43   44   45   46   47   48   49
5     :         50   51   52   53   54   55   56   57   58   59
6     :         60   61   62   63
```

clear qos statistics

Use the **clear qos statistics** EXEC mode command to clear the QoS statistics counters.

Syntax

clear qos statistics

Command Mode

EXEC mode

Example
The following example clears the QoS statistics counters.

```
Console# clear qos statistics
```

qos statistics policer

Use the **qos statistics policer** Interface Configuration (Ethernet, Port-channel) mode command to enable counting in-profile and out-of-profile. Use the **no** form of this command to disable counting.

Syntax
qos statistics policer *policy-map-name class-map-name*

no qos statistics policer *policy-map-name class-map-name*

Parameters

- **policy-map-name**—Specifies the policy map name.
- **class-map-name**—Specifies the class map name.

Default Configuration
Counting in-profile and out-of-profile is disabled.

Command Mode
Interface Configuration (Ethernet, Port-channel) mode

Example
The following example enables counting in-profile and out-of-profile on the interface.

```
Console(config-if)# qos statistics policer policy1 class1
```

qos statistics aggregate-policer

Use the **qos statistics aggregate-policer** Global Configuration mode command to enable counting in-profile and out-of-profile. Use the **no** form of this command to disable counting.

Syntax

qos statistics aggregate-policer *aggregate-policer-name*

no qos statistics aggregate-policer *aggregate-policer-name*

Parameters

aggregate-policer-name—Specifies the aggregate policer name.

Default Configuration

Counting in-profile and out-of-profile is disabled.

Command Mode

Global Configuration mode

Example

The following example enables counting in-profile and out-of-profile on the interface.

```
Console(config)# qos statistics aggregate-policer policer1
```

qos statistics queues

Use the **qos statistics queues** Global Configuration mode command to enable QoS statistics for output queues. Use the **no** form of this command to disable QoS statistics for output queues.

Syntax

qos statistics queues *set {queue | **all**} {dp | **all**} {interface | **all**}*

no qos statistics queues *set*

Parameters

- **set**—Specifies the counter set number.
- **interface**—Specifies the Ethernet port.
- **queue**—Specifies the output queue number.
- **dp**—Specifies the drop precedence. The available values are: **high**, **low**.

Default Configuration

Set 1: All interfaces, all queues, high DP.

Set 2: All interfaces, all queues, low DP.

Command Mode

Global Configuration mode

User Guidelines

There are no user guidelines for this command.

Example

The following example enables QoS statistics for output queues for counter set 1.

```
Console(config)# qos statistics queues 1 all all all
```

show qos statistics

Use the **show qos statistics** EXEC mode command to display Quality of Service statistical information.

Syntax

show qos statistics

Command Mode

EXEC mode

User Guidelines

Up to 16 sets of counters can be enabled for policers. The counters can be enabled in the creation of the policers.

Use the **qos statistics queues** Global Configuration mode command to enable QoS statistics for output queues.

Example

The following example displays Quality of Service statistical information.

```
Console# show qos statistics

Policers
---------

Interface   Policy map    Class Map   In-profile bytes   Out-of-profile
                                                         bytes
----------  ----------    ---------   ----------------   --------------
gi1/0/1     Policy1       Class1      7564575            5433
gi1/0/1     Policy1       Class2      8759               52
gi1/0/2     Policy1       Class1      746587458          3214
gi1/0/2     Policy1       Class2      5326               23

Aggregate Policers
------------------

Name        In-profile bytes          Out-of-profile bytes
---------   ----------------          --------------------
Policer1    7985687                   121322
```

```
Output Queues
-------------

Interface    Queue         DP          Total packets      %TD packets
---------    -----         --          -------------      -----------
gi1/0/1      2             High        799921             1.2%
gi1/0/2      All           High        5387326            0.2%
```