# Catalyst 2960-X Switch Interface and Hardware Component Configuration Guide, Cisco IOS Release 15.0(2)EX

**First Published:** July 10, 2013

**Americas Headquarters**
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Text Part Number: OL-29034-01

# CONTENTS


Preface

**Preface** ix

Document Conventions ix

Related Documentation xi

Obtaining Documentation and Submitting a Service Request xi

CHAPTER 1

**Using the Command-Line Interface** 1

Information About Using the Command-Line Interface 1

Command Modes 1

Understanding Abbreviated Commands 3

No and Default Forms of Commands 3

CLI Error Messages 4

Configuration Logging 4

Using the Help System 4

How to Use the CLI to Configure Features 6

Configuring the Command History 6

Changing the Command History Buffer Size 6

Recalling Commands 6

Disabling the Command History Feature 7

Enabling and Disabling Editing Features 7

Editing Commands Through Keystrokes 8

Editing Command Lines That Wrap 9

Searching and Filtering Output of show and more Commands 10

Accessing the CLI on a Switch Stack 11

Accessing the CLI Through a Console Connection or Through Telnet 11

CHAPTER 2

**Configuring Interface Characteristics** 13

Finding Feature Information 13

Information About Configuring Interface Characteristics 13
Interface Types 13
Port-Based VLANs 14
Switch Ports 14
Access Ports 14
Trunk Ports 15
Switch Virtual Interfaces 15
SVI Autostate Exclude 16
EtherChannel Port Groups 16
Power over Ethernet Ports 16
Using the Switch USB Ports 17
USB Mini-Type B Console Port 17
Console Port Change Logs 17
USB Type A Ports 18
Interface Connections 18
Interface Configuration Mode 19
Default Ethernet Interface Configuration 19
Interface Speed and Duplex Mode 21
Speed and Duplex Configuration Guidelines 21
IEEE 802.3x Flow Control 22
How to Configure Interface Characteristics 22
Configuring Interfaces 22
Adding a Description for an Interface 23
Configuring a Range of Interfaces 24
Configuring and Using Interface Range Macros 26
Configuring Ethernet Interfaces 28
Setting the Interface Speed and Duplex Parameters 28
Configuring IEEE 802.3x Flow Control 30
Configuring SVI Autostate Exclude 31
Shutting Down and Restarting the Interface 32
Configuring the Console Media Type 34
Configuring the USB Inactivity Timeout 35
Monitoring Interface Characteristics 36
Monitoring Interface Status 36
Clearing and Resetting Interfaces and Counters 37

Configuration Examples for Interface Characteristics 38
Adding a Description to an Interface: Example 38
Configuring a Range of Interfaces: Examples 38
Configuring and Using Interface Range Macros: Examples 38
Setting Interface Speed and Duplex Mode: Example 39
Configuring the Console Media Type: Example 39
Configuring the USB Inactivity Timeout: Example 40
Additional References for the Interface Characteristics Feature 40
Feature History and Information for Configuring Interface Characteristics 41

CHAPTER 3 **Configuring Auto-MDIX** 43
Prerequisites for Auto-MDIX 43
Restrictions for Auto-MDIX 43
Information about Configuring Auto-MDIX 43
Auto-MDIX on an Interface 43
How to Configure Auto-MDIX 44
Configuring Auto-MDIX on an Interface 44
Example for Configuring Auto-MDIX 45
Additional References 46
Feature History and Information for Auto-MDIX 46

CHAPTER 4 **Configuring Ethernet Management Port** 49
Finding Feature Information 49
Prerequisites for Ethernet Management Ports 49
Information about the Ethernet Management Port 49
Ethernet Management Port Direct Connection to a Switch 50
Ethernet Management Port Connection to Stack Switches using a Hub 50
Supported Features on the Ethernet Management Port 50
How to Configure the Ethernet Management Port 51
Disabling and Enabling the Ethernet Management Port 51
Additional References 52
Feature Information for Ethernet Management Ports 54

CHAPTER 5 **Configuring LLDP, LLDP-MED, and Wired Location Service** 55
Finding Feature Information 55

LLDP, LLDP-MED, and Wired Location Service Overview 55
LLDP 55
LLDP Supported TLVs 56
LLDP and Cisco Switch Stacks 56
LLDP and Cisco Medianet 56
LLDP-MED 56
LLDP-MED Supported TLVs 57
Wired Location Service 58
Default LLDP Configuration 59
Restrictions for LLDP 59
How to Configure LLDP, LLDP-MED, and Wired Location Service 60
Enabling LLDP 60
Configuring LLDP Characteristics 61
Configuring LLDP-MED TLVs 63
Configuring Network-Policy TLV 65
Configuring Location TLV and Wired Location Service 68
Enabling Wired Location Service on the Switch 70
Configuration Examples for LLDP, LLDP-MED, and Wired Location Service 72
Configuring Network-Policy TLV: Examples 72
Monitoring and Maintaining LLDP, LLDP-MED, and Wired Location Service 72
Additional References for LLDP, LLDP-MED, and Wired Location Service 73
Feature Information for LLDP, LLDP-MED, and Wired Location Service 74

CHAPTER 6 **Configuring System MTU** 75
Finding Feature Information 75
Information about the MTU 75
System MTU Guidelines 76
How to Configure MTU 76
Configuring the System MTU 76
Configuration Examples for System MTU 77
Additional References for System MTU 78
Feature Information for System MTU 78

CHAPTER 7 **Configuring PoE** 79
Finding Feature Information 79

Restrictions for PoE 79
Information about PoE 80
Power over Ethernet Ports 80
Supported Protocols and Standards 80
Powered-Device Detection and Initial Power Allocation 80
Power Management Modes 82
Power Monitoring and Power Policing 83
Maximum Power Allocation (Cutoff Power) on a PoE Port 83
Power Consumption Values 84
How to Configure PoE 85
Configuring a Power Management Mode on a PoE Port 85
Fast POE 86
Configuring Fast POE 87
Budgeting Power for Devices Connected to a PoE Port 88
Budgeting Power to All PoE ports 89
Budgeting Power to a Specific PoE Port 90
Configuring Power Policing 91
Monitoring Power Status 94
Configuration Examples for Configuring PoE 94
Budgeting Power: Example 94
Additional References 95

CHAPTER 8 **Configuring EEE** 97
Finding Feature Information 97
Information About EEE 97
EEE Overview 97
Default EEE Configuration 98
Restrictions for EEE 98
How to Configure EEE 98
Enabling or Disabling EEE 98
Monitoring EEE 99
Configuration Examples for Configuring EEE 100
Additional References 100
Feature History and Information for Configuring EEE 101

# Preface


- Document Conventions, page ix
- Related Documentation, page xi
- Obtaining Documentation and Submitting a Service Request, page xi


## Document Conventions

This document uses the following conventions:

| Convention | Description |
|---|---|
| ^ or Ctrl | Both the ^ symbol and Ctrl represent the Control (Ctrl) key on a keyboard. For example, the key combination **^D** or **Ctrl-D** means that you hold down the Control key while you press the D key. (Keys are indicated in capital letters but are not case sensitive.) |
| **bold** font | Commands and keywords and user-entered text appear in **bold** font. |
| *Italic* font | Document titles, new or emphasized terms, and arguments for which you supply values are in *italic* font. |
| `Courier` font | Terminal sessions and information the system displays appear in `courier` font. |
| **`Bold Courier`** font | **`Bold Courier`** font indicates text that the user must enter. |
| [x] | Elements in square brackets are optional. |
| ... | An ellipsis (three consecutive nonbolded periods without spaces) after a syntax element indicates that the element can be repeated. |
| \| | A vertical line, called a pipe, indicates a choice within a set of keywords or arguments. |
| [x \| y] | Optional alternative keywords are grouped in brackets and separated by vertical bars. |

| Convention | Description |
|---|---|
| {x \| y} | Required alternative keywords are grouped in braces and separated by vertical bars. |
| [x {y \| z}] | Nested set of square brackets or braces indicate optional or required choices within optional or required elements. Braces and a vertical bar within square brackets indicate a required choice within an optional element. |
| string | A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks. |
| < > | Nonprinting characters such as passwords are in angle brackets. |
| [ ] | Default responses to system prompts are in square brackets. |
| !, # | An exclamation point (!) or a pound sign (#) at the beginning of a line of code indicates a comment line. |

### Reader Alert Conventions

This document may use the following conventions for reader alerts:

**Note** Means *reader take note*. Notes contain helpful suggestions or references to material not covered in the manual.

**Tip** Means *the following information will help you solve a problem.*

**Caution** Means *reader be careful*. In this situation, you might do something that could result in equipment damage or loss of data.

**Timesaver** Means *the described action saves time.* You can save time by performing the action described in the paragraph.

**Warning** IMPORTANT SAFETY INSTRUCTIONS

This warning symbol means danger. You are in a situation that could cause bodily injury. Before you work on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents. Use the statement number provided at the end of each warning to locate its translation in the translated safety warnings that accompanied this device. Statement 1071

SAVE THESE INSTRUCTIONS

# Related Documentation

**Note** Before installing or upgrading the switch, refer to the switch release notes.

- Catalyst 2960-X Switch documentation, located at:

  http://www.cisco.com/go/cat2960x_docs

- Cisco SFP and SFP+ modules documentation, including compatibility matrixes, located at:

  http://www.cisco.com/en/US/products/hw/modules/ps5455/tsd_products_support_series_home.html

- Error Message Decoder, located at:

  https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi

# Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/c/en/us/td/docs/general/whatsnew/whatsnew.html

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS version 2.0.

CHAPTER 1

# Using the Command-Line Interface


- Information About Using the Command-Line Interface, page 1
- How to Use the CLI to Configure Features, page 6


# Information About Using the Command-Line Interface

## Command Modes

The Cisco IOS user interface is divided into many different modes. The commands available to you depend on which mode you are currently in. Enter a question mark (?) at the system prompt to obtain a list of commands available for each command mode.

You can start a CLI session through a console connection, through Telnet, an SSH, or by using the browser.

When you start a session, you begin in user mode, often called user EXEC mode. Only a limited subset of the commands are available in user EXEC mode. For example, most of the user EXEC commands are one-time commands, such as **show** commands, which show the current configuration status, and **clear** commands, which clear counters or interfaces. The user EXEC commands are not saved when the switch reboots.

To have access to all commands, you must enter privileged EXEC mode. Normally, you must enter a password to enter privileged EXEC mode. From this mode, you can enter any privileged EXEC command or enter global configuration mode.

Using the configuration modes (global, interface, and line), you can make changes to the running configuration. If you save the configuration, these commands are stored and used when the switch reboots. To access the various configuration modes, you must start at global configuration mode. From global configuration mode, you can enter interface configuration mode and line configuration mode .

This table describes the main command modes, how to access each one, the prompt you see in that mode, and how to exit the mode.

*Table 1: Command Mode Summary*

| Mode | Access Method | Prompt | Exit Method | About This Mode |
|---|---|---|---|---|
| User EXEC | Begin a session using Telnet, SSH, or console. | `Switch>` | Enter **logout** or **quit**. | Use this mode to<br>• Change terminal settings.<br>• Perform basic tests.<br>• Display system information. |
| Privileged EXEC | While in user EXEC mode, enter the **enable** command. | `Switch#` | Enter **disable** to exit. | Use this mode to verify commands that you have entered. Use a password to protect access to this mode. |
| Global configuration | While in privileged EXEC mode, enter the **configure** command. | `Switch(config)#` | To exit to privileged EXEC mode, enter **exit** or **end**, or press **Ctrl-Z**. | Use this mode to configure parameters that apply to the entire switch. |
| VLAN configuration | While in global configuration mode, enter the **vlan** *vlan-id* command. | `Switch(config-vlan)#` | To exit to global configuration mode, enter the **exit** command.<br>To return to privileged EXEC mode, press **Ctrl-Z** or enter **end**. | Use this mode to configure VLAN parameters. When VTP mode is transparent, you can create extended-range VLANs (VLAN IDs greater than 1005) and save configurations in the switch startup configuration file. |
| Interface configuration | While in global configuration mode, enter the **interface** command (with a specific interface). | `Switch(config-if)#` | | Use this mode to configure parameters for the Ethernet ports. |

| Mode | Access Method | Prompt | Exit Method | About This Mode |
|---|---|---|---|---|
| | | | To exit to global configuration mode, enter **exit**.<br>To return to privileged EXEC mode, press **Ctrl-Z** or enter **end**. | |
| Line configuration | While in global configuration mode, specify a line with the **line vty** or **line console** command. | `Switch(config-line)#` | To exit to global configuration mode, enter **exit**.<br>To return to privileged EXEC mode, press **Ctrl-Z** or enter **end**. | Use this mode to configure parameters for the terminal line. |

# Understanding Abbreviated Commands

You need to enter only enough characters for the switch to recognize the command as unique.

This example shows how to enter the **show configuration** privileged EXEC command in an abbreviated form:

```
Switch# show conf
```

# No and Default Forms of Commands

Almost every configuration command also has a **no** form. In general, use the **no** form to disable a feature or function or reverse the action of a command. For example, the **no shutdown** interface configuration command reverses the shutdown of an interface. Use the command without the keyword **no** to reenable a disabled feature or to enable a feature that is disabled by default.

Configuration commands can also have a **default** form. The **default** form of a command returns the command setting to its default. Most commands are disabled by default, so the **default** form is the same as the **no** form. However, some commands are enabled by default and have variables set to certain default values. In these cases, the **default** command enables the command and sets variables to their default values.

# CLI Error Messages

This table lists some error messages that you might encounter while using the CLI to configure your switch.

***Table 2: Common CLI Error Messages***

| Error Message | Meaning | How to Get Help |
|---|---|---|
| `% Ambiguous command: "show con"` | You did not enter enough characters for your switch to recognize the command. | Reenter the command followed by a question mark (?) without any space between the command and the question mark.<br>The possible keywords that you can enter with the command appear. |
| `% Incomplete command.` | You did not enter all of the keywords or values required by this command. | Reenter the command followed by a question mark (?) with a space between the command and the question mark.<br>The possible keywords that you can enter with the command appear. |
| `% Invalid input detected at '^' marker.` | You entered the command incorrectly. The caret (^) marks the point of the error. | Enter a question mark (?) to display all of the commands that are available in this command mode.<br>The possible keywords that you can enter with the command appear. |

# Configuration Logging

You can log and view changes to the switch configuration. You can use the Configuration Change Logging and Notification feature to track changes on a per-session and per-user basis. The logger tracks each configuration command that is applied, the user who entered the command, the time that the command was entered, and the parser return code for the command. This feature includes a mechanism for asynchronous notification to registered applications whenever the configuration changes. You can choose to have the notifications sent to the syslog.

**Note** Only CLI or HTTP changes are logged.

# Using the Help System

You can enter a question mark (?) at the system prompt to display a list of commands available for each command mode. You can also obtain a list of associated keywords and arguments for any command.

## SUMMARY STEPS

1. **help**
2. *abbreviated-command-entry* **?**
3. *abbreviated-command-entry* <Tab>
4. **?**
5. *command* **?**
6. *command keyword* **?**

## DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **help**<br><br>**Example:**<br>`Switch# help` | Obtains a brief description of the help system in any command mode. |
| **Step 2** | *abbreviated-command-entry* **?**<br><br>**Example:**<br>`Switch# di?`<br>`dir disable disconnect` | Obtains a list of commands that begin with a particular character string. |
| **Step 3** | *abbreviated-command-entry* <Tab><br><br>**Example:**<br>`Switch# sh conf<tab>`<br>`Switch# show configuration` | Completes a partial command name. |
| **Step 4** | **?**<br><br>**Example:**<br>`Switch> ?` | Lists all commands available for a particular command mode. |
| **Step 5** | *command* **?**<br><br>**Example:**<br>`Switch> show ?` | Lists the associated keywords for a command. |
| **Step 6** | *command keyword* **?**<br><br>**Example:**<br>`Switch(config)# cdp holdtime ?`<br>`  <10-255> Length of time (in sec) that receiver must keep this packet` | Lists the associated arguments for a keyword. |

# How to Use the CLI to Configure Features

## Configuring the Command History

The software provides a history or record of commands that you have entered. The command history feature is particularly useful for recalling long or complex commands or entries, including access lists. You can customize this feature to suit your needs.

### Changing the Command History Buffer Size

By default, the switch records ten command lines in its history buffer. You can alter this number for a current terminal session or for all sessions on a particular line. This procedure is optional.

#### SUMMARY STEPS

1. **terminal history** [**size** *number-of-lines*]

#### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **terminal history** [**size** *number-of-lines*]<br><br>**Example:**<br>`Switch# terminal history size 200` | Changes the number of command lines that the switch records during the current terminal session in privileged EXEC mode. You can configure the size from 0 to 256. |

### Recalling Commands

To recall commands from the history buffer, perform one of the actions listed in this table. These actions are optional.

**Note** The arrow keys function only on ANSI-compatible terminals such as VT100s.

#### SUMMARY STEPS

1. **Ctrl-P** or use the **up arrow** key
2. **Ctrl-N** or use the **down arrow** key
3. **show history**

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **Ctrl-P** or use the **up arrow** key | Recalls commands in the history buffer, beginning with the most recent command. Repeat the key sequence to recall successively older commands. |
| **Step 2** | **Ctrl-N** or use the **down arrow** key | Returns to more recent commands in the history buffer after recalling commands with **Ctrl-P** or the up arrow key. Repeat the key sequence to recall successively more recent commands. |
| **Step 3** | **show history**<br><br>**Example:**<br>`Switch# show history` | Lists the last several commands that you just entered in privileged EXEC mode. The number of commands that appear is controlled by the setting of the **terminal history** global configuration command and the **history** line configuration command. |

## Disabling the Command History Feature

The command history feature is automatically enabled. You can disable it for the current terminal session or for the command line. This procedure is optional.

### SUMMARY STEPS

1. **terminal no history**

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **terminal no history**<br><br>**Example:**<br>`Switch# terminal no history` | Disables the feature during the current terminal session in privileged EXEC mode. |

# Enabling and Disabling Editing Features

Although enhanced editing mode is automatically enabled, you can disable it and reenable it.

### SUMMARY STEPS

1. **terminal editing**
2. **terminal no editing**

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **terminal editing**<br><br>**Example:**<br>`Switch# terminal editing` | Reenables the enhanced editing mode for the current terminal session in privileged EXEC mode. |
| **Step 2** | **terminal no editing**<br><br>**Example:**<br>`Switch# terminal no editing` | Disables the enhanced editing mode for the current terminal session in privileged EXEC mode. |

## Editing Commands Through Keystrokes

The keystrokes help you to edit the command lines. These keystrokes are optional.

**Note** The arrow keys function only on ANSI-compatible terminals such as VT100s.

***Table 3: Editing Commands***

| Editing Commands | Description |
|---|---|
| **Ctrl-B** or use the **left arrow** key | Moves the cursor back one character. |
| **Ctrl-F** or use the **right arrow** key | Moves the cursor forward one character. |
| **Ctrl-A** | Moves the cursor to the beginning of the command line. |
| **Ctrl-E** | Moves the cursor to the end of the command line. |
| **Esc B** | Moves the cursor back one word. |
| **Esc F** | Moves the cursor forward one word. |
| **Ctrl-T** | Transposes the character to the left of the cursor with the character located at the cursor. |
| **Delete** or **Backspace** key | Erases the character to the left of the cursor. |
| **Ctrl-D** | Deletes the character at the cursor. |

| | |
|---|---|
| **Ctrl-K** | Deletes all characters from the cursor to the end of the command line. |
| **Ctrl-U** or **Ctrl-X** | Deletes all characters from the cursor to the beginning of the command line. |
| **Ctrl-W** | Deletes the word to the left of the cursor. |
| **Esc D** | Deletes from the cursor to the end of the word. |
| **Esc C** | Capitalizes at the cursor. |
| **Esc L** | Changes the word at the cursor to lowercase. |
| **Esc U** | Capitalizes letters from the cursor to the end of the word. |
| **Ctrl-V** or **Esc Q** | Designates a particular keystroke as an executable command, perhaps as a shortcut. |
| **Return** key | Scrolls down a line or screen on displays that are longer than the terminal screen can display.<br>**Note** The More prompt is used for any output that has more lines than can be displayed on the terminal screen, including **show** command output. You can use the **Return** and **Space** bar keystrokes whenever you see the More prompt. |
| **Space** bar | Scrolls down one screen. |
| **Ctrl-L** or **Ctrl-R** | Redisplays the current command line if the switch suddenly sends a message to your screen. |

## Editing Command Lines That Wrap

You can use a wraparound feature for commands that extend beyond a single line on the screen. When the cursor reaches the right margin, the command line shifts ten spaces to the left. You cannot see the first ten characters of the line, but you can scroll back and check the syntax at the beginning of the command. The keystroke actions are optional.

To scroll back to the beginning of the command entry, press **Ctrl-B** or the left arrow key repeatedly. You can also press **Ctrl-A** to immediately move to the beginning of the line.

**Note** The arrow keys function only on ANSI-compatible terminals such as VT100s.

The following example shows how to wrap a command line that extends beyond a single line on the screen.

### SUMMARY STEPS

1. **access-list**
2. **Ctrl-A**
3. **Return** key

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **access-list**<br><br>**Example:**<br>`Switch(config)# access-list 101 permit tcp 10.15.22.25 255.255.255.0 10.15.22.35`<br>`Switch(config)# $ 101 permit tcp 10.15.22.25 255.255.255.0 10.15.22.35 255.25`<br>`Switch(config)# $t tcp 10.15.22.25 255.255.255.0 131.108.1.20 255.255.255.0 eq`<br>`Switch(config)# $15.22.25 255.255.255.0 10.15.22.35 255.255.255.0 eq 45` | Displays the global configuration command entry that extends beyond one line.<br><br>When the cursor first reaches the end of the line, the line is shifted ten spaces to the left and redisplayed. The dollar sign ($) shows that the line has been scrolled to the left. Each time the cursor reaches the end of the line, the line is again shifted ten spaces to the left. |
| **Step 2** | **Ctrl-A**<br><br>**Example:**<br>`Switch(config)# access-list 101 permit tcp 10.15.22.25 255.255.255.0 10.15.2$` | Checks the complete syntax.<br><br>The dollar sign ($) appears at the end of the line to show that the line has been scrolled to the right. |
| **Step 3** | **Return** key | Execute the commands.<br><br>The software assumes that you have a terminal screen that is 80 columns wide. If you have a different width, use the **terminal width** privileged EXEC command to set the width of your terminal.<br><br>Use line wrapping with the command history feature to recall and modify previous complex command entries. |

# Searching and Filtering Output of show and more Commands

You can search and filter the output for **show** and **more** commands. This is useful when you need to sort through large amounts of output or if you want to exclude output that you do not need to see. Using these commands is optional.

### SUMMARY STEPS

1. {**show** | **more**} *command* | {**begin** | **include** | **exclude**} *regular-expression*

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | {**show** \| **more**} *command* \| {**begin** \| **include** \| **exclude**} *regular-expression*<br><br>**Example:**<br>`Switch# show interfaces \| include protocol`<br>`Vlan1 is up, line protocol is up`<br>`Vlan10 is up, line protocol is down`<br>`GigabitEthernet1/0/1 is up, line protocol is down`<br>`GigabitEthernet1/0/2 is up, line protocol is up` | Searches and filters the output.<br><br>Expressions are case sensitive. For example, if you enter **\| exclude output**, the lines that contain **output** are not displayed, but the lines that contain **output** appear. |

# Accessing the CLI on a Switch Stack

You can access the CLI through a console connection, through Telnet, a SSH, or by using the browser.

You manage the switch stack and the stack member interfaces through the stack master. You cannot manage stack members on an individual switch basis. You can connect to the stack master through the console port or the Ethernet management port of one or more stack members. Be careful with using multiple CLI sessions on the stack master. Commands that you enter in one session are not displayed in the other sessions. Therefore, it is possible to lose track of the session from which you entered commands.

**Note** We recommend using one CLI session when managing the switch stack.

If you want to configure a specific stack member port, you must include the stack member number in the CLI command interface notation.

# Accessing the CLI Through a Console Connection or Through Telnet

Before you can access the CLI, you must connect a terminal or a PC to the switch console or connect a PC to the Ethernet management port and then power on the switch, as described in the hardware installation guide that shipped with your switch.

If your switch is already configured, you can access the CLI through a local console connection or through a remote Telnet session, but your switch must first be configured for this type of access.

You can use one of these methods to establish a connection with the switch:

- Connect the switch console port to a management station or dial-up modem, or connect the Ethernet management port to a PC. For information about connecting to the console or Ethernet management port, see the switch hardware installation guide.
- Use any Telnet TCP/IP or encrypted Secure Shell (SSH) package from a remote management station. The switch must have network connectivity with the Telnet or SSH client, and the switch must have an enable secret password configured.

- The switch supports up to 16 simultaneous Telnet sessions. Changes made by one Telnet user are reflected in all other Telnet sessions.
- The switch supports up to five simultaneous secure SSH sessions.

After you connect through the console port, through the Ethernet management port, through a Telnet session or through an SSH session, the user EXEC prompt appears on the management station.

CHAPTER 2

# Configuring Interface Characteristics


- Finding Feature Information, page 13
- Information About Configuring Interface Characteristics, page 13
- How to Configure Interface Characteristics, page 22
- Monitoring Interface Characteristics, page 36
- Configuration Examples for Interface Characteristics, page 38
- Additional References for the Interface Characteristics Feature, page 40
- Feature History and Information for Configuring Interface Characteristics, page 41


## Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

## Information About Configuring Interface Characteristics

### Interface Types

This section describes the different types of interfaces supported by the switch. The rest of the chapter describes configuration procedures for physical interface characteristics.

**Note** The stack ports on the rear of the stacking-capable switches are not Ethernet ports and cannot be configured.

## Port-Based VLANs

A VLAN is a switched network that is logically segmented by function, team, or application, without regard to the physical location of the users. Packets received on a port are forwarded only to ports that belong to the same VLAN as the receiving port. Network devices in different VLANs cannot communicate with one another without a Layer 3 device to route traffic between the VLANs.

VLAN partitions provide hard firewalls for traffic in the VLAN, and each VLAN has its own MAC address table. A VLAN comes into existence when a local port is configured to be associated with the VLAN, when the VLAN Trunking Protocol (VTP) learns of its existence from a neighbor on a trunk, or when a user creates a VLAN. VLANs can be formed with ports across the stack.

To configure VLANs, use the **vlan** *vlan-id* global configuration command to enter VLAN configuration mode. The VLAN configurations for normal-range VLANs (VLAN IDs 1 to 1005) are saved in the VLAN database. If VTP is version 1 or 2, to configure extended-range VLANs (VLAN IDs 1006 to 4094), you must first set VTP mode to transparent. Extended-range VLANs created in transparent mode are not added to the VLAN database but are saved in the switch running configuration. With VTP version 3, you can create extended-range VLANs in client or server mode. These VLANs are saved in the VLAN database.

In a switch stack, the VLAN database is downloaded to all switches in a stack, and all switches in the stack build the same VLAN database. The running configuration and the saved configuration are the same for all switches in a stack.

Add ports to a VLAN by using the **switchport** interface configuration commands:

- Identify the interface.
- For a trunk port, set trunk characteristics, and, if desired, define the VLANs to which it can belong.
- For an access port, set and define the VLAN to which it belongs.

## Switch Ports

Switch ports are Layer 2-only interfaces associated with a physical port. Switch ports belong to one or more VLANs. A switch port can be an access port or a trunk port. You can configure a port as an access port or trunk port or let the Dynamic Trunking Protocol (DTP) operate on a per-port basis to set the switchport mode by negotiating with the port on the other end of the link. switch ports are used for managing the physical interface and associated Layer 2 protocols and do not handle routing or bridging.

Configure switch ports by using the **switchport** interface configuration commands.

### Access Ports

An access port belongs to and carries the traffic of only one VLAN (unless it is configured as a voice VLAN port). Traffic is received and sent in native formats with no VLAN tagging. Traffic arriving on an access port is assumed to belong to the VLAN assigned to the port. If an access port receives a tagged packet (Inter-Switch Link [ISL] or IEEE 802.1Q tagged), the packet is dropped, and the source address is not learned.

The types of access ports supported are:

- Static access ports are manually assigned to a VLAN (or through a RADIUS server for use with IEEE 802.1x.
- VLAN membership of dynamic access ports is learned through incoming packets. By default, a dynamic access port is not a member of any VLAN, and forwarding to and from the port is enabled only when the VLAN membership of the port is discovered. Dynamic access ports on the switch are assigned to a VLAN by a VLAN Membership Policy Server (VMPS). The VMPS can be a Catalyst 6500 series switch; the switch cannot be a VMPS server.

You can also configure an access port with an attached Cisco IP Phone to use one VLAN for voice traffic and another VLAN for data traffic from a device attached to the phone.

### Trunk Ports

A trunk port carries the traffic of multiple VLANs and by default is a member of all VLANs in the VLAN database.

The switch supports only IEEE 802.1Q trunk ports. An IEEE 802.1Q trunk port supports simultaneous tagged and untagged traffic. An IEEE 802.1Q trunk port is assigned a default port VLAN ID (PVID), and all untagged traffic travels on the port default PVID. All untagged traffic and tagged traffic with a NULL VLAN ID are assumed to belong to the port default PVID. A packet with a VLAN ID equal to the outgoing port default PVID is sent untagged. All other traffic is sent with a VLAN tag.

Although by default, a trunk port is a member of every VLAN known to the VTP, you can limit VLAN membership by configuring an allowed list of VLANs for each trunk port. The list of allowed VLANs does not affect any other port but the associated trunk port. By default, all possible VLANs (VLAN ID 1 to 4094) are in the allowed list. A trunk port can become a member of a VLAN only if VTP knows of the VLAN and if the VLAN is in the enabled state. If VTP learns of a new, enabled VLAN and the VLAN is in the allowed list for a trunk port, the trunk port automatically becomes a member of that VLAN and traffic is forwarded to and from the trunk port for that VLAN. If VTP learns of a new, enabled VLAN that is not in the allowed list for a trunk port, the port does not become a member of the VLAN, and no traffic for the VLAN is forwarded to or from the port.

## Switch Virtual Interfaces

A switch virtual interface (SVI) represents a VLAN of switch ports as one interface to the routing or bridging function in the system. You can associate only one SVI with a VLAN. You configure an SVI for a VLAN only to route between VLANs or to provide IP host connectivity to the switch. By default, an SVI is created for the default VLAN (VLAN 1) to permit remote switch administration. Additional SVIs must be explicitly configured.

**Note** You cannot delete interface VLAN 1.

SVIs provide IP host connectivity only to the system. SVIs are created the first time that you enter the **vlan** interface configuration command for a VLAN interface. The VLAN corresponds to the VLAN tag associated with data frames on an ISL or IEEE 802.1Q encapsulated trunk or the VLAN ID configured for an access port. Configure a VLAN interface for each VLAN for which you want to route traffic, and assign it an IP address.

Although the switch stack or switch supports a total of 1005 VLANs and SVIs, the interrelationship between the number of SVIs and routed ports and the number of other features being configured might impact CPU performance because of hardware limitations.

When you create an SVI, it does not become active until it is associated with a physical port.

### SVI Autostate Exclude

The line state of an SVI with multiple ports on a VLAN is in the *up* state when it meets these conditions:

- The VLAN exists and is active in the VLAN database on the switch
- The VLAN interface exists and is not administratively down.
- At least one Layer 2 (access or trunk) port exists, has a link in the *up* state on this VLAN, and is in the spanning-tree forwarding state on the VLAN.

**Note** The protocol link state for VLAN interfaces come up when the first switchport belonging to the corresponding VLAN link comes up and is in STP forwarding state.

The default action, when a VLAN has multiple ports, is that the SVI goes down when all ports in the VLAN go down. You can use the SVI autostate exclude feature to configure a port so that it is not included in the SVI line-state up-or-down calculation. For example, if the only active port on the VLAN is a monitoring port, you might configure autostate exclude on that port so that the VLAN goes down when all other ports go down. When enabled on a port, **autostate exclude** applies to all VLANs that are enabled on that port.

The VLAN interface is brought up when one Layer 2 port in the VLAN has had time to converge (transition from STP listening-learning state to forwarding state). This prevents features such as routing protocols from using the VLAN interface as if it were fully operational and minimizes other problems, such as routing black holes.

## EtherChannel Port Groups

EtherChannel port groups treat multiple switch ports as one switch port. These port groups act as a single logical port for high-bandwidth connections between switches or between switches and servers. An EtherChannel balances the traffic load across the links in the channel. If a link within the EtherChannel fails, traffic previously carried over the failed link changes to the remaining links. You can group multiple trunk ports into one logical trunk port or multiple access ports into one logical access port. Most protocols operate over either single ports or aggregated switch ports and do not recognize the physical ports within the port group. Exceptions are the DTP, the Cisco Discovery Protocol (CDP), and the Port Aggregation Protocol (PAgP), which operate only on physical ports.

When you configure an EtherChannel, you create a port-channel logical interface and assign an interface to the EtherChannel. For Layer 2 interfaces, use the **channel-group** interface configuration command to dynamically create the port-channel logical interface. This command binds the physical and logical ports together.

## Power over Ethernet Ports

A PoE-capable switch port automatically supplies power to one of these connected devices if the switch senses that there is no power on the circuit:

- a Cisco pre-standard powered device (such as a Cisco IP Phone or a Cisco Aironet Access Point)
- an IEEE 802.3af-compliant powered device

A powered device can receive redundant power when it is connected to a PoE switch port and to an AC power source. The device does not receive redundant power when it is only connected to the PoE port.

# Using the Switch USB Ports

Theswitch has three USB ports on the front panel — a USB mini-Type B console port and two USB Type A ports.

## USB Mini-Type B Console Port

The switch has the following console ports:

- USB mini-Type B console connection
- RJ-45 console port

Console output appears on devices connected to both ports, but console input is active on only one port at a time. By default, the USB connector takes precedence over the RJ-45 connector.

**Note** Windows PCs require a driver for the USB port. See the hardware installation guide for driver installation instructions.

Use the supplied USB Type A-to-USB mini-Type B cable to connect a PC or other device to the switch. The connected device must include a terminal emulation application. When the switch detects a valid USB connection to a powered-on device that supports host functionality (such as a PC), input from the RJ-45 console is immediately disabled, and input from the USB console is enabled. Removing the USB connection immediately reenables input from the RJ-45 console connection. An LED on the switch shows which console connection is in use.

### Console Port Change Logs

At software startup, a log shows whether the USB or the RJ-45 console is active. Each switch in a stack issues this log. Every switch always first displays the RJ-45 media type.

In the sample output, Switch 1 has a connected USB console cable. Because the bootloader did not change to the USB console, the first log from Switch 1 shows the RJ-45 console. A short time later, the console changes and the USB console log appears. Switch 2 and Switch 3 have connected RJ-45 console cables.

```
switch-stack-1
*Mar  1 00:01:00.171: %USB_CONSOLE-6-MEDIA_RJ45: Console media-type is RJ45.
*Mar  1 00:01:00.431: %USB_CONSOLE-6-MEDIA_USB: Console media-type is USB.

switch-stack-2
*Mar  1 00:01:09.835: %USB_CONSOLE-6-MEDIA_RJ45: Console media-type is RJ45.

switch-stack-3
*Mar  1 00:01:10.523: %USB_CONSOLE-6-MEDIA_RJ45: Console media-type is RJ45.
```

When the USB cable is removed or the PC de-activates the USB connection, the hardware automatically changes to the RJ-45 console interface:

```
switch-stack-1
Mar  1 00:20:48.635: %USB_CONSOLE-6-MEDIA_RJ45: Console media-type is RJ45.
```

You can configure the console type to always be RJ-45, and you can configure an inactivity timeout for the USB connector.

### USB Type A Ports

The USB Type A ports provide access to external USB flash devices, also known as thumb drives or USB keys. The switch supports Cisco 64 MB, 256 MB, 512 MB, 1 GB, 4 GB, and 8 GB flash drives. You can use standard Cisco IOS command- line interface (CLI) commands to read, write, erase, and copy to or from the flash device. You can also configure the switch to boot from the USB flash drive.

For information about configuring the switch to boot from a USB flash drive, refer to the *Catalyst 2960-X Switch System Management Configuration Guide*.

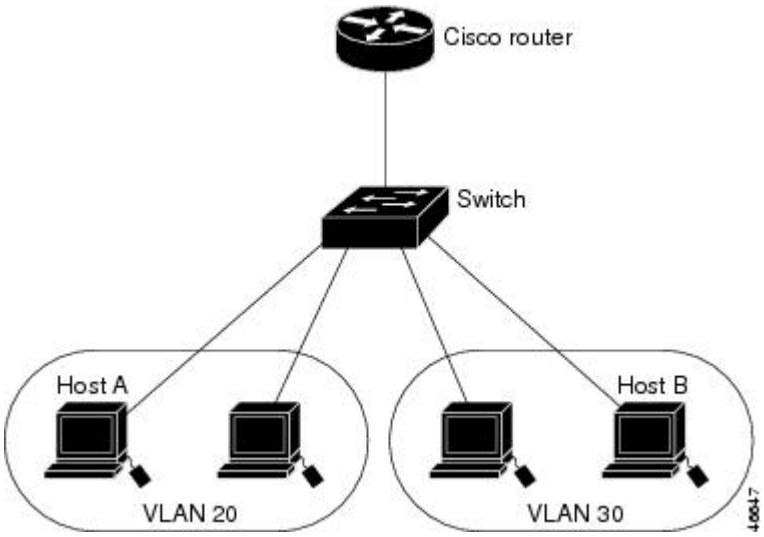
For information about reading, writing, erasing, and copying files to or from the flash device, refer to the *Catalyst 2960-X Switch Managing Cisco IOS Image Files Configuration Guide*.

## Interface Connections

Devices within a single VLAN can communicate directly through any switch. Ports in different VLANs cannot exchange data without going through a routing device.

In the following configuration example, when Host A in VLAN 20 sends data to Host B in VLAN 30, the data must go from Host A to the switch, to the router, back to the switch, and then to Host B.

***Figure 1: Connecting VLANs with the Switch***




With a standard Layer 2 switch, ports in different VLANs have to exchange information through a router.

# Interface Configuration Mode

The switch supports these interface types:

- Physical ports—switch ports and routed ports
- VLANs—switch virtual interfaces
- Port channels—EtherChannel interfaces

You can also configure a range of interfaces.

To configure a physical interface (port), specify the interface type, module number, and switch port number, and enter interface configuration mode.

- Type—Gigabit Ethernet (gigabitethernet or gi) for 10/100/1000 Mb/s Ethernet ports, or small form-factor pluggable (SFP) module Gigabit Ethernet interfaces (gigabitethernet or gi).
- Stack member number—The number that identifies the switch within the stack. The range is 1 to 8 for a stack of Catalyst 2960-X switches, and 1 to 4 for a mixed stack of Catalyst 2960-X and Catalyst 2960-S switches. The switch number is assigned the first time the switch initializes. The default switch number, before it is integrated into a switch stack, is 1. When a switch has been assigned a stack member number, it keeps that number until another is assigned to it.

  You can use the switch port LEDs in Stack mode to identify the stack member number of a switch.
- Module number—The module or slot number on the switch (always 0).
- Port number—The interface number on the switch. The 10/100/1000 port numbers always begin at 1, starting with the far left port when facing the front of the switch, for example, gigabitethernet1/0/1 or gigabitethernet1/0/8. For a switch with 10/100/1000 ports and SFP module ports, SFP module ports are numbered consecutively following the 10/100/1000 ports.

You can identify physical interfaces by physically checking the interface location on the switch. You can also use the **show** privileged EXEC commands to display information about a specific interface or all the interfaces on the switch. The remainder of this chapter primarily provides physical interface configuration procedures.

These are examples of how to identify interfaces on a stacking-capable switch:

- To configure 10/100/1000 port 4 on a standalone switch, enter this command:

```
Switch(config)# interface gigabitethernet1/0/4
```

- To configure 10/100/1000 port 4 on stack member 3, enter this command:

```
Switch(config)# interface gigabitethernet3/0/4
```

# Default Ethernet Interface Configuration

This table shows the Ethernet interface default configuration, including some features that apply only to Layer 2 interfaces.

*Table 4: Default Layer 2 Ethernet Interface Configuration*

| Feature | Default Setting |
|---|---|
| Operating mode | Layer 2 or switching mode (**switchport** command). |
| Allowed VLAN range | VLANs 1– 4094. |
| Default VLAN (for access ports) | VLAN 1. |
| Native VLAN (for IEEE 802.1Q trunks) | VLAN 1. |
| 802.1p priority-tagged traffic | Drop all packets tagged with VLAN 0. |
| VLAN trunking | Switchport mode dynamic auto (supports DTP). |
| Port enable state | All ports are enabled. |
| Port description | None defined. |
| Speed | Autonegotiate. (Not supported on the 10-Gigabit interfaces.) |
| Duplex mode | Autonegotiate. (Not supported on the 10-Gigabit interfaces.) |
| Flow control | Flow control is set to **receive: off**. It is always off for sent packets. |
| EtherChannel (PAgP) | Disabled on all Ethernet ports. |
| Port blocking (unknown multicast and unknown unicast traffic) | Disabled (not blocked). |
| Broadcast, multicast, and unicast storm control | Disabled. |
| Protected port | Disabled. |
| Port security | Disabled. |
| Port Fast | Disabled. |
| Auto-MDIX | Enabled.<br>**Note** The switch might not support a pre-standard powered device—such as Cisco IP phones and access points that do not fully support IEEE 802.3af—if that powered device is connected to the switch through a crossover cable. This is regardless of whether auto-MIDX is enabled on the switch port. |

| Feature | Default Setting |
|---|---|
| Power over Ethernet (PoE) | Enabled (auto). |
| Keepalive messages | Disabled on SFP module ports; enabled on all other ports. |

# Interface Speed and Duplex Mode

Ethernet interfaces on the switch operate at 10, 100, or 1000 Mb/s and in either full- or half-duplex mode. In full-duplex mode, two stations can send and receive traffic at the same time. Normally, 10-Mb/s ports operate in half-duplex mode, which means that stations can either receive or send traffic.

Switch models include Gigabit Ethernet (10/100/1000-Mb/s) ports and small form-factor pluggable (SFP) module slots supporting SFP modules.

# Speed and Duplex Configuration Guidelines

When configuring an interface speed and duplex mode, note these guidelines:

- Gigabit Ethernet (10/100/1000-Mb/s) ports support all speed options and all duplex options (auto, half, and full). However, Gigabit Ethernet ports operating at 1000 Mb/s do not support half-duplex mode.
- For SFP module ports, the speed and duplex CLI options change depending on the SFP module type:
  - The 1000BASE-*x* (where -*x* is -BX, -CWDM, -LX, -SX, and -ZX) SFP module ports support the **nonegotiate** keyword in the **speed** interface configuration command. Duplex options are not supported.
  - The 1000BASE-T SFP module ports support the same speed and duplex options as the 10/100/1000-Mb/s ports.
- If both ends of the line support autonegotiation, we highly recommend the default setting of **auto** negotiation.
- If one interface supports autonegotiation and the other end does not, configure duplex and speed on both interfaces; do not use the **auto** setting on the supported side.
- When STP is enabled and a port is reconfigured, the switch can take up to 30 seconds to check for loops. The port LED is amber while STP reconfigures.

**Caution** Changing the interface speed and duplex mode configuration might shut down and re-enable the interface during the reconfiguration.

# IEEE 802.3x Flow Control

Flow control enables connected Ethernet ports to control traffic rates during congestion by allowing congested nodes to pause link operation at the other end. If one port experiences congestion and cannot receive any more traffic, it notifies the other port by sending a pause frame to stop sending until the condition clears. Upon receipt of a pause frame, the sending device stops sending any data packets, which prevents any loss of data packets during the congestion period.

**Note** The switch ports can receive, but not send, pause frames.

You use the **flowcontrol** interface configuration command to set the interface's ability to **receive** pause frames to **on**, **off**, or **desired**. The default state is **off**.

When set to **desired**, an interface can operate with an attached device that is required to send flow-control packets or with an attached device that is not required to but can send flow-control packets.

These rules apply to flow control settings on the device:

- **receive on** (or **desired**): The port cannot send pause frames but can operate with an attached device that is required to or can send pause frames; the port can receive pause frames.
- **receive off**: Flow control does not operate in either direction. In case of congestion, no indication is given to the link partner, and no pause frames are sent or received by either device.

**Note** For details on the command settings and the resulting flow control resolution on local and remote ports, see the **flowcontrol** interface configuration command in the command reference for this release.

# How to Configure Interface Characteristics

## Configuring Interfaces

These general instructions apply to all interface configuration processes.

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br><br>**Example:**<br>`Switch> enable` | Enables privileged EXEC mode. Enter your password if prompted. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 2** | **configure terminal**<br><br>**Example:**<br><br>`Switch# configure terminal` | Enters the global configuration mode. |
| **Step 3** | **interface**<br><br>**Example:**<br><br>`Switch(config)# interface gigabitethernet1/0/1`<br>`Switch(config-if)#` | Identifies the interface type, the switch number (only on stacking-capable switches), and the number of the connector.<br><br>**Note** You do not need to add a space between the interface type and the interface number. For example, in the preceding line, you can specify either **gigabitethernet 1/0/1**, **gigabitethernet1/0/1**, **gi 1/0/1**, or **gi1/0/1**. |
| **Step 4** | Follow each **interface** command with the interface configuration commands that the interface requires. | Defines the protocols and applications that will run on the interface. The commands are collected and applied to the interface when you enter another interface command or enter **end** to return to privileged EXEC mode. |
| **Step 5** | **interface range** or **interface range macro** | (Optional) Configures a range of interfaces.<br>**Note** Interfaces configured in a range must be the same type and must be configured with the same feature options. |
| **Step 6** | **show interfaces** | Displays a list of all interfaces on or configured for the switch. A report is provided for each interface that the device supports or for the specified interface. |

# Adding a Description for an Interface

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *interface-id*
4. **description** *string*
5. **end**
6. **show interfaces** *interface-id* **description**
7. **copy running-config startup-config**

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br><br>**Example:**<br>`Switch> enable` | Enables privileged EXEC mode. Enter your password if prompted. |
| **Step 2** | **configure terminal**<br><br>**Example:**<br>`Switch# configure terminal` | Enters global configuration mode. |
| **Step 3** | **interface** *interface-id*<br><br>**Example:**<br>`Switch(config)# interface gigabitethernet1/0/2` | Specifies the interface for which you are adding a description, and enter interface configuration mode. |
| **Step 4** | **description** *string*<br><br>**Example:**<br>`Switch(config-if)# description Connects to Marketing` | Adds a description (up to 240 characters) for an interface. |
| **Step 5** | **end**<br><br>**Example:**<br>`Switch(config-if)# end` | Returns to privileged EXEC mode. |
| **Step 6** | **show interfaces** *interface-id* **description** | Verifies your entry. |
| **Step 7** | **copy running-config startup-config**<br><br>**Example:**<br>`Switch# copy running-config startup-config` | (Optional) Saves your entries in the configuration file. |

# Configuring a Range of Interfaces

To configure multiple interfaces with the same configuration parameters, use the **interface range** global configuration command. When you enter the interface-range configuration mode, all command parameters that you enter are attributed to all interfaces within that range until you exit this mode.

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface range** {*port-range* | **macro** *macro_name*}
4. **end**
5. **show interfaces** [*interface-id*]
6. **copy running-config startup-config**

## DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br><br>**Example:**<br><br>`Switch> enable` | Enables privileged EXEC mode. Enter your password if prompted. |
| **Step 2** | **configure terminal**<br><br>**Example:**<br><br>`Switch# configure terminal` | Enters global configuration mode. |
| **Step 3** | **interface range** {*port-range* \| **macro** *macro_name*}<br><br>**Example:**<br><br>`Switch(config)# interface range macro` | Specifies the range of interfaces (VLANs or physical ports) to be configured, and enter interface-range configuration mode.<br><br>• You can use the **interface range** command to configure up to five port ranges or a previously defined macro.<br><br>• The **macro** variable is explained in the Configuring and Using Interface Range Macros, on page 26.<br><br>• In a comma-separated *port-range*, you must enter the interface type for each entry and enter spaces before and after the comma.<br><br>• In a hyphen-separated *port-range*, you do not need to re-enter the interface type, but you must enter a space before the hyphen.<br><br>**Note** Use the normal configuration commands to apply the configuration parameters to all interfaces in the range. Each command is executed as it is entered. |
| **Step 4** | **end**<br><br>**Example:**<br><br>`Switch(config)# end` | Returns to privileged EXEC mode. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 5** | **show interfaces** [*interface-id*]<br><br>**Example:**<br><br>`Switch# show interfaces` | Verifies the configuration of the interfaces in the range. |
| **Step 6** | **copy running-config startup-config**<br><br>**Example:**<br><br>`Switch# copy running-config startup-config` | (Optional) Saves your entries in the configuration file. |

# Configuring and Using Interface Range Macros

You can create an interface range macro to automatically select a range of interfaces for configuration. Before you can use the **macro** keyword in the **interface range macro** global configuration command string, you must use the **define interface-range** global configuration command to define the macro.

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **define interface-range** *macro_name interface-range*
4. **interface range macro** *macro_name*
5. **end**
6. **show running-config | include define**
7. **copy running-config startup-config**

## DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br><br>**Example:**<br><br>`Switch> enable` | Enables privileged EXEC mode. Enter your password if prompted. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 2** | **configure terminal**<br><br>**Example:**<br><br>`Switch# configure terminal` | Enters global configuration mode. |
| **Step 3** | **define interface-range** *macro_name interface-range*<br><br>**Example:**<br><br>`Switch(config)# define interface-range enet_list gigabitethernet1/0/1 - 2` | Defines the interface-range macro, and save it in NVRAM.<br>• The *macro_name* is a 32-character maximum character string.<br>• A macro can contain up to five comma-separated interface ranges.<br>• Each *interface-range* must consist of the same port type.<br><br>**Note** Before you can use the **macro** keyword in the **interface range macro** global configuration command string, you must use the **define interface-range** global configuration command to define the macro. |
| **Step 4** | **interface range macro** *macro_name*<br><br>**Example:**<br><br>`Switch(config)# interface range macro enet_list` | Selects the interface range to be configured using the values saved in the interface-range macro called *macro_name*.<br>You can now use the normal configuration commands to apply the configuration to all interfaces in the defined macro. |
| **Step 5** | **end**<br><br>**Example:**<br><br>`Switch(config)# end` | Returns to privileged EXEC mode. |
| **Step 6** | **show running-config \| include define**<br><br>**Example:**<br><br>`Switch# show running-config \| include define` | Shows the defined interface range macro configuration. |
| **Step 7** | **copy running-config startup-config**<br><br>**Example:**<br><br>`Switch# copy running-config startup-config` | (Optional) Saves your entries in the configuration file. |

# Configuring Ethernet Interfaces

## Setting the Interface Speed and Duplex Parameters

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *interface-id*
4. **speed** {**10** | **100** | **1000** | **2500** | **5000** | **10000** | **auto** [**10** | **100** | **1000** | **2500** | **5000** | **10000**] | **nonegotiate**}
5. **duplex** {**auto** | **full** | **half**}
6. **end**
7. **show interfaces** *interface-id*
8. **copy running-config startup-config**
9. **copy running-config startup-config**

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br><br>**Example:**<br>`Switch> enable` | Enables privileged EXEC mode. Enter your password if prompted. |
| **Step 2** | **configure terminal**<br><br>**Example:**<br>`Switch# configure terminal` | Enters global configuration mode. |
| **Step 3** | **interface** *interface-id*<br><br>**Example:**<br>`Switch(config)# interface gigabitethernet1/0/3` | Specifies the physical interface to be configured, and enter interface configuration mode. |
| **Step 4** | **speed** {**10** \| **100** \| **1000** \| **2500** \| **5000** \| **10000** \| **auto** [**10** \| **100** \| **1000** \| **2500** \| **5000** \| **10000**] \| **nonegotiate**}<br><br>**Example:**<br>`Switch(config-if)# speed 10` | Enter the appropriate speed parameter for the interface:<br>• Enter **10**, **100**, **1000 2500**, **5000**, or **10000** to set a specific speed for the interface.<br>• Enter **auto** to enable the interface to autonegotiate speed with the connected device. If you specify a speed and also set the |

| | Command or Action | Purpose |
|---|---|---|
| | | **auto** keyword, the port autonegotiates only at the specified speeds.<br>• The **nonegotiate** keyword is available only for SFP module ports. SFP module ports operate only at 1000 Mb/s but can be configured to not negotiate if connected to a device that does not support autonegotiation. |
| **Step 5** | **duplex** {**auto** \| **full** \| **half**}<br><br>**Example:**<br><br>`Switch(config-if)# duplex half` | This command is not available on a 10-Gigabit Ethernet interface.<br>Enter the duplex parameter for the interface.<br>Enable half-duplex mode (for interfaces operating only at 10 or 100 Mb/s). You cannot configure half-duplex mode for interfaces operating at 1000 Mb/s.<br>You can configure the duplex setting when the speed is set to **auto**. |
| **Step 6** | **end**<br><br>**Example:**<br><br>`Switch(config-if)# end` | Returns to privileged EXEC mode. |
| **Step 7** | **show interfaces** *interface-id*<br><br>**Example:**<br><br>`Switch# show interfaces gigabitethernet1/0/3` | Displays the interface speed and duplex mode configuration. |
| **Step 8** | **copy running-config startup-config**<br><br>**Example:**<br><br>`Switch# copy running-config startup-config` | (Optional) Saves your entries in the configuration file. |
| **Step 9** | **copy running-config startup-config**<br><br>**Example:**<br><br>`Switch# copy running-config startup-config` | (Optional) Saves your entries in the configuration file. |

# Configuring IEEE 802.3x Flow Control

## SUMMARY STEPS

1. **configure terminal**
2. **interface** *interface-id*
3. **flowcontrol** {**receive**} {**on** | **off** | **desired**}
4. **end**
5. **show interfaces** *interface-id*
6. **copy running-config startup-config**

## DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **configure terminal**<br><br>**Example:**<br>`Switch# configure terminal` | Enters global configuration mode |
| **Step 2** | **interface** *interface-id*<br><br>**Example:**<br>`Switch(config)# interface gigabitethernet1/0/1` | Specifies the physical interface to be configured, and enter interface configuration mode. |
| **Step 3** | **flowcontrol** {**receive**} {**on** | **off** | **desired**}<br><br>**Example:**<br>`Switch(config-if)# flowcontrol receive on` | Configures the flow control mode for the port. |
| **Step 4** | **end**<br><br>**Example:**<br>`Switch(config-if)# end` | Returns to privileged EXEC mode. |
| **Step 5** | **show interfaces** *interface-id*<br><br>**Example:**<br>`Switch# show interfaces gigabitethernet1/0/1` | Verifies the interface flow control settings. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 6** | **copy running-config startup-config**<br><br>**Example:**<br><br>`Switch# copy running-config startup-config` | (Optional) Saves your entries in the configuration file. |

# Configuring SVI Autostate Exclude

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *interface-id*
4. **switchport autostate exclude**
5. **end**
6. **show running config interface** *interface-id*
7. **copy running-config startup-config**

## DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br><br>**Example:**<br><br>`Switch> enable` | Enables privileged EXEC mode. Enter your password if prompted. |
| **Step 2** | **configure terminal**<br><br>**Example:**<br><br>`Switch# configure terminal` | Enters global configuration mode. |
| **Step 3** | **interface** *interface-id*<br><br>**Example:**<br><br>`Switch(config)# interface gigabitethernet1/0/2` | Specifies a Layer 2 interface (physical port or port channel), and enter interface configuration mode. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 4** | **switchport autostate exclude**<br><br>**Example:**<br><br>`Switch(config-if)# switchport autostate exclude` | Excludes the access or trunk port when defining the status of an SVI line state (up or down) |
| **Step 5** | **end**<br><br>**Example:**<br><br>`Switch(config-if)# end` | Returns to privileged EXEC mode. |
| **Step 6** | **show running config interface** *interface-id* | (Optional) Shows the running configuration.<br>Verifies the configuration. |
| **Step 7** | **copy running-config startup-config**<br><br>**Example:**<br><br>`Switch# copy running-config startup-config` | (Optional) Saves your entries in the configuration file. |

# Shutting Down and Restarting the Interface

Shutting down an interface disables all functions on the specified interface and marks the interface as unavailable on all monitoring command displays. This information is communicated to other network servers through all dynamic routing protocols. The interface is not mentioned in any routing updates.

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** {**vlan** *vlan-id*} | { **gigabitethernet***interface-id*} | {**port-channel** *port-channel-number*}
4. **shutdown**
5. **no shutdown**
6. **end**
7. **show running-config**

## DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br><br>**Example:**<br>`Switch> enable` | Enables privileged EXEC mode. Enter your password if prompted. |
| **Step 2** | **configure terminal**<br><br>**Example:**<br>`Switch# configure terminal` | Enters global configuration mode. |
| **Step 3** | **interface** {**vlan** *vlan-id*} \| { **gigabitethernet***interface-id*} \| {**port-channel** *port-channel-number*}<br><br>**Example:**<br>`Switch(config)# interface gigabitethernet1/0/2` | Selects the interface to be configured. |
| **Step 4** | **shutdown**<br><br>**Example:**<br>`Switch(config-if)# shutdown` | Shuts down an interface. |
| **Step 5** | **no shutdown**<br><br>**Example:**<br>`Switch(config-if)# no shutdown` | Restarts an interface. |
| **Step 6** | **end**<br><br>**Example:**<br>`Switch(config-if)# end` | Returns to privileged EXEC mode. |
| **Step 7** | **show running-config**<br><br>**Example:**<br>`Switch# show running-config` | Verifies your entries. |

# Configuring the Console Media Type

Follow these steps to set the console media type to RJ-45. If you configure the console as RJ-45, USB console operation is disabled, and input comes only through the RJ-45 connector.

This configuration applies to all switches in a stack.

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **line console 0**
4. **media-type rj45**
5. **end**
6. **copy running-config startup-config**

## DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br><br>**Example:**<br>`Switch> enable` | Enables privileged EXEC mode. Enter your password if prompted. |
| **Step 2** | **configure terminal**<br><br>**Example:**<br>`Switch# configure terminal` | Enters the global configuration mode. |
| **Step 3** | **line console 0**<br><br>**Example:**<br>`Switch(config)# line console 0` | Configures the console and enters line configuration mode. |
| **Step 4** | **media-type rj45**<br><br>**Example:**<br>`Switch(config-line)# media-type rj45` | Configures the console media type to be only RJ-45 port. If you do not enter this command and both types are connected, the USB port is used by default. |
| **Step 5** | **end**<br><br>**Example:**<br>`Switch(config)# end` | Returns to privileged EXEC mode. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 6** | **copy running-config startup-config**<br><br>**Example:**<br>`Switch# copy running-config startup-config` | (Optional) Saves your entries in the configuration file. |

# Configuring the USB Inactivity Timeout

The configurable inactivity timeout reactivates the RJ-45 console port if the USB console port is activated but no input activity occurs on it for a specified time period. When the USB console port is deactivated due to a timeout, you can restore its operation by disconnecting and reconnecting the USB cable.

**Note** The configured inactivity timeout applies to all switches in a stack. However, a timeout on one switch does not cause a timeout on other switches in the stack.

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **line console 0**
4. **usb-inactivity-timeout** *timeout-minutes*
5. **copy running-config startup-config**

## DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br><br>**Example:**<br>`Switch> enable` | Enables privileged EXEC mode. Enter your password if prompted. |
| **Step 2** | **configure terminal**<br><br>**Example:**<br>`Switch# configure terminal` | Enters the global configuration mode. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 3** | **line console 0**<br><br>**Example:**<br>`Switch(config)# line console 0` | Configures the console and enters line configuration mode. |
| **Step 4** | **usb-inactivity-timeout** *timeout-minutes*<br><br>**Example:**<br>`Switch(config-line)# usb-inactivity-timeout 30` | Specify an inactivity timeout for the console port. The range is 1 to 240 minutes. The default is to have no timeout configured. |
| **Step 5** | **copy running-config startup-config**<br><br>**Example:**<br>`Switch# copy running-config startup-config` | (Optional) Saves your entries in the configuration file. |

# Monitoring Interface Characteristics

## Monitoring Interface Status

Commands entered at the privileged EXEC prompt display information about the interface, including the versions of the software and the hardware, the configuration, and statistics about the interfaces.

***Table 5: Show Commands for Interfaces***

| Command | Purpose |
|---|---|
| **show interfaces** *interface-id* **status** [**err-disabled**] | Displays interface status or a list of interfaces in the error-disabled state. |
| **show interfaces** [*interface-id*] **switchport** | Displays administrative and operational status of switching (nonrouting) ports. You can use this command to find out if a port is in routing or in switching mode. |
| **show interfaces** [*interface-id*] **description** | Displays the description configured on an interface or all interfaces and the interface status. |
| **show ip interface** [*interface-id*] | Displays the usability status of all interfaces configured for IP routing or the specified interface. |

| Command | Purpose |
|---|---|
| **show interface** [*interface-id*] **stats** | Displays the input and output packets by the switching path for the interface. |
| **show interfaces** *interface-id* | (Optional) Displays speed and duplex on the interface. |
| **show interfaces transceiver dom-supported-list** | (Optional) Displays Digital Optical Monitoring (DOM) status on the connect SFP modules. |
| **show interfaces transceiver properties** | (Optional) Displays temperature, voltage, or amount of current on the interface. |
| **show interfaces** [*interface-id*] [{**transceiver properties** \| **detail**}] *module number*] | Displays physical and operational status about an SFP module. |
| **show running-config interface** [*interface-id*] | Displays the running configuration in RAM for the interface. |
| **show version** | Displays the hardware configuration, software version, the names and sources of configuration files, and the boot images. |
| **show controllers ethernet-controller** *interface-id* **phy** | Displays the operational state of the auto-MDIX feature on the interface. |

# Clearing and Resetting Interfaces and Counters

***Table 6: Clear Commands for Interfaces***

| Command | Purpose |
|---|---|
| **clear counters** [*interface-id*] | Clears interface counters. |
| **clear interface** *interface-id* | Resets the hardware logic on an interface. |
| **clear line** [*number* \| **console 0** \| **vty** *number*] | Resets the hardware logic on an asynchronous serial line. |

**Note** The **clear counters** privileged EXEC command does not clear counters retrieved by using Simple Network Management Protocol (SNMP), but only those seen with the **show interface** privileged EXEC command.

# Configuration Examples for Interface Characteristics

## Adding a Description to an Interface: Example

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTRL/Z.
Switch(config)# interface gigabitethernet1/0/2
Switch(config-if)# description Connects to Marketing
Switch(config-if)# end
Switch# show interfaces gigabitethernet1/0/2 description
Interface Status         Protocol Description
Gi1/0/2   admin down     down     Connects to Marketing
```

## Configuring a Range of Interfaces: Examples

This example shows how to use the **interface range** global configuration command to set the speed to 100 Mb/s on ports 1 to 4 on switch 1:

```
Switch# configure terminal
Switch(config)# interface range gigabitethernet1/0/1 - 4
Switch(config-if-range)# speed 100
```

This example shows how to use a comma to add different interface type strings to the range to enable Gigabit Ethernet ports 1 to 3 and 10-Gigabit Ethernet ports 1 and 2 to receive flow-control pause frames:

```
Switch# configure terminal
Switch(config)# interface range gigabitethernet1/0/1 - 3 , tengigabitethernet1/0/1 - 2
Switch(config-if-range)# flowcontrol receive on
```

If you enter multiple configuration commands while you are in interface-range mode, each command is executed as it is entered. The commands are not batched and executed after you exit interface-range mode. If you exit interface-range configuration mode while the commands are being executed, some commands might not be executed on all interfaces in the range. Wait until the command prompt reappears before exiting interface-range configuration mode.

## Configuring and Using Interface Range Macros: Examples

This example shows how to define an interface-range named *enet_list* to include ports 1 and 2 on switch 1 and to verify the macro configuration:

```
Switch# configure terminal
Switch(config)# define interface-range enet_list gigabitethernet1/0/1 - 2
Switch(config)# end
Switch# show running-config | include define
define interface-range enet_list GigabitEthernet1/0/1 - 2
```

This example shows how to create a multiple-interface macro named *macro1*:

```
Switch# configure terminal
Switch(config)# define interface-range macro1 gigabitethernet1/0/1 - 2, gigabitethernet1/0/5
 - 7, tengigabitethernet1/0/1 -2
```

```
Switch(config)# end
```

This example shows how to enter interface-range configuration mode for the interface-range macro *enet_list*:

```
Switch# configure terminal
Switch(config)# interface range macro enet_list
Switch(config-if-range)#
```

This example shows how to delete the interface-range macro *enet_list* and to verify that it was deleted.

```
Switch# configure terminal
Switch(config)# no define interface-range enet_list
Switch(config)# end
Switch# show run | include define
Switch#
```

# Setting Interface Speed and Duplex Mode: Example

This example shows how to set the interface speed to 100 Mb/s and the duplex mode to half on a 10/100/1000 Mb/s port:

```
Switch# configure terminal
Switch(config)# interface gigabitethernet1/0/3
Switch(config-if)# speed 10
Switch(config-if)# duplex half
```

This example shows how to set the interface speed to 100 Mb/s on a 10/100/1000 Mb/s port:

```
Switch# configure terminal
Switch(config)# interface gigabitethernet1/0/2
Switch(config-if)# speed 100
```

# Configuring the Console Media Type: Example

This example disables the USB console media type and enables the RJ-45 console media type.

```
Switch# configure terminal
Switch(config)# line console 0
Switch(config-line)# media-type rj45
```

This configuration terminates any active USB console media type in the stack. A log shows that this termination has occurred. This example shows that the console on switch 1 reverted to RJ-45.

```
*Mar  1 00:25:36.860: %USB_CONSOLE-6-CONFIG_DISABLE: Console media-type USB disabled by
system configuration, media-type reverted to RJ45.
```

At this point no switches in the stack allow a USB console to have input. A log entry shows when a console cable is attached. If a USB console cable is connected to switch 2, it is prevented from providing input.

```
*Mar  1 00:34:27.498: %USB_CONSOLE-6-CONFIG_DISALLOW: Console media-type USB is disallowed
 by system configuration, media-type remains RJ45. (switch-stk-2)
```

This example reverses the previous configuration and immediately activates any USB console that is connected.

```
Switch# configure terminal
Switch(config)# line console 0
Switch(config-line)# no media-type rj45
```

# Configuring the USB Inactivity Timeout: Example

This example configures the inactivity timeout to 30 minutes:

```
Switch# configure terminal
Switch(config)# line console 0
Switch(config-line)# usb-inactivity-timeout 30
```

To disable the configuration, use these commands:

```
Switch# configure terminal
Switch(config)# line console 0
Switch(config-line)# no usb-inactivity-timeout
```

If there is no (input) activity on a USB console port for the configured number of minutes, the inactivity timeout setting applies to the RJ-45 port, and a log shows this occurrence:

```
*Mar  1 00:47:25.625: %USB_CONSOLE-6-INACTIVITY_DISABLE: Console media-type USB disabled
due to inactivity, media-type reverted to RJ45.
```

At this point, the only way to reactivate the USB console port is to disconnect and reconnect the cable.

When the USB cable on the switch has been disconnected and reconnected, a log similar to this appears:

```
*Mar  1 00:48:28.640: %USB_CONSOLE-6-MEDIA_USB: Console media-type is USB.
```

# Additional References for the Interface Characteristics Feature

### Error Message Decoder

| Description | Link |
|---|---|
| To help you research and resolve system error messages in this release, use the Error Message Decoder tool. | https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi |

### Standards and RFCs

| Standard/RFC | Title |
|---|---|
| None | -- |

### MIBs

| MIB | MIBs Link |
|---|---|
| All supported MIBs for this release. | To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:<br>http://www.cisco.com/go/mibs |

### Technical Assistance

| Description | Link |
|---|---|
| The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.<br>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.<br>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password. | http://www.cisco.com/support |

# Feature History and Information for Configuring Interface Characteristics

| Release | Modification |
|---|---|
| Cisco IOS 15.0(2)EX | This feature was introduced. |

CHAPTER 3

# Configuring Auto-MDIX


- Prerequisites for Auto-MDIX, page 43
- Restrictions for Auto-MDIX, page 43
- Information about Configuring Auto-MDIX, page 43
- How to Configure Auto-MDIX, page 44
- Example for Configuring Auto-MDIX, page 45
- Additional References, page 46
- Feature History and Information for Auto-MDIX, page 46


## Prerequisites for Auto-MDIX

Automatic medium-dependent interface crossover (auto-MDIX) is enabled by default.

Auto-MDIX is supported on all 10/100/1000-Mb/s and on 10/100/1000BASE-TX small form-factor pluggable (SFP)-module interfaces. It is not supported on 1000BASE-SX or -LX SFP module interfaces.

## Restrictions for Auto-MDIX

The switch might not support a pre-standard powered device—such as Cisco IP phones and access points that do not fully support IEEE 802.3af—if that powered device is connected to the switch through a crossover cable. This is regardless of whether auto-MIDX is enabled on the switch port.

## Information about Configuring Auto-MDIX

### Auto-MDIX on an Interface

When automatic medium-dependent interface crossover (auto-MDIX) is enabled on an interface, the interface automatically detects the required cable connection type (straight through or crossover) and configures the

connection appropriately. When connecting switches without the auto-MDIX feature, you must use straight-through cables to connect to devices such as servers, workstations, or routers and crossover cables to connect to other switches or repeaters. With auto-MDIX enabled, you can use either type of cable to connect to other devices, and the interface automatically corrects for any incorrect cabling. For more information about cabling requirements, see the hardware installation guide.

This table shows the link states that result from auto-MDIX settings and correct and incorrect cabling.

***Table 7: Link Conditions and Auto-MDIX Settings***

| Local Side Auto-MDIX | Remote Side Auto-MDIX | With Correct Cabling | With Incorrect Cabling |
|---|---|---|---|
| On | On | Link up | Link up |
| On | Off | Link up | Link up |
| Off | On | Link up | Link up |
| Off | Off | Link up | Link down |

# How to Configure Auto-MDIX

## Configuring Auto-MDIX on an Interface

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *interface-id*
4. **speed auto**
5. **duplex auto**
6. **end**
7. **copy running-config startup-config**

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br><br>**Example:**<br><br>`Switch> enable` | Enables privileged EXEC mode. Enter your password if prompted. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 2** | **configure terminal**<br><br>**Example:**<br><br>`Switch#` **configure terminal** | Enters global configuration mode |
| **Step 3** | **interface** *interface-id*<br><br>**Example:**<br><br>`Switch(config)#` **interface gigabitethernet1/0/1** | Specifies the physical interface to be configured, and enter interface configuration mode. |
| **Step 4** | **speed auto**<br><br>**Example:**<br><br>`Switch(config-if)#` **speed auto** | Configures the interface to autonegotiate speed with the connected device. |
| **Step 5** | **duplex auto**<br><br>**Example:**<br><br>`Switch(config-if)#` **duplex auto** | Configures the interface to autonegotiate duplex mode with the connected device. |
| **Step 6** | **end**<br><br>**Example:**<br><br>`Switch(config-if)#` **end** | Returns to privileged EXEC mode. |
| **Step 7** | **copy running-config startup-config**<br><br>**Example:**<br><br>`Switch#` **copy running-config startup-config** | (Optional) Saves your entries in the configuration file. |

# Example for Configuring Auto-MDIX

This example shows how to enable auto-MDIX on a port:

```
Switch# configure terminal
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# speed auto
Switch(config-if)# duplex auto
Switch(config-if)# mdix auto
Switch(config-if)# end
```

# Additional References

### Error Message Decoder

| Description | Link |
|---|---|
| To help you research and resolve system error messages in this release, use the Error Message Decoder tool. | https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi |

### MIBs

| MIB | MIBs Link |
|---|---|
| All supported MIBs for this release. | To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:<br>http://www.cisco.com/go/mibs |

### Technical Assistance

| Description | Link |
|---|---|
| The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.<br>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.<br>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password. | http://www.cisco.com/support |

# Feature History and Information for Auto-MDIX

| Release | Modification |
|---|---|
| Cisco IOS 15.0(2)EX | This feature was introduced. |

CHAPTER 4

# Configuring Ethernet Management Port


- Finding Feature Information, page 49
- Prerequisites for Ethernet Management Ports, page 49
- Information about the Ethernet Management Port, page 49
- How to Configure the Ethernet Management Port, page 51
- Additional References, page 52
- Feature Information for Ethernet Management Ports, page 54


## Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

## Prerequisites for Ethernet Management Ports

When connecting a PC to the Ethernet management port, you must first assign an IP address.

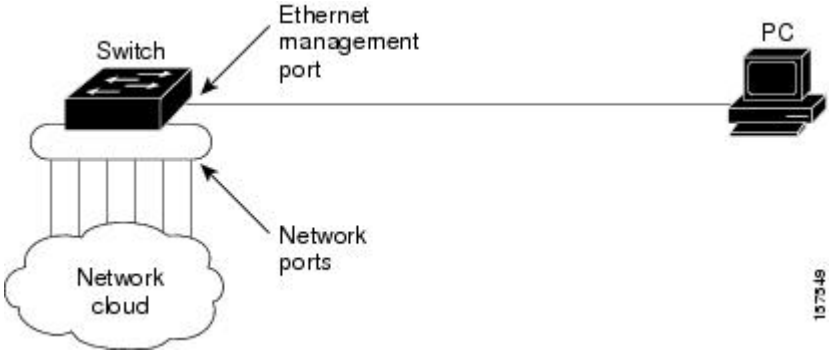
## Information about the Ethernet Management Port

The Ethernet management port, also referred to as the *Fa0* or *fastethernet0* port, is a Layer 3 host port to which you can connect a PC. You can use the Ethernet management port instead of the switch console port for network management. When managing a switch stack, connect the PC to the Ethernet management port on a stack member.

# Ethernet Management Port Direct Connection to a Switch

This figure displays how to connect the Ethernet management port to the PC for a switch or a standalone switch.

***Figure 2: Connecting a Switch to a PC***

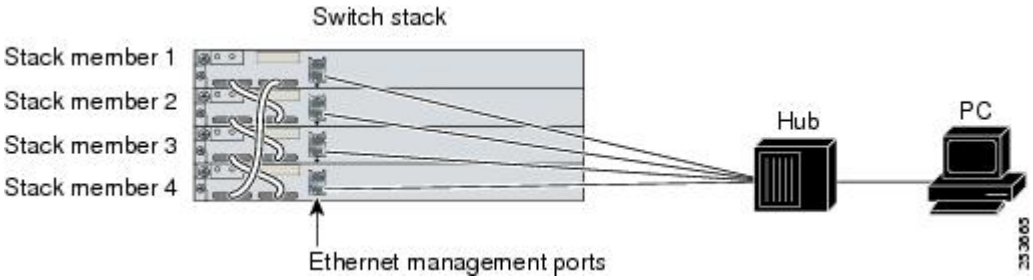



# Ethernet Management Port Connection to Stack Switches using a Hub

In a stack with only stack switches, all the Ethernet management ports on the stack members are connected to a hub to which the PC is connected. The active link is from the Ethernet management port on the stack masterthrough the hub, to the PC. If the activeswitch fails and a new active switch is elected, the active link is now from the Ethernet management port on the new active switch to the PC.

This figure displays how a PC uses a hub to connect to a switch stack.

***Figure 3: Connecting a Switch Stack to a PC***




# Supported Features on the Ethernet Management Port

The Ethernet management port supports these features:

- Express Setup (only in switch stacks)
- Network Assistant
- Telnet with passwords

- TFTP
- Secure Shell (SSH)
- DHCP-based autoconfiguration
- SMNP (only the ENTITY-MIB and the IF-MIB)
- IP ping
- Interface features
  - Speed—10 Mb/s, 100 Mb/s, and autonegotiation
  - Duplex mode—Full, half, and autonegotiation
  - Loopback detection
- Cisco Discovery Protocol (CDP)
- DHCP relay agent
- IPv4 access control lists (ACLs)

**Caution** Before enabling a feature on the Ethernet management port, make sure that the feature is supported. If you try to configure an unsupported feature on the Ethernet Management port, the feature might not work properly, and the switch might fail.

# How to Configure the Ethernet Management Port

## Disabling and Enabling the Ethernet Management Port

### SUMMARY STEPS

1. **configure terminal**
2. **interface fastethernet0**
3. **shutdown**
4. **no shutdown**
5. **exit**
6. **show interfaces fastethernet0**

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **configure terminal**<br><br>**Example:**<br>`Switch# configure terminal` | Enters global configuration mode. |
| **Step 2** | **interface fastethernet0**<br><br>**Example:**<br>`Switch(config)# interface fastethernet0` | Specifies the Ethernet management port in the CLI. |
| **Step 3** | **shutdown**<br><br>**Example:**<br>`Switch(config-if)# shutdown` | Disables the Ethernet management port. |
| **Step 4** | **no shutdown**<br><br>**Example:**<br>`Switch(config-if)# no shutdown` | Enables the Ethernet management port. |
| **Step 5** | **exit**<br><br>**Example:**<br>`Switch(config-if)# exit` | Exits interface configuration mode. |
| **Step 6** | **show interfaces fastethernet0**<br><br>**Example:**<br>`Switch# show interfaces fastethernet0` | Displays the link status.<br><br>To find out the link status to the PC, you can monitor the LED for the Ethernet management port. The LED is green (on) when the link is active, and the LED is off when the link is down. The LED is amber when there is a POST failure. |

### What to Do Next

Proceed to manage or configure your switch using the Ethernet management port. Refer to the *Catalyst 2960-X Switch Network Management Configuration Guide*.

# Additional References

### Related Documents

| Related Topic | Document Title |
|---|---|
| **Bootloader configuration** | *Catalyst 2960-X Switch System Management Configuration Guide* |

| Related Topic | Document Title |
|---|---|
| **Bootloader commands** | *Catalyst 2960-X Switch System Management Configuration Guide* |

### Error Message Decoder

| Description | Link |
|---|---|
| To help you research and resolve system error messages in this release, use the Error Message Decoder tool. | https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi |

### MIBs

| MIB | MIBs Link |
|---|---|
| All supported MIBs for this release. | To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:<br>http://www.cisco.com/go/mibs |

### Technical Assistance

| Description | Link |
|---|---|
| The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.<br>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.<br>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password. | http://www.cisco.com/support |

# Feature Information for Ethernet Management Ports

| Release | Modification |
|---|---|
| Cisco IOS 15.0(2)EX | This feature was introduced. |

CHAPTER 5

# Configuring LLDP, LLDP-MED, and Wired Location Service


- Finding Feature Information, page 55
- LLDP, LLDP-MED, and Wired Location Service Overview, page 55
- How to Configure LLDP, LLDP-MED, and Wired Location Service, page 60
- Configuration Examples for LLDP, LLDP-MED, and Wired Location Service, page 72
- Monitoring and Maintaining LLDP, LLDP-MED, and Wired Location Service, page 72
- Additional References for LLDP, LLDP-MED, and Wired Location Service, page 73
- Feature Information for LLDP, LLDP-MED, and Wired Location Service, page 74


## Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

## LLDP, LLDP-MED, and Wired Location Service Overview

### LLDP

The Cisco Discovery Protocol (CDP) is a device discovery protocol that runs over Layer 2 (the data link layer) on all Cisco-manufactured devices (routers, bridges, access servers, switches, and controllers). CDP allows

network management applications to automatically discover and learn about other Cisco devices connected to the network.

To support non-Cisco devices and to allow for interoperability between other devices, the switch supports the IEEE 802.1AB Link Layer Discovery Protocol (LLDP). LLDP is a neighbor discovery protocol that is used for network devices to advertise information about themselves to other devices on the network. This protocol runs over the data-link layer, which allows two systems running different network layer protocols to learn about each other.

## LLDP Supported TLVs

LLDP supports a set of attributes that it uses to discover neighbor devices. These attributes contain type, length, and value descriptions and are referred to as TLVs. LLDP supported devices can use TLVs to receive and send information to their neighbors. This protocol can advertise details such as configuration information, device capabilities, and device identity.

The switch supports these basic management TLVs. These are mandatory LLDP TLVs.

- Port description TLV
- System name TLV
- System description TLV
- System capabilities TLV
- Management address TLV

These organizationally specific LLDP TLVs are also advertised to support LLDP-MED.

- Port VLAN ID TLV (IEEE 802.1 organizationally specific TLVs)
- MAC/PHY configuration/status TLV (IEEE 802.3 organizationally specific TLVs)

## LLDP and Cisco Switch Stacks

A switch stack appears as a single switch in the network. Therefore, LLDP discovers the switch stack, not the individual stack members.

## LLDP and Cisco Medianet

When you configure LLDP or CDP location information on a per-port basis, remote devices can send Cisco Medianet location information to the switch. For information, go to http://www.cisco.com/en/US/docs/ios/netmgmt/configuration/guide/nm_cdp_discover.html.

# LLDP-MED

LLDP for Media Endpoint Devices (LLDP-MED) is an extension to LLDP that operates between endpoint devices such as IP phones and network devices such as switches. It specifically provides support for voice over IP (VoIP) applications and provides additional TLVs for capabilities discovery, network policy, Power over Ethernet, inventory management and location information. By default, all LLDP-MED TLVs are enabled.

## LLDP-MED Supported TLVs

LLDP-MED supports these TLVs:

- LLDP-MED capabilities TLV

  Allows LLDP-MED endpoints to determine the capabilities that the connected device supports and has enabled.

- Network policy TLV

  Allows both network connectivity devices and endpoints to advertise VLAN configurations and associated Layer 2 and Layer 3 attributes for the specific application on that port. For example, the switch can notify a phone of the VLAN number that it should use. The phone can connect to any switch, obtain its VLAN number, and then start communicating with the call control.

  By defining a network-policy profile TLV, you can create a profile for voice and voice-signaling by specifying the values for VLAN, class of service (CoS), differentiated services code point (DSCP), and tagging mode. These profile attributes are then maintained centrally on the switch and propagated to the phone.

- Power management TLV

  Enables advanced power management between LLDP-MED endpoint and network connectivity devices. Allows switches and phones to convey power information, such as how the device is powered, power priority, and how much power the device needs.

  LLDP-MED also supports an extended power TLV to advertise fine-grained power requirements, end-point power priority, and end-point and network connectivity-device power status. LLDP is enabled and power is applied to a port, the power TLV determines the actual power requirement of the endpoint device so that the system power budget can be adjusted accordingly. The switch processes the requests and either grants or denies power based on the current power budget. If the request is granted, the switch updates the power budget. If the request is denied, the switch turns off power to the port, generates a syslog message, and updates the power budget. If LLDP-MED is disabled or if the endpoint does not support the LLDP-MED power TLV, the initial allocation value is used throughout the duration of the connection.

  You can change power settings by entering the **power inline** {**auto** [**max** *max-wattage*] | **never** | **static** [**max** *max-wattage*]} interface configuration command. By default the PoE interface is in **auto** mode; If no value is specified, the maximum is allowed (30 W).

- Inventory management TLV

  Allows an endpoint to send detailed inventory information about itself to the switch, including information hardware revision, firmware version, software version, serial number, manufacturer name, model name, and asset ID TLV.

- Location TLV

  Provides location information from the switch to the endpoint device. The location TLV can send this information:

  - Civic location information

    Provides the civic address information and postal information. Examples of civic location information are street address, road name, and postal community name information.

  - ELIN location information

Provides the location information of a caller. The location is determined by the Emergency location identifier number (ELIN), which is a phone number that routes an emergency call to the local public safety answering point (PSAP) and which the PSAP can use to call back the emergency caller.

# Wired Location Service

The switch uses the location service feature to send location and attachment tracking information for its connected devices to a Cisco Mobility Services Engine (MSE). The tracked device can be a wireless endpoint, a wired endpoint, or a wired switch or controller. The switch notifies the MSE of device link up and link down events through the Network Mobility Services Protocol (NMSP) location and attachment notifications.

The MSE starts the NMSP connection to the switch, which opens a server port. When the MSE connects to the switch there are a set of message exchanges to establish version compatibility and service exchange information followed by location information synchronization. After connection, the switch periodically sends location and attachment notifications to the MSE. Any link up or link down events detected during an interval are aggregated and sent at the end of the interval.

When the switch determines the presence or absence of a device on a link-up or link-down event, it obtains the client-specific information such as the MAC address, IP address, and username. If the client is LLDP-MED- or CDP-capable, the switch obtains the serial number and UDI through the LLDP-MED location TLV or CDP.

Depending on the device capabilities, the switch obtains this client information at link up:

- Slot and port specified in port connection
- MAC address specified in the client MAC address
- IP address specified in port connection
- 802.1X username if applicable
- Device category is specified as a *wired station*
- State is specified as *new*
- Serial number, UDI
- Model number
- Time in seconds since the switch detected the association

Depending on the device capabilities, the switch obtains this client information at link down:

- Slot and port that was disconnected
- MAC address
- IP address
- 802.1X username if applicable
- Device category is specified as a *wired station*
- State is specified as *delete*
- Serial number, UDI

- Time in seconds since the switch detected the disassociation

When the switch shuts down, it sends an attachment notification with the state *delete* and the IP address before closing the NMSP connection to the MSE. The MSE interprets this notification as disassociation for all the wired clients associated with the switch.

If you change a location address on the switch, the switch sends an NMSP location notification message that identifies the affected ports and the changed address information.

# Default LLDP Configuration

***Table 8: Default LLDP Configuration***

| Feature | Default Setting |
|---|---|
| LLDP global state | Disabled |
| LLDP holdtime (before discarding) | 120 seconds |
| LLDP timer (packet update frequency) | 30 seconds |
| LLDP reinitialization delay | 2 seconds |
| LLDP tlv-select | Disabled to send and receive all TLVs |
| LLDP interface state | Disabled |
| LLDP receive | Disabled |
| LLDP transmit | Disabled |
| LLDP med-tlv-select | Disabled to send all LLDP-MED TLVs. When LLDP is globally enabled, LLDP-MED-TLV is also enabled. |

# Restrictions for LLDP

- If the interface is configured as a tunnel port, LLDP is automatically disabled.
- If you first configure a network-policy profile on an interface, you cannot apply the **switchport voice vlan** command on the interface. If the **switchport voice vlan** *vlan-id* is already configured on an interface, you can apply a network-policy profile on the interface. This way the interface has the voice or voice-signaling VLAN network-policy profile applied on the interface.
- You cannot configure static secure MAC addresses on an interface that has a network-policy profile.

# How to Configure LLDP, LLDP-MED, and Wired Location Service

## Enabling LLDP

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **lldp run**
4. **interface** *interface-id*
5. **lldp transmit**
6. **lldp receive**
7. **end**
8. **show lldp**
9. **copy running-config startup-config**

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br><br>**Example:**<br><br>`Switch> enable` | Enables privileged EXEC mode. Enter your password if prompted. |
| **Step 2** | **configure terminal**<br><br>**Example:**<br><br>`Switch# configure terminal` | Enters global configuration mode. |
| **Step 3** | **lldp run**<br><br>**Example:**<br><br>`Switch (config)# lldp run` | Enables LLDP globally on the switch. |
| **Step 4** | **interface** *interface-id*<br><br>**Example:**<br><br>`Switch (config)# interface gigabitethernet2/0/1` | Specifies the interface on which you are enabling LLDP, and enter interface configuration mode. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 5** | **lldp transmit**<br><br>**Example:**<br>`Switch(config-if)# lldp transmit` | Enables the interface to send LLDP packets. |
| **Step 6** | **lldp receive**<br><br>**Example:**<br>`Switch(config-if)# lldp receive` | Enables the interface to receive LLDP packets. |
| **Step 7** | **end**<br><br>**Example:**<br>`Switch(config-if)# end` | Returns to privileged EXEC mode. |
| **Step 8** | **show lldp**<br><br>**Example:**<br>`Switch# show lldp` | Verifies the configuration. |
| **Step 9** | **copy running-config startup-config**<br><br>**Example:**<br>`Switch# copy running-config startup-config` | (Optional) Saves your entries in the configuration file. |

# Configuring LLDP Characteristics

You can configure the frequency of LLDP updates, the amount of time to hold the information before discarding it, and the initialization delay time. You can also select the LLDP and LLDP-MED TLVs to send and receive.

**Note** Steps 2 through 5 are optional and can be performed in any order.

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **lldp holdtime** *seconds*
4. **lldp reinit** *delay*
5. **lldp timer** *rate*
6. **lldp tlv-select**
7. **interface** *interface-id*
8. **lldp med-tlv-select**
9. **end**
10. **show lldp**
11. **copy running-config startup-config**

## DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br><br>**Example:**<br>`Switch> enable` | Enables privileged EXEC mode. Enter your password if prompted. |
| **Step 2** | **configure terminal**<br><br>**Example:**<br>`Switch# configure terminal` | Enters global configuration mode. |
| **Step 3** | **lldp holdtime** *seconds*<br><br>**Example:**<br>`Switch(config)# lldp holdtime 120` | (Optional) Specifies the amount of time a receiving device should hold the information from your device before discarding it.<br>The range is 0 to 65535 seconds; the default is 120 seconds. |
| **Step 4** | **lldp reinit** *delay*<br><br>**Example:**<br>`Switch(config)# lldp reinit 2` | (Optional) Specifies the delay time in seconds for LLDP to initialize on an interface.<br>The range is 2 to 5 seconds; the default is 2 seconds. |
| **Step 5** | **lldp timer** *rate*<br><br>**Example:**<br>`Switch(config)# lldp timer 30` | (Optional) Sets the sending frequency of LLDP updates in seconds.<br>The range is 5 to 65534 seconds; the default is 30 seconds. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 6** | **lldp tlv-select**<br><br>**Example:**<br><br>`Switch(config)# tlv-select` | (Optional) Specifies the LLDP TLVs to send or receive. |
| **Step 7** | **interface** *interface-id*<br><br>**Example:**<br><br>`Switch (config)# interface gigabitethernet2/0/1` | Specifies the interface on which you are enabling LLDP, and enter interface configuration mode. |
| **Step 8** | **lldp med-tlv-select**<br><br>**Example:**<br><br>`Switch (config-if)# lldp med-tlv-select inventory management` | (Optional) Specifies the LLDP-MED TLVs to send or receive. |
| **Step 9** | **end**<br><br>**Example:**<br><br>`Switch (config-if)# end` | Returns to privileged EXEC mode. |
| **Step 10** | **show lldp**<br><br>**Example:**<br><br>`Switch# show lldp` | Verifies the configuration. |
| **Step 11** | **copy running-config startup-config**<br><br>**Example:**<br><br>`Switch# copy running-config startup-config` | (Optional) Saves your entries in the configuration file. |

# Configuring LLDP-MED TLVs

By default, the switch only sends LLDP packets until it receives LLDP-MED packets from the end device. It then sends LLDP packets with MED TLVs, as well. When the LLDP-MED entry has been aged out, it again only sends LLDP packets.

By using the **lldp** interface configuration command, you can configure the interface not to send the TLVs listed in the following table.

*Table 9: LLDP-MED TLVs*

| LLDP-MED TLV | Description |
|---|---|
| inventory-management | LLDP-MED inventory management TLV |
| location | LLDP-MED location TLV |
| network-policy | LLDP-MED network policy TLV |
| power-management | LLDP-MED power management TLV |

Follow these steps to enable a TLV on an interface:

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *interface-id*
4. **lldp med-tlv-select**
5. **end**
6. **copy running-config startup-config**

## DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br><br>**Example:**<br><br>`Switch> enable` | Enables privileged EXEC mode. Enter your password if prompted. |
| **Step 2** | **configure terminal**<br><br>**Example:**<br><br>`Switch# configure terminal` | Enters global configuration mode. |
| **Step 3** | **interface** *interface-id*<br><br>**Example:**<br><br>`Switch (config)# interface gigabitethernet2/0/1` | Specifies the interface on which you are enabling LLDP, and enter interface configuration mode. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 4** | **lldp med-tlv-select**<br><br>**Example:**<br>`Switch(config-if)# lldp med-tlv-select inventory management` | Specifies the TLV to enable. |
| **Step 5** | **end**<br><br>**Example:**<br>`Switch(config-if)# end` | Returns to privileged EXEC mode. |
| **Step 6** | **copy running-config startup-config**<br><br>**Example:**<br>`Switch# copy running-config startup-config` | (Optional) Saves your entries in the configuration file. |

# Configuring Network-Policy TLV

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **network-policy profile** *profile number*
4. {**voice** | **voice-signaling**} **vlan** [*vlan-id* {**cos** *cvalue* | **dscp** *dvalue*}] | [[**dot1p** {**cos** *cvalue* | **dscp** *dvalue*}] | **none** | **untagged**]
5. **exit**
6. **interface** *interface-id*
7. **network-policy** *profile number*
8. **lldp med-tlv-select network-policy**
9. **end**
10. **show network-policy profile**
11. **copy running-config startup-config**

## DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable** | Enables privileged EXEC mode. Enter your password if prompted. |

| | Command or Action | Purpose |
|---|---|---|
| | **Example:**<br>`Switch> enable` | |
| **Step 2** | **configure terminal**<br>**Example:**<br>`Switch# configure terminal` | Enters global configuration mode. |
| **Step 3** | **network-policy profile** *profile number*<br>**Example:**<br>`Switch(config)# network-policy profile 1` | Specifies the network-policy profile number, and enter network-policy configuration mode. The range is 1 to 4294967295. |
| **Step 4** | {**voice** \| **voice-signaling**} **vlan** [*vlan-id* {**cos** *cvalue* \| **dscp** *dvalue*}] \| [[**dot1p** {**cos** *cvalue* \| **dscp** *dvalue*}] \| **none** \| **untagged**]<br>**Example:**<br>`Switch(config-network-policy)# voice vlan 100 cos 4` | Configures the policy attributes:<br>• **voice—**Specifies the voice application type.<br>• **voice-signaling—**Specifies the voice-signaling application type.<br>• **vlan—**Specifies the native VLAN for voice traffic.<br>• *vlan-id*—(Optional) Specifies the VLAN for voice traffic. The range is 1 to 4094.<br>• **cos** *cvalue*—(Optional) Specifies the Layer 2 priority class of service (CoS) for the configured VLAN. The range is 0 to 7; the default is 5.<br>• **dscp** *dvalue*—(Optional) Specifies the differentiated services code point (DSCP) value for the configured VLAN. The range is 0 to 63; the default is 46.<br>• **dot1p—**(Optional) Configures the telephone to use IEEE 802.1p priority tagging and use VLAN 0 (the native VLAN).<br>• **none—**(Optional) Do not instruct the IP telephone about the voice VLAN. The telephone uses the configuration from the telephone key pad.<br>• **untagged—**(Optional) Configures the telephone to send untagged voice traffic. This is the default for the telephone.<br>• **untagged—**(Optional) Configures the telephone to send untagged voice traffic. This is the default for the telephone. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 5** | **exit**<br><br>**Example:**<br><br>`Switch(config)# exit` | Returns to global configuration mode. |
| **Step 6** | **interface** *interface-id*<br><br>**Example:**<br><br>`Switch (config)# interface gigabitethernet2/0/1` | Specifies the interface on which you are configuring a network-policy profile, and enter interface configuration mode. |
| **Step 7** | **network-policy** *profile number*<br><br>**Example:**<br><br>`Switch(config-if)# network-policy 1` | Specifies the network-policy profile number. |
| **Step 8** | **lldp med-tlv-select network-policy**<br><br>**Example:**<br><br>`Switch(config-if)# lldp med-tlv-select network-policy` | Specifies the network-policy TLV. |
| **Step 9** | **end**<br><br>**Example:**<br><br>`Switch(config)# end` | Returns to privileged EXEC mode. |
| **Step 10** | **show network-policy profile**<br><br>**Example:**<br><br>`Switch# show network-policy profile` | Verifies the configuration. |
| **Step 11** | **copy running-config startup-config**<br><br>**Example:**<br><br>`Switch# copy running-config startup-config` | (Optional) Saves your entries in the configuration file. |

# Configuring Location TLV and Wired Location Service

Beginning in privileged EXEC mode, follow these steps to configure location information for an endpoint and to apply it to an interface.

## SUMMARY STEPS

1. **configure terminal**
2. **location** {**admin-tag** *string* | **civic-location identifier** {*id* | **host**} | **elin-location** *string* **identifier** *id* | **custom-location identifier** {*id* | **host**} | **geo-location identifier** {*id* | **host**}}
3. **exit**
4. **interface** *interface-id*
5. **location** {**additional-location-information** *word* | **civic-location-id** {*id* | **host**} | **elin-location-id** *id* | **custom-location-id** {*id* | **host**} | **geo-location-id** {*id* | **host**} }
6. **end**
7. Use one of the following:
   - **show location admin-tag** *string*
   - **show location civic-location identifier** *id*
   - **show location elin-location identifier** *id*
8. **copy running-config startup-config**

## DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **configure terminal**<br><br>**Example:**<br>`Switch# configure terminal` | Enters global configuration mode. |
| **Step 2** | **location** {**admin-tag** *string* \| **civic-location identifier** {*id* \| **host**} \| **elin-location** *string* **identifier** *id* \| **custom-location identifier** {*id* \| **host**} \| **geo-location identifier** {*id* \| **host**}}<br><br>**Example:**<br>`Switch(config)# location civic-location identifier 1` | Specifies the location information for an endpoint.<br>• **admin-tag—**Specifies an administrative tag or site information.<br>• **civic-location—**Specifies civic location information.<br>• **elin-location—**Specifies emergency location information (ELIN).<br>• **custom-location—**Specifies custom location information. |

| | Command or Action | Purpose |
|---|---|---|
| | `Switch(config-civic)# number 3550`<br>`Switch(config-civic)# primary-road-name "Cisco Way"`<br>`Switch(config-civic)# city "San Jose"`<br>`Switch(config-civic)# state CA`<br>`Switch(config-civic)# building 19`<br>`Switch(config-civic)# room C6`<br>`Switch(config-civic)# county "Santa Clara"`<br>`Switch(config-civic)# country US` | • **geo-location**—Specifies geo-spatial location information.<br>• **identifier** *id*—Specifies the ID for the civic, ELIN, custom, or geo location.<br>• **host**—Specifies the host civic, custom, or geo location.<br>• *string*—Specifies the site or location information in alphanumeric format. |
| **Step 3** | **exit**<br><br>**Example:**<br><br>`Switch(config-civic)# exit` | Returns to global configuration mode. |
| **Step 4** | **interface** *interface-id*<br><br>**Example:**<br><br>`Switch (config)# interface gigabitethernet2/0/1` | Specifies the interface on which you are configuring the location information, and enter interface configuration mode. |
| **Step 5** | **location** {**additional-location-information** *word* \| **civic-location-id** {*id* \| **host**} \| **elin-location-id** *id* \| **custom-location-id** {*id* \| **host**} \| **geo-location-id** {*id* \| **host**} }<br><br>**Example:**<br><br>`Switch(config-if)# location elin-location-id 1` | Enters location information for an interface:<br>• **additional-location-information**—Specifies additional information for a location or place.<br>• **civic-location-id**—Specifies global civic location information for an interface.<br>• **elin-location-id**—Specifies emergency location information for an interface.<br>• **custom-location-id**—Specifies custom location information for an interface.<br>• **geo-location-id**—Specifies geo-spatial location information for an interface.<br>• **host**—Specifies the host location identifier.<br>• *word*—Specifies a word or phrase with additional location information.<br>• *id*—Specifies the ID for the civic, ELIN, custom, or geo location. The ID range is 1 to 4095. |
| **Step 6** | **end**<br><br>**Example:**<br><br>`Switch(config-if)# end` | Returns to privileged EXEC mode. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 7** | Use one of the following:<br>• **show location admin-tag** *string*<br>• **show location civic-location identifier** *id*<br>• **show location elin-location identifier** *id*<br><br>**Example:**<br>`Switch# show location admin-tag`<br>or<br>`Switch# show location civic-location identifier`<br>or<br>`Switch# show location elin-location identifier` | Verifies the configuration. |
| **Step 8** | **copy running-config startup-config**<br><br>**Example:**<br>`Switch# copy running-config startup-config` | (Optional) Saves your entries in the configuration file. |

## Enabling Wired Location Service on the Switch

### Before You Begin

For wired location to function, you must first enter the **ip device tracking** global configuration command.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **nmsp notification interval** {**attachment** | **location**} *interval-seconds*
4. **end**
5. **show network-policy profile**
6. **copy running-config startup-config**

## DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br><br>**Example:**<br><br>`Switch> enable` | Enables privileged EXEC mode. Enter your password if prompted. |
| **Step 2** | **configure terminal**<br><br>**Example:**<br><br>`Switch# configure terminal` | Enters global configuration mode. |
| **Step 3** | **nmsp notification interval** {**attachment** \| **location**} *interval-seconds*<br><br>**Example:**<br><br>`Switch(config)# nmsp notification interval location 10` | Specifies the NMSP notification interval.<br><br>**attachment**—Specifies the attachment notification interval.<br><br>**location**—Specifies the location notification interval.<br><br>*interval-seconds*—Duration in seconds before the switch sends the MSE the location or attachment updates. The range is 1 to 30; the default is 30. |
| **Step 4** | **end**<br><br>**Example:**<br><br>`Switch(config)# end` | Returns to privileged EXEC mode. |
| **Step 5** | **show network-policy profile**<br><br>**Example:**<br><br>`Switch# show network-policy profile` | Verifies the configuration. |
| **Step 6** | **copy running-config startup-config**<br><br>**Example:**<br><br>`Switch# copy running-config startup-config` | (Optional) Saves your entries in the configuration file. |

# Configuration Examples for LLDP, LLDP-MED, and Wired Location Service

## Configuring Network-Policy TLV: Examples

This example shows how to configure VLAN 100 for voice application with CoS and to enable the network-policy profile and network-policy TLV on an interface:

```
Switch# configure terminal
Switch(config)# network-policy 1
Switch(config-network-policy)# voice vlan 100 cos 4
Switch(config-network-policy)# exit
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# network-policy profile 1
Switch(config-if)# lldp med-tlv-select network-policy
```

This example shows how to configure the voice application type for the native VLAN with priority tagging:

```
Switchconfig-network-policy)# voice vlan dot1p cos 4
Switchconfig-network-policy)# voice vlan dot1p dscp 34
```

# Monitoring and Maintaining LLDP, LLDP-MED, and Wired Location Service

Commands for monitoring and maintaining LLDP, LLDP-MED, and wired location service.

| Command | Description |
|---|---|
| **clear lldp counters** | Resets the traffic counters to zero. |
| **clear lldp table** | Deletes the LLDP neighbor information table. |
| **clear nmsp statistics** | Clears the NMSP statistic counters. |
| **show lldp** | Displays global information, such as frequency of transmissions, the holdtime for packets being sent, and the delay time before LLDP initializes on an interface. |
| **show lldp entry** *entry-name* | Displays information about a specific neighbor.<br>You can enter an asterisk (*) to display all neighbors, or you can enter the neighbor name. |
| **show lldp interface** [*interface-id*] | Displays information about interfaces with LLDP enabled.<br>You can limit the display to a specific interface. |

| Command | Description |
|---|---|
| **show lldp neighbors** [*interface-id*] [**detail**] | Displays information about neighbors, including device type, interface type and number, holdtime settings, capabilities, and port ID.<br>You can limit the display to neighbors of a specific interface or expand the display for more detailed information. |
| **show lldp traffic** | Displays LLDP counters, including the number of packets sent and received, number of packets discarded, and number of unrecognized TLVs. |
| **show location admin-tag** *string* | Displays the location information for the specified administrative tag or site. |
| **show location civic-location identifier** *id* | Displays the location information for a specific global civic location. |
| **show location elin-location identifier** *id* | Displays the location information for an emergency location |
| **show network-policy profile** | Displays the configured network-policy profiles. |
| **show nmsp** | Displays the NMSP information |

# Additional References for LLDP, LLDP-MED, and Wired Location Service

### Error Message Decoder

| Description | Link |
|---|---|
| To help you research and resolve system error messages in this release, use the Error Message Decoder tool. | https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi |

### MIBs

| MIB | MIBs Link |
|---|---|
| All supported MIBs for this release. | To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:<br>http://www.cisco.com/go/mibs |

### Technical Assistance

| Description | Link |
|---|---|
| The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.<br>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.<br>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password. | http://www.cisco.com/support |

# Feature Information for LLDP, LLDP-MED, and Wired Location Service

| Release | Modification |
|---|---|
| Cisco IOS 15.0(2)EX | This feature was introduced. |

CHAPTER 6

# Configuring System MTU


- Finding Feature Information, page 75
- Information about the MTU, page 75
- How to Configure MTU , page 76
- Configuration Examples for System MTU, page 77
- Additional References for System MTU, page 78
- Feature Information for System MTU, page 78


## Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

## Information about the MTU

The default maximum transmission unit (MTU) size for frames received and transmitted on all interfaces is 1500 bytes. You can increase the MTU size for all interfaces operating at 10 or 100 Mb/s by using the **system mtu** global configuration command. You can increase the MTU size to support jumbo frames on all Gigabit Ethernet interfaces by using the **system mtu jumbo** global configuration command.

**Note** The switch supports jumbo frames at CPU.

## System MTU Guidelines

When configuring the system MTU values, follow these guidelines:

- The default maximum transmission unit (MTU) size for frames received and transmitted on all interfaces is 1500 bytes. You can increase the MTU size for all interfaces operating at 10 or 100 Mb/s by using the **system mtu** global configuration command. You can increase the MTU size to support jumbo frames on all Gigabit Ethernet interfaces by using the **system mtu jumbo** global configuration command.
- Gigabit Ethernet ports are not affected by the **system mtu** command; 10/100 ports are not affected by the **system mtu jumbo** command. If you do not configure the **system mtu jumbo** command, the setting of the **system mtu** command applies to all Gigabit Ethernet interfaces.

# How to Configure MTU

## Configuring the System MTU

Beginning in privileged EXEC mode, follow these steps to change the MTU size for all 10/100 or Gigabit Ethernet interfaces:

### SUMMARY STEPS

1. **configure terminal**
2. **system mtu** *bytes*
3. **system mtu jumbo** *bytes*
4. **end**
5. **copy running-config startup-config**
6. **reload**
7. **show system mtu**

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **configure terminal**<br><br>**Example:**<br>`Switch# configure terminal` | Enters global configuration mode. |
| **Step 2** | **system mtu** *bytes*<br><br>**Example:**<br>`Switch(config)# system mtu 2500` | (Optional) Change the MTU size for all interfaces on the switch stack that are operating at 10 or 100 Mb/s.<br>The range is 1500 to 1998 bytes; the default is 1500 bytes. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 3** | **system mtu jumbo** *bytes*<br><br>**Example:**<br>`Switch(config)# system mtu jumbo 7500` | (Optional) Changes the MTU size for all Gigabit Ethernet interfaces on the switch or the switch stack.<br><br>The range is 1500 to 9198 bytes; the default is 1500 bytes. |
| **Step 4** | **end**<br><br>**Example:**<br>`Switch(config)# end` | Returns to privileged EXEC mode. |
| **Step 5** | **copy running-config startup-config**<br><br>**Example:**<br>`Switch# copy running-config startup-config` | Saves your entries in the configuration file. |
| **Step 6** | **reload**<br><br>**Example:**<br>`Switch# reload` | Reloads the operating system. |
| **Step 7** | **show system mtu**<br><br>**Example:**<br>`Switch# show system mtu` | Verifies your settings. |

# Configuration Examples for System MTU

This example shows how to set the maximum packet size for a Gigabit Ethernet port to 7500 bytes:

```
Switch(config)# system mtu 1900
Switch(config)# system mtu jumbo 7500
Switch(config)# exit
```

If you enter a value that is outside the allowed range for the specific type of interface, the value is not accepted. This example shows the response when you try to set Gigabit Ethernet interfaces to an out-of-range number:

```
Switch(config)# system mtu jumbo 25000
                                 ^
% Invalid input detected at '^' marker.
```

This is an example of output from the **show system mtu** command:

```
Switch# show system mtu
Global Ethernet MTU is 1500 bytes.
```

# Additional References for System MTU

### Error Message Decoder

| Description | Link |
|---|---|
| To help you research and resolve system error messages in this release, use the Error Message Decoder tool. | https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi |

### MIBs

| MIB | MIBs Link |
|---|---|
| All supported MIBs for this release. | To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:<br>http://www.cisco.com/go/mibs |

### Technical Assistance

| Description | Link |
|---|---|
| The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.<br>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.<br>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password. | http://www.cisco.com/support |

# Feature Information for System MTU

| Release | Modification |
|---|---|
| Cisco IOS 15.0(2)EX | This feature was introduced. |

CHAPTER 7

# Configuring PoE


- Finding Feature Information, page 79
- Restrictions for PoE, page 79
- Information about PoE, page 80
- How to Configure PoE, page 85
- Monitoring Power Status, page 94
- Configuration Examples for Configuring PoE, page 94
- Additional References, page 95


## Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

## Restrictions for PoE

**Note** This feature is supported only on the LAN Base image.

# Information about PoE

## Power over Ethernet Ports

A PoE-capable switch port automatically supplies power to one of these connected devices if the switch senses that there is no power on the circuit:

- a Cisco pre-standard powered device (such as a Cisco IP Phone or a Cisco Aironet Access Point)
- an IEEE 802.3af-compliant powered device

A powered device can receive redundant power when it is connected to a PoE switch port and to an AC power source. The device does not receive redundant power when it is only connected to the PoE port.

### Supported Protocols and Standards

The switch uses these protocols and standards to support PoE:

- CDP with power consumption—The powered device notifies the switch of the amount of power it is consuming. The switch does not reply to the power-consumption messages. The switch can only supply power to or remove power from the PoE port.
- Cisco intelligent power management—The powered device and the switch negotiate through power-negotiation CDP messages for an agreed-upon power-consumption level. The negotiation allows a high-power Cisco powered device, which consumes more than 7 W, to operate at its highest power mode. The powered device first boots up in low-power mode, consumes less than 7 W, and negotiates to obtain enough power to operate in high-power mode. The device changes to high-power mode only when it receives confirmation from the switch.

  High-power devices can operate in low-power mode on switches that do not support power-negotiation CDP.

  Cisco intelligent power management is backward-compatible with CDP with power consumption; the switch responds according to the CDP message that it receives. CDP is not supported on third-party powered devices; therefore, the switch uses the IEEE classification to determine the power usage of the device.
- IEEE 802.3af—The major features of this standard are powered-device discovery, power administration, disconnect detection, and optional powered-device power classification. For more information, see the standard.

### Powered-Device Detection and Initial Power Allocation

The switch detects a Cisco pre-standard or an IEEE-compliant powered device when the PoE-capable port is in the no-shutdown state, PoE is enabled (the default), and the connected device is not being powered by an AC adaptor.

After device detection, the switch determines the device power requirements based on its type:

- The initial power allocation is the maximum amount of power that a powered device requires. The switch initially allocates this amount of power when it detects and powers the powered device. As the switch

receives CDP messages from the powered device and as the powered device negotiates power levels with the switch through CDP power-negotiation messages, the initial power allocation might be adjusted.

- The switch classifies the detected IEEE device within a power consumption class. Based on the available power in the power budget, the switch determines if a port can be powered. Table 10: IEEE Power Classifications, on page 81 lists these levels.

***Table 10: IEEE Power Classifications***

| Class | Maximum Power Level Required from the Switch |
|---|---|
| 0 (class status unknown) | 15.4 W |
| 1 | 4 W |
| 2 | 7 W |
| 3 | 15.4 W |
| 4 | 30 W (For IEEE 802.3at Type 2 powered devices) |

The switch monitors and tracks requests for power and grants power only when it is available. The switch tracks its power budget (the amount of power available on the switch for PoE). Theswitch performs power-accounting calculations when a port is granted or denied power to keep the power budget up to date.

After power is applied to the port, the switch uses CDP to determine the *CDP-specific* power consumption requirement of the connected Cisco powered devices, which is the amount of power to allocate based on the CDP messages. The switch adjusts the power budget accordingly. This does not apply to third-party PoE devices. The switch processes a request and either grants or denies power. If the request is granted, the switch updates the power budget. If the request is denied, the switch ensures that power to the port is turned off, generates a syslog message, and updates the LEDs. Powered devices can also negotiate with the switch for more power.

With PoE+, powered devices use IEEE 802.3at and LLDP power with media dependent interface (MDI) type, length, and value descriptions (TLVs), Power-via-MDI TLVs, for negotiating power up to 30 W. Cisco pre-standard devices and Cisco IEEE powered devices can use CDP or the IEEE 802.3at power-via-MDI power negotiation mechanism to request power levels up to 30 W.

**Note** The initial allocation for Class 0, Class 3, and Class 4 powered devices is 15.4 W. When a device starts up and uses CDP or LLDP to send a request for more than 15.4 W, it can be allocated up to the maximum of 30 W.

**Note** The CDP-specific power consumption requirement is referred to as the *actual* power consumption requirement in the software configuration guides and command references.

If the switch detects a fault caused by an undervoltage, overvoltage, overtemperature, oscillator-fault, or short-circuit condition, it turns off power to the port, generates a syslog message, and updates the power budget and LEDs.

The PoE feature operates the same whether or not the switch is a stack member. The power budget is per switch and independent of any other switch in the stack. Election of a new active switch does not affect PoE operation. The active switch keeps track of the PoE status for all switches and ports in the stack and includes the status in output displays.

## Power Management Modes

The switch supports these PoE modes:

- **auto—**The switch automatically detects if the connected device requires power. If the switch discovers a powered device connected to the port and if the switch has enough power, it grants power, updates the power budget, turns on power to the port on a first-come, first-served basis, and updates the LEDs. For LED information, see the hardware installation guide.

  If the switch has enough power for all the powered devices, they all come up. If enough power is available for all powered devices connected to the switch, power is turned on to all devices. If there is not enough available PoE, or if a device is disconnected and reconnected while other devices are waiting for power, it cannot be determined which devices are granted or are denied power.

  If granting power would exceed the system power budget, the switch denies power, ensures that power to the port is turned off, generates a syslog message, and updates the LEDs. After power has been denied, the switch periodically rechecks the power budget and continues to attempt to grant the request for power.

  If a device being powered by the switch is then connected to wall power, the switch might continue to power the device. The switch might continue to report that it is still powering the device whether the device is being powered by the switch or receiving power from an AC power source.

  If a powered device is removed, the switch automatically detects the disconnect and removes power from the port. You can connect a nonpowered device without damaging it.

  You can specify the maximum wattage that is allowed on the port. If the IEEE class maximum wattage of the powered device is greater than the configured maximum value, the switch does not provide power to the port. If the switch powers a powered device, but the powered device later requests through CDP messages more than the configured maximum value, the switch removes power to the port. The power that was allocated to the powered device is reclaimed into the global power budget. If you do not specify a wattage, the switch delivers the maximum value. Use the **auto** setting on any PoE port. The auto mode is the default setting.

- **static—**The switch pre-allocates power to the port (even when no powered device is connected) and guarantees that power will be available for the port. The switch allocates the port configured maximum wattage, and the amount is never adjusted through the IEEE class or by CDP messages from the powered device. Because power is pre-allocated, any powered device that uses less than or equal to the maximum wattage is guaranteed to be powered when it is connected to the static port. The port no longer participates in the first-come, first-served model.

  However, if the powered-device IEEE class is greater than the maximum wattage, the switch does not supply power to it. If the switch learns through CDP messages that the powered device is consuming more than the maximum wattage, the switch shuts down the powered device.

  If you do not specify a wattage, the switch pre-allocates the maximum value. The switch powers the port only if it discovers a powered device. Use the **static** setting on a high-priority interface.

- **never—**The switch disables powered-device detection and never powers the PoE port even if an unpowered device is connected. Use this mode only when you want to make sure that power is never applied to a PoE-capable port, making the port a data-only port.

For most situations, the default configuration (auto mode) works well, providing plug-and-play operation. No further configuration is required. However, perform this task to configure a PoE port for a higher priority, to make it data only, or to specify a maximum wattage to disallow high-power powered devices on a port.

## Power Monitoring and Power Policing

When policing of the real-time power consumption is enabled, the switch takes action when a powered device consumes more power than the maximum amount allocated, also referred to as the *cutoff-power value*.

When PoE is enabled, the switch senses the real-time power consumption of the powered device. The switch monitors the real-time power consumption of the connected powered device; this is called *power monitoring* or *power sensing*. The switch also polices the power usage with the *power policing* feature.

Power monitoring is backward-compatible with Cisco intelligent power management and CDP-based power consumption. It works with these features to ensure that the PoE port can supply power to the powered device.

The switch senses the real-time power consumption of the connected device as follows:

1. The switch monitors the real-time power consumption on individual ports.
2. The switch records the power consumption, including peak power usage. The switch reports the information through the CISCO-POWER-ETHERNET-EXT-MIB.
3. If power policing is enabled, the switch polices power usage by comparing the real-time power consumption to the maximum power allocated to the device. The maximum power consumption is also referred to as the *cutoff power* on a PoE port.

   If the device uses more than the maximum power allocation on the port, the switch can either turn off power to the port, or the switch can generate a syslog message and update the LEDs (the port LED is now blinking amber) while still providing power to the device based on the switch configuration. By default, power-usage policing is disabled on all PoE ports.

   If error recovery from the PoE error-disabled state is enabled, the switch automatically takes the PoE port out of the error-disabled state after the specified amount of time.

   If error recovery is disabled, you can manually re-enable the PoE port by using the **shutdown** and **no shutdown** interface configuration commands.
4. If policing is disabled, no action occurs when the powered device consumes more than the maximum power allocation on the PoE port, which could adversely affect the switch.

## Maximum Power Allocation (Cutoff Power) on a PoE Port

When power policing is enabled, the switch determines one of the these values as the cutoff power on the PoE port in this order:

1. Manually when you set the user-defined power level that the switch budgets for the port by using the **power inline consumption default** *wattage* global or interface configuration command
2. Manually when you set the user-defined power level that limits the power allowed on the port by using the **power inline auto max** *max-wattage* or the **power inline static max** *max-wattage* interface configuration command
3. Automatically when the switch sets the power usage of the device by using CDP power negotiation or by the IEEE classification and LLDP power negotiation.

Use the first or second method in the previous list to manually configure the cutoff-power value by entering the **power inline consumption default** *wattage* or the **power inline** [**auto** | **static max**] *max-wattage* command.

If you do not manually configure the cutoff-power value, the switch automatically determines it by using CDP power negotiation or the device IEEE classification and LLDP power negotiation. If CDP or LLDP are not enabled, the default value of 30 W is applied. However without CDP or LLDP, the switch does not allow devices to consume more than 15.4 W of power because values from 15400 to 30000 mW are only allocated based on CDP or LLDP requests. If a powered device consumes more than 15.4 W without CDP or LLDP negotiation, the device might be in violation of the maximum current (*Imax*) limitation and might experience an *Icut* fault for drawing more current than the maximum. The port remains in the fault state for a time before attempting to power on again. If the port continuously draws more than 15.4 W, the cycle repeats.

**Note** When a powered device connected to a PoE+ port restarts and sends a CDP or LLDP packet with a power TLV, the switch locks to the power-negotiation protocol of that first packet and does not respond to power requests from the other protocol. For example, if the switch is locked to CDP, it does not provide power to devices that send LLDP requests. If CDP is disabled after the switch has locked on it, the switch does not respond to LLDP power requests and can no longer power on any accessories. In this case, you should restart the powered device.

## Power Consumption Values

You can configure the initial power allocation and the maximum power allocation on a port. However, these values are only the configured values that determine when the switch should turn on or turn off power on the PoE port. The maximum power allocation is not the same as the actual power consumption of the powered device. The actual cutoff power value that the switch uses for power policing is not equal to the configured power value.

When power policing is enabled, the switch polices the power usage *at the switch port*, which is greater than the power consumption of the device. When you are manually set the maximum power allocation, you must consider the power loss over the cable from the switch port to the powered device. The cutoff power is the sum of the rated power consumption of the powered device and the worst-case power loss over the cable.

We recommend that you enable power policing when PoE is enabled on your switch. For example, if policing is disabled and you set the cutoff-power value by using the **power inline auto max 6300** interface configuration command, the configured maximum power allocation on the PoE port is 6.3 W (6300 mW). The switch provides power to the connected devices on the port if the device needs up to 6.3 W. If the CDP-power negotiated value or the IEEE classification value exceeds the configured cutoff value, the switch does not provide power to the connected device. After the switch turns on power on the PoE port, the switch does not police the real-time power consumption of the device, and the device can consume more power than the maximum allocated amount, which could adversely affect the switch and the devices connected to the other PoE ports.

Because the switch supports internal power supplies and the Cisco Redundant Power System 2300 (also referred to as the RPS 2300), the total amount of power available for the powered devices varies depending on the power supply configuration.

# How to Configure PoE

## Configuring a Power Management Mode on a PoE Port

**Note** When you make PoE configuration changes, the port being configured drops power. Depending on the new configuration, the state of the other PoE ports, and the state of the power budget, the port might not be powered up again. For example, port 1 is in the auto and on state, and you configure it for static mode. The switch removes power from port 1, detects the powered device, and repowers the port. If port 1 is in the auto and on state and you configure it with a maximum wattage of 10 W, the switch removes power from the port and then redetects the powered device. The switch repowers the port only if the powered device is a class 1, class 2, or a Cisco-only powered device.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *interface-id*
4. **power inline** {**auto** [**max** *max-wattage*] | **never** | **static** [**max** *max-wattage*]}
5. **end**
6. **show power inline** [*interface-id* | **module** *switch-number*]
7. **copy running-config startup-config**

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br><br>**Example:**<br>`Switch> enable` | Enables privileged EXEC mode. Enter your password if prompted. |
| **Step 2** | **configure terminal**<br><br>**Example:**<br>`Switch# configure terminal` | Enters global configuration mode. |
| **Step 3** | **interface** *interface-id*<br><br>**Example:**<br>`Switch(config)# interface gigabitethernet2/0/1` | Specifies the physical port to be configured, and enters interface configuration mode. |
| **Step 4** | **power inline** {**auto** [**max** *max-wattage*] \| **never** \| **static** [**max** *max-wattage*]} | Configures the PoE mode on the port. The keywords have these meanings: |

| | Command or Action | Purpose |
|---|---|---|
| | **Example:**<br>`Switch(config-if)# power inline auto` | • **auto—**Enables powered-device detection. If enough power is available, automatically allocates power to the PoE port after device detection. This is the default setting.<br>• **max** *max-wattage***—**Limits the power allowed on the port. If no value is specified, the maximum is allowed.<br>• **max** *max-wattage***—**Limits the power allowed on the port. The range is 4000 to 30000 mW. If no value is specified, the maximum is allowed.<br>• **never —**Disables device detection, and disable power to the port.<br>**Note** If a port has a Cisco powered device connected to it, do not use the **power inline never** command to configure the port. A false link-up can occur, placing the port into the error-disabled state.<br>• **static—**Enables powered-device detection. Pre-allocate (reserve) power for a port before the switch discovers the powered device. The switch reserves power for this port even when no device is connected and guarantees that power will be provided upon device detection.<br>The switch allocates power to a port configured in static mode before it allocates power to a port configured in auto mode. |
| **Step 5** | **end**<br>**Example:**<br>`Switch(config-if)# end` | Returns to privileged EXEC mode. |
| **Step 6** | **show power inline** [*interface-id* \| **module** *switch-number*]<br>**Example:**<br>`Switch# show power inline` | Displays PoE status for a switch or a switch stack, for the specified interface, or for a specified stack member.<br>The **module** *switch-number* keywords are supported only on stacking-capable switches. |
| **Step 7** | **copy running-config startup-config**<br>**Example:**<br>`Switch# copy running-config startup-config` | (Optional) Saves your entries in the configuration file. |

# Fast POE

**Fast PoE** - This feature remembers the last power drawn from a particular PSE port and switches on power the moment AC power is plugged in (within 15 to 20 seconds of switching on power) without waiting for IOS to boot up. When **poe-ha** is enabled on a particular port, the switch on a recovery after power failure, provides power to the connected endpoint devices within short duration before even the IOS forwarding starts up.

This feature can be configured by the command **poe-ha**. If the user replaces the power device connected to a port when the switch is powered off, then this new device will get the power which the previous device was drawing.

# Configuring Fast POE

To configure Fast POE, perform the following steps:

**Note** You will need to configure the **poe-ha** command before connecting the PD, or you will need to manually shut/unshut the port after configuring **poe-ha**.

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *interface-id*
4. **power inline port poe-ha**
5. **end**

## DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br><br>**Example:**<br>`Switch> enable` | Enables privileged EXEC mode. Enter your password if prompted. |
| **Step 2** | **configure terminal**<br><br>**Example:**<br>`Switch# configure terminal` | Enters global configuration mode. |
| **Step 3** | **interface** *interface-id*<br><br>**Example:**<br>`Switch(config)# interface gigabitethernet2/0/1` | Specifies the physical port to be configured, and enters interface configuration mode. |
| **Step 4** | **power inline port poe-ha**<br><br>**Example:**<br>`Switch(config-if)# power inline port poe-ha` | Configures POE High Availability. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 5** | **end**<br><br>**Example:**<br>`Switch(config-if)# end` | Returns to privileged EXEC mode. |

# Budgeting Power for Devices Connected to a PoE Port

When Cisco powered devices are connected to PoE ports, the switch uses Cisco Discovery Protocol (CDP) to determine the *CDP-specific* power consumption of the devices, and the switch adjusts the power budget accordingly. This does not apply to IEEE third-party powered devices. For these devices, when the switch grants a power request, the switch adjusts the power budget according to the powered-device IEEE classification. If the powered device is a class 0 (class status unknown) or a class 3, the switch budgets 15,400 mW for the device, regardless of the CDP-specific amount of power needed. If the powered device reports a higher class than its CDP-specific consumption or does not support power classification (defaults to class 0), the switch can power fewer devices because it uses the IEEE class information to track the global power budget.

By using the **power inline consumption** *wattage* interface configuration command or the **power inline consumption default** *wattage* global configuration command, you can override the default power requirement specified by the IEEE classification. The difference between what is mandated by the IEEE classification and what is actually needed by the device is reclaimed into the global power budget for use by additional devices. You can then extend the switch power budget and use it more effectively.

**Caution** You should carefully plan your switch power budget, enable the power monitoring feature, and make certain not to oversubscribe the power supply.

**Note** When you manually configure the power budget, you must also consider the power loss over the cable between the switch and the powered device.

## Budgeting Power to All PoE ports

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **no cdp run**
4. **power inline consumption default** *wattage*
5. **end**
6. **show power inline consumption default**
7. **copy running-config startup-config**

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br><br>**Example:**<br>`Switch> enable` | Enables privileged EXEC mode. Enter your password if prompted. |
| **Step 2** | **configure terminal**<br><br>**Example:**<br>`Switch# configure terminal` | Enters global configuration mode. |
| **Step 3** | **no cdp run**<br><br>**Example:**<br>`Switch(config)# no cdp run` | (Optional) Disables CDP. |
| **Step 4** | **power inline consumption default** *wattage*<br><br>**Example:**<br>`Switch(config)# power inline consumption default 5000` | Configures the power consumption of powered devices connected to each PoE port.<br><br>The range for each device is 4000 to 30000 mW (PoE+). The default is 30000 mW.<br><br>**Note** |
| **Step 5** | **end**<br><br>**Example:**<br>`Switch(config)# end` | Returns to privileged EXEC mode. |
| **Step 6** | **show power inline consumption default**<br><br>**Example:**<br>`Switch# show power inline consumption default` | Displays the power consumption status. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 7** | **copy running-config startup-config**<br><br>**Example:**<br>`Switch# copy running-config startup-config` | (Optional) Saves your entries in the configuration file. |

## Budgeting Power to a Specific PoE Port

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **no cdp run**
4. **interface** *interface-id*
5. **power inline consumption** *wattage*
6. **end**
7. **show power inline consumption**
8. **copy running-config startup-config**

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br><br>**Example:**<br>`Switch> enable` | Enables privileged EXEC mode. Enter your password if prompted. |
| **Step 2** | **configure terminal**<br><br>**Example:**<br>`Switch# configure terminal` | Enters global configuration mode. |
| **Step 3** | **no cdp run**<br><br>**Example:**<br>`Switch(config)# no cdp run` | (Optional) Disables CDP. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 4** | **interface** *interface-id*<br><br>**Example:**<br>`Switch(config)# interface gigabitethernet2/0/1` | Specifies the physical port to be configured, and enter interface configuration mode. |
| **Step 5** | **power inline consumption** *wattage*<br><br>**Example:**<br>`Switch(config-if)# power inline consumption 5000` | Configures the power consumption of a powered device connected to a PoE port on the switch.<br><br>The range for each device is 4000 to 30000 mW (PoE+). The default is 30000 mW (PoE+). |
| **Step 6** | **end**<br><br>**Example:**<br>`Switch(config-if)# end` | Returns to privileged EXEC mode. |
| **Step 7** | **show power inline consumption**<br><br>**Example:**<br>`Switch# show power inline consumption` | Displays the power consumption data. |
| **Step 8** | **copy running-config startup-config**<br><br>**Example:**<br><br>`Switch# copy running-config startup-config` | (Optional) Saves your entries in the configuration file. |

# Configuring Power Policing

By default, the switch monitors the real-time power consumption of connected powered devices. You can configure the switch to police the power usage. By default, policing is disabled.

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *interface-id*
4. **power inline police** [**action** {**log** | **errdisable**}]
5. **exit**
6. Use one of the following:
   - **errdisable detect cause inline-power**
   - **errdisable recovery cause inline-power**
   - **errdisable recovery interval** *interval*
7. **exit**
8. Use one of the following:
   - **show power inline police**
   - **show errdisable recovery**
9. **copy running-config startup-config**

## DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br><br>**Example:**<br>`Switch> enable` | Enables privileged EXEC mode. Enter your password if prompted. |
| **Step 2** | **configure terminal**<br><br>**Example:**<br>`Switch# configure terminal` | Enters global configuration mode. |
| **Step 3** | **interface** *interface-id*<br><br>**Example:**<br>`Switch(config)# interface gigabitethernet2/0/1` | Specifies the physical port to be configured, and enter interface configuration mode. |
| **Step 4** | **power inline police** [**action** {**log** \| **errdisable**}]<br><br>**Example:**<br>`Switch(config-if)# power inline police` | If the real-time power consumption exceeds the maximum power allocation on the port, configures the switch to take one of these actions:<br>• **power inline police—**Shuts down the PoE port, turns off power to it, and puts it in the error-disabled state. |

| | Command or Action | Purpose |
|---|---|---|
| | | **Note** You can enable error detection for the PoE error-disabled cause by using the **errdisable detect cause inline-power** global configuration command. You can also enable the timer to recover from the PoE error-disabled state by using the **errdisable recovery cause inline-power interval** *interval* global configuration command.<br>• **power inline police action errdisable—**Turns off power to the port if the real-time power consumption exceeds the maximum power allocation on the port.<br>• **power inline police action log—**Generates a syslog message while still providing power to the port.<br>If you do not enter the **action log** keywords, the default action shuts down the port and puts the port in the error-disabled state. |
| **Step 5** | **exit**<br>**Example:**<br>`Switch(config-if)# exit` | Returns to global configuration mode. |
| **Step 6** | Use one of the following:<br>• **errdisable detect cause inline-power**<br>• **errdisable recovery cause inline-power**<br>• **errdisable recovery interval** *interval*<br>**Example:**<br>`Switch(config)# errdisable detect cause inline-power`<br>`Switch(config)# errdisable recovery cause inline-power`<br>`Switch(config)# errdisable recovery interval 100` | (Optional) Enables error recovery from the PoE error-disabled state, and configures the PoE recover mechanism variables.<br>By default, the recovery interval is 300 seconds.<br>For **interval** *interval*, specifies the time in seconds to recover from the error-disabled state. The range is 30 to 86400. |
| **Step 7** | **exit**<br>**Example:**<br>`Switch(config)# exit` | Returns to privileged EXEC mode. |
| **Step 8** | Use one of the following:<br>• **show power inline police**<br>• **show errdisable recovery** | Displays the power monitoring status, and verify the error recovery settings. |

| | Command or Action | Purpose |
|---|---|---|
| | **Example:**<br>`Switch# show power inline police`<br>`Switch# show errdisable recovery` | |
| **Step 9** | **copy running-config startup-config**<br>**Example:**<br>`Switch# copy running-config startup-config` | (Optional) Saves your entries in the configuration file. |

# Monitoring Power Status

*Table 11: Show Commands for Power Status*

| Command | Purpose |
|---|---|
| **show env power switch** [*switch-number*] | (Optional) Displays the status of the internal power supplies for each switch in the stack or for the specified switch.<br>The range is 1 to , depending on the switch member numbers in the stack. These keywords are available only on stacking-capable switches. |
| **show power inline** [*interface-id* \| **module** *switch-number*] | Displays PoE status for a switch or switch stack, for an interface, or for a specific switch in the stack. |
| **show power inline police** | Displays the power policing data. |

# Configuration Examples for Configuring PoE

## Budgeting Power: Example

When you enter one of the following commands,

- [**no**] **power inline consumption default** *wattage* global configuration command
- [**no**] **power inline consumption** *wattage*

interface configuration command

this caution message appears:

```
%CAUTION: Interface Gi1/0/1: Misconfiguring the 'power inline  consumption/allocation'
command may cause damage to the
switch and void your warranty. Take precaution not to oversubscribe the power supply. It
is recommended to enable power
policing if the switch supports it. Refer to documentation.
```

# Additional References

### Error Message Decoder

| Description | Link |
|---|---|
| To help you research and resolve system error messages in this release, use the Error Message Decoder tool. | https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi |

### MIBs

| MIB | MIBs Link |
|---|---|
| All supported MIBs for this release. | To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:<br>http://www.cisco.com/go/mibs |

### Technical Assistance

| Description | Link |
|---|---|
| The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.<br>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.<br>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password. | http://www.cisco.com/support |

CHAPTER 8

# Configuring EEE


- Finding Feature Information, page 97
- Information About EEE, page 97
- Restrictions for EEE, page 98
- How to Configure EEE, page 98
- Monitoring EEE, page 99
- Configuration Examples for Configuring EEE, page 100
- Additional References, page 100
- Feature History and Information for Configuring EEE, page 101


# Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

# Information About EEE

## EEE Overview

Energy Efficient Ethernet (EEE) is an IEEE 802.3az standard that is designed to reduce power consumption in Ethernet networks during idle periods.

EEE can be enabled on devices that support low power idle (LPI) mode. Such devices can save power by entering LPI mode during periods of low utilization. In LPI mode, systems on both ends of the link can save

power by shutting down certain services. EEE provides the protocol needed to transition into and out of LPI mode in a way that is transparent to upper layer protocols and applications.

## Default EEE Configuration

EEE is enabled by default.

# Restrictions for EEE

EEE has the following restrictions:

- Changing the EEE configuration resets the interface because the device has to restart Layer 1 autonegotiation.
- You might want to enable the Link Layer Discovery Protocol (LLDP) for devices that require longer wakeup times before they are able to accept data on their receive paths. Doing so enables the device to negotiate for extended system wakeup times from the transmitting link partner.

# How to Configure EEE

You can enable or disable EEE on an interface that is connected to an EEE-capable link partner.

## Enabling or Disabling EEE

### SUMMARY STEPS

1. **configure terminal**
2. **interface** *interface-id*
3. **power efficient-ethernet auto**
4. **no power efficient-ethernet auto**
5. **end**
6. **copy running-config startup-config**

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **configure terminal**<br><br>**Example:**<br>`Switch# configure terminal` | Enters global configuration mode. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 2** | **interface** *interface-id*<br><br>**Example:**<br><br>`Switch(config)# interface gigabitethernet1/0/1` | Specifies the interface to be configured, and enter interface configuration mode. |
| **Step 3** | **power efficient-ethernet auto**<br><br>**Example:**<br><br>`Switch(config-if)# power efficient-ethernet auto` | Enables EEE on the specified interface. When EEE is enabled, the device advertises and autonegotiates EEE to its link partner. |
| **Step 4** | **no power efficient-ethernet auto**<br><br>**Example:**<br><br>`Switch(config-if)# no power efficient-ethernet auto` | Disables EEE on the specified interface. |
| **Step 5** | **end**<br><br>**Example:**<br><br>`Switch(config-if)# end` | Returns to privileged EXEC mode. |
| **Step 6** | **copy running-config startup-config**<br><br>**Example:**<br><br>`Switch# copy running-config startup-config` | (Optional) Saves your entries in the configuration file. |

# Monitoring EEE

***Table 12: Commands for Displaying EEE Settings***

| Command | Purpose |
|---|---|
| **show eee capabilities interface** *interface-id* | Displays EEE capabilities for the specified interface. |
| **show eee status interface** *interface-id* | Displays EEE status information for the specified interface. |

# Configuration Examples for Configuring EEE

This example shows how to enable EEE for an interface:

```
Switch# configure terminal
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# power efficient-ethernet auto
```

This example shows how to disable EEE for an interface:

```
Switch# configure terminal
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# no power efficient-ethernet auto
```

# Additional References

### Error Message Decoder

| Description | Link |
|---|---|
| To help you research and resolve system error messages in this release, use the Error Message Decoder tool. | https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi |

### MIBs

| MIB | MIBs Link |
|---|---|
| All supported MIBs for this release. | To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:<br>http://www.cisco.com/go/mibs |

### Technical Assistance

| Description | Link |
|---|---|
| The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.<br>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.<br>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password. | http://www.cisco.com/support |

# Feature History and Information for Configuring EEE

| Release | Modification |
|---|---|
| Cisco IOS 15.0(2)EX | This feature was introduced. |

# INDEX


## A

active link 49
and routing 49
and routing protocols 49
auto mode 82
auto-MDIX 44
    configuring 44
    described 44
auto-MDIX, configuring 44

## B

Budgeting Power 94
    Example command 94

## C

CDP 55, 80
    defined with LLDP 55
    power negotiation extensions 80
CDP with power consumption, described 80
CDP with power negotiation, described 80
Cisco intelligent power management 80
civic location 57
Configuration Examples for Configuring PoE command 94
configuring 44

## D

default configuration 59
    LLDP 59
default setting 49
described 44, 49
devices supported 16, 80

## E

ELIN location 57
enhanced PoE 80, 90
Ethernet management port 49, 50
    active link 49
    and routing 49
    and routing protocols 49
    default setting 49
    described 49
    for network management 49
    supported features 50
    unsupported features 50
Ethernet management port configuration 51
Ethernet management port, internal 49, 50
    and routing 49
    and routing protocols 49
    unsupported features 50
Example for Configuring Auto-MDIX command 45
Examples for Configuring the System MTU command 77

## F

Fa0 port 49
    See Ethernet management port 49
fastethernet0 port 49
    See Ethernet management port 49
for network management 49

## H

high-power devices operating in low-power mode 80
hub 50

## I

IEEE power classification levels 80
interface 94

interfaces 44
auto-MDIX, configuring 44
inventory management TLV 57

## L

LLDP 55, 59, 60, 61
transmission timer and holdtime, setting 61
configuring 59
default configuration 59
enabling 60
overview 55
switch stack considerations 55
LLDP-MED 56, 63
configuring 63
TLVs 63
overview 56
supported TLVs 56
location TLV 57

## M

MAC/PHY configuration status TLV 55
management address TLV 55
monitoring 83
monitoring power 91
MTU 75
system 75

## N

network policy TLV 57

## P

PoE 16, 80, 82, 83, 91
auto mode 82
CDP with power consumption, described 80
CDP with power negotiation, described 80
Cisco intelligent power management 80
devices supported 16, 80
high-power devices operating in low-power mode 80
IEEE power classification levels 80
monitoring 83
monitoring power 91
policing power consumption 91
policing power usage 83
PoE *(continued)*
power management modes 82
power negotiation extensions to CDP 80
powered-device detection and initial power allocation 80
standards supported 80
static mode 82
supported watts per port 16, 80
policing power consumption 91
policing power usage 83
port description TLV 55
port VLAN ID TLV 55
power management modes 82
power management TLV 57
power negotiation extensions 80
power negotiation extensions to CDP 80
powered-device detection and initial power allocation 80

## S

See Ethernet management port 49
standards supported 80
static mode 82
statistics 94
interface 94
supported features 50
supported watts per port 16, 80
system 75
system capabilities TLV 55
system description TLV 55
system name TLV 55

## T

TLVs 55
defined 55

## U

unsupported features 50

## W

wired location service 57, 58, 68
configuring 68
location TLV 57
understanding 58