



Interface and Hardware Component Configuration Guide, Cisco IOS XE Release 3SE (Catalyst 3650 Switches)

First Published: 2013-10-04

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-30459-01



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

Using the Help System 3

Understanding Abbreviated Commands 4

No and Default Forms of Commands 4

CLI Error Messages 4

Configuration Logging 5

How to Use the CLI to Configure Features 5

Configuring the Command History 5

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

Using the Web Graphical User Interface 13

Prerequisites for Using the Web GUI 13

Information About Using The Web GUI	13
Web GUI Features	13
Connecting the Console Port of the Switch	15
Logging On to the Web GUI	15
Enabling Web and Secure Web Modes	15
Configuring the Switch Web GUI	16
<hr/>	
CHAPTER 3	Configuring Interface Characteristics 21
Finding Feature Information	21
Information About Configuring Interface Characteristics	21
Interface Types	21
Port-Based VLANs	22
Switch Ports	22
Access Ports	22
Trunk Ports	23
Tunnel Ports	23
Routed Ports	23
Switch Virtual Interfaces	24
SVI Autostate Exclude	24
EtherChannel Port Groups	25
Power over Ethernet Ports	25
Using the Switch USB Ports	26
USB Mini-Type B Console Port	26
Console Port Change Logs	26
Interface Connections	27
Default Ethernet Interface Configuration	27
Interface Speed and Duplex Mode	28
Speed and Duplex Configuration Guidelines	29
IEEE 802.3x Flow Control	29
Layer 3 Interfaces	30
How to Configure Interface Characteristics	31
Configuring Interfaces Procedure	31
Adding a Description for an Interface	32
Configuring a Range of Interfaces	33
Configuring and Using Interface Range Macros	34

Configuring Ethernet Interfaces	35
Setting the Interface Speed and Duplex Parameters	35
Configuring IEEE 802.3x Flow Control	37
Configuring Layer 3 Interfaces	38
Configuring Logical Layer 3 GRE Tunnel Interfaces	39
Configuring SVI Autostate Exclude	41
Shutting Down and Restarting the Interface	42
Configuring the Console Media Type	43
Configuring the USB Inactivity Timeout	44
Monitoring Interface Characteristics	45
Monitoring Interface Status	45
Clearing and Resetting Interfaces and Counters	46
Configuration Examples for Interface Characteristics	46
Adding a Description to an Interface: Example	46
Configuring a Range of Interfaces: Examples	47
Configuring and Using Interface Range Macros: Examples	47
Setting Interface Speed and Duplex Mode: Example	48
Configuring Layer 3 Interfaces: Example	48
Configuring the Console Media Type: Example	48
Configuring the USB Inactivity Timeout: Example	49
Additional References for the Interface Characteristics Feature	49
Feature History and Information for Configuring Interface Characteristics	50

CHAPTER 4**Configuring Auto-MDIX 51**

Prerequisites for Auto-MDIX	51
Restrictions for Auto-MDIX	51
Information about Configuring Auto-MDIX	52
Auto-MDIX on an Interface	52
How to Configure Auto-MDIX	52
Configuring Auto-MDIX on an Interface	52
Monitoring Auto-MDIX	54
Example for Configuring Auto-MDIX	54
Additional References	54
Feature History and Information for Auto-MDIX	55

CHAPTER 5**Configuring Ethernet Management Port 57**

- Finding Feature Information 57
- Prerequisites for Ethernet Management Ports 57
- Information about the Ethernet Management Port 57
 - Ethernet Management Port Direct Connection to a Switch 58
 - Ethernet Management Port Connection to Stack Switches using a Hub 58
 - Ethernet Management Port and Routing 58
 - Supported Features on the Ethernet Management Port 59
- How to Configure the Ethernet Management Port 60
 - Disabling and Enabling the Ethernet Management Port 60
- Additional References 61
- Feature Information for Ethernet Management Ports 62

CHAPTER 6**Configuring LLDP, LLDP-MED, and Wired Location Service 63**

- Finding Feature Information 63
- LLDP, LLDP-MED, and Wired Location Service Overview 63
 - LLDP 63
 - LLDP Supported TLVs 64
 - LLDP and Cisco Switch Stacks 64
 - LLDP and Cisco Medianet 64
 - LLDP-MED 64
 - LLDP-MED Supported TLVs 65
 - Wired Location Service 66
 - Default LLDP Configuration 67
 - Configuration Guidelines 67
- How to Configure LLDP, LLDP-MED, and Wired Location Service 68
 - Enabling LLDP 68
 - Configuring LLDP Characteristics 69
 - Configuring LLDP-MED TLVs 71
 - Configuring Network-Policy TLV 73
 - Configuring Location TLV and Wired Location Service 75
 - Enabling Wired Location Service on the Switch 78
- Configuration Examples for LLDP, LLDP-MED, and Wired Location Service 79
 - Configuring Network-Policy TLV: Examples 79

Monitoring and Maintaining LLDP, LLDP-MED, and Wired Location Service	80
Additional References for LLDP, LLDP-MED, and Wired Location Service	81
Feature Information for LLDP, LLDP-MED, and Wired Location Service	82

CHAPTER 7**Configuring System MTU 83**

Finding Feature Information	83
Information about the MTU	83
System MTU Values	83
Restrictions for System MTU	84
System MTU Value Application	84
How to Configure MTU Sizes	84
Configuring the System MTU	84
Configuring Protocol-Specific MTU	85
Configuration Examples for System MTU	86
Additional References for System MTU	87
Feature Information for System MTU	88

CHAPTER 8**Configuring Internal Power Supplies 89**

Information About Internal Power Supplies	89
How to Configure Internal Power Supplies	89
Configuring an Internal Power Supply	89
Monitoring Internal Power Supplies	90
Configuration Examples for Internal Power Supplies	90
Additional References	91
Feature History and Information for Internal Power Supplies	92

CHAPTER 9**Configuring PoE 93**

Finding Feature Information	93
Information about PoE	93
Power over Ethernet Ports	93
Supported Protocols and Standards	94
Powered-Device Detection and Initial Power Allocation	94
Power Management Modes	96
Power Monitoring and Power Policing	97
Power Consumption Values	97

How to Configure PoE	98
Configuring a Power Management Mode on a PoE Port	98
Configuring Power Policing	99
Monitoring Power Status	102
Additional References	102
Feature Information for PoE	103

CHAPTER 10

Configuring EEE	105
Finding Feature Information	105
Information About EEE	105
EEE Overview	105
Default EEE Configuration	106
Restrictions for EEE	106
How to Configure EEE	106
Enabling or Disabling EEE	106
Monitoring EEE	107
Configuration Examples for Configuring EEE	108
Additional References	108
Feature History and Information for Configuring EEE	109



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 .
<i>Italic font</i>	Document titles, new or emphasized terms, and arguments for which you supply values are in <i>italic font</i> .
Courier font	Terminal sessions and information the system displays appear in <i>courier font</i> .
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.

- Cisco Catalyst 3650 Switch documentation, located at:
http://www.cisco.com/go/cat3650_docs
- Cisco SFP, SFP+, and QSFP+ 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 5](#)

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, a 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 <ul style="list-style-type: none"> • Change terminal settings. • Perform basic tests. • 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 <i>vlan-id</i> command.	Switch(config-vlan)#	To exit to global configuration mode, enter the exit command. 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)#	To exit to global configuration mode, enter exit . To return to privileged EXEC mode, press Ctrl-Z or enter end .	Use this mode to configure parameters for the Ethernet ports.

Mode	Access Method	Prompt	Exit Method	About This Mode
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 . To return to privileged EXEC mode, press Ctrl-Z or enter end .	Use this mode to configure parameters for the terminal line.

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 Example: Switch# help	Obtains a brief description of the help system in any command mode.
Step 2	<i>abbreviated-command-entry ?</i> Example: Switch# di? dir disable disconnect	Obtains a list of commands that begin with a particular character string.
Step 3	<i>abbreviated-command-entry <Tab></i> Example: Switch# sh conf<tab> Switch# show configuration	Completes a partial command name.

	Command or Action	Purpose
Step 4	? Example: Switch> ?	Lists all commands available for a particular command mode.
Step 5	<i>command</i> ? Example: Switch> show ?	Lists the associated keywords for a command.
Step 6	<i>command keyword</i> ? Example: Switch(config)# cdp holdtime ? <10-255> Length of time (in sec) that receiver must keep this packet	Lists the associated arguments for a keyword.

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. 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. 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. 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.

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 [<i>size number-of-lines</i>] Example: 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.

	Command or Action	Purpose
Step 3	show history Example: Switch# <code>show history</code>	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 Example: Switch# <code>terminal no history</code>	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 reenble it.

SUMMARY STEPS

1. `terminal editing`
2. `terminal no editing`

DETAILED STEPS

	Command or Action	Purpose
Step 1	terminal editing Example: Switch# <code>terminal editing</code>	Reenables the enhanced editing mode for the current terminal session in privileged EXEC mode.

	Command or Action	Purpose
Step 2	terminal no editing Example: Switch# <code>terminal no editing</code>	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. 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 Example: <pre>Switch(config)# access-list 101 permit tcp 10.15.22.25 255.255.255.0 10.15.22.35 Switch(config)# \$ 101 permit tcp 10.15.22.25 255.255.255.0 10.15.22.35 255.25 Switch(config)# \$t tcp 10.15.22.25 255.255.255.0 131.108.1.20 255.255.255.0 eq Switch(config)# \$15.22.25 255.255.255.0 10.15.22.35 255.255.255.0 eq 45</pre>	<p>Displays the global configuration command entry that extends beyond one line.</p> <p>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.</p>
Step 2	Ctrl-A Example: <pre>Switch(config)# access-list 101 permit tcp 10.15.22.25 255.255.255.0 10.15.25\$</pre>	<p>Checks the complete syntax.</p> <p>The dollar sign (\$) appears at the end of the line to show that the line has been scrolled to the right.</p>
Step 3	Return key	<p>Execute the commands.</p> <p>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.</p> <p>Use line wrapping with the command history feature to recall and modify previous complex command entries.</p>

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	<code>{show more} command {begin include exclude} regular-expression</code>	Searches and filters the output.

	Command or Action	Purpose
	<p>Example:</p> <pre>Switch# show interfaces include protocol Vlan1 is up, line protocol is up Vlan10 is up, line protocol is down GigabitEthernet1/0/1 is up, line protocol is down GigabitEthernet1/0/2 is up, line protocol is up</pre>	<p>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.</p>

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 active switch. You cannot manage stack members on an individual switch basis. You can connect to the active switch through the console port or the Ethernet management port of one or more stack members. Be careful with using multiple CLI sessions on the active switch. 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.

To debug the standby switch, use the **session standby ios** privileged EXEC command from the active switch to access the IOS console of the standby switch. To debug a specific stack member, use the **session switch stack-member-number** privileged EXEC command from the active switch to access the diagnostic shell of the stack member. For more information about these commands, see the switch command reference.

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.



Using the Web Graphical User Interface

- [Prerequisites for Using the Web GUI, page 13](#)
- [Information About Using The Web GUI, page 13](#)
- [Connecting the Console Port of the Switch , page 15](#)
- [Logging On to the Web GUI, page 15](#)
- [Enabling Web and Secure Web Modes , page 15](#)
- [Configuring the Switch Web GUI, page 16](#)

Prerequisites for Using the Web GUI

- The GUI must be used on a PC running Windows 7, Windows XP SP1 (or later releases), or Windows 2000 SP4 (or later releases).
- The switch GUI is compatible with Microsoft Internet Explorer version 10.x, Mozilla Firefox 20.x, or Google Chrome 26.x.

Information About Using The Web GUI

A web browser, or graphical user interface (GUI), is built into each switch.

You can use either the service port interface or the management interface to access the GUI. We recommend that you use the service-port interface. Click Help at the top of any page in the GUI to display online help. You might need to disable your browser's pop-up blocker to view the online help.

Web GUI Features

The switch web GUI supports the following:

The Configuration Wizard—After initial configuration of the IP address and the local username/password or auth via the authentication server (privilege 15 needed), the wizard provides a method to complete the initial

wireless configuration. Start the wizard through Configuration -> Wizard and follow the nine-step process to configure the following:

- Admin Users
- SNMP System Summary
- Management Port
- Wireless Management
- RF Mobility and Country code
- Mobility configuration
- WLANs
- 802.11 Configuration
- Set Time

The Monitor tab:

- Displays summary details of switch, clients, and access points.
- Displays all radio and AP join statistics.
- Displays air quality on access points.
- Displays list of all Cisco Discovery Protocol (CDP) neighbors on all interfaces and the CDP traffic information.
- Displays all rogue access points based on their classification-friendly, malicious, ad hoc, classified, and unclassified.

The Configuration tab:

- Enables you to configure the switch for all initial operation using the web Configuration Wizard. The wizard allows you to configure user details, management interface, and so on.
- Enables you to configure the system, internal DHCP server, management, and mobility management parameters.
- Enables you to configure the switch, WLAN, and radios.
- Enables you to configure and set security policies on your switch.
- Enables you to access the switch operating system software management commands.

The Administration tab enables you to configure system logs.

Connecting the Console Port of the Switch

Before You Begin

Before you can configure the switch for basic operations, you need to connect it to a PC that uses a VT-100 terminal emulation program (such as HyperTerminal, ProComm, Minicom, or Tip).

-
- Step 1** Connect one end of a null-modem serial cable to the switch's RJ-45 console port and the other end to your PC's serial port.
- Step 2** Plug the AC power cord into the switch and a grounded 100 to 240 VAC, 50/60-Hz electrical outlet. Turn on the power supply. The bootup script displays operating system software initialization (code download and power-on self-test verification) and basic configuration. If the switch passes the power-on self-test, the bootup script runs the configuration wizard, which prompts you for basic configuration input.
- Step 3** Enter **yes**. Proceed with basic initial setup configuration parameters in the CLI setup wizard. Specify the IP address for the service port which is the gigabitethernet 0/0 interface.
After entering the configuration parameters in the configuration wizard, you can access the Web GUI. Now, the switch is configured with the IP address for service port.
-

Logging On to the Web GUI

Enter the switch IP address in your browser's address bar. For a secure connection, enter `https://ip-address`. For a less secure connection, enter `http://ip-address`.

Enabling Web and Secure Web Modes

-
- Step 1** Choose **Configuration > Switch > Management > Protocol Management > HTTP-HTTPS**.
The **HTTP-HTTPS Configuration** page appears.
- Step 2** To enable web mode, which allows users to access the switch GUI using "http://ip-address," choose Enabled from the HTTP Access drop-down list. Otherwise, choose Disabled. Web mode (HTTP) is not a secure connection.

- Step 3** To enable secure web mode, which allows users to access the switch GUI using “https://ip-address,” choose Enabled from the HTTPS Access drop-down list. Otherwise, choose Disabled. Secure web mode (HTTPS) is a secure connection.
- Step 4** Choose to track the device in the IP Device Tracking check box.
- Step 5** Choose to enable the trust point in the Enable check box.
- Step 6** Choose the trustpoints from the Trustpoints drop-down list.
- Step 7** Enter the amount of time, in seconds, before the web session times out due to inactivity in the HTTP Timeout-policy (1 to 600 sec) text box.
The valid range is from 1 to 600 seconds.
- Step 8** Enter the server life time in the Server Life Time (1 to 86400 sec) text box.
The valid range is from 1 to 86400 seconds.
- Step 9** Enter the maximum number of connection requests that the server can accept in the Maximum number of Requests (1 to 86400) text box.
The valid range is from 1 to 86400 connections.
- Step 10** Click **Apply**.
- Step 11** Click **Save Configuration**.
-

Configuring the Switch Web GUI

The configuration wizard enables you to configure basic settings on the switch. You can run the wizard after you receive the switch from the factory or after the switch has been reset to factory defaults. The configuration wizard is available in both GUI and CLI formats.

- Step 1** Connect your PC to the service port and configure an IPv4 address to use the same subnet as the switch. The switch is loaded with IOS XE image and the service port interface is configured as gigabitethernet 0/0.
- Step 2** Start Internet Explorer 10 (or later), Firefox 2.0.0.11 (or later), or Google Chrome on your PC and enter the management interface IP address on the browser window. The management interface IP address is same as the gigabitethernet 0/0 (also known as service port interface). When you log in for the first time, you need to enter HTTP username and password. By default, the username is **admin** and the password is **cisco**.
You can use both HTTP and HTTPS when using the service port interface. HTTPS is enabled by default and HTTP can also be enabled.
When you log in for the first time, the **Accessing Cisco Switch <Model Number> <Hostname>** page appears.
- Step 3** On the **Accessing Cisco Switch** page, click the **Wireless Web GUI** link to access switch web GUI **Home** page.
- Step 4** Choose **Configuration > Wizard** to perform all steps that you need to configure the switch initially.
The **Admin Users** page appears.
- Step 5** On the **Admin Users** page, enter the administrative username to be assigned to this switch in the User Name text box and the administrative password to be assigned to this switch in the Password and Confirm Password text boxes. Click **Next**.
The default username is **admin** and the default password is **cisco**. You can also create a new administrator user for the switch. You can enter up to 24 ASCII characters for username and password.

The **SNMP System Summary** page appears.

Step 6 On the **SNMP System Summary** page, enter the following SNMP system parameters for the switch, and click **Next**:

- Customer-definable switch location in the Location text box.
- Customer-definable contact details such as phone number with names in the Contact text box.
- Choose **enabled** to send SNMP notifications for various SNMP traps or **disabled** not to send SNMP notifications for various SNMP traps from the SNMP Global Trap drop-down list.
- Choose **enabled** to send system log messages or **disabled** not to send system log messages from the SNMP Logging drop-down list.

Note The SNMP trap server, must be reachable through the distribution ports (and not through the gigabitethernet0/0 service or management interface).

The **Management Port** page appears.

Step 7 In the **Management Port** page, enter the following parameters for the management port interface (gigabitethernet 0/0) and click **Next**.

- Interface IP address that you assigned for the service port in the IP Address text box.
- Network mask address of the management port interface in the Netmask text box.
- The IPv4 Dynamic Host Configuration Protocol (DHCP) address for the selected port in the IPv4 DHCP Server text box.

The **Wireless Management** page appears.

Step 8 In the **Wireless Management** page, enter the following wireless interface management details, and click **Next**.

- Choose the interface—VLAN, or Ten Gigabit Ethernet from the Select Interface drop-down list.
- VLAN tag identifier, or 0 for no VLAN tag in the VLAN id text box.
- IP address of wireless management interface where access points are connected in the IP Address text box.
- Network mask address of the wireless management interface in the Netmask text box.
- DHCP IPv4 IP address in the IPv4 DHCP Server text box.

When selecting VLAN as interface, you can specify the ports as –Trunk or Access ports from the selected list displayed in the Switch Port Configuration text box.

The **RF Mobility and Country Code** page appears.

Step 9 In the **RF Mobility and Country Code** page, enter the RF mobility domain name in the RF Mobility text box, choose current country code from the Country Code drop-down list, and click **Next**. From the GUI, you can select only one country code.

Note Before configuring RF grouping parameters and mobility configuration, ensure that you refer to the relevant conceptual content and then proceed with the configuration.

The **Mobility Configuration** page with mobility global configuration settings appears.

Step 10 In the **Mobility Configuration** page, view and enter the following mobility global configuration settings, and click **Next**.

- Choose **Mobility Controller** or **Mobility Agent** from the Mobility Role drop-down list:

- If Mobility Agent is chosen, enter the mobility controller IP address in the Mobility Controller IP Address text box and mobility controller IP address in the Mobility Controller Public IP Address text box.
- If Mobility Controller is chosen, then the mobility controller IP address and mobility controller public IP address are displayed in the respective text boxes.
- Displays mobility protocol port number in the Mobility Protocol Port text box.
- Displays the mobility switch peer group name in the Mobility Switch Peer Group Name text box.
- Displays whether DTLS is enabled in the DTLS Mode text box.
DTLS is a standards-track Internet Engineering Task Force (IETF) protocol based on TLS.
- Displays mobility domain identifier for 802.11 radios in the Mobility Domain ID for 802.11 radios text box.
- The amount of time (in seconds) between each ping request sent to an peer switch in the Mobility Keepalive Interval (1-30)sec text box.
Valid range is from 1 to 30 seconds, and the default value is 10 seconds.
- Number of times a ping request is sent to an peer switch before the peer is considered to be unreachable in the Mobility Keepalive Count (3-20) text box.
The valid range is from 3 to 20, and the default value is 3.
- The DSCP value that you can set for the mobility switch in the Mobility Control Message DSCP Value (0-63) text box.
The valid range is 0 to 63, and the default value is 0.
- Displays the number of mobility switch peer group member configured in the Switch Peer Group Members Configured text box.

The **WLANs** page appears.

Step 11 In the **WLANs** page, enter the following WLAN configuration parameters, and click **Next**.

- WLAN identifier in the WLAN ID text box.
- SSID of the WLAN that the client is associated with in the SSID text box.
- Name of the WLAN used by the client in the Profile Name text box.

The **802.11 Configuration** page appears.

Step 12 In the **802.11 Configuration** page, check either one or both 802.11a/n/ac and 802.11b/g/n check boxes to enable the 802.11 radios, and click **Next**.

The **Set Time** page appears.

Step 13 In the **Set Time** page, you can configure the time and date on the switch based on the following parameters, and click **Next**.

- Displays current timestamp on the switch in the Current Time text box.
- Choose either Manual or NTP from the Mode drop-down list.
On using the NTP server, all access points connected to the switch, synchronizes its time based on the NTP server settings available.

- Choose date on the switch from the Year, Month, and Day drop-down list.
- Choose time from the Hours, Minutes, and Seconds drop-down list.
- Enter the time zone in the Zone text box and select the off setting required when compared to the current time configured on the switch from the Offset drop-down list.

The **Save Wizard** page appears.

Step 14

In the **Save Wizard** page, you can review the configuration settings performed on the switch using these steps, and if you wish to change any configuration value, click **Previous** and navigate to that page. You can save the switch configuration created using the wizard only if a success message is displayed for all the wizards. If the **Save Wizard** page displays errors, you must recreate the wizard for initial configuration of the switch.



Configuring Interface Characteristics

- [Finding Feature Information, page 21](#)
- [Information About Configuring Interface Characteristics, page 21](#)
- [How to Configure Interface Characteristics, page 31](#)
- [Monitoring Interface Characteristics, page 45](#)
- [Configuration Examples for Interface Characteristics, page 46](#)
- [Additional References for the Interface Characteristics Feature, page 49](#)
- [Feature History and Information for Configuring Interface Characteristics, page 50](#)

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release.

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).

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.

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.

Tunnel Ports

Tunnel ports are used in IEEE 802.1Q tunneling to segregate the traffic of customers in a service-provider network from other customers who are using the same VLAN number. You configure an asymmetric link from a tunnel port on a service-provider edge switch to an IEEE 802.1Q trunk port on the customer switch. Packets entering the tunnel port on the edge switch, already IEEE 802.1Q-tagged with the customer VLANs, are encapsulated with another layer of an IEEE 802.1Q tag (called the metro tag), containing a VLAN ID unique in the service-provider network, for each customer. The double-tagged packets go through the service-provider network keeping the original customer VLANs separate from those of other customers. At the outbound interface, also a tunnel port, the metro tag is removed, and the original VLAN numbers from the customer network are retrieved.

Tunnel ports cannot be trunk ports or access ports and must belong to a VLAN unique to each customer.

Routed Ports

A routed port is a physical port that acts like a port on a router; it does not have to be connected to a router. A routed port is not associated with a particular VLAN, as is an access port. A routed port behaves like a regular router interface, except that it does not support VLAN subinterfaces. Routed ports can be configured with a Layer 3 routing protocol. A routed port is a Layer 3 interface only and does not support Layer 2 protocols, such as DTP and STP.

Configure routed ports by putting the interface into Layer 3 mode with the **no switchport** interface configuration command. Then assign an IP address to the port, enable routing, and assign routing protocol characteristics by using the **ip routing** and **router protocol** global configuration commands.



Note

Entering a **no switchport** interface configuration command shuts down the interface and then re-enables it, which might generate messages on the device to which the interface is connected. When you put an interface that is in Layer 2 mode into Layer 3 mode, the previous configuration information related to the affected interface might be lost.

The number of routed ports that you can configure is not limited by software. However, the interrelationship between this number and the number of other features being configured might impact CPU performance because of hardware limitations.



Note The IP base feature set supports static routing and the Routing Information Protocol (RIP). For full Layer 3 routing or for fallback bridging, you must enable the IP services feature set on the standalone switch, or the active switch.

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.

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.

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.



Note 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, group multiple access ports into one logical access port, group multiple tunnel ports into one logical tunnel port, or group multiple routed ports into one logical routed 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 3 interfaces, you manually create the logical interface by using the **interface port-channel** global configuration command. Then you manually assign an interface to the EtherChannel by using the **channel-group** interface configuration command. 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
- an IEEE 802.3at-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.

After the switch detects a powered device, the switch determines the device power requirements and then grants or denies power to the device. The switch can also sense the real-time power consumption of the device by monitoring and policing the power usage.

Using the Switch USB Ports

USB Mini-Type B Console Port

The switch has the following console ports available on its front panel:

- 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:

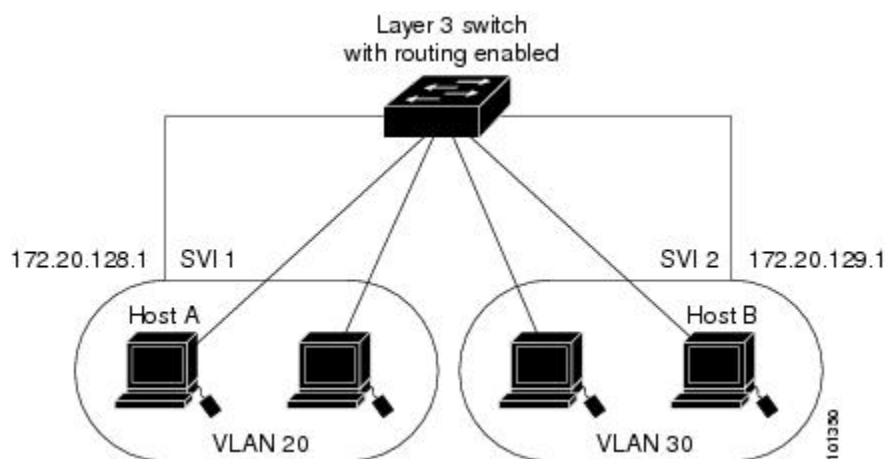
```
switch-stack-1
Mar  1 00:20:48.635: %USB_CONSOLE-6-MEDIA_RJ45: Console media-type is RJ45.
```

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

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. With a standard Layer 2 switch, ports in different VLANs have to exchange information through a router. By using the switch with routing enabled, when you configure both VLAN 20 and VLAN 30 with an SVI to which an IP address is assigned, packets can be sent from Host A to Host B directly through the switch with no need for an external router.

Figure 1: Connecting VLANs with the Switch



Default Ethernet Interface Configuration

To configure Layer 2 parameters, if the interface is in Layer 3 mode, you must enter the **switchport** interface configuration command without any parameters to put the interface into Layer 2 mode. This shuts down the interface and then re-enables it, which might generate messages on the device to which the interface is connected. When you put an interface that is in Layer 3 mode into Layer 2 mode, the previous configuration information related to the affected interface might be lost, and the interface is returned to its default 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 (Layer 2 interfaces only).
Native VLAN (for IEEE 802.1Q trunks)	VLAN 1 (Layer 2 interfaces only).

Feature	Default Setting
VLAN trunking	Switchport mode dynamic auto (supports DTP) (Layer 2 interfaces only).
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) (Layer 2 interfaces only).
Broadcast, multicast, and unicast storm control	Disabled.
Protected port	Disabled (Layer 2 interfaces only).
Port security	Disabled (Layer 2 interfaces only).
Port Fast	Disabled.
Auto-MDIX	Enabled. 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.
Power over Ethernet (PoE)	Enabled (auto).

Interface Speed and Duplex Mode

Ethernet interfaces on the switch operate at 10, 100, 1000, or 10,000 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, 10-Gigabit Ethernet 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:

- The 10-Gigabit Ethernet ports do not support the speed and duplex features. These ports operate only at 10,000 Mb/s and in full-duplex mode.
- 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.

For information about which SFP modules are supported on your switch, see the product release notes.

- 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.

Layer 3 Interfaces

The switch supports these types of Layer 3 interfaces:

- **SVIs**: You should configure SVIs for any VLANs for which you want to route traffic. SVIs are created when you enter a VLAN ID following the **interface vlan** global configuration command. To delete an SVI, use the **no interface vlan** global configuration command. You cannot delete interface VLAN 1.


Note

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

When configuring SVIs, you can also configure SVI autostate exclude on a port in the SVI to exclude that port from being included in determining SVI line-state status.

- **Routed ports**: Routed ports are physical ports configured to be in Layer 3 mode by using the **no switchport** interface configuration command.
- **Layer 3 EtherChannel ports**: EtherChannel interfaces made up of routed ports.

A Layer 3 switch can have an IP address assigned to each routed port and SVI.

There is no defined limit to the number of SVIs and routed ports that can be configured in a switch or in a switch stack. However, the interrelationship between the number of SVIs and routed ports and the number of other features being configured might have an impact on CPU usage because of hardware limitations. If the switch is using its maximum hardware resources, attempts to create a routed port or SVI have these results:

- If you try to create a new routed port, the switch generates a message that there are not enough resources to convert the interface to a routed port, and the interface remains as a switchport.
- If you try to create an extended-range VLAN, an error message is generated, and the extended-range VLAN is rejected.
- If the switch is notified by VLAN Trunking Protocol (VTP) of a new VLAN, it sends a message that there are not enough hardware resources available and shuts down the VLAN. The output of the **show vlan** user EXEC command shows the VLAN in a suspended state.

- If the switch attempts to boot up with a configuration that has more VLANs and routed ports than hardware can support, the VLANs are created, but the routed ports are shut down, and the switch sends a message that this was due to insufficient hardware resources.

All Layer 3 interfaces require an IP address to route traffic. This procedure shows how to configure an interface as a Layer 3 interface and how to assign an IP address to an interface.



Note If the physical port is in Layer 2 mode (the default), you must enter the **no switchport** interface configuration command to put the interface into Layer 3 mode. Entering a **no switchport** command disables and then re-enables the interface, which might generate messages on the device to which the interface is connected. Furthermore, when you put an interface that is in Layer 2 mode into Layer 3 mode, the previous configuration information related to the affected interface might be lost, and the interface is returned to its default configuration

How to Configure Interface Characteristics

Configuring Interfaces Procedure

These general instructions apply to all interface configuration processes.

DETAILED STEPS

	Command or Action	Purpose
Step 1	Enter the configure terminal command at the privileged EXEC prompt: Example: Switch# configure terminal Enter configuration commands, one per line. End with CNTL/Z. Switch(config)#	
Step 2	Enter the interface global configuration command. Identify the interface type, the switch number (only on stacking-capable switches), and the number of the connector. In this example, Gigabit Ethernet port 1 on switch 1 is selected: Example: Switch(config)# interface gigabitethernet1/0/1 Switch(config-if)#	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 3	Follow each interface command with the interface configuration commands that the interface requires. The commands that you enter define the protocols and applications that will run on the	You can also configure a range of interfaces by using the interface range or interface range macro global configuration commands. Interfaces configured in a

	Command or Action	Purpose
	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.	range must be the same type and must be configured with the same feature options.
Step 4	After you configure an interface, verify its status by using the show privileged EXEC commands. Example:	Enter the show interfaces privileged EXEC command to see 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. **configure terminal**
2. **interface** *interface-id*
3. **description** *string*
4. **end**
5. **show interfaces** *interface-id* **description**

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure terminal Example: Switch# configure terminal	Enters global configuration mode.
Step 2	interface <i>interface-id</i> Example: Switch(config)# interface gigabitethernet1/0/2	Specifies the interface for which you are adding a description, and enter interface configuration mode.
Step 3	description <i>string</i> Example: Switch(config-if)# description Connects to Marketing	Adds a description (up to 240 characters) for an interface.

	Command or Action	Purpose
Step 4	end Example: Switch(config-if) # end	Returns to privileged EXEC mode.
Step 5	show interfaces <i>interface-id</i> description	Verifies your entry.

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. **configure terminal**
2. **interface range** {*port-range* | **macro** *macro_name*}
3. **end**
4. **show interfaces** [*interface-id*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure terminal Example: Switch# configure terminal	Enters global configuration mode.
Step 2	interface range { <i>port-range</i> macro <i>macro_name</i> } Example: Switch(config) # interface range macro	Specifies the range of interfaces (VLANs or physical ports) to be configured, and enter interface-range configuration mode. <ul style="list-style-type: none"> • You can use the interface range command to configure up to five port ranges or a previously defined macro. • The macro variable is explained in the Configuring and Using Interface Range Macros, on page 34. • In a comma-separated <i>port-range</i>, you must enter the interface type for each entry and enter spaces before and after the comma. • In a hyphen-separated <i>port-range</i>, you do not need to re-enter the interface type, but you must enter a space before the hyphen.

	Command or Action	Purpose
		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 3	end Example: Switch(config)# end	Returns to privileged EXEC mode.
Step 4	show interfaces [<i>interface-id</i>] Example: Switch# show interfaces	Verifies the configuration of the interfaces in the range.

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. **configure terminal**
2. **define interface-range** *macro_name* *interface-range*
3. **interface range macro** *macro_name*
4. **end**
5. **show running-config | include define**

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure terminal Example: Switch# configure terminal	Enters global configuration mode.
Step 2	define interface-range <i>macro_name</i> <i>interface-range</i>	Defines the interface-range macro, and save it in NVRAM. <ul style="list-style-type: none"> • The <i>macro_name</i> is a 32-character maximum character string.

	Command or Action	Purpose
	<p>Example:</p> <pre>Switch(config)# define interface-range enet_list gigabitethernet1/0/1 - 2</pre>	<ul style="list-style-type: none"> • A macro can contain up to five comma-separated interface ranges. • Each <i>interface-range</i> must consist of the same port type. <p>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.</p>
Step 3	<p>interface range macro <i>macro_name</i></p> <p>Example:</p> <pre>Switch(config)# interface range macro enet_list</pre>	<p>Selects the interface range to be configured using the values saved in the interface-range macro called <i>macro_name</i>.</p> <p>You can now use the normal configuration commands to apply the configuration to all interfaces in the defined macro.</p>
Step 4	<p>end</p> <p>Example:</p> <pre>Switch(config)# end</pre>	<p>Returns to privileged EXEC mode.</p>
Step 5	<p>show running-config include define</p> <p>Example:</p> <pre>Switch# show running-config include define</pre>	<p>Shows the defined interface range macro configuration.</p>

Configuring Ethernet Interfaces

Setting the Interface Speed and Duplex Parameters

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure terminal Example: Switch# configure terminal	Enters global configuration mode.
Step 2	interface <i>interface-id</i> Example: Switch(config)# interface gigabitethernet1/0/3	Specifies the physical interface to be configured, and enter interface configuration mode.
Step 3	speed {10 100 1000 auto [10 100 1000] nonegotiate} Example: Switch(config-if)# speed 10	<p>This command is not available on a 10-Gigabit Ethernet interface.</p> <p>Enter the appropriate speed parameter for the interface:</p> <ul style="list-style-type: none"> • Enter 10, 100, or 1000 to set a specific speed for the interface. The 1000 keyword is available only for 10/100/1000 Mb/s ports. • Enter auto to enable the interface to autonegotiate speed with the connected device. If you use the 10, 100, or the 1000 keywords with the auto keyword, the port autonegotiates only at the specified speeds. • 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 4	duplex {auto full half} Example: Switch(config-if)# duplex half	<p>This command is not available on a 10-Gigabit Ethernet interface.</p> <p>Enter the duplex parameter for the interface.</p> <p>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.</p> <p>You can configure the duplex setting when the speed is set to auto.</p>
Step 5	end Example: Switch(config-if)# end	Returns to privileged EXEC mode.
Step 6	show interfaces <i>interface-id</i> Example: Switch# show interfaces	Displays the interface speed and duplex mode configuration.

	Command or Action	Purpose
	<code>gigabitethernet1/0/3</code>	
Step 7	copy running-config startup-config Example: <pre>Switch# copy running-config startup-config</pre>	(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*

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure terminal Example: <pre>Switch# configure terminal</pre>	Enters global configuration mode
Step 2	interface <i>interface-id</i> Example: <pre>Switch(config)# interface gigabitethernet1/0/1</pre>	Specifies the physical interface to be configured, and enter interface configuration mode.
Step 3	flowcontrol {receive} {on off desired} Example: <pre>Switch(config-if)# flowcontrol receive on</pre>	Configures the flow control mode for the port.

	Command or Action	Purpose
Step 4	end Example: Switch(config-if)# end	Returns to privileged EXEC mode.
Step 5	show interfaces <i>interface-id</i> Example: Switch# show interfaces gigabitethernet1/0/1	Verifies the interface flow control settings.

Configuring Layer 3 Interfaces

SUMMARY STEPS

1. **configure terminal**
2. **interface** {gigabitethernet *interface-id*} | {vlan *vlan-id*} | {port-channel *port-channel-number*}
3. **no switchport**
4. **ip address** *ip_address subnet_mask*
5. **no shutdown**
6. **end**
7. **show interfaces** [*interface-id*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure terminal Example: Switch# configure terminal	Enters global configuration mode.
Step 2	interface {gigabitethernet <i>interface-id</i> } {vlan <i>vlan-id</i> } {port-channel <i>port-channel-number</i> } Example: Switch(config)# interface gigabitethernet1/0/2	Specifies the interface to be configured as a Layer 3 interface, and enter interface configuration mode.

	Command or Action	Purpose
Step 3	no switchport Example: Switch(config-if)# no switchport	For physical ports only, enters Layer 3 mode.
Step 4	ip address ip_address subnet_mask Example: Switch(config-if)# ip address 192.20.135.21 255.255.255.0	Configures the IP address and IP subnet.
Step 5	no shutdown Example: Switch(config-if)# no shutdown	Enables the interface.
Step 6	end Example: Switch(config-if)# end	Returns to privileged EXEC mode.
Step 7	show interfaces [interface-id]	Verifies the configuration.

Configuring Logical Layer 3 GRE Tunnel Interfaces

Before You Begin

Generic Routing Encapsulation (GRE) is a tunneling protocol used to encapsulate network layer protocols inside virtual point-to-point links. A GRE tunnel only provides encapsulation and not encryption.



Attention

Beginning in Cisco IOS XE Release 3.7.2E, GRE tunnels are supported on the hardware on Cisco Catalyst switches. When GRE is configured without tunnel options, packets are hardware-switched. When GRE is configured with tunnel options (such as key, checksum, etc.), packets are switched in the software. A maximum of 10 GRE tunnels are supported.



Note

Other features like Access Control Lists (ACL) and Quality of Service (QoS) are not supported for the GRE tunnels.

To configure a GRE tunnel, perform this task:

SUMMARY STEPS

1. **interface** *tunnel number*
2. **ip address** *ip_address subnet_mask*
3. **tunnel source** {*ip_address* | *type_number*}
4. **tunnel destination** {*host_name* | *ip_address*}
5. **tunnel mode gre ip**
6. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	interface <i>tunnel number</i> Example: Switch(config)# interface tunnel 2	Enables tunneling on the interface.
Step 2	ip address <i>ip_address subnet_mask</i> Example: Switch(config)# ip address 100.1.1.1 255.255.255.0	Configures the IP address and IP subnet.
Step 3	tunnel source { <i>ip_address</i> <i>type_number</i> }	Configures the tunnel source.
	Example: Switch(config)# tunnel source 10.10.10.1	
Step 4	tunnel destination { <i>host_name</i> <i>ip_address</i> }	Configures the tunnel destination.
	Example: Switch(config)# tunnel destination 10.10.10.2	
Step 5	tunnel mode gre ip Example: Switch(config)# tunnel mode gre ip	Configures the tunnel mode.
Step 6	end Example: Switch(config)# end	Exit configuration mode.

Configuring SVI Autostate Exclude

SUMMARY STEPS

1. **configure terminal**
2. **interface *interface-id***
3. **switchport autostate exclude**
4. **end**
5. **show running config interface *interface-id***

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure terminal Example: Switch# configure terminal	Enters global configuration mode.
Step 2	interface <i>interface-id</i> Example: Switch(config)# interface gigabitethernet1/0/2	Specifies a Layer 2 interface (physical port or port channel), and enter interface configuration mode.
Step 3	switchport autostate exclude Example: 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 4	end Example: Switch(config-if)# end	Returns to privileged EXEC mode.
Step 5	show running config interface <i>interface-id</i>	(Optional) Shows the running configuration. Verifies the configuration.

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. **configure terminal**
2. **interface** {vlan *vlan-id*} | {**gigabitethernet** *interface-id*} | {**port-channel** *port-channel-number*}
3. **shutdown**
4. **no shutdown**
5. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure terminal Example: Switch# configure terminal	Enters global configuration mode.
Step 2	interface {vlan <i>vlan-id</i> } { gigabitethernet <i>interface-id</i> } { port-channel <i>port-channel-number</i> } Example: Switch(config)# interface gigabitethernet1/0/2	Selects the interface to be configured.
Step 3	shutdown Example: Switch(config-if)# shutdown	Shuts down an interface.
Step 4	no shutdown Example: Switch(config-if)# no shutdown	Restarts an interface.
Step 5	end Example: Switch(config-if)# end	Returns to privileged EXEC mode.

Configuring the Console Media Type

Beginning in privileged EXEC mode, 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. **configure terminal**
2. **line console 0**
3. **media-type rj45**
4. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure terminal Example: Switch# configure terminal	Enters the global configuration mode.
Step 2	line console 0 Example: Switch(config)# line console 0	Configures the console and enters line configuration mode.
Step 3	media-type rj45 Example: 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 4	end Example: Switch(config)# end	Returns to privileged EXEC mode.

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.

Beginning in privileged EXEC mode, follow these steps to configure an inactivity timeout.

SUMMARY STEPS

1. **configure terminal**
2. **line console 0**
3. **usb-inactivity-timeout** *timeout-minutes*

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure terminal Example: Switch# configure terminal	Enters the global configuration mode.
Step 2	line console 0 Example: Switch(config)# line console 0	Configures the console and enters line configuration mode.
Step 3	usb-inactivity-timeout <i>timeout-minutes</i> Example: 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.

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.

This table lists some of the available interface monitoring commands.

Table 5: Show Commands for Interfaces

Command	Purpose
show interfaces [<i>interface-id</i>]	Displays the status and configuration of all interfaces or a specific interface.
show interfaces <i>interface-id</i> status [err-disabled]	Displays interface status or a list of interfaces in the error-disabled state.
show interfaces [<i>interface-id</i>] 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 [<i>interface-id</i>] description	Displays the description configured on an interface or all interfaces and the interface status.
show ip interface [<i>interface-id</i>]	Displays the usability status of all interfaces configured for IP routing or the specified interface.
show interface [<i>interface-id</i>] stats	Displays the input and output packets by the switching path for the interface.
show interfaces <i>interface-id</i>	(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 [<i>interface-id</i>] [{transceiver properties detail}] <i>module number</i>	Displays physical and operational status about an SFP module.
show running-config interface [<i>interface-id</i>]	Displays the running configuration in RAM for the interface.

Command	Purpose
<code>show version</code>	Displays the hardware configuration, software version, the names and sources of configuration files, and the boot images.
<code>show controllers ethernet-controller <i>interface-id</i> phy</code>	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
<code>clear counters [<i>interface-id</i>]</code>	Clears interface counters.
<code>clear interface <i>interface-id</i></code>	Resets the hardware logic on an interface.
<code>clear line [<i>number</i> console 0 vty <i>number</i>]</code>	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 Layer 3 Interfaces: Example

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface gigabitethernet1/0/2
Switch(config-if)# no switchport
Switch(config-if)# ip address 192.20.135.21 255.255.255.0
Switch(config-if)# no shutdown
```

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

Technical Assistance

Description	Link
<p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>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.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p>	<p>http://www.cisco.com/support</p>

Feature History and Information for Configuring Interface Characteristics

Release	Modification
Cisco IOS XE 3.3SE	This feature was introduced.



Configuring Auto-MDIX

- [Prerequisites for Auto-MDIX, page 51](#)
- [Restrictions for Auto-MDIX, page 51](#)
- [Information about Configuring Auto-MDIX, page 52](#)
- [How to Configure Auto-MDIX, page 52](#)
- [Monitoring Auto-MDIX, page 54](#)
- [Example for Configuring Auto-MDIX, page 54](#)
- [Additional References, page 54](#)
- [Feature History and Information for Auto-MDIX, page 55](#)

Prerequisites for Auto-MDIX

To configure Layer 2 parameters, if the interface is in Layer 3 mode, you must enter the **switchport** interface configuration command without any parameters to put the interface into Layer 2 mode. This shuts down the interface and then re-enables it, which might generate messages on the device to which the interface is connected. When you put an interface that is in Layer 3 mode into Layer 2 mode, the previous configuration information related to the affected interface might be lost, and the interface is returned to its default configuration.

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

Monitoring Auto-MDIX

Command	Purpose
<code>show controllers ethernet-controller <i>interface-id</i> phy</code>	Verifies the operational state of the auto-MDIX feature on the interface.

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

Technical Assistance

Description	Link
<p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>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.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p>	http://www.cisco.com/support

Feature History and Information for Auto-MDIX

Release	Modification
Cisco IOS XE 3.3SE	This feature was introduced.



Configuring Ethernet Management Port

- [Finding Feature Information, page 57](#)
- [Prerequisites for Ethernet Management Ports, page 57](#)
- [Information about the Ethernet Management Port, page 57](#)
- [How to Configure the Ethernet Management Port, page 60](#)
- [Additional References, page 61](#)
- [Feature Information for Ethernet Management Ports, page 62](#)

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release.

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.

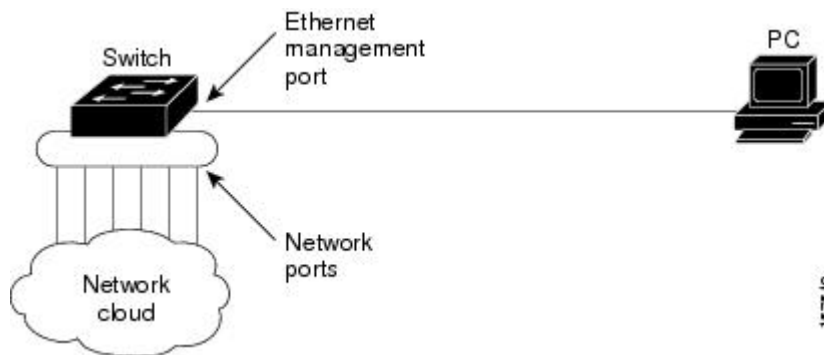
Information about the Ethernet Management Port

The Ethernet management port, also referred to as the *Gi0/0* or *GigabitEthernet0/0* port, is a VRF (VPN routing/forwarding) interface 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 active switch through the hub, to the PC. If the active switch 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.

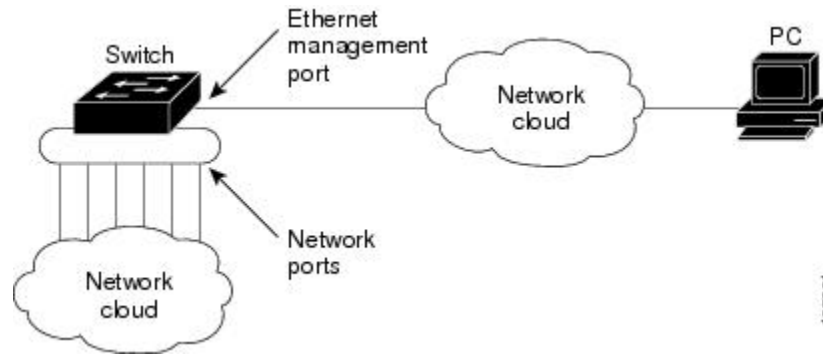
Figure 3: Connecting a Switch Stack to a PC

Ethernet Management Port and Routing

By default, the Ethernet management port is enabled. The switch cannot route packets from the Ethernet management port to a network port, and the reverse. Even though the Ethernet management port does not support routing, you may need to enable routing protocols on the port.

In the following figure, you must enable routing protocols on the Ethernet management port when the PC is multiple hops away from the switch and the packets must pass through multiple Layer 3 devices to reach the PC.

Figure 4: Network Example with Routing Protocols Enabled



In the above figure, if the Ethernet management port and the network ports are associated with the same routing process, the routes are propagated as follows:

- The routes from the Ethernet management port are propagated through the network ports to the network.
- The routes from the network ports are propagated through the Ethernet management port to the network.

Because routing is not supported between the Ethernet management port and the network ports, traffic between these ports cannot be sent or received. If this happens, data packet loops occur between the ports, which disrupt the switch and network operation. To prevent the loops, configure route filters to avoid routes between the Ethernet management port and the network ports.

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 and IPv6 access control lists (ACLs)
- Routing protocols

**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

To disable or enable the Ethernet management port in the CLI, follow this procedure.

SUMMARY STEPS

1. **configure terminal**
2. **interface gigabitethernet0/0**
3. **shutdown**
4. **no shutdown**
5. **exit**
6. **show interfaces gigabitethernet0/0**

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure terminal Example: Switch# configure terminal	Enters global configuration mode.
Step 2	interface gigabitethernet0/0 Example: Switch(config)# interface gigabitethernet0/0	Specifies the Ethernet management port in the CLI.
Step 3	shutdown Example: Switch(config-if)# shutdown	Disables the Ethernet management port.

	Command or Action	Purpose
Step 4	no shutdown Example: Switch(config-if)# no shutdown	Enables the Ethernet management port.
Step 5	exit Example: Switch(config-if)# exit	Exits interface configuration mode.
Step 6	show interfaces gigabitethernet0/0 Example: Switch# show interfaces gigabitethernet0/0	Displays the link status. 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 *Network Management Configuration Guide (Catalyst 3650 Switches)*.

Additional References

Related Documents

Related Topic	Document Title
Bootloader configuration	<i>System Management Configuration Guide (Catalyst 3650 Switches)</i>
Bootloader commands	<i>System Management Command Reference (Catalyst 3650 Switches)</i>

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

Technical Assistance

Description	Link
<p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>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.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p>	http://www.cisco.com/support

Feature Information for Ethernet Management Ports

Release	Modification
Cisco IOS XE 3.3SE	This feature was introduced.



CHAPTER 6

Configuring LLDP, LLDP-MED, and Wired Location Service

- [Finding Feature Information, page 63](#)
- [LLDP, LLDP-MED, and Wired Location Service Overview, page 63](#)
- [How to Configure LLDP, LLDP-MED, and Wired Location Service, page 68](#)
- [Configuration Examples for LLDP, LLDP-MED, and Wired Location Service, page 79](#)
- [Monitoring and Maintaining LLDP, LLDP-MED, and Wired Location Service, page 80](#)
- [Additional References for LLDP, LLDP-MED, and Wired Location Service, page 81](#)
- [Feature Information for LLDP, LLDP-MED, and Wired Location Service, page 82](#)

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release.

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, and switches). 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.

- Geographic location information

Provides the geographical details of a switch location such as latitude, longitude, and altitude of a switch.

- custom location

Provides customized name and value of a switch location.

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.

Configuration Guidelines

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

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

Enabling LLDP

Beginning in privileged EXEC mode, follow these steps to enable LLDP:

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure terminal Example: Switch# configure terminal	Enters global configuration mode.
Step 2	lldp run Example: Switch (config)# lldp run	Enables LLDP globally on the switch.
Step 3	interface <i>interface-id</i> Example: 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 transmit Example: Switch(config-if)# lldp transmit	Enables the interface to send LLDP packets.
Step 5	lldp receive Example: Switch(config-if)# lldp receive	Enables the interface to receive LLDP packets.
Step 6	end Example: Switch(config-if)# end	Returns to privileged EXEC mode.
Step 7	show lldp Example: Switch# show lldp	Verifies the configuration.
Step 8	copy running-config startup-config Example: 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.

Beginning in privileged EXEC mode, follow these steps to configure the LLDP characteristics.



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

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure terminal Example: Switch# configure terminal	Enters global configuration mode.
Step 2	lldp holdtime <i>seconds</i> Example: Switch(config)# lldp holdtime 120	(Optional) Specifies the amount of time a receiving device should hold the information from your device before discarding it. The range is 0 to 65535 seconds; the default is 120 seconds.
Step 3	lldp reinit <i>delay</i> Example: Switch(config)# lldp reinit 2	(Optional) Specifies the delay time in seconds for LLDP to initialize on an interface. The range is 2 to 5 seconds; the default is 2 seconds.
Step 4	lldp timer <i>rate</i> Example: Switch(config)# lldp timer 30	(Optional) Sets the sending frequency of LLDP updates in seconds. The range is 5 to 65534 seconds; the default is 30 seconds.
Step 5	lldp tlv-select Example: Switch(config)# tlv-select	(Optional) Specifies the LLDP TLVs to send or receive.

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

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

Beginning in privileged EXEC mode, follow these steps to enable a TLV on an interface:

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure terminal Example: Switch# configure terminal	Enters global configuration mode.
Step 2	interface <i>interface-id</i> Example: Switch(config)# interface gigabitethernet2/0/1	Specifies the interface on which you are configuring an LLDP-MED TLV, and enter interface configuration mode.
Step 3	lldp med-tlv-select Example: Switch(config-if)# lldp med-tlv-select inventory management	Specifies the TLV to enable.
Step 4	end Example: Switch(config-if)# end	Returns to privileged EXEC mode.

	Command or Action	Purpose
Step 5	copy running-config startup-config Example: Switch# copy running-config startup-config	(Optional) Saves your entries in the configuration file.

Configuring Network-Policy TLV

Beginning in privileged EXEC mode, follow these steps to create a network-policy profile, configure the policy attributes, and apply it to an interface.

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure terminal Example: Switch# configure terminal	Enters global configuration mode.
Step 2	network-policy profile <i>profile number</i> Example: Switch(config)# network-policy profile 1	Specifies the network-policy profile number, and enter network-policy configuration mode. The range is 1 to 4294967295.

	Command or Action	Purpose
Step 3	<p>{voice voice-signaling} vlan [<i>vlan-id</i> {cos <i>cvalue</i> dscp <i>dvalue</i>}] [[dot1p {cos <i>cvalue</i> dscp <i>dvalue</i>}] none untagged]</p> <p>Example:</p> <pre>Switch(config-network-policy)# voice vlan 100 cos 4</pre>	<p>Configures the policy attributes:</p> <ul style="list-style-type: none"> • voice—Specifies the voice application type. • voice-signaling—Specifies the voice-signaling application type. • vlan—Specifies the native VLAN for voice traffic. • <i>vlan-id</i>—(Optional) Specifies the VLAN for voice traffic. The range is 1 to 4094. • cos <i>cvalue</i>—(Optional) Specifies the Layer 2 priority class of service (CoS) for the configured VLAN. The range is 0 to 7; the default is 5. • dscp <i>dvalue</i>—(Optional) Specifies the differentiated services code point (DSCP) value for the configured VLAN. The range is 0 to 63; the default is 46. • dot1p—(Optional) Configures the telephone to use IEEE 802.1p priority tagging and use VLAN 0 (the native VLAN). • none—(Optional) Do not instruct the IP telephone about the voice VLAN. The telephone uses the configuration from the telephone key pad. • untagged—(Optional) Configures the telephone to send untagged voice traffic. This is the default for the telephone. • untagged—(Optional) Configures the telephone to send untagged voice traffic. This is the default for the telephone.
Step 4	<p>exit</p> <p>Example:</p> <pre>Switch(config)# exit</pre>	<p>Returns to global configuration mode.</p>
Step 5	<p>interface <i>interface-id</i></p> <p>Example:</p> <pre>Switch (config)# interface gigabitethernet2/0/1</pre>	<p>Specifies the interface on which you are configuring a network-policy profile, and enter interface configuration mode.</p>
Step 6	<p>network-policy <i>profile number</i></p> <p>Example:</p> <pre>Switch(config-if)# network-policy 1</pre>	<p>Specifies the network-policy profile number.</p>

	Command or Action	Purpose
Step 7	lldp med-tlv-select network-policy Example: <pre>Switch(config-if)# lldp med-tlv-select network-policy</pre>	Specifies the network-policy TLV.
Step 8	end Example: <pre>Switch(config)# end</pre>	Returns to privileged EXEC mode.
Step 9	show network-policy profile Example: <pre>Switch# show network-policy profile</pre>	Verifies the configuration.
Step 10	copy running-config startup-config Example: <pre>Switch# copy running-config startup-config</pre>	(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	<p>configure terminal</p> <p>Example:</p> <pre>Switch# configure terminal</pre>	Enters global configuration mode.
Step 2	<p>location {admin-tag <i>string</i> civic-location identifier {<i>id</i> host} elin-location <i>string identifier id</i> custom-location identifier {<i>id</i> host} geo-location identifier {<i>id</i> host}}</p> <p>Example:</p> <pre>Switch(config)# location civic-location identifier 1 Switch(config-civic)# number 3550 Switch(config-civic)# primary-road-name "Cisco Way" Switch(config-civic)# city "San Jose" Switch(config-civic)# state CA Switch(config-civic)# building 19 Switch(config-civic)# room C6 Switch(config-civic)# county "Santa Clara" Switch(config-civic)# country US</pre>	<p>Specifies the location information for an endpoint.</p> <ul style="list-style-type: none"> • admin-tag—Specifies an administrative tag or site information. • civic-location—Specifies civic location information. • elin-location—Specifies emergency location information (ELIN). • custom-location—Specifies custom location information. • geo-location—Specifies geo-spatial location information. • identifier <i>id</i>—Specifies the ID for the civic, ELIN, custom, or geo location. • host—Specifies the host civic, custom, or geo location. • string—Specifies the site or location information in alphanumeric format.

	Command or Action	Purpose
Step 3	exit Example: Switch(config-civic)# exit	Returns to global configuration mode.
Step 4	interface <i>interface-id</i> Example: 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 <i>word</i> civic-location-id { <i>id</i> <i>host</i> } elin-location-id <i>id</i> custom-location-id { <i>id</i> <i>host</i> } geo-location-id { <i>id</i> <i>host</i> } } Example: Switch(config-if)# location elin-location-id 1	Enters location information for an interface: <ul style="list-style-type: none"> • additional-location-information—Specifies additional information for a location or place. • civic-location-id—Specifies global civic location information for an interface. • elin-location-id—Specifies emergency location information for an interface. • custom-location-id—Specifies custom location information for an interface. • geo-location-id—Specifies geo-spatial location information for an interface. • host—Specifies the host location identifier. • <i>word</i>—Specifies a word or phrase with additional location information. • <i>id</i>—Specifies the ID for the civic, ELIN, custom, or geo location. The ID range is 1 to 4095.
Step 6	end Example: Switch(config-if)# end	Returns to privileged EXEC mode.
Step 7	Use one of the following: <ul style="list-style-type: none"> • show location admin-tag <i>string</i> • show location civic-location identifier <i>id</i> • show location elin-location identifier <i>id</i> 	Verifies the configuration.

	Command or Action	Purpose
	<p>Example:</p> <pre>Switch# show location admin-tag</pre> <p>OR</p> <pre>Switch# show location civic-location identifier</pre> <p>OR</p> <pre>Switch# show location elin-location identifier</pre>	
Step 8	<p>copy running-config startup-config</p> <p>Example:</p> <pre>Switch# copy running-config startup-config</pre>	(Optional) Saves your entries in the configuration file.

Enabling Wired Location Service on the Switch

Beginning in privileged EXEC mode, follow these steps to enable wired location service on the switch.

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	<p>configure terminal</p> <p>Example:</p> <pre>Switch# configure terminal</pre>	Enters global configuration mode.

	Command or Action	Purpose
Step 2	nmosp notification interval {attachment location} <i>interval-seconds</i> Example: <pre>Switch(config)# nmosp notification interval location 10</pre>	Specifies the NMSP notification interval. attachment —Specifies the attachment notification interval. location —Specifies the location notification interval. <i>interval-seconds</i> —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 3	end Example: <pre>Switch(config)# end</pre>	Returns to privileged EXEC mode.
Step 4	show network-policy profile Example: <pre>Switch# show network-policy profile</pre>	Verifies the configuration.
Step 5	copy running-config startup-config Example: <pre>Switch# copy running-config startup-config</pre>	(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
<code>clear lldp counters</code>	Resets the traffic counters to zero.
<code>clear lldp table</code>	Deletes the LLDP neighbor information table.
<code>clear nmosp statistics</code>	Clears the NMSP statistic counters.
<code>show lldp</code>	Displays global information, such as frequency of transmissions, the holdtime for packets being sent, and the delay time before LLDP initializes on an interface.
<code>show lldp entry <i>entry-name</i></code>	Displays information about a specific neighbor. You can enter an asterisk (*) to display all neighbors, or you can enter the neighbor name.
<code>show lldp interface [<i>interface-id</i>]</code>	Displays information about interfaces with LLDP enabled. You can limit the display to a specific interface.
<code>show lldp neighbors [<i>interface-id</i>] [<i>detail</i>]</code>	Displays information about neighbors, including device type, interface type and number, holdtime settings, capabilities, and port ID. You can limit the display to neighbors of a specific interface or expand the display for more detailed information.
<code>show lldp traffic</code>	Displays LLDP counters, including the number of packets sent and received, number of packets discarded, and number of unrecognized TLVs.
<code>show location admin-tag <i>string</i></code>	Displays the location information for the specified administrative tag or site.
<code>show location civic-location identifier <i>id</i></code>	Displays the location information for a specific global civic location.

Command	Description
<code>show location elin-location identifier <i>id</i></code>	Displays the location information for an emergency location
<code>show network-policy profile</code>	Displays the configured network-policy profiles.
<code>show nmosp</code>	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: http://www.cisco.com/go/mibs

Technical Assistance

Description	Link
<p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>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.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p>	<p>http://www.cisco.com/support</p>

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

Release	Modification
Cisco IOS XE 3.3SE	This feature was introduced.



Configuring System MTU

- [Finding Feature Information, page 83](#)
- [Information about the MTU, page 83](#)
- [How to Configure MTU Sizes, page 84](#)
- [Configuration Examples for System MTU, page 86](#)
- [Additional References for System MTU, page 87](#)
- [Feature Information for System MTU, page 88](#)

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release.

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 sent on all switch interfaces is 1500 bytes.

System MTU Values

The following MTU values can be configured:

- **System MTU**--This value applies to switched packets on the Gigabit Ethernet and 10-Gigabit Ethernet ports of the switch. Use the **system mtu bytes** global configuration command to specify the system jumbo MTU value.

- System Jumbo MTU--This value applies to switched packets on the Gigabit Ethernet and 10-Gigabit Ethernet ports of the switch. Use the **system mtu jumbo bytes** global configuration command to specify the system jumbo MTU value.
- Protocol-specific MTU--This value applies only to routed packets on all routed ports of the switch or switch stack. Use the **ip mtu bytes** or **ipv6 mtu bytes** interface configuration command to specify the protocol-specific MTU value.

Restrictions for System MTU

When configuring the system MTU values, follow these guidelines:

- The switch does not support the MTU on a per-interface basis.
- If you enter the **system mtu bytes** global configuration command, the command does not take effect on the switch. This command only affects the system MTU size on Fast Ethernet switch ports.

System MTU Value Application

The upper limit of the IP or IPv6 MTU value is based on the switch or switch stack configuration and refers to the currently applied system MTU or the system jumbo MTU value. For more information about setting the MTU sizes, see the **system mtu** global configuration command in the command reference for this release.

How to Configure MTU Sizes

Configuring the System MTU

Follow these steps to change the MTU size for switched packets:

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Switch> enable	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	configure terminal Example: Switch# configure terminal	Enters global configuration mode.
Step 3	system mtu bytes Example: Switch(config)# system mtu 1900	(Optional) Changes the MTU size for all Gigabit Ethernet and 10-Gigabit Ethernet interfaces.
Step 4	end Example: Switch(config)# end	Returns to privileged EXEC mode.
Step 5	copy running-config startup-config Example: Switch# copy running-config startup-config	Saves your entries in the configuration file.
Step 6	show system mtu Example: Switch# show system mtu	Verifies your settings.

Configuring Protocol-Specific MTU

Beginning in privileged EXEC mode, follow these steps to change the MTU size for routed ports:

SUMMARY STEPS

1. **configure terminal**
2. **interface interface**
3. **ip mtu bytes**
4. **ipv6 mtu bytes**
5. **end**
6. **copy running-config startup-config**
7. **show system mtu**

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure terminal Example: Switch# configure terminal	Enters global configuration mode.
Step 2	interface interface Example: Switch(config)# interface gigabitethernet0/0	Enters interface configuration mode.
Step 3	ip mtu bytes Example: Switch(config-if)# ip mtu 68	Changes the IPv4 MTU size
Step 4	ipv6 mtu bytes Example: Switch(config-if)# ipv6 mtu 1280	(Optional) Changes the IPv6 MTU size.
Step 5	end Example: Switch(config-if)# end	Returns to privileged EXEC mode.
Step 6	copy running-config startup-config Example: Switch# copy running-config startup-config	Saves your entries in the configuration file.
Step 7	show system mtu Example: 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 7500
Switch(config)#
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 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: http://www.cisco.com/go/mibs

Technical Assistance

Description	Link
<p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>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.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p>	http://www.cisco.com/support

Feature Information for System MTU

Release	Modification
Cisco IOS XE 3.3SE	This feature was introduced.



CHAPTER 8

Configuring Internal Power Supplies

- [Information About Internal Power Supplies](#) , page 89
- [How to Configure Internal Power Supplies](#), page 89
- [Monitoring Internal Power Supplies](#), page 90
- [Configuration Examples for Internal Power Supplies](#), page 90
- [Additional References](#), page 91
- [Feature History and Information for Internal Power Supplies](#), page 92

Information About Internal Power Supplies

See the switch installation guide for information about the power supplies.

How to Configure Internal Power Supplies

Configuring an Internal Power Supply

You can use the **power supply** EXEC command to configure and manage the internal power supply on the switch. The switch does not support the **no power supply** EXEC command.

SUMMARY STEPS

1. **power supply** *switch_number* slot{A | B} { off | on }
2. **show environment power**

DETAILED STEPS

	Command or Action	Purpose
Step 1	<p>power supply <i>switch_number</i> slot{A B} { off on }</p> <p>Example:</p> <pre>Switch# power supply 1 slot A on</pre>	<p>Sets the specified power supply to off or on by using one of these keywords:</p> <ul style="list-style-type: none"> • A —Selects the power supply in slot A. • B —Selects power supply in slot B. <p>Note Power supply slot B is the closest to the outer edge of the switch.</p> <ul style="list-style-type: none"> • off —Set the power supply off. • on —Set the power supply on. <p>By default, the switch power supply is on.</p>
Step 2	<p>show environment power</p> <p>Example:</p> <pre>Switch# show environment power</pre>	<p>Verifies your settings.</p>

Monitoring Internal Power Supplies

Table 10: Show Commands for Power Supplies

Command	Purpose
<p>show environment power [all switch <i>switch_number</i>]</p>	<p>(Optional) Displays the status of the internal power supplies for each switch in the stack or for the specified switch. The range is 1 to 9, depending on the switch member numbers in the stack.</p>

Configuration Examples for Internal Power Supplies

This example shows how to set the power supply in slot A to off:

```
Switch# power supply 1 slot A off
Disabling Power supply A may result in a power loss to PoE devices and/or switches ...
Continue? (yes/[no]): yes
Switch#
Jun 10 04:52:54.389: %PLATFORM_ENV-6-FRU_PS_OIR: FRU Power Supply 1 powered off
Jun 10 04:52:56.717: %PLATFORM_ENV-1-FAN_NOT_PRESENT: Fan is not present
```

```
Switch#
```

This example shows how to set the power supply in slot A to on:

```
Switch# power supply 1 slot A on
Jun 10 04:54:39.600: %PLATFORM_ENV-6-FRU_PS_OIR: FRU Power Supply 1 powered on
```

This example shows the output of the **show env power** command:

```
Switch# show env power

SW  PID                Serial#      Status          Sys Pwr  PoE Pwr  Watts
---  -
1A  PWR-C2-640WAC        DCB1705B05B OK           Good     Good     640
1B  Not Present
```

Switch#

Table 11: show env power Status Descriptions

Field	Description
OK	The power supply is present and power is good.
Not Present	No power supply is installed.
No Input Power	The power supply is present but there is no input power.
Disabled	The power supply and input power are present, but power supply is switched off by CLI.
Not Responding	The power supply is not recognizable or is faulty.
Failure-Fan	The power supply fan is faulty.

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

Technical Assistance

Description	Link
<p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>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.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p>	http://www.cisco.com/support

Feature History and Information for Internal Power Supplies

Release	Modification
Cisco IOS XE 3.3SE	This feature was introduced.



Configuring PoE

- [Finding Feature Information, page 93](#)
- [Information about PoE, page 93](#)
- [How to Configure PoE, page 98](#)
- [Monitoring Power Status, page 102](#)
- [Additional References, page 102](#)
- [Feature Information for PoE, page 103](#)

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release.

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 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
- an IEEE 802.3at-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.

After the switch detects a powered device, the switch determines the device power requirements and then grants or denies power to the device. The switch can also sense the real-time power consumption of the device by monitoring and policing the power usage.

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.
- IEEE 802.3at—The PoE+ standard increases the maximum power that can be drawn by a powered device from 15.4 W per port to 30 W per port.

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:

- A Cisco prestandard powered device does not provide its power requirement when the switch detects it, so the switch allocates 15.4 W as the initial allocation for power budgeting.

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 12: IEEE Power Classifications](#), on page 95 lists these levels.

Table 12: 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). The switch 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.

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.

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.

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 a standalone switch supports internal power supplies, the total amount of power available for the powered devices varies depending on the power supply configuration.

- If a power supply is removed and replaced by a new power supply with less power and the switch does not have enough power for the powered devices, the switch denies power to the PoE ports in auto mode in descending order of the port numbers. If the switch still does not have enough power, the switch then denies power to the PoE ports in static mode in descending order of the port numbers.
- If the new power supply supports more power than the previous one and the switch now has more power available, the switch grants power to the PoE ports in static mode in ascending order of the port numbers. If it still has power available, the switch then grants power to the PoE ports in auto mode in ascending order of the port numbers.

How to Configure PoE

Configuring a Power Management Mode on a PoE Port

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure terminal Example: Switch# configure terminal	Enters global configuration mode.

	Command or Action	Purpose
Step 2	interface <i>interface-id</i> Example: Switch(config)# interface gigabitethernet2/0/1	Specifies the physical port to be configured, and enters interface configuration mode.
Step 3	power inline { auto [max <i>max-wattage</i>] never static [max <i>max-wattage</i>]} Example: Switch(config-if)# power inline auto	Configures the PoE mode on the port. The keywords have these meanings: <ul style="list-style-type: none"> • 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. • max <i>max-wattage</i>—Limits the power allowed on the port. The range for PoE+ ports is 4000 to 30000 mW. If no value is specified, the maximum is allowed. • never —Disables device detection, and disable power to the port. <p>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.</p> <ul style="list-style-type: none"> • 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. <p>The switch allocates power to a port configured in static mode before it allocates power to a port configured in auto mode.</p>
Step 4	end Example: Switch(config-if)# end	Returns to privileged EXEC mode.
Step 5	show power inline [<i>interface-id</i> module <i>switch-number</i>] Example: Switch# show power inline	Displays PoE status for a switch or a switch stack, for the specified interface, or for a specified stack member. The module <i>switch-number</i> keywords are supported only on stacking-capable switches.

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure terminal Example: Switch# configure terminal	Enters global configuration mode.
Step 2	interface <i>interface-id</i> Example: Switch(config)# interface gigabitethernet2/0/1	Specifies the physical port to be configured, and enter interface configuration mode.
Step 3	power inline police [action {log errdisable}] Example: Switch(config-if)# power inline police	<p>If the real-time power consumption exceeds the maximum power allocation on the port, configures the switch to take one of these actions:</p> <ul style="list-style-type: none"> • power inline police—Shuts down the PoE port, turns off power to it, and puts it in the error-disabled state. <p>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 <i>interval</i> global configuration command.</p> <ul style="list-style-type: none"> • 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.

	Command or Action	Purpose
		<ul style="list-style-type: none"> • power inline police action log—Generates a syslog message while still providing power to the port. <p>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.</p>
Step 4	exit Example: Switch(config-if)# exit	Returns to global configuration mode.
Step 5	Use one of the following: <ul style="list-style-type: none"> • errdisable detect cause inline-power • errdisable recovery cause inline-power • errdisable recovery interval <i>interval</i> Example: Switch(config)# errdisable detect cause inline-power Switch(config)# errdisable recovery cause inline-power Switch(config)# errdisable recovery interval 100	(Optional) Enables error recovery from the PoE error-disabled state, and configures the PoE recover mechanism variables. By default, the recovery interval is 300 seconds. For interval <i>interval</i> , specifies the time in seconds to recover from the error-disabled state. The range is 30 to 86400.
Step 6	exit Example: Switch(config)# exit	Returns to privileged EXEC mode.
Step 7	Use one of the following: <ul style="list-style-type: none"> • show power inline police • show errdisable recovery Example: Switch# show power inline police Switch# show errdisable recovery	Displays the power monitoring status, and verify the error recovery settings.

Monitoring Power Status

Table 13: Show Commands for Power Status

Command	Purpose
show env power switch [<i>switch-number</i>]	(Optional) Displays the status of the internal power supplies for each switch in the stack or for the specified switch. The range is 1 to 9, depending on the switch member numbers in the stack. These keywords are available only on stacking-capable switches.
show power inline [<i>interface-id</i> module <i>switch-number</i>]	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.

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

Technical Assistance

Description	Link
<p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>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.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p>	http://www.cisco.com/support

Feature Information for PoE

Release	Modification
Cisco IOS XE 3.3SE	This feature was introduced.



Configuring EEE

- [Finding Feature Information, page 105](#)
- [Information About EEE, page 105](#)
- [Restrictions for EEE, page 106](#)
- [How to Configure EEE, page 106](#)
- [Monitoring EEE, page 107](#)
- [Configuration Examples for Configuring EEE, page 108](#)
- [Additional References, page 108](#)
- [Feature History and Information for Configuring EEE, page 109](#)

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release.

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 disabled 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 Example: Switch# configure terminal	Enters global configuration mode.

	Command or Action	Purpose
Step 2	interface <i>interface-id</i> Example: Switch(config)# interface gigabitethernet1/0/1	Specifies the interface to be configured, and enter interface configuration mode.
Step 3	power efficient-ethernet auto Example: 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 Example: Switch(config-if)# no power efficient-ethernet auto	Disables EEE on the specified interface.
Step 5	end Example: Switch(config-if)# end	Returns to privileged EXEC mode.
Step 6	copy running-config startup-config Example: Switch# copy running-config startup-config	(Optional) Saves your entries in the configuration file.

Monitoring EEE

Table 14: Commands for Displaying EEE Settings

Command	Purpose
show eee capabilities interface <i>interface-id</i>	Displays EEE capabilities for the specified interface.
show eee status interface <i>interface-id</i>	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: http://www.cisco.com/go/mibs

Technical Assistance

Description	Link
<p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>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.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p>	http://www.cisco.com/support

Feature History and Information for Configuring EEE

Release	Modification
Cisco IOS XE 3.3SE	This feature was introduced.



INDEX

- A**
 - active link [57](#)
 - and routing [57](#)
 - and routing protocols [57](#)
 - auto mode [96](#)
 - auto-MDIX [52](#)
 - configuring [52](#)
 - described [52](#)
 - auto-MDIX, configuring [52](#)

- C**
 - CDP [63, 94](#)
 - defined with LLDP [63](#)
 - power negotiation extensions [94](#)
 - CDP with power consumption, described [94](#)
 - CDP with power negotiation, described [94](#)
 - Cisco intelligent power management [94](#)
 - civic location [65](#)
 - configuring [52, 89](#)
 - custom location [66](#)

- D**
 - default configuration [67](#)
 - LLDP [67](#)
 - default setting [57](#)
 - described [52, 57](#)
 - devices supported [25, 93](#)

- E**
 - ELIN location [65](#)
 - enhanced PoE [94](#)
 - Ethernet management port [57, 58, 59](#)
 - active link [57](#)
 - and routing [57](#)
 - Ethernet management port (*continued*)
 - and routing protocols [57](#)
 - default setting [57](#)
 - described [57](#)
 - for network management [57](#)
 - supported features [59](#)
 - unsupported features [59](#)
 - Ethernet management port configuration [60](#)
 - Ethernet management port, internal [57, 59](#)
 - and routing [57](#)
 - and routing protocols [57](#)
 - unsupported features [59](#)
 - Example for Configuring Auto-MDIX command [54](#)
 - Example for Configuring Layer 3 Interfaces command [48](#)
 - Examples for Configuring the System MTU command [86](#)

- F**
 - Fa0 port [57](#)
 - See Ethernet management port [57](#)
 - fastethernet0 port [57](#)
 - See Ethernet management port [57](#)
 - for network management [57](#)

- G**
 - geo location [66](#)

- H**
 - high-power devices operating in low-power mode [94](#)
 - hub [58](#)

- I**
 - IEEE power classification levels [94](#)
 - interface [90, 102](#)

interfaces [52](#)
 auto-MDIX, configuring [52](#)
 internal power supplies [89](#)
 See power supplies [89](#)
 inventory management TLV [65](#)

L

LLDP [63, 67, 68, 69](#)
 transmission timer and holdtime, setting [69](#)
 configuring [67](#)
 default configuration [67](#)
 enabling [68](#)
 overview [63](#)
 switch stack considerations [63](#)
 LLDP-MED [64, 71](#)
 configuring [71](#)
 TLVs [71](#)
 overview [64](#)
 supported TLVs [64](#)
 location TLV [65](#)

M

MAC/PHY configuration status TLV [63](#)
 management address TLV [63](#)
 managing [89](#)
 monitoring [97](#)
 monitoring power [99](#)
 MTU [83, 84](#)
 system [83, 84](#)
 system jumbo [83, 84](#)
 system routing [83, 84](#)

N

network policy TLV [65](#)

P

PoE [25, 93, 94, 96, 97, 99](#)
 auto mode [96](#)
 CDP with power consumption, described [94](#)
 CDP with power negotiation, described [94](#)
 Cisco intelligent power management [94](#)
 devices supported [25, 93](#)
 high-power devices operating in low-power mode [94](#)
 IEEE power classification levels [94](#)
 monitoring [97](#)

PoE (*continued*)

monitoring power [99](#)
 policing power consumption [99](#)
 policing power usage [97](#)
 power management modes [96](#)
 power negotiation extensions to CDP [94](#)
 powered-device detection and initial power allocation [94](#)
 standards supported [94](#)
 static mode [96](#)
 supported watts per port [25, 93](#)
 policing power consumption [99](#)
 policing power usage [97](#)
 port description TLV [63](#)
 port VLAN ID TLV [63](#)
 power management modes [96](#)
 power management TLV [65](#)
 power negotiation extensions [94](#)
 power negotiation extensions to CDP [94](#)
 power supply [89](#)
 configuring [89](#)
 managing [89](#)
 powered-device detection and initial power allocation [94](#)

R

routing [58](#)

S

See Ethernet management port [57](#)
 See power supplies [89](#)
 standards supported [94](#)
 static mode [96](#)
 statistics [90, 102](#)
 interface [90, 102](#)
 supported features [59](#)
 supported watts per port [25, 93](#)
 system [83, 84](#)
 system capabilities TLV [63](#)
 system description TLV [63](#)
 system jumbo [83, 84](#)
 system MTU [84](#)
 System MTU [84](#)
 system name TLV [63](#)
 system routing [83, 84](#)

T

TLVs [63](#)
 defined [63](#)

U

unsupported features [59](#)

W

wired location service [65, 66, 75](#)
 configuring [75](#)
 location TLV [65](#)
 understanding [66](#)

