System Management Configuration Guide, Cisco IOS XE Release 3SE (Catalyst 3850 Switches)

First Published: 2013-01-29

Last Modified: 2013-10-07

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-27590-02

CONTENTS

Preface

Document Conventions

This document uses the following conventions:

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

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

Reader Alert Conventions

This document may use the following conventions for reader alerts:

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

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

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

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

Warning IMPORTANT SAFETY INSTRUCTIONS

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

SAVE THESE INSTRUCTIONS

Related Documentation

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

- Cisco Catalyst 3850 Switch documentation, located at:

  http://www.cisco.com/go/cat3850_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

- Cisco Validated Designs documents, located at:

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

- 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

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.	`SwitchControllerDevice>`	Enter **logout** or **quit**.	Use this mode to • Change terminal settings. • Perform basic tests. • Display system information.
Privileged EXEC	While in user EXEC mode, enter the **enable** command.	`SwitchControllerDevice#`	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.	`SwitchControllerDevice(config)#`	To exit to privileged EXEC mode, enter **exit** or **end**, or press **Ctrl-Z**.	Use this mode to configure parameters that apply to the entire switch.
VLAN configuration	While in global configuration mode, enter the **vlan** *vlan-id* command.	`SwitchControllerDevice(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).	`SwitchControllerDevice(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.	SwitchControllerDevice(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:** `SwitchControllerDevice# help`	Obtains a brief description of the help system in any command mode.

Step 2	*abbreviated-command-entry* **?**
	
	Example:
	`SwitchControllerDevice# di?`
	`dir disable disconnect`
		Obtains a list of commands that begin with a particular character string.

Step 3	*abbreviated-command-entry* <Tab>
	
	Example:
	`SwitchControllerDevice# sh conf<tab>`
	`SwitchControllerDevice# show configuration`
		Completes a partial command name.

	Command or Action	Purpose
Step 4	**?** **Example:** `SwitchControllerDevice> ?`	Lists all commands available for a particular command mode.
Step 5	*command* **?** **Example:** `SwitchControllerDevice> show ?`	Lists the associated keywords for a command.

Step 6	*command keyword* **?**
	
	Example:
	`SwitchControllerDevice(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:

```
SwitchControllerDevice# 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** [**size** *number-of-lines*] **Example:** `SwitchControllerDevice#` **`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:** `SwitchControllerDevice#` **`show history`**	Lists the last several commands that you just entered in privileged EXEC mode. The number of commands that appear is controlled by the setting of the **terminal history** global configuration command and the **history** line configuration command.

Disabling the Command History Feature

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

SUMMARY STEPS

1. **terminal no history**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**terminal no history** **Example:** `SwitchControllerDevice#` **`terminal no history`**	Disables the feature during the current terminal session in privileged EXEC mode.

Enabling and Disabling Editing Features

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

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	**terminal editing** **Example:** `SwitchControllerDevice#` **`terminal editing`**	Reenables the enhanced editing mode for the current terminal session in privileged EXEC mode.

	Command or Action	Purpose
Step 2	**terminal no editing** **Example:** `SwitchControllerDevice# terminal no editing`	Disables the enhanced editing mode for the current terminal session in privileged EXEC mode.

Editing Commands Through Keystrokes

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

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

Table 3: Editing Commands

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

Esc D	Deletes from the cursor to the end of the word.
Esc C	Capitalizes at the cursor.
Esc L	Changes the word at the cursor to lowercase.
Esc U	Capitalizes letters from the cursor to the end of the word.
Ctrl-V or **Esc Q**	Designates a particular keystroke as an executable command, perhaps as a shortcut.
Return key	Scrolls down a line or screen on displays that are longer than the terminal screen can display. **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:
	
	`SwitchControllerDevice(config)# access-list 101 permit tcp 10.15.22.25 255.255.255.0 10.15.22.35`
	`SwitchControllerDevice(config)# $ 101 permit tcp 10.15.22.25 255.255.255.0 10.15.22.35 255.25`
	`SwitchControllerDevice(config)# $t tcp 10.15.22.25 255.255.255.0 131.108.1.20 255.255.255.0 eq`
	`SwitchControllerDevice(config)# $15.22.25 255.255.255.0 10.15.22.35 255.255.255.0 eq 45`
		Displays the global configuration command entry that extends beyond one line.
		
		When the cursor first reaches the end of the line, the line is shifted ten spaces to the left and redisplayed. The dollar sign ($) shows that the line has been scrolled to the left. Each time the cursor reaches the end of the line, the line is again shifted ten spaces to the left.

Step 2	**Ctrl-A** **Example:** `SwitchControllerDevice(config)# access-list 101 permit tcp 10.15.22.25 255.255.255.0 10.15.2$`	Checks the complete syntax. The dollar sign ($) appears at the end of the line to show that the line has been scrolled to the right.
Step 3	**Return** key	Execute the commands. 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. Use line wrapping with the command history feature to recall and modify previous complex command entries.

Searching and Filtering Output of show and more Commands

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

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose

Step 1	{**show** | **more**} *command* | {**begin** | **include** | **exclude**} *regular-expression*
	
	Example:
	`SwitchControllerDevice# 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`
		Searches and filters the output.
		
		Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain **output** are not displayed, but the lines that contain **output** appear.

Accessing the CLI on a Switch Stack

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

You manage the switch stack and the stack member interfaces through the 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.

CHAPTER 2

Using the Web Graphical User Interface

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 from1 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.

CHAPTER 3

Administering the System

Finding Feature Information

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

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

Related Topics

Feature History and Information for Troubleshooting Software Configuration, on page 336

Information About Administering the Switch

System Time and Date Management

You can manage the system time and date on your switch using automatic configuration methods (RTC and NTP), or manual configuration methods.

System Clock

The basis of the time service is the system clock. This clock runs from the moment the system starts up and keeps track of the date and time.

The system clock can then be set from these sources:

- NTP
- Manual configuration

The system clock can provide time to these services:

- User **show** commands
- Logging and debugging messages

The system clock keeps track of time internally based on Coordinated Universal Time (UTC), also known as Greenwich Mean Time (GMT). You can configure information about the local time zone and summer time (daylight saving time) so that the time appears correctly for the local time zone.

The system clock keeps track of whether the time is *authoritative* or not (that is, whether it has been set by a time source considered to be authoritative). If it is not authoritative, the time is available only for display purposes and is not redistributed.

Network Time Protocol

The NTP is designed to time-synchronize a network of devices. NTP runs over User Datagram Protocol (UDP), which runs over IP. NTP is documented in RFC 1305.

An NTP network usually gets its time from an authoritative time source, such as a radio clock or an atomic clock attached to a time server. NTP then distributes this time across the network. NTP is extremely efficient; no more than one packet per minute is necessary to synchronize two devices to within a millisecond of one another.

NTP Stratum

NTP uses the concept of a *stratum* to describe how many NTP hops away a device is from an authoritative time source. A stratum 1 time server has a radio or atomic clock directly attached, a stratum 2 time server receives its time through NTP from a stratum 1 time server, and so on. A device running NTP automatically chooses as its time source the device with the lowest stratum number with which it communicates through NTP. This strategy effectively builds a self-organizing tree of NTP speakers.

NTP avoids synchronizing to a device whose time might not be accurate by never synchronizing to a device that is not synchronized. NTP also compares the time reported by several devices and does not synchronize to a device whose time is significantly different than the others, even if its stratum is lower.

NTP Associations

The communications between devices running NTP (known as *associations*) are usually statically configured; each device is given the IP address of all devices with which it should form associations. Accurate timekeeping is possible by exchanging NTP messages between each pair of devices with an association. However, in a

LAN environment, NTP can be configured to use IP broadcast messages instead. This alternative reduces configuration complexity because each device can simply be configured to send or receive broadcast messages. However, in that case, information flow is one-way only.

NTP Security

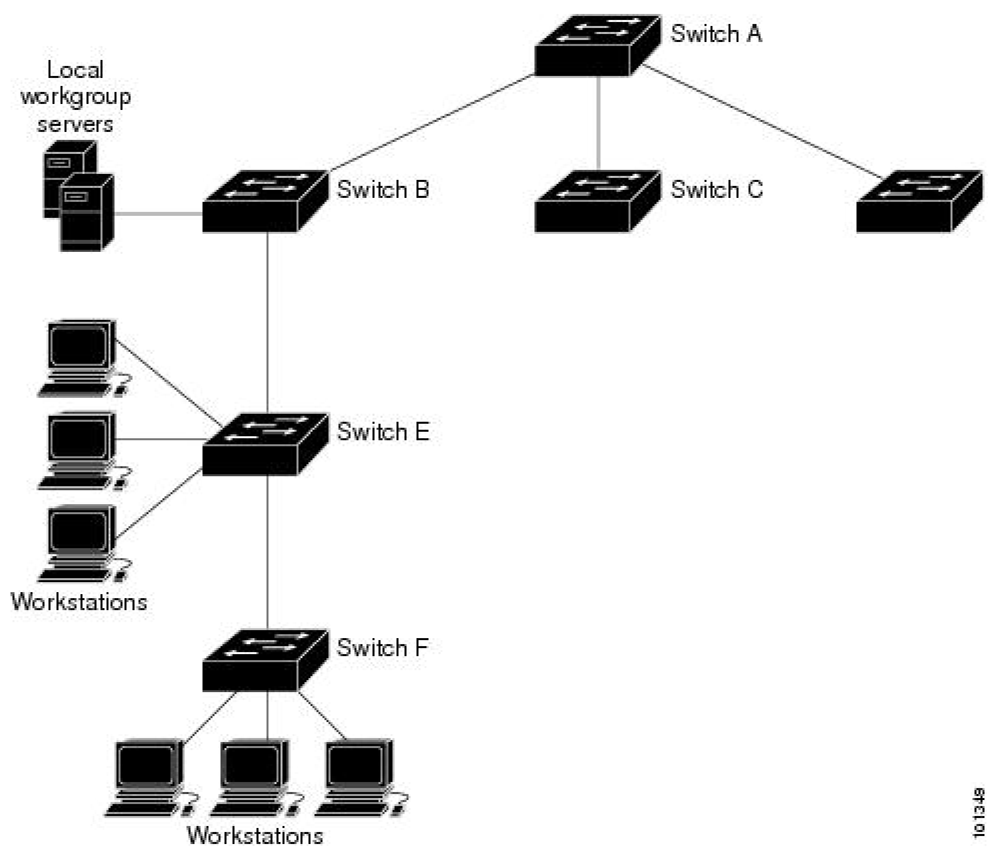
The time kept on a device is a critical resource; you should use the security features of NTP to avoid the accidental or malicious setting of an incorrect time. Two mechanisms are available: an access list-based restriction scheme and an encrypted authentication mechanism.

NTP Implementation

Implementation of NTP does not support stratum 1 service; it is not possible to connect to a radio or atomic clock. We recommend that the time service for your network be derived from the public NTP servers available on the IP Internet.

The following figure shows a typical network example using NTP. Switch A is the NTP master, with the Switch B, C, and D configured in NTP server mode, in server association with Switch A. Switch E is configured as an NTP peer to the upstream and downstream switches, Switch B and Switch F, respectively.

Figure 1: Typical NTP Network Configuration



If the network is isolated from the Internet, NTP allows a device to act as if it is synchronized through NTP, when in fact it has learned the time by using other means. Other devices then synchronize to that device through NTP.

When multiple sources of time are available, NTP is always considered to be more authoritative. NTP time overrides the time set by any other method.

Several manufacturers include NTP software for their host systems, and a publicly available version for systems running UNIX and its various derivatives is also available. This software allows host systems to be time-synchronized as well.

NTP Version 4

NTP version 4 is implemented on the switch. NTPv4 is an extension of NTP version 3. NTPv4 supports both IPv4 and IPv6 and is backward-compatible with NTPv3.

NTPv4 provides these capabilities:

- Support for IPv6.
- Improved security compared to NTPv3. The NTPv4 protocol provides a security framework based on public key cryptography and standard X509 certificates.
- Automatic calculation of the time-distribution hierarchy for a network. Using specific multicast groups, NTPv4 automatically configures the hierarchy of the servers to achieve the best time accuracy for the lowest bandwidth cost. This feature leverages site-local IPv6 multicast addresses.

System Name and Prompt

You configure the system name on the switch to identify it. By default, the system name and prompt are Switch.

If you have not configured a system prompt, the first 20 characters of the system name are used as the system prompt. A greater-than symbol [>] is appended. The prompt is updated whenever the system name changes.

Stack System Name and Prompt

If you are accessing a stack member through the active switch, you must use the **session** *stack-member-number* privileged EXEC command. The stack member number range is from 1 through 4. When you use this command, the stack member number is appended to the system prompt. For example, Switch-2# is the prompt in privileged EXEC mode for stack member 2, and the system prompt for the switch stack is Switch.

Default System Name and Prompt Configuration

The default switch system name and prompt is *Switch*.

DNS

The DNS protocol controls the Domain Name System (DNS), a distributed database with which you can map hostnames to IP addresses. When you configure DNS on your switch, you can substitute the hostname for the IP address with all IP commands, such as **ping**, **telnet**, **connect**, and related Telnet support operations.

IP defines a hierarchical naming scheme that allows a device to be identified by its location or domain. Domain names are pieced together with periods (.) as the delimiting characters. For example, Cisco Systems is a commercial organization that IP identifies by a *com* domain name, so its domain name is *cisco.com*. A specific device in this domain, for example, the File Transfer Protocol (FTP) system is identified as *ftp.cisco.com*.

To keep track of domain names, IP has defined the concept of a domain name server, which holds a cache (or database) of names mapped to IP addresses. To map domain names to IP addresses, you must first identify the hostnames, specify the name server that is present on your network, and enable the DNS.

Default DNS Settings

Table 4: Default DNS Settings

Feature	Default Setting
DNS enable state	Enabled.
DNS default domain name	None configured.
DNS servers	No name server addresses are configured.

Login Banners

You can configure a message-of-the-day (MOTD) and a login banner. The MOTD banner is displayed on all connected terminals at login and is useful for sending messages that affect all network users (such as impending system shutdowns).

The login banner is also displayed on all connected terminals. It appears after the MOTD banner and before the login prompts.

The MOTD and login banners are not configured.

Default Banner Configuration

The MOTD and login banners are not configured.

MAC Address Table

The MAC address table contains address information that the switch uses to forward traffic between ports. All MAC addresses in the address table are associated with one or more ports. The address table includes these types of addresses:

- Dynamic address—A source MAC address that the switch learns and then ages when it is not in use.
- Static address—A manually entered unicast address that does not age and that is not lost when the switch resets.

The address table lists the destination MAC address, the associated VLAN ID, and port number associated with the address and the type (static or dynamic).

MAC Address Table Creation

With multiple MAC addresses supported on all ports, you can connect any port on the switch to other network devices. The switch provides dynamic addressing by learning the source address of packets it receives on each port and adding the address and its associated port number to the address table. As devices are added or removed from the network, the switch updates the address table, adding new dynamic addresses and aging out those that are not in use.

The aging interval is globally configured. However, the switch maintains an address table for each VLAN, and STP can accelerate the aging interval on a per-VLAN basis.

The switch sends packets between any combination of ports, based on the destination address of the received packet. Using the MAC address table, the switch forwards the packet only to the port associated with the destination address. If the destination address is on the port that sent the packet, the packet is filtered and not forwarded. The switch always uses the store-and-forward method: complete packets are stored and checked for errors before transmission.

MAC Addresses and VLANs

All addresses are associated with a VLAN. An address can exist in more than one VLAN and have different destinations in each. Unicast addresses, for example, could be forwarded to port 1 in VLAN 1 and ports 9, 10, and 1 in VLAN 5.

Each VLAN maintains its own logical address table. A known address in one VLAN is unknown in another until it is learned or statically associated with a port in the other VLAN.

MAC Addresses and Switch Stacks

The MAC address tables on all stack members are synchronized. At any given time, each stack member has the same copy of the address tables for each VLAN. When an address ages out, the address is removed from the address tables on all stack members. When a switch joins a switch stack, that switch receives the addresses for each VLAN learned on the other stack members. When a stack member leaves the switch stack, the remaining stack members age out or remove all addresses learned by the former stack member.

Default MAC Address Table Settings

The following table shows the default settings for the MAC address table.

Table 5: Default Settings for the MAC Address

Feature	Default Setting
Aging time	300 seconds
Dynamic addresses	Automatically learned
Static addresses	None configured

ARP Table Management

To communicate with a device (over Ethernet, for example), the software first must learn the 48-bit MAC address or the local data link address of that device. The process of learning the local data link address from an IP address is called address resolution.

The Address Resolution Protocol (ARP) associates a host IP address with the corresponding media or MAC addresses and the VLAN ID. Using an IP address, ARP finds the associated MAC address. When a MAC address is found, the IP-MAC address association is stored in an ARP cache for rapid retrieval. Then the IP datagram is encapsulated in a link-layer frame and sent over the network. Encapsulation of IP datagrams and ARP requests and replies on IEEE 802 networks other than Ethernet is specified by the Subnetwork Access Protocol (SNAP). By default, standard Ethernet-style ARP encapsulation (represented by the **arpa** keyword) is enabled on the IP interface.

ARP entries added manually to the table do not age and must be manually removed.

How to Administer the Switch

Configuring the Time and Date Manually

System time remains accurate through restarts and reboot, however, you can manually configure the time and date after the system is restarted.

We recommend that you use manual configuration only when necessary. If you have an outside source to which the switch can synchronize, you do not need to manually set the system clock.

Note You must reconfigure this setting if you have manually configured the system clock before the active switch fails and a different stack member assumes the role of active switch.

Setting the System Clock

If you have an outside source on the network that provides time services, such as an NTP server, you do not need to manually set the system clock.

SUMMARY STEPS

1. Use one of the following:
   - **clock set** *hh:mm:ss day month year*
   - **clock set** *hh:mm:ss month day year*

DETAILED STEPS

	Command or Action	Purpose
Step 1	Use one of the following: • **clock set** *hh:mm:ss day month year* • **clock set** *hh:mm:ss month day year* **Example:** `SwitchControllerDevice#` **`clock set 13:32:00 23 March 2013`**	Sets the system clock using one of these formats: • *hh:mm:ss*—Specifies the time in hours (24-hour format), minutes, and seconds. The time specified is relative to the configured time zone. • *day*—Specifies the day by date in the month. • *month*—Specifies the month by name. • *year*—Specifies the year (no abbreviation).

Configuring the Time Zone

SUMMARY STEPS

1. **configure terminal**
2. **clock timezone** *zone hours-offset* [*minutes-offset*]
3. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `SwitchControllerDevice#` **`configure terminal`**	Enters global configuration mode.
Step 2	**clock timezone** *zone hours-offset* [*minutes-offset*] **Example:** `SwitchControllerDevice(config)#` **`clock timezone AST -3 30`**	Sets the time zone. Internal time is kept in Coordinated Universal Time (UTC), so this command is used only for display purposes and when the time is manually set. • *zone*—Enters the name of the time zone to be displayed when standard time is in effect. The default is UTC. • *hours-offset*—Enters the hours offset from UTC. • (Optional) *minutes-offset*—Enters the minutes offset from UTC. This available where the local time zone is a percentage of an hour different from UTC.

	Command or Action	Purpose
Step 3	**end** **Example:** `SwitchControllerDevice(config)# end`	Returns to privileged EXEC mode.

Configuring Summer Time (Daylight Saving Time)

To configure summer time (daylight saving time) in areas where it starts and ends on a particular day of the week each year, perform this task:

SUMMARY STEPS

1. **configure terminal**
2. **clock summer-time** *zone* **date** *date month year hh:mm date month year hh:mm* [*offset*]]
3. **clock summer-time** *zone* **recurring** [*week day month hh:mm week day month hh:mm* [*offset*]]
4. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `SwitchControllerDevice# configure terminal`	Enters global configuration mode.
Step 2	**clock summer-time** *zone* **date** *date month year hh:mm date month year hh:mm* [*offset*]] **Example:** `SwitchControllerDevice(config)# clock summer-time PDT date 10 March 2013 2:00 3 November 2013 2:00`	Configures summer time to start and end on specified days every year.
Step 3	**clock summer-time** *zone* **recurring** [*week day month hh:mm week day month hh:mm* [*offset*]] **Example:** `SwitchControllerDevice(config)# clock summer-time`	Configures summer time to start and end on the specified days every year. All times are relative to the local time zone. The start time is relative to standard time. The end time is relative to summer time. Summer time is disabled by default. If you specify **clock summer-time** *zone* **recurring** without parameters, the summer time rules default to the United States rules.

	Command or Action	Purpose
	`PDT recurring 10 March 2013 2:00 3 November 2013 2:00`	If the starting month is after the ending month, the system assumes that you are in the southern hemisphere. • *zone*—Specifies the name of the time zone (for example, PDT) to be displayed when summer time is in effect. • (Optional) *week*— Specifies the week of the month (1 to 4, **first**, or **last**). • (Optional) *day*—Specifies the day of the week (Sunday, Monday...). • (Optional) *month*—Specifies the month (January, February...). • (Optional) *hh:mm*—Specifies the time (24-hour format) in hours and minutes. • (Optional) *offset*—Specifies the number of minutes to add during summer time. The default is 60.
Step 4	**end** **Example:** `SwitchControllerDevice(config)# end`	Returns to privileged EXEC mode.

Configuring a System Name

SUMMARY STEPS

1. **configure terminal**
2. **hostname** *name*
3. **end**

DETAILED STEPS

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

	Command or Action	Purpose
Step 2	**hostname** *name* **Example:** `SwitchControllerDevice(config)# hostname remote-users`	Configures a system name. When you set the system name, it is also used as the system prompt. The default setting is SwitchControllerDevice. The name must follow the rules for ARPANET hostnames. They must start with a letter, end with a letter or digit, and have as interior characters only letters, digits, and hyphens. Names can be up to 63 characters.
Step 3	**end** **Example:** `SwitchControllerDevice(config)# end`	Returns to privileged EXEC mode.

Setting Up DNS

If you use the switch IP address as its hostname, the IP address is used and no DNS query occurs. If you configure a hostname that contains no periods (.), a period followed by the default domain name is appended to the hostname before the DNS query is made to map the name to an IP address. The default domain name is the value set by the **ip domain-name** global configuration command. If there is a period (.) in the hostname, the Cisco IOS software looks up the IP address without appending any default domain name to the hostname.

SUMMARY STEPS

1. **configure terminal**
2. **ip domain-name** *name*
3. **ip name-server** *server-address1* [*server-address2 ... server-address6*]
4. **ip domain-lookup** [**nsap** | **source-interface** *interface*]
5. **end**

DETAILED STEPS

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

	Command or Action	Purpose
Step 2	**ip domain-name** *name* **Example:** `SwitchControllerDevice(config)# ip domain-name Cisco.com`	Defines a default domain name that the software uses to complete unqualified hostnames (names without a dotted-decimal domain name). Do not include the initial period that separates an unqualified name from the domain name. At boot time, no domain name is configured; however, if the switch configuration comes from a BOOTP or Dynamic Host Configuration Protocol (DHCP) server, then the default domain name might be set by the BOOTP or DHCP server (if the servers were configured with this information).
Step 3	**ip name-server** *server-address1* [*server-address2 ... server-address6*] **Example:** `SwitchControllerDevice(config)# ip name-server 192.168.1.100 192.168.1.200 192.168.1.300`	Specifies the address of one or more name servers to use for name and address resolution. You can specify up to six name servers. Separate each server address with a space. The first server specified is the primary server. The switch sends DNS queries to the primary server first. If that query fails, the backup servers are queried.
Step 4	**ip domain-lookup** [**nsap** | **source-interface** *interface*] **Example:** `SwitchControllerDevice(config)# ip domain-lookup`	(Optional) Enables DNS-based hostname-to-address translation on your switch. This feature is enabled by default. If your network devices require connectivity with devices in networks for which you do not control name assignment, you can dynamically assign device names that uniquely identify your devices by using the global Internet naming scheme (DNS).
Step 5	**end** **Example:** `SwitchControllerDevice(config)# end`	Returns to privileged EXEC mode.

Configuring a Message-of-the-Day Login Banner

You can create a single or multiline message banner that appears on the screen when someone logs in to the switch

SUMMARY STEPS

1. **configure terminal**
2. **banner motd** *c message c*
3. **end**

DETAILED STEPS

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

Step 2	**banner motd** *c message c*
	
	Example:
	
	`SwitchControllerDevice(config)# banner motd #`
	`This is a secure site. Only`
	`authorized users are allowed.`
	`For access, contact technical`
	`support.`
	`#`
		Specifies the message of the day.
		
		c—Enters the delimiting character of your choice, for example, a pound sign (#), and press the **Return** key. The delimiting character signifies the beginning and end of the banner text. Characters after the ending delimiter are discarded.
		
		message—Enters a banner message up to 255 characters. You cannot use the delimiting character in the message.

Step 3	**end** **Example:** `SwitchControllerDevice(config)# end`	Returns to privileged EXEC mode.

Configuring a Login Banner

You can configure a login banner to be displayed on all connected terminals. This banner appears after the MOTD banner and before the login prompt.

SUMMARY STEPS

1. **configure terminal**
2. **banner login** *c message c*
3. **end**

DETAILED STEPS

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

Step 2	**banner login** *c message c*
	
	Example:
	
	`SwitchControllerDevice(config)# banner login $`
	`Access for authorized users only. Please enter your username and password.`
	`$`
		Specifies the login message.
		
		c— Enters the delimiting character of your choice, for example, a pound sign (#), and press the **Return** key. The delimiting character signifies the beginning and end of the banner text. Characters after the ending delimiter are discarded.
		
		message—Enters a login message up to 255 characters. You cannot use the delimiting character in the message.

Step 3	**end** **Example:** `SwitchControllerDevice(config)# end`	Returns to privileged EXEC mode.

Managing the MAC Address Table

Changing the Address Aging Time

SUMMARY STEPS

1. **configure terminal**
2. **mac address-table aging-time** [*0* | *10-1000000*] [**routed-mac** | **vlan** *vlan-id*]
3. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `SwitchControllerDevice# configure terminal`	Enters global configuration mode.
Step 2	**mac address-table aging-time** [*0* | *10-1000000*] [**routed-mac** | **vlan** *vlan-id*] **Example:** `SwitchControllerDevice(config)# mac address-table aging-time 500 vlan 2`	Sets the length of time that a dynamic entry remains in the MAC address table after the entry is used or updated. The range is 10 to 1000000 seconds. The default is 300. You can also enter 0, which disables aging. Static address entries are never aged or removed from the table. *vlan-id*—Valid IDs are 1 to 4094.
Step 3	**end** **Example:** `SwitchControllerDevice(config)# end`	Returns to privileged EXEC mode.

Configuring MAC Address Change Notification Traps

SUMMARY STEPS

1. **configure terminal**
2. **snmp-server host** *host-addr community-string notification-type* { **informs** | **traps** } {**version** {**1** | **2c** | **3**}} {**vrf** *vrf instance name*}
3. **snmp-server enable traps mac-notification change**
4. **mac address-table notification change**
5. **mac address-table notification change** [**interval** *value*] [**history-size** *value*]
6. **interface** *interface-id*
7. **snmp trap mac-notification change** {**added** | **removed**}
8. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `SwitchControllerDevice# configure terminal`	Enters global configuration mode.
Step 2	**snmp-server host** *host-addr community-string notification-type* { **informs** | **traps** } {**version** {**1** | **2c** | **3**}} {**vrf** *vrf instance name*} **Example:** `SwitchControllerDevice(config)# snmp-server host 172.20.10.10 traps private mac-notification`	Specifies the recipient of the trap message. • *host-addr*—Specifies the name or address of the NMS. • **traps** (the default)—Sends SNMP traps to the host. • **informs**—Sends SNMP informs to the host. • **version**—Specifies the SNMP version to support. Version 1, the default, is not available with informs. • *community-string*—Specifies the string to send with the notification operation. Though you can set this string by using the **snmp-server host** command, we recommend that you define this string by using the **snmp-server community** command before using the **snmp-server host** command. • *notification-type*—Uses the **mac-notification** keyword. • **vrf** *vrf instance name*—Specifies the VPN routing/forwarding instance for this host.
Step 3	**snmp-server enable traps mac-notification change** **Example:** `SwitchControllerDevice(config)# snmp-server enable traps mac-notification change`	Enables the switch to send MAC address change notification traps to the NMS.
Step 4	**mac address-table notification change** **Example:** `SwitchControllerDevice(config)# mac address-table notification change`	Enables the MAC address change notification feature.
Step 5	**mac address-table notification change** [**interval** *value*] [**history-size** *value*] **Example:** `SwitchControllerDevice(config)# mac address-table`	Enters the trap interval time and the history table size. • (Optional) **interval** *value*—Specifies the notification trap interval in seconds between each set of traps that are generated to the NMS. The range is 0 to 2147483647 seconds; the default is 1 second.

	Command or Action	Purpose
	`notification change interval 123` `SwitchControllerDevice(config)#`**`mac address-table`** **`notification change history-size 100`**	• (Optional) **history-size** *value*—Specifies the maximum number of entries in the MAC notification history table. The range is 0 to 500; the default is 1.
Step 6	**interface** *interface-id* **Example:** `SwitchControllerDevice(config)#` **`interface gigabitethernet1/0/2`**	Enters interface configuration mode, and specifies the Layer 2 interface on which to enable the SNMP MAC address notification trap.
Step 7	**snmp trap mac-notification change** {**added** | **removed**} **Example:** `SwitchControllerDevice(config-if)#` **`snmp trap`** **`mac-notification change added`**	Enables the MAC address change notification trap on the interface. • Enables the trap when a MAC address is **added** on this interface. • Enables the trap when a MAC address is **removed** from this interface.
Step 8	**end** **Example:** `SwitchControllerDevice(config-if)#` **`end`**	Returns to privileged EXEC mode.

Configuring MAC Address Move Notification Traps

When you configure MAC-move notification, an SNMP notification is generated and sent to the network management system whenever a MAC address moves from one port to another within the same VLAN.

Beginning in privileged EXEC mode, follow these steps to configure the switch to send MAC address-move notification traps to an NMS host:

SUMMARY STEPS

1. **configure terminal**
2. **snmp-server host** *host-addr* {**traps** | **informs**} {**version** {**1** | **2c** | **3**}} *community-string notification-type*
3. **snmp-server enable traps mac-notification move**
4. **mac address-table notification mac-move**
5. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `SwitchControllerDevice# configure terminal`	Enters global configuration mode.
Step 2	**snmp-server host** *host-addr* {**traps** | **informs**} {**version** {**1** | **2c** | **3**}} *community-string notification-type* **Example:** `SwitchControllerDevice(config)# snmp-server host 172.20.10.10 traps private mac-notification`	Specifies the recipient of the trap message. • *host-addr*—Specifies the name or address of the NMS. • **traps** (the default)—Sends SNMP traps to the host. • **informs**—Sends SNMP informs to the host. • **version**—Specifies the SNMP version to support. Version 1, the default, is not available with informs. • *community-string*—Specifies the string to send with the notification operation. Though you can set this string by using the **snmp-server host** command, we recommend that you define this string by using the **snmp-server community** command before using the **snmp-server host** command. • *notification-type*—Uses the **mac-notification** keyword.
Step 3	**snmp-server enable traps mac-notification move** **Example:** `SwitchControllerDevice(config)# snmp-server enable traps mac-notification move`	Enables the switch to send MAC address move notification traps to the NMS.
Step 4	**mac address-table notification mac-move** **Example:** `SwitchControllerDevice(config)# mac address-table notification mac-move`	Enables the MAC address move notification feature.
Step 5	**end** **Example:** `SwitchControllerDevice(config)# end`	Returns to privileged EXEC mode.

Configuring MAC Threshold Notification Traps

When you configure MAC threshold notification, an SNMP notification is generated and sent to the network management system when a MAC address table threshold limit is reached or exceeded.

SUMMARY STEPS

1. **configure terminal**
2. **snmp-server host** *host-addr* {**traps** | **informs**} {**version** {**1** | **2c** | **3**}} *community-string notification-type*
3. **snmp-server enable traps mac-notification threshold**
4. **mac address-table notification threshold**
5. **mac address-table notification threshold** [**limit** *percentage*] | [**interval** *time*]
6. **end**

DETAILED STEPS

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

Step 2	**snmp-server host** *host-addr* {**traps** | **informs**} {**version** {**1** | **2c** | **3**}} *community-string notification-type*
	
	Example:
	
	`SwitchControllerDevice(config)# snmp-server host`
	`172.20.10.10 traps private`
	`mac-notification`
		Specifies the recipient of the trap message.
		• *host-addr*—Specifies the name or address of the NMS.
		• **traps** (the default)—Sends SNMP traps to the host.
		• **informs**—Sends SNMP informs to the host.
		• **version**—Specifies the SNMP version to support. Version 1, the default, is not available with informs.
		• *community-string*—Specifies the string to send with the notification operation. You can set this string by using the **snmp-server host** command, but we recommend that you define this string by using the **snmp-server community** command before using the **snmp-server host** command.
		• *notification-type*—Uses the **mac-notification** keyword.

Step 3	**snmp-server enable traps mac-notification threshold**
	
	Example:
	
	`SwitchControllerDevice(config)# snmp-server enable traps`
	`mac-notification threshold`
		Enables MAC threshold notification traps to the NMS.

	Command or Action	Purpose
Step 4	**mac address-table notification threshold** **Example:** `SwitchControllerDevice(config)# mac address-table notification threshold`	Enables the MAC address threshold notification feature.

Step 5	**mac address-table notification threshold** [**limit** *percentage*] | [**interval** *time*]
	
	Example:
	`SwitchControllerDevice(config)# mac address-table notification threshold interval 123`
	`SwitchControllerDevice(config)# mac address-table notification threshold limit 78`
		Enters the threshold value for the MAC address threshold usage monitoring.
		• (Optional) **limit** *percentage*—Specifies the percentage of the MAC address table use; valid values are from 1 to 100 percent. The default is 50 percent.
		• (Optional) **interval** *time*—Specifies the time between notifications; valid values are greater than or equal to 120 seconds. The default is 120 seconds.

Step 6	**end** **Example:** `SwitchControllerDevice(config)# end`	Returns to privileged EXEC mode.

Adding and Removing Static Address Entries

SUMMARY STEPS

1. **configure terminal**
2. **mac address-table static** *mac-addr* **vlan** *vlan-id* **interface** *interface-id*
3. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `SwitchControllerDevice# configure terminal`	Enters global configuration mode.
Step 2	**mac address-table static** *mac-addr* **vlan** *vlan-id* **interface** *interface-id*	Adds a static address to the MAC address table.

	Command or Action	Purpose
	Example: `SwitchControllerDevice(config)# mac address-table static c2f3.220a.12f4 vlan 4 interface gigabitethernet 1/0/1`	• *mac-addr*—Specifies the destination MAC unicast address to add to the address table. Packets with this destination address received in the specified VLAN are forwarded to the specified interface. • *vlan-id*—Specifies the VLAN for which the packet with the specified MAC address is received. Valid VLAN IDs are 1 to 4094. • *interface-id*—Specifies the interface to which the received packet is forwarded. Valid interfaces include physical ports or port channels. For static multicast addresses, you can enter multiple interface IDs. For static unicast addresses, you can enter only one interface at a time, but you can enter the command multiple times with the same MAC address and VLAN ID.
Step 3	**end** **Example:** `SwitchControllerDevice(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Configuring Unicast MAC Address Filtering

SUMMARY STEPS

1. **configure terminal**
2. **mac address-table static** *mac-addr* **vlan** *vlan-id* **drop**
3. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `SwitchControllerDevice# configure terminal`	Enters global configuration mode.
Step 2	**mac address-table static** *mac-addr* **vlan** *vlan-id* **drop** **Example:** `SwitchControllerDevice(config)# mac address-table`	Enables unicast MAC address filtering and configure the switch to drop a packet with the specified source or destination unicast static address. • *mac-addr*—Specifies a source or destination unicast MAC address (48-bit). Packets with this MAC address are dropped.

	Command or Action	Purpose
	`static c2f3.220a.12f4 vlan 4 drop`	• *vlan-id*—Specifies the VLAN for which the packet with the specified MAC address is received. Valid VLAN IDs are 1 to 4094.
Step 3	**end** **Example:** `SwitchControllerDevice(config)# end`	Returns to privileged EXEC mode.

Monitoring and Maintaining Administration of the Switch

Command	Purpose
clear mac address-table dynamic	Removes all dynamic entries.
clear mac address-table dynamic address *mac-address*	Removes a specific MAC address.
clear mac address-table dynamic interface *interface-id*	Removes all addresses on the specified physical port or port channel.
clear mac address-table dynamic vlan *vlan-id*	Removes all addresses on a specified VLAN.
show clock [*detail*]	Displays the time and date configuration.
show ip igmp snooping groups	Displays the Layer 2 multicast entries for all VLANs or the specified VLAN.
show mac address-table address *mac-address*	Displays MAC address table information for the specified MAC address.
show mac address-table aging-time	Displays the aging time in all VLANs or the specified VLAN.
show mac address-table count	Displays the number of addresses present in all VLANs or the specified VLAN.
show mac address-table dynamic	Displays only dynamic MAC address table entries.
show mac address-table interface *interface-name*	Displays the MAC address table information for the specified interface.

Command	Purpose
show mac address-table move update	Displays the MAC address table move update information.
show mac address-table multicast	Displays a list of multicast MAC addresses.
show mac address-table notification {change | mac-move | threshold}	Displays the MAC notification parameters and history table.
show mac address-table secure	Displays the secure MAC addresses.
show mac address-table static	Displays only static MAC address table entries.
show mac address-table vlan *vlan-id*	Displays the MAC address table information for the specified VLAN.

Configuration Examples for Switch Administration

Example: Setting the System Clock

This example shows how to manually set the system clock:

```
SwitchControllerDevice# clock set 13:32:00 23 July 2013
```

Examples: Configuring Summer Time

This example (for daylight savings time) shows how to specify that summer time starts on March 10 at 02:00 and ends on November 3 at 02:00:

```
SwitchControllerDevice(config)# clock summer-time PDT recurring PST date
10 March 2013 2:00 3 November 2013 2:00
```

This example shows how to set summer time start and end dates:

```
SwitchControllerDevice(config)#clock summer-time PST date
20 March 2013 2:00 20 November 2013 2:00
```

Example: Configuring a MOTD Banner

This example shows how to configure a MOTD banner by using the pound sign (#) symbol as the beginning and ending delimiter:

```
SwitchControllerDevice(config)# banner motd #
```

```
This is a secure site. Only authorized users are allowed.
For access, contact technical support.

#

SwitchControllerDevice(config)#
```

This example shows the banner that appears from the previous configuration:

```
Unix> telnet 192.0.2.15

Trying 192.0.2.15...

Connected to 192.0.2.15.

Escape character is '^]'.

This is a secure site. Only authorized users are allowed.

For access, contact technical support.

User Access Verification

Password:
```

Example: Configuring a Login Banner

This example shows how to configure a login banner by using the dollar sign ($) symbol as the beginning and ending delimiter:

```
SwitchControllerDevice(config)# banner login $

Access for authorized users only. Please enter your username and password.

$

SwitchControllerDevice(config)#
```

Example: Configuring MAC Address Change Notification Traps

This example shows how to specify 172.20.10.10 as the NMS, enable MAC address notification traps to the NMS, enable the MAC address-change notification feature, set the interval time to 123 seconds, set the history-size to 100 entries, and enable traps whenever a MAC address is added on the specified port:

```
SwitchControllerDevice(config)# snmp-server host 172.20.10.10 traps private mac-notification
SwitchControllerDevice(config)# snmp-server enable traps mac-notification change
SwitchControllerDevice(config)# mac address-table notification change
SwitchControllerDevice(config)# mac address-table notification change interval 123
SwitchControllerDevice(config)# mac address-table notification change history-size 100
SwitchControllerDevice(config)# interface gigabitethernet1/2/1
SwitchControllerDevice(config-if)# snmp trap mac-notification change added
```

Example: Configuring MAC Threshold Notification Traps

This example shows how to specify 172.20.10.10 as the NMS, enable the MAC address threshold notification feature, set the interval time to 123 seconds, and set the limit to 78 per cent:

```
SwitchControllerDevice(config)# snmp-server host 172.20.10.10 traps private mac-notification
SwitchControllerDevice(config)# snmp-server enable traps mac-notification threshold
SwitchControllerDevice(config)# mac address-table notification threshold
SwitchControllerDevice(config)# mac address-table notification threshold interval 123
SwitchControllerDevice(config)# mac address-table notification threshold limit 78
```

Example: Adding the Static Address to the MAC Address Table

This example shows how to add the static address c2f3.220a.12f4 to the MAC address table. When a packet is received in VLAN 4 with this MAC address as its destination address, the packet is forwarded to the specified port:

```
SwitchControllerDevice(config)# mac address-table static c2f3.220a.12f4 vlan 4 interface
gigabitethernet1/1/1
```

Example: Configuring Unicast MAC Address Filtering

This example shows how to enable unicast MAC address filtering and how to configure drop packets that have a source or destination address of c2f3.220a.12f4. When a packet is received in VLAN 4 with this MAC address as its source or destination, the packet is dropped:

```
SwitchControllerDevice(config)# mac address-table static c2f3.220a.12f4 vlan 4 drop
```

Additional References for Switch Administration

Related Documents

Related Topic	Document Title
System management commands	*System Management Command Reference (Catalyst 3850 Switches)*
Network management configuration	*Network Management Configuration Guide (Catalyst 3850 Switches)*
Layer 2 configuration	*Layer 2/3 Configuration Guide (Catalyst 3850 Switches)*

Related Topic	Document Title
VLAN configuration	*VLAN Configuration Guide (Catalyst 3850 Switches)*
Platform-independent command references	*Configuration Fundamentals Command Reference, Cisco IOS XE Release 3S (Catalyst 3850 Switches)*
Platform-independent configuration information	*Configuration Fundamentals Configuration Guide, Cisco IOS XE Release 3S (Catalyst 3850 Switches)* *IP Addressing Configuration Guide Library, Cisco IOS XE Release 3S (Catalyst 3850 Switches)*

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

Feature History and Information for Switch Administration

Release	Modification
Cisco IOS XE 3.2SE	This feature was introduced.

CHAPTER 4

Performing Switch Setup Configuration

Finding Feature Information

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

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

Related Topics

Feature History and Information for Troubleshooting Software Configuration, on page 336

Information About Performing Switch Setup Configuration

Review the sections in this module before performing your initial switch configuration tasks that include IP address assignments and DHCP autoconfiguration.

Switch Boot Process

To start your switch, you need to follow the procedures in the hardware installation guide for installing and powering on the switch and setting up the initial switch configuration (IP address, subnet mask, default gateway, secret and Telnet passwords, and so forth).

The normal boot process involves the operation of the boot loader software and includes these activities:

- Locates the bootable (base) package in the bundle or installed package set.
- Performs low-level CPU initialization. It initializes the CPU registers, which control where physical memory is mapped, its quantity, its speed, and so forth.
- Performs power-on self-test (POST) for the CPU subsystem and tests the system DRAM.
- Initializes the file systems on the system board.
- Loads a default operating system software image into memory and boots up the switch.

The boot loader provides access to the file systems before the operating system is loaded. Normally, the boot loader is used only to load, decompress, and start the operating system. After the boot loader gives the operating system control of the CPU, the boot loader is not active until the next system reset or power-on.

The boot loader also provides trap-door access into the system if the operating system has problems serious enough that it cannot be used. The trap-door mechanism provides enough access to the system so that if it is necessary, you can reinstall the operating system software image by using the **emergency-install** command and restart the operating system.

Before you can assign switch information, make sure you have connected a PC or terminal to the console port or a PC to the Ethernet management port, and make sure you have configured the PC or terminal-emulation software baud rate and character format to match these of the switch console port:

- Baud rate default is 9600.
- Data bits default is 8.

Note If the data bits option is set to 8, set the parity option to none.

- Stop bits default is 2 (minor).
- Parity settings default is none.

Software Installer Features

The following software installer features are supported on your switch:

- Software bundle installation on a standalone switch, a switch stack, or a subset of switches in a stack. The default is installation on all the switches if a switch stack is configured.
- In a stack of switches, Cisco recommends all switches in install mode.
- Software rollback to a previously installed package set.
- Emergency installation in the event that no valid installed packages reside on the boot flash.

- Auto-upgrade of a switch that joins the switch stack with incompatible software.
- Installation using packages on one switch as the source for installing packages on another switch in the switch stack.

Note Software installation and rollback must be performed while running only in installed mode. You can use the **software expand** EXEC command to convert bundle boot mode to install mode.

Software Boot Modes

Your switch supports two modes to boot the software packages:

- Installed mode
- Bundle mode

Related Topics

Examples: Displaying Software Bootup in Install Mode, on page 79
Example: Emergency Installation, on page 80

Installed Boot Mode

You can boot your switch in installed mode by booting the software package provisioning file that resides in flash:

```
switch: boot flash:packages.conf
```

The provisioning file contains a list of software packages to boot, mount, and run. The ISO file system in each installed package is mounted to the root file system directly from flash.

Note The packages and provisioning file used to boot in installed mode must reside in flash. Booting in installed mode from usbflash0: or tftp: is not supported.

Related Topics

Examples: Displaying Software Bootup in Install Mode, on page 79
Example: Emergency Installation, on page 80

Bundle Boot Mode

You can boot your switch in bundle boot mode by booting the bundle (.bin) file:

```
switch:  boot flash:cat3850-universalk9.SSA.03.08.83.EMD.150-8.83.EMD.bin
```

The provisioning file contained in a bundle is used to decide which packages to boot, mount, and run. Packages are extracted from the bundle and copied to RAM. The ISO file system in each package is mounted to the root file system.

Unlike install boot mode, additional memory that is equivalent to the size of the bundle is used when booting in bundle mode.

Unlike install boot mode, bundle boot mode is available from several locations:

- flash:
- usbflash0:
- tftp:

Note Auto install and smart install functionality is not supported in bundle boot mode.

Note The AP image pre-download feature is not supported in bundle boot mode. For more information about the pre-download feature see the Cisco WLC 5700 Series *Preloading an Image to Access Points* chapter.

Related Topics

Examples: Displaying Software Bootup in Install Mode, on page 79

Example: Emergency Installation, on page 80

Boot Mode for a Switch Stack

All the switches in a stack must be running in installed mode or bundle boot mode. A mixed mode stack is not supported. If a new switch tries to join the stack in a different boot mode then the active switch, the new switch is given a V-mismatch state.

If a mixed mode switch stack is booted at the same time, then all the switches except for the active switch is given a V-mismatch state. If the boot mode does not support auto-upgrade, then the switch stack members must be re-booted in the same boot mode as the active switch.

If the stack is running in installed mode, the auto-upgrade feature can be used to automatically upgrade the new switch that is attempting to join the switch stack.

The auto-upgrade feature changes the boot mode of the new switch to installed mode. If the stack is running in bundle boot mode, the auto-upgrade feature is not available. You will be required to use the bundle mode to boot the new switch so that it can join the switch stack.

This is an example of the state of a switch that attempts to join the switch stack when the boot mode is not compatible with the active switch:

```
SwitchControllerDevice# show switch

Switch/Stack Mac Address : 6400.f125.1100 - Local Mac Address
Mac persistency wait time: Indefinite
H/W Current
Switch#   Role   Mac Address    Priority Version   State
-----------------------------------------------------------
 1       Member 6400 f125.1a00   1        0        V-Mismatch
*2       Active 6400.f125.1100   1        V01      Ready
SwitchControllerDevice
```

Switches Information Assignment

You can assign IP information through the switch setup program, through a DHCP server, or manually.

Use the switch setup program if you want to be prompted for specific IP information. With this program, you can also configure a hostname and an enable secret password.

It gives you the option of assigning a Telnet password (to provide security during remote management) and configuring your switch as a command or member switch of a cluster or as a standalone switch.

The switch stack is managed through a single IP address. The IP address is a system-level setting and is not specific to the stack master or to any other stack member. You can still manage the stack through the same IP address even if you remove the stack master or any other stack member from the stack, provided there is IP connectivity.

Note Stack members retain their IP address when you remove them from a switch stack. To avoid a conflict by having two devices with the same IP address in your network, change the IP address of the switch that you removed from the switch stack.

Use a DHCP server for centralized control and automatic assignment of IP information after the server is configured.

Note If you are using DHCP, do not respond to any of the questions in the setup program until the switch receives the dynamically assigned IP address and reads the configuration file.

If you are an experienced user familiar with the switch configuration steps, manually configure the switch. Otherwise, use the setup program described in the *Boot Process* section.

Default Switch Information

Table 6: Default Switch Information

Feature	Default Setting
IP address and subnet mask	No IP address or subnet mask are defined.
Default gateway	No default gateway is defined.
Enable secret password	No password is defined.
Hostname	The factory-assigned default hostname is Switch.
Telnet password	No password is defined.

DHCP-Based Autoconfiguration Overview

DHCP provides configuration information to Internet hosts and internetworking devices. This protocol consists of two components: one for delivering configuration parameters from a DHCP server to a device and an operation for allocating network addresses to devices. DHCP is built on a client-server model, in which designated DHCP servers allocate network addresses and deliver configuration parameters to dynamically configured devices. The switch can act as both a DHCP client and a DHCP server.

During DHCP-based autoconfiguration, your switch (DHCP client) is automatically configured at startup with IP address information and a configuration file.

With DHCP-based autoconfiguration, no DHCP client-side configuration is needed on your switch. However, you need to configure the DHCP server for various lease options associated with IP addresses.

If you want to use DHCP client autoconfiguration, you need to configure a Trivial File Transfer Protocol (TFTP) server to fetch the configuration file. The DHCP client then applies the new configuration file to its running configuration.

Note If the new configuration is downloaded to a switch that already has a configuration, the downloaded configuration is appended to the configuration file stored on the switch. (Any existing configuration is not overwritten by the downloaded one.)

Note We recommend a redundant connection between a switch stack and the DHCP, DNS, and TFTP servers. This is to help ensure that these servers remain accessible in case one of the connected stack members is removed from the switch stack.

The DHCP server for your switch can be on the same LAN or on a different LAN than the switch. If the DHCP server is running on a different LAN, you should configure a DHCP relay device between your switch and the DHCP server. A relay device forwards broadcast traffic between two directly connected LANs. A router does not forward broadcast packets, but it forwards packets based on the destination IP address in the received packet.

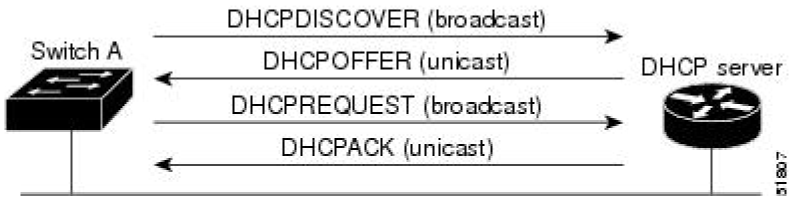
DHCP-based autoconfiguration replaces the BOOTP client functionality on your switch.

DHCP Client Request Process

When you boot up your switch, the DHCP client is invoked and requests configuration information from a DHCP server when the configuration file is not present on the switch. If the configuration file is present and the configuration includes the **ip address dhcp** interface configuration command on specific routed interfaces, the DHCP client is invoked and requests the IP address information for those interfaces.

This is the sequence of messages that are exchanged between the DHCP client and the DHCP server.

Figure 2: DHCP Client and Server Message Exchange



The client, Switch A, broadcasts a DHCPDISCOVER message to locate a DHCP server. The DHCP server offers configuration parameters (such as an IP address, subnet mask, gateway IP address, DNS IP address, a lease for the IP address, and so forth) to the client in a DHCPOFFER unicast message.

In a DHCPREQUEST broadcast message, the client returns a formal request for the offered configuration information to the DHCP server. The formal request is broadcast so that all other DHCP servers that received the DHCPDISCOVER broadcast message from the client can reclaim the IP addresses that they offered to the client.

The DHCP server confirms that the IP address has been allocated to the client by returning a DHCPACK unicast message to the client. With this message, the client and server are bound, and the client uses configuration information received from the server. The amount of information the switch receives depends on how you configure the DHCP server.

If the configuration parameters sent to the client in the DHCPOFFER unicast message are invalid (a configuration error exists), the client returns a DHCPDECLINE broadcast message to the DHCP server.

The DHCP server sends the client a DHCPNAK denial broadcast message, which means that the offered configuration parameters have not been assigned, that an error has occurred during the negotiation of the parameters, or that the client has been slow in responding to the DHCPOFFER message (the DHCP server assigned the parameters to another client).

A DHCP client might receive offers from multiple DHCP or BOOTP servers and can accept any of the offers; however, the client usually accepts the first offer it receives. The offer from the DHCP server is not a guarantee that the IP address is allocated to the client; however, the server usually reserves the address until the client has had a chance to formally request the address. If the switch accepts replies from a BOOTP server and configures itself, the switch broadcasts, instead of unicasts, TFTP requests to obtain the switch configuration file.

The DHCP hostname option allows a group of switches to obtain hostnames and a standard configuration from the central management DHCP server. A client (switch) includes in its DCHPDISCOVER message an option 12 field used to request a hostname and other configuration parameters from the DHCP server. The configuration files on all clients are identical except for their DHCP-obtained hostnames.

If a client has a default hostname (the **hostname** *name* global configuration command is not configured or the **no hostname** global configuration command is entered to remove the hostname), the DHCP hostname option is not included in the packet when you enter the **ip address dhcp** interface configuration command. In this case, if the client receives the DCHP hostname option from the DHCP interaction while acquiring an IP address for an interface, the client accepts the DHCP hostname option and sets the flag to show that the system now has a hostname configured.

DHCP-based Autoconfiguration and Image Update

You can use the DHCP image upgrade features to configure a DHCP server to download both a new image and a new configuration file to one or more switches in a network. Simultaneous image and configuration upgrade for all switches in the network helps ensure that each new switch added to a network are synchronous with the network.

There are two types of DHCP image upgrades: DHCP autoconfiguration and DHCP auto-image update.

Restrictions for DHCP-based Autoconfiguration

- The DHCP-based autoconfiguration with a saved configuration process stops if there is not at least one Layer 3 interface in an up state without an assigned IP address in the network.
- Unless you configure a timeout, the DHCP-based autoconfiguration with a saved configuration feature tries indefinitely to download an IP address.
- The auto-install process stops if a configuration file cannot be downloaded or if the configuration file is corrupted.
- The configuration file that is downloaded from TFTP is merged with the existing configuration in the running configuration but is not saved in the NVRAM unless you enter the **write memory** or **copy running-configuration startup-configuration** privileged EXEC command. If the downloaded configuration is saved to the startup configuration, the feature is not triggered during subsequent system restarts.

DHCP Autoconfiguration

DHCP autoconfiguration downloads a configuration file to one or more switches in your network from a DHCP server. The downloaded configuration file becomes the running configuration of the switch. It does not over write the bootup configuration saved in the flash, until you reload the switch.

DHCP Auto-Image Update

You can use DHCP auto-image upgrade with DHCP autoconfiguration to download both a configuration and a new image to one or more switches in your network. The switch (or switches) downloading the new configuration and the new image can be blank (or only have a default factory configuration loaded).

To enable a DHCP auto-image update on the switch, the TFTP server where the image and configuration files are located must be configured with the correct option 67 (the configuration filename), option 66 (the DHCP server hostname) option 150 (the TFTP server address), and option 125 (description of the Cisco IOS image file) settings.

After you install the switch in your network, the auto-image update feature starts. The downloaded configuration file is saved in the running configuration of the switch, and the new image is downloaded and installed on the switch. When you reboot the switch, the configuration is stored in the saved configuration on the switch.

DHCP Server Configuration Guidelines

Follow these guidelines if you are configuring a device as a DHCP server:

- You should configure the DHCP server with reserved leases that are bound to each switch by the switch hardware address.
- If you want the switch to receive IP address information, you must configure the DHCP server with these lease options:
    - IP address of the client (required)
    - Subnet mask of the client (required)
    - DNS server IP address (optional)
    - Router IP address (default gateway address to be used by the switch) (required)
- If you want the switch to receive the configuration file from a TFTP server, you must configure the DHCP server with these lease options:
    - TFTP server name (required)
    - Boot filename (the name of the configuration file that the client needs) (recommended)
    - Hostname (optional)
- Depending on the settings of the DHCP server, the switch can receive IP address information, the configuration file, or both.
- If you do not configure the DHCP server with the lease options described previously, it replies to client requests with only those parameters that are configured. If the IP address and the subnet mask are not in the reply, the switch is not configured. If the router IP address or the TFTP server name are not found, the switch might send broadcast, instead of unicast, TFTP requests. Unavailability of other lease options does not affect autoconfiguration.
- The switch can act as a DHCP server. By default, the Cisco IOS DHCP server and relay agent features are enabled on your switch but are not configured.

Purpose of the TFTP Server

Based on the DHCP server configuration, the switch attempts to download one or more configuration files from the TFTP server. If you configured the DHCP server to respond to the switch with all the options required for IP connectivity to the TFTP server, and if you configured the DHCP server with a TFTP server name, address, and configuration filename, the switch attempts to download the specified configuration file from the specified TFTP server.

If you did not specify the configuration filename, the TFTP server, or if the configuration file could not be downloaded, the switch attempts to download a configuration file by using various combinations of filenames and TFTP server addresses. The files include the specified configuration filename (if any) and these files: network-config, cisconet.cfg, *hostname*.config, or *hostname*.cfg, where *hostname* is the switch's current hostname. The TFTP server addresses used include the specified TFTP server address (if any) and the broadcast address (255.255.255.255).

For the switch to successfully download a configuration file, the TFTP server must contain one or more configuration files in its base directory. The files can include these files:

- The configuration file named in the DHCP reply (the actual switch configuration file).
- The network-confg or the cisconet.cfg file (known as the default configuration files).

- The router-confg or the ciscortr.cfg file (These files contain commands common to all switches. Normally, if the DHCP and TFTP servers are properly configured, these files are not accessed.)

If you specify the TFTP server name in the DHCP server-lease database, you must also configure the TFTP server name-to-IP-address mapping in the DNS-server database.

If the TFTP server to be used is on a different LAN from the switch, or if it is to be accessed by the switch through the broadcast address (which occurs if the DHCP server response does not contain all the required information described previously), a relay must be configured to forward the TFTP packets to the TFTP server. The preferred solution is to configure the DHCP server with all the required information.

Purpose of the DNS Server

The DHCP server uses the DNS server to resolve the TFTP server name to an IP address. You must configure the TFTP server name-to-IP address map on the DNS server. The TFTP server contains the configuration files for the switch.

You can configure the IP addresses of the DNS servers in the lease database of the DHCP server from where the DHCP replies will retrieve them. You can enter up to two DNS server IP addresses in the lease database.

The DNS server can be on the same LAN or on a different LAN from the switch. If it is on a different LAN, the switch must be able to access it through a router.

How to Obtain Configuration Files

Depending on the availability of the IP address and the configuration filename in the DHCP reserved lease, the switch obtains its configuration information in these ways:

- The IP address and the configuration filename is reserved for the switch and provided in the DHCP reply (one-file read method).

  The switch receives its IP address, subnet mask, TFTP server address, and the configuration filename from the DHCP server. The switch sends a unicast message to the TFTP server to retrieve the named configuration file from the base directory of the server and upon receipt, it completes its boot up process.

- The IP address and the configuration filename is reserved for the switch, but the TFTP server address is not provided in the DHCP reply (one-file read method).

  The switch receives its IP address, subnet mask, and the configuration filename from the DHCP server. The switch sends a broadcast message to a TFTP server to retrieve the named configuration file from the base directory of the server, and upon receipt, it completes its boot-up process.

- Only the IP address is reserved for the switch and provided in the DHCP reply. The configuration filename is not provided (two-file read method).

  The switch receives its IP address, subnet mask, and the TFTP server address from the DHCP server. The switch sends a unicast message to the TFTP server to retrieve the network-confg or cisconet.cfg default configuration file. (If the network-confg file cannot be read, the switch reads the cisconet.cfg file.)

  The default configuration file contains the hostnames-to-IP-address mapping for the switch. The switch fills its host table with the information in the file and obtains its hostname. If the hostname is not found in the file, the switch uses the hostname in the DHCP reply. If the hostname is not specified in the DHCP reply, the switch uses the default *Switch* as its hostname.

After obtaining its hostname from the default configuration file or the DHCP reply, the switch reads the configuration file that has the same name as its hostname (*hostname*-confg or *hostname*.cfg, depending on whether network-confg or cisconet.cfg was read earlier) from the TFTP server. If the cisconet.cfg file is read, the filename of the host is truncated to eight characters.

If the switch cannot read the network-confg, cisconet.cfg, or the hostname file, it reads the router-confg file. If the switch cannot read the router-confg file, it reads the ciscortr.cfg file.

Note The switch broadcasts TFTP server requests if the TFTP server is not obtained from the DHCP replies, if all attempts to read the configuration file through unicast transmissions fail, or if the TFTP server name cannot be resolved to an IP address.

How to Control Environment Variables

With a normally operating switch, you enter the boot loader mode only through the console connection configured for 9600 bps. Unplug the switch power cord, and press the **Mode** button while reconnecting the power cord. You can release the **Mode** button after all the amber system LEDs turn on and remain solid. The boot loader switch prompt then appears.

The switch boot loader software provides support for nonvolatile environment variables, which can be used to control how the boot loader, or any other software running on the system, operates. Boot loader environment variables are similar to environment variables that can be set on UNIX or DOS systems.

Environment variables that have values are stored in flash memory outside of the flash file system.

Each line in these files contains an environment variable name and an equal sign followed by the value of the variable. A variable has no value if it is not present; it has a value if it is listed even if the value is a null string. A variable that is set to a null string (for example, “ ”) is a variable with a value. Many environment variables are predefined and have default values.

You can change the settings of the environment variables by accessing the boot loader or by using Cisco IOS commands. Under normal circumstances, it is not necessary to alter the setting of the environment variables.

Environment Variables for TFTP

When the switch is connected to a PC through the Ethernet management port, you can download or upload a configuration file to the boot loader by using TFTP. Make sure the environment variables in this table are configured.

Table 7: Environment Variables for TFTP

Variable	Description
MAC_ADDR	Specifies the MAC address of the switch. **Note** We recommend that you do not modify this variable. However, if you modify this variable after the boot loader is up or the value is different from the saved value, enter this command before using TFTP.
IP_ADDR	Specifies the IP address and the subnet mask for the associated IP subnet of the switch.
DEFAULT_ROUTER	Specifies the IP address and subnet mask of the default gateway.

Scheduled Reload of the Software Image

You can schedule a reload of the software image to occur on the switch at a later time (for example, late at night or during the weekend when the switch is used less), or you can synchronize a reload network-wide (for example, to perform a software upgrade on all switches in the network).

Note A scheduled reload must take place within approximately 24 days.

You have these reload options:

- Reload of the software to take affect in the specified minutes or hours and minutes. The reload must take place within approximately 24 hours. You can specify the reason for the reload in a string up to 255 characters in length.
- Reload of the software to take place at the specified time (using a 24-hour clock). If you specify the month and day, the reload is scheduled to take place at the specified time and date. If you do not specify the month and day, the reload takes place at the specified time on the current day (if the specified time is later than the current time) or on the next day (if the specified time is earlier than the current time). Specifying 00:00 schedules the reload for midnight.

The **reload** command halts the system. If the system is not set to manually boot up, it reboots itself.

If your switch is configured for manual booting, do not reload it from a virtual terminal. This restriction prevents the switch from entering the boot loader mode and then taking it from the remote user's control.

If you modify your configuration file, the switch prompts you to save the configuration before reloading. During the save operation, the system requests whether you want to proceed with the save if the CONFIG_FILE environment variable points to a startup configuration file that no longer exists. If you proceed in this situation, the system enters setup mode upon reload.

To cancel a previously scheduled reload, use the **reload cancel** privileged EXEC command.

How to Perform Switch Setup Configuration

Using DHCP to download a new image and a new configuration to a switch requires that you configure at least two switches. One switch acts as a DHCP and TFTP server and the second switch (client) is configured to download either a new configuration file or a new configuration file and a new image file.

Configuring DHCP Autoconfiguration (Only Configuration File)

This task describes how to configure DHCP autoconfiguration of the TFTP and DHCP settings on an existing switch in the network so that it can support the autoconfiguration of a new switch.

SUMMARY STEPS

1. **configure terminal**
2. **ip dhcp pool** *poolname*
3. **boot** *filename*
4. **network** *network-number mask prefix-length*
5. **default-router** *address*
6. **option 150** *address*
7. **exit**
8. **tftp-server flash**:*filename.text*
9. **interface** *interface-id*
10. **no switchport**
11. **ip address** *address mask*
12. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `SwitchControllerDevice# configure terminal`	Enters global configuration mode.
Step 2	**ip dhcp pool** *poolname* **Example:** `SwitchControllerDevice(config)# ip dhcp pool pool`	Creates a name for the DHCP server address pool, and enters DHCP pool configuration mode.

	Command or Action	Purpose
Step 3	**boot** *filename* **Example:** `SwitchControllerDevice(dhcp-config)# boot config-boot.text`	Specifies the name of the configuration file that is used as a boot image.
Step 4	**network** *network-number mask prefix-length* **Example:** `SwitchControllerDevice(dhcp-config)# network 10.10.10.0 255.255.255.0`	Specifies the subnet network number and mask of the DHCP address pool. **Note** The prefix length specifies the number of bits that comprise the address prefix. The prefix is an alternative way of specifying the network mask of the client. The prefix length must be preceded by a forward slash (/).
Step 5	**default-router** *address* **Example:** `SwitchControllerDevice(dhcp-config)# default-router 10.10.10.1`	Specifies the IP address of the default router for a DHCP client.
Step 6	**option 150** *address* **Example:** `SwitchControllerDevice(dhcp-config)# option 150 10.10.10.1`	Specifies the IP address of the TFTP server.
Step 7	**exit** **Example:** `SwitchControllerDevice(dhcp-config)# exit`	Returns to global configuration mode.
Step 8	**tftp-server flash**:*filename.text* **Example:** `SwitchControllerDevice(config)# tftp-server flash:config-boot.text`	Specifies the configuration file on the TFTP server.
Step 9	**interface** *interface-id* **Example:** `SwitchControllerDevice(config)# interface gigabitethernet1/0/4`	Specifies the address of the client that will receive the configuration file.

	Command or Action	Purpose
Step 10	**no switchport** **Example:** `SwitchControllerDevice(config-if)#` **`no switchport`**	Puts the interface into Layer 3 mode.
Step 11	**ip address** *address mask* **Example:** `SwitchControllerDevice(config-if)#` **`ip address 10.10.10.1 255.255.255.0`**	Specifies the IP address and mask for the interface.
Step 12	**end** **Example:** `SwitchControllerDevice(config-if)#` **`end`**	Returns to privileged EXEC mode.

Related Topics

Example: Configuring a Switch as a DHCP Server, on page 82

Configuring DHCP Auto-Image Update (Configuration File and Image)

This task describes DHCP autoconfiguration to configure TFTP and DHCP settings on an existing switch to support the installation of a new switch.

Before You Begin

You must first create a text file (for example, autoinstall_dhcp) that will be uploaded to the switch. In the text file, put the name of the image that you want to download.

SUMMARY STEPS

1. **configure terminal**
2. **ip dhcp pool** *poolname*
3. **boot** *filename*
4. **network** *network-number mask prefix-length*
5. **default-router** *address*
6. **option 150** *address*
7. **option 125** *hex*
8. **copy tftp flash** *filename.txt*
9. **copy tftp flash** *imagename.bin*
10. **exit**
11. **tftp-server flash:** *config.text*
12. **tftp-server flash:** *imagename.bin*
13. **tftp-server flash:** *filename.txt*
14. **interface** *interface-id*
15. **no switchport**
16. **ip address** *address mask*
17. **end**
18. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `SwitchControllerDevice#` **`configure terminal`**	Enters global configuration mode.
Step 2	**ip dhcp pool** *poolname* **Example:** `SwitchControllerDevice(config)#` **`ip dhcp pool pool1`**	Creates a name for the DHCP server address pool and enter DHCP pool configuration mode.
Step 3	**boot** *filename* **Example:** `SwitchControllerDevice(dhcp-config)#` **`boot config-boot.text`**	Specifies the name of the file that is used as a boot image.

	Command or Action	Purpose
Step 4	**network** *network-number mask prefix-length* **Example:** `SwitchControllerDevice(dhcp-config)# network 10.10.10.0 255.255.255.0`	Specifies the subnet network number and mask of the DHCP address pool. **Note** The prefix length specifies the number of bits that comprise the address prefix. The prefix is an alternative way of specifying the network mask of the client. The prefix length must be preceded by a forward slash (/).
Step 5	**default-router** *address* **Example:** `SwitchControllerDevice(dhcp-config)# default-router 10.10.10.1`	Specifies the IP address of the default router for a DHCP client.
Step 6	**option 150** *address* **Example:** `SwitchControllerDevice(dhcp-config)# option 150 10.10.10.1`	Specifies the IP address of the TFTP server.
Step 7	**option 125** *hex* **Example:** `SwitchControllerDevice(dhcp-config)# option 125 hex 0000.0009.0a05.08661.7574.6f69.6e73.7461.6c6c.5f64.686370`	Specifies the path to the text file that describes the path to the image file.
Step 8	**copy tftp flash** *filename.txt* **Example:** `SwitchControllerDevice(config)# copy tftp flash image.bin`	Uploads the text file to the switch.
Step 9	**copy tftp flash** *imagename.bin* **Example:** `SwitchControllerDevice(config)# copy tftp flash image.bin`	Uploads the tar file for the new image to the switch.
Step 10	**exit** **Example:** `SwitchControllerDevice(dhcp-config)# exit`	Returns to global configuration mode.

	Command or Action	Purpose
Step 11	**tftp-server flash:** *config.text* **Example:** `SwitchControllerDevice(config)#` **`tftp-server flash:config-boot.text`**	Specifies the Cisco IOS configuration file on the TFTP server.
Step 12	**tftp-server flash:** *imagename.bin* **Example:** `SwitchControllerDevice(config)#` **`tftp-server flash:image.bin`**	Specifies the image name on the TFTP server.
Step 13	**tftp-server flash:** *filename.txt* **Example:** `SwitchControllerDevice(config)#` **`tftp-server flash:boot-config.text`**	Specifies the text file that contains the name of the image file to download
Step 14	**interface** *interface-id* **Example:** `SwitchControllerDevice(config)#` **`interface gigabitEthernet1/0/4`**	Specifies the address of the client that will receive the configuration file.
Step 15	**no switchport** **Example:** `SwitchControllerDevice(config-if)#` **`no switchport`**	Puts the interface into Layer 3 mode.
Step 16	**ip address** *address mask* **Example:** `SwitchControllerDevice(config-if)#` **`ip address 10.10.10.1 255.255.255.0`**	Specifies the IP address and mask for the interface.
Step 17	**end** **Example:** `SwitchControllerDevice(config-if)#` **`end`**	Returns to privileged EXEC mode.

	Command or Action	Purpose
Step 18	**copy running-config startup-config** **Example:** `SwitchControllerDevice(config-if)# end`	(Optional) Saves your entries in the configuration file.

Related Topics

Example: Configuring DHCP Auto-Image Update, on page 82

Configuring the Client to Download Files from DHCP Server

Note You should only configure and enable the Layer 3 interface. Do not assign an IP address or DHCP-based autoconfiguration with a saved configuration.

SUMMARY STEPS

1. **configure terminal**
2. **boot host dhcp**
3. **boot host retry timeout** *timeout-value*
4. **banner config-save ^C** *warning-message* **^C**
5. **end**
6. **show boot**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `SwitchControllerDevice# configure terminal`	Enters global configuration mode.
Step 2	**boot host dhcp** **Example:** `SwitchControllerDevice(conf)# boot host dhcp`	Enables autoconfiguration with a saved configuration.

	Command or Action	Purpose
Step 3	**boot host retry timeout** *timeout-value* **Example:** `SwitchControllerDevice(conf)#` **`boot host retry timeout 300`**	(Optional) Sets the amount of time the system tries to download a configuration file. **Note** If you do not set a timeout, the system will try indefinitely to obtain an IP address from the DHCP server.
Step 4	**banner config-save ^C** *warning-message* **^C** **Example:** `SwitchControllerDevice(conf)#` **`banner config-save ^C Caution - Saving Configuration File to NVRAM May Cause You to No longer Automatically Download Configuration Files at Reboot^C`**	(Optional) Creates warning messages to be displayed when you try to save the configuration file to NVRAM.
Step 5	**end** **Example:** `SwitchControllerDevice(config-if)#` **`end`**	Returns to privileged EXEC mode.
Step 6	**show boot** **Example:** `SwitchControllerDevice#` **`show boot`**	Verifies the configuration.

Related Topics

Example: Configuring a Switch to Download Configurations from a DHCP Server, on page 83

Manually Assigning IP Information to Multiple SVIs

This task describes how to manually assign IP information to multiple switched virtual interfaces (SVIs):

SUMMARY STEPS

1. **configure terminal**
2. **interface vlan** *vlan-id*
3. **ip address** *ip-address subnet-mask*
4. **exit**
5. **ip default-gateway** *ip-address*
6. **end**
7. **show interfaces vlan** *vlan-id*
8. **show ip redirects**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `SwitchControllerDevice# configure terminal`	Enters global configuration mode.
Step 2	**interface vlan** *vlan-id* **Example:** `SwitchControllerDevice(config)# interface vlan 99`	Enters interface configuration mode, and enters the VLAN to which the IP information is assigned. The range is 1 to 4094.
Step 3	**ip address** *ip-address subnet-mask* **Example:** `SwitchControllerDevice(config-vlan)# ip address 10.10.10.2 255.255.255.0`	Enters the IP address and subnet mask.
Step 4	**exit** **Example:** `SwitchControllerDevice(config-vlan)# exit`	Returns to global configuration mode.
Step 5	**ip default-gateway** *ip-address* **Example:** `SwitchControllerDevice(config)# ip default-gateway 10.10.10.1`	Enters the IP address of the next-hop router interface that is directly connected to the switch where a default gateway is being configured. The default gateway receives IP packets with unresolved destination IP addresses from the switch. Once the default gateway is configured, the switch has connectivity to the remote networks with which a host needs to communicate.

	Command or Action	Purpose
		Note When your switch is configured to route with IP, it does not need to have a default gateway set. **Note** The switch capwap relays on default-gateway configuration to support routed access point join the switch.
Step 6	**end** **Example:** `SwitchControllerDevice(config)# end`	Returns to privileged EXEC mode.
Step 7	**show interfaces vlan** *vlan-id* **Example:** `SwitchControllerDevice# show interfaces vlan 99`	Verifies the configured IP address.
Step 8	**show ip redirects** **Example:** `SwitchControllerDevice# show ip redirects`	Verifies the configured default gateway.

Modifying the Switch Startup Configuration

Specifying the Filename to Read and Write the System Configuration

By default, the Cisco IOS software uses the config.text file to read and write a nonvolatile copy of the system configuration. However, you can specify a different filename, which will be loaded during the next boot cycle.

Before You Begin

Use a standalone switch for this task.

SUMMARY STEPS

1. **configure terminal**
2. **boot flash**:/*file-url*
3. **end**
4. **show boot**
5. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `SwitchControllerDevice#` **`configure terminal`**	Enters global configuration mode.
Step 2	**boot flash**:/*file-url* **Example:** `SwitchControllerDevice(config)#` **`boot flash:config.text`**	Specifies the configuration file to load during the next boot cycle. *file-url*—The path (directory) and the configuration filename. Filenames and directory names are case-sensitive.
Step 3	**end** **Example:** `SwitchControllerDevice(config)#` **`end`**	Returns to privileged EXEC mode.
Step 4	**show boot** **Example:** `SwitchControllerDevice#` **`show boot`**	Verifies your entries. The **boot** global configuration command changes the setting of the CONFIG_FILE environment variable.
Step 5	**copy running-config startup-config** **Example:** `SwitchControllerDevice#` **`copy running-config startup-config`**	(Optional) Saves your entries in the configuration file.

Manually Booting the Switch

By default, the switch automatically boots up; however, you can configure it to manually boot up.

Before You Begin

Use a standalone switch for this task.

SUMMARY STEPS

1. **configure terminal**
2. **boot manual**
3. **end**
4. **show boot**
5. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `SwitchControllerDevice# configure terminal`	Enters global configuration mode.
Step 2	**boot manual** **Example:** `SwitchControllerDevice(config)# boot manual`	Enables the switch to manually boot up during the next boot cycle.
Step 3	**end** **Example:** `SwitchControllerDevice(config)# end`	Returns to privileged EXEC mode.
Step 4	**show boot** **Example:** `SwitchControllerDevice# show boot`	Verifies your entries. The **boot manual** global command changes the setting of the MANUAL_BOOT environment variable. The next time you reboot the system, the switch is in boot loader mode, shown by the *switch:* prompt. To boot up the system, use the **boot** boot loader command in installed boot mode or bundle boot mode. • `switch: boot flash:packages.conf` • `switch: boot flash:cat3850-universalk9.SSA.03.08.83.EMD.150-8.83.EMD.bin` Filenames and directory names are case-sensitive.
Step 5	**copy running-config startup-config** **Example:** `SwitchControllerDevice# copy`	(Optional) Saves your entries in the configuration file.

	Command or Action	Purpose
	`running-config startup-config`	

Booting the SwitchControllerDevice in Installed Mode

SUMMARY STEPS

1. **cp** *source_file_path destination_file_path*
2. **software expand file** *source_file_path*
3. **reload**
4. **boot flash:packages.conf**
5. **show version**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**cp** *source_file_path destination_file_path* **Example:** `SwitchControllerDevice#` **`copy`** **`tftp://10.0.0.6/cat3k_caa-universalk9.SSA.03.12.02.EZP.150-12.02.EZP.150-12.02.EZP.bin`** **`flash:`**	(Optional) Copies the bin file (`image.bin`) from the FTP or TFTP server to flash or USB flash.

Step 2	**software expand file** *source_file_path*
	
	Example:
	Expanding the bin file from the TFTP server:
	`Switch#` **`software expand file`**
	`tftp://10.0.0.2/cat3k_caa-universalk9.SSA.03.09.37.EXP.150-9.37.EXP.bin to flash:`
	`Preparing expand operation ...`
	`[1]: Downloading file`
	`tftp://10.0.0.2/cat3k_caa-universalk9.SSA.03.09.37.EXP.150-9.37.EXP.bin to active switch 1`
	`[1]: Finished downloading file`
	`tftp://10.0.0.2/cat3k_caa-universalk9.SSA.03.09.37.EXP.150-9.37.`
	`EXP.bin to active switch 1`
	`[1]: Copying software from active switch 1 to switch 2`
	`[1]: Finished copying software to switch 2`
	`[1 2]: Expanding bundle cat3k_caa-universalk9.SSA.03.09.37.EXP.150-9.37.EXP.bin`
	`[1 2]: Copying package files`
	`[1 2]: Package files copied`
	`[1 2]: Finished expanding bundle cat3k_caa-universalk9.SSA.03.09.37.EXP.150-9.37.EXP.bin`
	
	`18 -rw- 74387812 Dec 7 2012 05:55:43 +00:00 cat3k_caa-base.SSA.03.09.37.EXP.pkg`
	
	`19 -rw- 2738868 Dec 7 2012 05:55:44 +00:00`
	`cat3k_caa-drivers.SSA.03.09.37.EXP.pkg`
	`20 -rw- 32465772 Dec 7 2012 05:55:44 +00:00`
		Expands the bin file stored in flash, FTP, TFTP, HTTP, or HTTPS server on the booted switch.
		Note Ensure that the `packages.conf` file is available in the expanded list.

	Command or Action	Purpose

	`cat3k_caa-infra.SSA.03.09.37.EXP.pkg`
	`21 -rw- 30389036 Dec 7 2012 05:55:44 +00:00`
	`cat3k_caa-iosd-universalk9.SSA.150-9.37.EXP.pkg`
	`22 -rw- 18342624 Dec 7 2012 05:55:44 +00:00`
	`cat3k_caa-platform.SSA.03.09.37.EXP.pkg`
	`23 -rw- 63374028 Dec 7 2012 05:55:44 +00:00 cat3k_caa-wcm.SSA.10.0.10.14.pkg`
	
	`17 -rw- 1239 Dec 7 2012 05:56:29 +00:00 packages.conf`	

Step 3	**reload** **Example:** `SwitchControllerDevice: reload`	Reloads the switch. **Note** You can boot the switch manually or automatically using the `packages.conf` file. If you are booting manually, you can proceed to Step 4. Otherwise, the switch boots up automatically.
Step 4	**boot flash:packages.conf** **Example:** `switch: boot flash:packages.conf`	Boots the switch with the `packages.conf` file.

Step 5	**show version**
	
	Example:
	`switch# show version`
	
	`Switch Ports Model SW Version SW Image Mode`
	`------ ----- ----- ---------- ---------- ----`
	`1 6 WS-C3850-6DS-S 03.09.26.EXP ct3850-ipservicesk9 INSTALL`
		Verifies that the switch is in the **INSTALL** mode.

Booting the SwitchControllerDevice in Bundle Mode

There are several methods by which you can boot the switch—either by copying the bin file from the TFTP server and then boot the switch, or by booting the switch straight from flash or USB flash using the commands **boot flash:<image.bin>** or **boot usbflash0:<image.bin>** .

The following procedure explains how to boot the switch from th TFTP server in the bundle mode.

SUMMARY STEPS

1. **cp** *source_file_path destination_file_path*
2. **switch:BOOT=<source path of .bin file>**
3. **boot**
4. **show version**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**cp** *source_file_path destination_file_path* **Example:** `SwitchControllerDevice#` **`copy`** **`tftp://10.0.0.6/cat3k_caa-universalk9.SSA.03.12.02.EZP.150-12.02.EZP.150-12.02.EZP.bin`** **`flash:`**	(Optional) Copies the bin file (`image.bin`) from the FTP or TFTP server to flash or USB flash.
Step 2	**switch:BOOT=<source path of .bin file>** **Example:** `SwitchControllerDevice:` **`switch:BOOT=tftp://10.0.0.2/cat3k_caa-universalk9.SSA.03.09.37.EXP.150-9.37.EXP.bin`**	Sets the boot parameters.
Step 3	**boot** **Example:** `switch:` **`boot`**	Boots the switch.

Step 4	**show version**
	
	Example:
	`switch#` **`show version`**
	`Switch Ports Model             SW Version        SW Image              Mode`
	`------ ----- -----             ----------        ----------            ----`
	`     1 6     WS-C3850-6DS-S    03.09.40.EXP      ct3850-ipservicesk9   BUNDLE`
		Verifies that the switch is in the **BUNDLE** mode.

Booting a Specific Software Image On a Switch Stack

SUMMARY STEPS

1. **configure terminal**
2. **boot system switch** {*number* | **all**} **flash:***image_file*| **tftp:** *image_file* | **usbflash0:** *image_file*
3. **end**
4. **show boot system**
5. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `SwitchControllerDevice# configure terminal`	Enters global configuration mode.
Step 2	**boot system switch** {*number* | **all**} **flash:***image_file*| **tftp:** *image_file* | **usbflash0:** *image_file* **Example:** `Switch(config)# boot system switch 2 flash:cat3850-universalk9.SSA.03.08.83.EMD.150-8.83.EMD.bin`	(Optional) For switches in a stack, specifies the switch members on which the system image is loaded during the next boot cycle: • Use *number* to specify a stack member. (Specify only one stack member.) • Use **all** to specify all stack members.
Step 3	**end** **Example:** `SwitchControllerDevice(config)# end`	Returns to privileged EXEC mode.
Step 4	**show boot system** **Example:** `SwitchControllerDevice# show boot system`	Verifies your entries. The **boot system** global command changes the setting of the BOOT environment variable. During the next boot cycle, the switch attempts to automatically boot up the system using information in the BOOT environment variable.
Step 5	**copy running-config startup-config** **Example:** `SwitchControllerDevice# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

Configuring a Scheduled Software Image Reload

This task describes how to configure your switch to reload the software image at a later time.

SUMMARY STEPS

1. **configure terminal**
2. **copy running-config startup-config**
3. **reload in** [*hh*:]*mm* [*text*]
4. **reload slot** [*stack-member-number*]
5. **reload at** *hh*: *mm* [*month day* | *day month*] [*text*]
6. **reload cancel**
7. **show reload**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `SwitchControllerDevice# configure terminal`	Enters global configuration mode.
Step 2	**copy running-config startup-config** **Example:** `copy running-config startup-config`	Saves your switch configuration information to the startup configuration before you use the **reload** command.

Step 3	**reload in** [*hh*:]*mm* [*text*]
	
	Example:
	`SwitchControllerDevice(config)# reload in 12`
	
	`System configuration has been modified. Save? [yes/no]: y`
		Schedules a reload of the software to take affect in the specified minutes or hours and minutes. The reload must take place within approximately 24 days. You can specify the reason for the reload in a string up to 255 characters in length.

Step 4	**reload slot** [*stack-member-number*]
	
	Example:
	`SwitchControllerDevice(config)# reload slot 6`
	
	`Proceed with reload? [confirm] y`
		Schedules a reload of the software in a switch stack.

Step 5	**reload at** *hh*: *mm* [*month day* | *day month*] [*text*] **Example:** `SwitchControllerDevice(config)# reload at 14:00`	Specifies the time in hours and minutes for the reload to occur. **Note** Use the **at** keyword only if the switch system clock has been set (through Network Time Protocol (NTP), the hardware calendar, or manually). The time is relative to the configured time zone on the switch. To schedule reloads across several switches to occur simultaneously, the time on each switch must be synchronized with NTP.

	Command or Action	Purpose
Step 6	**reload cancel** **Example:** `SwitchControllerDevice(config)# reload cancel`	Cancels a previously scheduled reload.
Step 7	**show reload** **Example:** `show reload`	Displays information about a previously scheduled reload or identifies if a reload has been scheduled on the switch.

Monitoring Switch Setup Configuration

Example: Verifying the Switch Running Configuration

```
SwitchControllerDevice# show running-config
Building configuration...

Current configuration: 1363 bytes
!
version 12.4
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname Stack1
!
enable secret 5 $1$ej9.$DMUvAUnZOAmvmgqBEzIxE0
!
.
<output truncated>
.
interface gigabitethernet6/0/2
mvr type source

<output truncated>

...!
interface VLAN1
 ip address 172.20.137.50 255.255.255.0
 no ip directed-broadcast
!
ip default-gateway 172.20.137.1 !
!
snmp-server community private RW
snmp-server community public RO
snmp-server community private@es0 RW
snmp-server community public@es0 RO
snmp-server chassis-id 0x12
!
end
```

Examples: Displaying Software Bootup in Install Mode

This example displays software bootup in install mode:

```
switch: boot flash:packages.conf

Getting rest of image
Reading full image into memory....done
Reading full base package into memory...: done = 74596432
Nova Bundle Image
--------------------------------------
Kernel Address : 0x6042f354
Kernel Size : 0x318412/3245074
Initramfs Address : 0x60747768
Initramfs Size : 0xdc08e8/14420200
Compression Format: .mzip

Bootable image at @ ram:0x6042f354
Bootable image segment 0 address range [0x81100000, 0x81b80000] is in range [0x80180000,
0x90000000].
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@boot_system:
 377
Loading Linux kernel with entry point 0x811060f0 ...
Bootloader: Done loading app on core_mask: 0xf

### Launching Linux Kernel (flags = 0x5)

All packages are Digitally Signed
Starting System Services
Nov 7 09:57:05 %IOSXE-1-PLATFORM: process stack-mgr: %STACKMGR-1-DISC_START: Switch 2 is
starting stack discovery
##########################################################################################
Nov 7 09:59:07 %IOSXE-1-PLATFORM: process stack-mgr: %STACKMGR-1-DISC_DONE: Switch 2 has
finished stack discovery
Nov 7 09:59:07 %IOSXE-1-PLATFORM: process stack-mgr: %STACKMGR-1-SWITCH_ADDED: Switch 2 has
 been added to the stack
Nov 7 09:59:14 %IOSXE-1-PLATFORM: process stack-mgr: %STACKMGR-1-ACTIVE_ELECTED: Switch 2
has been elected ACTIVE

Restricted Rights Legend

Use, duplication, or disclosure by the Government is
subject to restrictions as set forth in subparagraph
(c) of the Commercial Computer Software - Restricted
Rights clause at FAR sec. 52.227-19 and subparagraph
(c) (1) (ii) of the Rights in Technical Data and Computer
Software clause at DFARS sec. 252.227-7013.

cisco Systems, Inc.
170 West Tasman Drive
San Jose, California 95134-1706



Cisco IOS Software, IOS-XE Software, Catalyst L3 Switch Software (CAT3K_CAA-UNIVERSALK9-M),

Version 03.09.12.EMD EARLY DEPLOYMENT ENGINEERING NOVA_WEEKLY BUILD, synced to
DSGS_PI2_POSTPC_FLO_DSBU7_NG3K_1105
Copyright (c) 1986-2012 by Cisco Systems, Inc.
Compiled Sun 04-Nov-12 22:53 by gereddy
License level to iosd is ipservices
```

This example display software bootup in bundle mode:

```
switch: boot flash:cat3k_caa-universalk9.SSA.03.09.12.EMD.150-9.12.EMD.bin


Reading full image into
memory..................................................................done
Nova Bundle Image
```

```
--------------------------------------
Kernel Address : 0x6042ff38
Kernel Size : 0x318412/3245074
Initramfs Address : 0x6074834c
Initramfs Size : 0xdc08e8/14420200
Compression Format: .mzip

Bootable image at @ ram:0x6042ff38
Bootable image segment 0 address range [0x81100000, 0x81b80000] is in range [0x80180000,
0x90000000].
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
File "flash:cat3k_caa-universalk9.SSA.03.09.12.EMD.150-9.12.EMD.bin" uncompressed and
installed, entry point: 0x811060f0
Loading Linux kernel with entry point 0x811060f0 ...
Bootloader: Done loading app on core_mask: 0xf

### Launching Linux Kernel (flags = 0x5)

All packages are Digitally Signed
Starting System Services
Nov 7 09:45:49 %IOSXE-1-PLATFORM: process stack-mgr: %STACKMGR-1-DISC_START: Switch 2 is
starting stack discovery
##########################################################################################
Nov 7 09:47:50 %IOSXE-1-PLATFORM: process stack-mgr: %STACKMGR-1-DISC_DONE: Switch 2 has
finished stack discovery
Nov 7 09:47:50 %IOSXE-1-PLATFORM: process stack-mgr: %STACKMGR-1-SWITCH_ADDED: Switch 2 has
 been added to the stack
Nov 7 09:47:58 %IOSXE-1-PLATFORM: process stack-mgr: %STACKMGR-1-ACTIVE_ELECTED: Switch 2
has been elected ACTIVE

Restricted Rights Legend

Use, duplication, or disclosure by the Government is
subject to restrictions as set forth in subparagraph
(c) of the Commercial Computer Software - Restricted
Rights clause at FAR sec. 52.227-19 and subparagraph
(c) (1) (ii) of the Rights in Technical Data and Computer
Software clause at DFARS sec. 252.227-7013.

cisco Systems, Inc.
170 West Tasman Drive
San Jose, California 95134-1706



Cisco IOS Software, IOS-XE Software, Catalyst L3 Switch Software (CAT3K_CAA-UNIVERSALK9-M),
 Version 03.09.12.EMD
EARLY DEPLOYMENT ENGINEERING NOVA_WEEKLY BUILD, synced to DSGS_PI2_POSTPC_FLO_DSBU7_NG3K_1105
Copyright (c) 1986-2012 by Cisco Systems, Inc.
Compiled Sun 04-Nov-12 22:53 by gereddy
License level to iosd is ipservices
```

Related Topics

Software Boot Modes, on page 51

Installed Boot Mode, on page 51

Bundle Boot Mode, on page 51

Example: Emergency Installation

This sample output is an example when the **emergency-install** boot command is initiated:

```
switch: emergency-install
tftp://192.0.2.47/cat3k/cat3k_caa-universalk9.SSA.03.09.12.EMD.150-9.12.EMD.bin
```

```
The bootflash will be erased during install operation, continue (y/n)?y
Starting emergency recovery
(tftp://192.0.2.47/cat3k/cat3k_caa-universalk9.SSA.03.09.12.EMD.150-9.12.EMD.bin)...
Reading full image into memory......................done
Nova Bundle Image
--------------------------------------
Kernel Address : 0x6042e5cc
Kernel Size : 0x318261/3244641
Initramfs Address : 0x60746830
Initramfs Size : 0xdb0fb9/14356409
Compression Format: .mzip

Bootable image at @ ram:0x6042e5cc
Bootable image segment 0 address range [0x81100000, 0x81b80000] is in range [0x80180000,
0x90000000].
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
File "sda9:c3850-recovery.bin" uncompressed and installed, entry point: 0x811060f0
Loading Linux kernel with entry point 0x811060f0 ...
Bootloader: Done loading app on core_mask: 0xf

### Launching Linux Kernel (flags = 0x5)



Initiating Emergency Installation of bundle
tftp://172.19.211.47/cstohs/cat3k_caa-universalk9.SSA.03.09.12.EMD.150-9.12.EMD.bin


Downloading bundle
tftp://192.0.2.47/cat3k/cat3k_caa-universalk9.SSA.03.09.12.EMD.150-9.12.EMD.bin...
Validating bundle
tftp://192.0.2.47/cat3k/cat3k_caa-universalk9.SSA.03.09.12.EMD.150-9.12.EMD.bin...
Installing bundle
tftp://192.0.2.47/cat3k/cat3k_caa-universalk9.SSA.03.09.12.EMD.150-9.12.EMD.bin...
Verifying bundle
tftp://192.0.2.47/cat3k/cat3k_caa-universalk9.SSA.03.09.12.EMD.150-9.12.EMD.bin...
Package cat3k_caa-base.SSA.03.09.12.EMD.pkg is Digitally Signed
Package cat3k_caa-drivers.SSA.03.09.12.EMD.pkg is Digitally Signed
Package cat3k_caa-infra.SSA.03.09.12.EMD.pkg is Digitally Signed
Package cat3k_caa-iosd-universalk9.SSA.150-9.12.EMD.pkg is Digitally Signed
Package cat3k_caa-platform.SSA.03.09.12.EMD.pkg is Digitally Signed
Package cat3k_caa-wcm.SSA.03.09.12.EMD.pkg is Digitally Signed
Preparing flash...
Syncing device...
Emergency Install successful... Rebooting
Restarting system.


Booting...(use DDR clock 667 MHz)Initializing and Testing RAM +++@@@@####...++@@++@@++@@++@
```

Related Topics

[Software Boot Modes, on page 51]
[Installed Boot Mode, on page 51]
[Bundle Boot Mode, on page 51]

Configuration Examples for Performing Switch Setup

Example: Configuring a Switch as a DHCP Server

```
SwitchControllerDevice# configure terminal
SwitchControllerDevice(config)# ip dhcp pool pool1
SwitchControllerDevice(dhcp-config)# network 10.10.10.0 255.255.255.0
SwitchControllerDevice(dhcp-config)# boot config-boot.text
SwitchControllerDevice(dhcp-config)# default-router 10.10.10.1
SwitchControllerDevice(dhcp-config)# option 150 10.10.10.1
SwitchControllerDevice(dhcp-config)# exit
SwitchControllerDevice(config)# tftp-server flash:config-boot.text
SwitchControllerDevice(config)# interface gigabitethernet1/0/4
SwitchControllerDevice(config-if)# no switchport
SwitchControllerDevice(config-if)# ip address 10.10.10.1 255.255.255.0
SwitchControllerDevice(config-if)# end
```

Related Topics

Configuring DHCP Autoconfiguration (Only Configuration File), on page 61

Example: Configuring DHCP Auto-Image Update

```
SwitchControllerDevice# configure terminal
SwitchControllerDevice(config)# ip dhcp pool pool1
SwitchControllerDevice(dhcp-config)# network 10.10.10.0 255.255.255.0
SwitchControllerDevice(dhcp-config)# boot config-boot.text
SwitchControllerDevice(dhcp-config)# default-router 10.10.10.1
SwitchControllerDevice(dhcp-config)# option 150 10.10.10.1
SwitchControllerDevice(dhcp-config)# option 125 hex
0000.0009.0a05.08661.7574.6f69.6e73.7461.6c6c.5f64.686370
SwitchControllerDevice(dhcp-config)# exit
SwitchControllerDevice(config)# tftp-server flash:config-boot.text
SwitchControllerDevice(config)# tftp-server flash:image_name
SwitchControllerDevice(config)# tftp-server flash:boot-config.text
SwitchControllerDevice(config)# tftp-server flash: autoinstall_dhcp
SwitchControllerDevice(config)# interface gigabitethernet1/0/4
SwitchControllerDevice(config-if)# no switchport
SwitchControllerDevice(config-if)# ip address 10.10.10.1 255.255.255.0
SwitchControllerDevice(config-if)# end
```

Related Topics

Configuring DHCP Auto-Image Update (Configuration File and Image), on page 63

Example: Configuring a Switch to Download Configurations from a DHCP Server

This example uses a Layer 3 SVI interface on VLAN 99 to enable DHCP-based autoconfiguration with a saved configuration:

```
SwitchControllerDevice# configure terminal
SwitchControllerDevice(config)# boot host dhcp
SwitchControllerDevice(config)# boot host retry timeout 300
SwitchControllerDevice(config)# banner config-save ^C Caution - Saving Configuration File
to NVRAM May Cause You to No longer Automatically Download Configuration Files at Reboot^C
SwitchControllerDevice(config)# vlan 99
SwitchControllerDevice(config-vlan)# interface vlan 99
SwitchControllerDevice(config-if)# no shutdown
SwitchControllerDevice(config-if)# end
SwitchControllerDevice# show boot
BOOT path-list:
Config file:          flash:/config.text
Private Config file:  flash:/private-config.text
Enable Break:         no
Manual Boot:          no
HELPER path-list:
NVRAM/Config file
      buffer size:    32768
Timeout for Config
          Download:    300 seconds
Config Download
       via DHCP:       enabled (next boot: enabled)
SwitchControllerDevice#
```

Related Topics

Configuring the Client to Download Files from DHCP Server, on page 67

Examples: Scheduling Software Image Reload

This example shows how to reload the software on the switch on the current day at 7:30 p.m:

```
SwitchControllerDevice# reload at 19:30
Reload scheduled for 19:30:00 UTC Wed Jun 5 2013 (in 2 hours and 25 minutes)
Proceed with reload? [confirm]
```

This example shows how to reload the software on the switch at a future time:

```
SwitchControllerDevice# reload at 02:00 jun 20
Reload scheduled for 02:00:00 UTC Thu Jun 20 2013 (in 344 hours and 53 minutes)
Proceed with reload? [confirm]
```

Additional References For Performing Switch Setup

Related Documents

Related Topic	Document Title
Switch setup commands Boot loader commands	*System Management Command Reference (Catalyst 3850 Switches)*
Pre-download feature	*System Management Configuration Guide (Cisco WLC 5700 Series)*
IOS XE DHCP configuration	*IP Addressing Configuration Guide Library, Cisco IOS XE Release 3S (Catalyst 3850 Switches)*
Hardware installation	*Catalyst 3850 Switch Hardware Installation Guide*
Platform-independent command references	*Configuration Fundamentals Command Reference, Cisco IOS XE Release 3S (Catalyst 3850 Switches)*
Platform-independent configuration information	*Configuration Fundamentals Configuration Guide, Cisco IOS XE Release 3S (Catalyst 3850 Switches)*

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

Feature History and Information For Performing Switch Setup Configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This feature was introduced.

CHAPTER 5

Configuring Right-To-Use Licenses

Finding Feature Information

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

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

Related Topics

Feature History and Information for Troubleshooting Software Configuration, on page 336

Restrictions for Configuring RTU Licenses

The following are the restrictions for configuring and using RTU licenses.

- AP count licenses can be ordered and pre-activated on your switch.

- Imaged based licenses can be upgraded. AP count licenses can be deactivated and moved between switches and controllers.
- To activate a permanent license, you must reboot your switch after configuring the new image level. The AP-count license does not require a reboot to activate.
- An expired image based evaluation license can not be reactivated after reboot.
- Stack members of a switch stack must run the same license level.
- Your switch is pre-installed with the image that you ordered. If an image was not pre-ordered, then the switch is booted with a LAN base image by default.
- Adder AP-count licenses are installed in the factory.

Related Topics

Activating an Imaged Based License, on page 91
Examples: Activating RTU Image Based Licenses, on page 97

Information About Configuring RTU Licenses

Right-To-Use Licensing

Right-to-use (RTU) licensing allows you to order and activate a specific license type and level, and then to manage license usage on your switch. The types of licenses available to order are:

- Permanent licenses—Purchased with a specific feature set with no expiration date.
- Evaluation licenses—Pre-installed on the switch and is valid for only a 90 day in-use period.

To activate a permanent or evaluation license, you are required to accept the End-User License Agreement (EULA). For the evaluation license, you are notified to purchase a permanent license or deactivate the license before the 90 day period expires.

A permanent license can be moved from one device to another. To activate a license, you must reboot your switch.

An evaluation license is a manufacturing image on your switch and is not transferable to another switch. This type of license cannot be reactivated after reboot.

Related Topics

Activating an Imaged Based License, on page 91
Examples: Activating RTU Image Based Licenses, on page 97

Right-To-Use Image Based Licenses

Right-to-use imaged licenses support a set of features based on a specific image-based license:

- LAN Base—Layer 2 features.

- IP Base—Layer 2 and Layer 3 features.
- IP Services—Layer 2, Layer 3, and IPv6 features. (Applicable only to switches and not controllers.)

The default image based license is LAN Base.

Right-To-Use License States

After you configure a specific license type and level, you can manage your licenses by monitoring the license state.

Table 8: RTU License States

License State	Description
Active, In Use	EULA was accepted and the license is in use after device reboot.
Active, Not In Use	EULA was accepted and the switch is ready to use when the license is enabled.
Not Activated	EULA was not accepted.

Guidelines to follow when monitoring your image based license state:

- A purchased permanent license is set to *Active, In Use* state only after a switch reboot.
- If more than one license was purchased, a reboot will activate the license with the highest feature set. For instance, the IP Services license is activated and not the LAN Base license.
- Remaining licenses purchased after switch reboot, stay in **Active, Not In Use** state.

Note For the AP count license, to change the state to Active, In Use, you must first make sure that the evaluation AP count license is deactivated.

License Activation for Switch Stacks

Right-to-use licensing is supported on switch stacks. A switch is a set of up to nine stacking-capable switches connected through theirStackWise-480 ports. You can connect only one switch type in a stack. One switch in the stack is identified as the active switch and the remaining switches are standby switches. The active switch is the switch that is activated with an RTU license and from its active console, the license level for the standby switches in the stack can be activated at the same time.

A new switch is allowed to join the switch stack if its license level matches. If there is a mismatch, then the active switch can reconfigure the license level and reboot it to allow it to join the stack.

Mobility Controller Mode

AP-count licenses are used only when the switch is in Mobility Controller mode. The MC is the gatekeeper for tracking the AP-count licenses and allows an access point to join or not.

Management of AP-count licenses is performed by the switch in mobility controller mode configurable through the CLI.

Related Topics

Changing Mobility Mode, on page 95

Right-To-Use AP-Count Licensing

Right-to-use licensing (RTU) allows you to order and activate a specific license type, and then to manage license usage on your switch.

You can order your switch with support for a specific number of adder access point count licenses, but the total number of licenses ordered should not exceed 50. You can also order your adder access point count licenses after receiving the switch.

For example, if you have ordered 50 new adder licenses, you can add only those ordered adder licenses to the switch. The licenses can be added in increments of 1, but the total number of licenses added for the switch should not exceed 50 .

You can configure your switch to manage the access point count licenses and view the number of access points currently in use from the CLI.

The following are two different types of access point licenses:

1. Permanent licenses for the access points
    - Adder access point count license—You can purchase the adder license to increase the switch capacity at a later time. You can transfer the adder access point count license from one switch to another.
2. Evaluation licenses for the access points
    - You can activate these licenses to evaluate more access points before purchasing the licenses.
    - The maximum number of access points that can be evaluated is 50 .
    - The evaluation period for using the access point licenses is 90 days.
    - You can activate and deactivate the evaluation licenses from the CLI.

Related Topics

Activating an AP-Count License, on page 93
Obtaining an Upgrade or Capacity Adder License, on page 93
Rehosting a License, on page 94

Right-to-Use AP-Count Evaluation Licenses

If you are considering upgrading to a license with a higher access point count, you can try an evaluation license before upgrading to a permanent version of the license. For example, if you are using a permanent license with a 10 access-point count and want to try an evaluation license with a 40-access-point count, you can try out the evaluation license for 90 days.

When an evaluation license is activated, the permanent AP-count licenses are ignored. The maximum supported licenses of 50 access points are available for 90 days.

To prevent disruptions in operation, the switch does not change licenses when an evaluation license expires. A warning expiry message is displayed daily starting five days prior to the expiry date. After 90 days, the evaluation license expires with a warning message. You must disable the evaluation license and then purchase the permanent license.

When the switch reboots after the evaluation license expiry, the license defaults to a permanent license.

Related Topics

Activating an AP-Count License, on page 93

Obtaining an Upgrade or Capacity Adder License, on page 93

Rehosting a License, on page 94

Right-To-Use Adder AP-Count Rehosting Licenses

Revoking a license from one device and installing it on another is called rehosting. You might want to rehost a license to change the purpose of a device.

To rehost a license, you must deactivate the adder ap-count license from one device and activate the same license on another device.

Evaluation licenses cannot be rehosted.

How to Configure RTU Licenses

Activating an Imaged Based License

SUMMARY STEPS

1. **license right-to-use activate**{**ipbase** |**ipservices** | **lanbase**} {**all** | **evaluation all** } [**slot** *slot-number*] [**acceptEULA**]
2. **reload** [*LINE* | **at** | **cancel** | **in** | **slot** *stack-member-number* | **standby-cpu**]
3. **show license right-to-use usage** [**slot** *slot-number*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**license right-to-use activate**{**ipbase** |**ipservices** | **lanbase**} {**all** | **evaluation all** } [**slot** *slot-number*] [**acceptEULA**] **Example:** `SwitchControllerDevice#` **`license right-to-use activate ipservices all acceptEULA`**	Activates a type of image based license. Activation can happen on all switches and also include the EULA acceptance. **Note** If you do not accept EULA, the modified configuration will not take effect after reload. The default license (or a license that was not deactivated) becomes active after reload.
Step 2	**reload** [*LINE* | **at** | **cancel** | **in** | **slot** *stack-member-number* | **standby-cpu**] **Example:** `SwitchControllerDevice#` **`reload slot 1`** `Proceed with reload? [confirm]` **`y`**	Reloads a specific stack member to complete the activation process for the RTU adder AP-count license. **Note** The reminder to accept a EULA is displayed after reload if it was not accepted earlier.

Step 3	**show license right-to-use usage** [**slot** *slot-number*]
	
	Example:
	
	`SwitchControllerDevice#` **`show license right-to-use usage`**
	
	`Slot#  License Name   Type   usage-duration(y:m:d)  In-Use  EULA`
	`----------------------------------------------------------------------`
	`1  ipservices  permanent  0 :10 :0  yes  yes`
	`1  ipbase  permanent  0 :0 :0  no  no`
	`1  ipbase  evaluation  0 :0 :0  no  no`
	`1  lanbase  permanent  0 :0 :7  no  yes`
	`1  apcount  evaluation  0 :0 :0  no  no`
	`1  apcount  base  0 :0 :0  no  no`
	`1  apcount  adder  0 :0 :0  no  no`
	
	`Switch#`
		Displays detailed usage information.

Related Topics

Restrictions for Configuring RTU Licenses, on page 87
Right-To-Use Licensing, on page 88
Monitoring and Maintaining RTU Licenses, on page 96
Examples: Activating RTU Image Based Licenses, on page 97

Activating an AP-Count License

SUMMARY STEPS

1. **license right-to-use activate**{**apcount** *ap-number* **slot** *slot-num*} | **evaluation**} [**acceptEULA**]
2. **show license right-to-use usage** [**slot** *slot-number*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**license right-to-use activate**{**apcount** *ap-number* **slot** *slot-num*} | **evaluation**} [**acceptEULA**] **Example:** `SwitchControllerDevice# license right to use activate apcount 5 slot 1 acceptEULA`	Activates one or more adder AP-count licenses and immediately accepts the EULA.
Step 2	**show license right-to-use usage** [**slot** *slot-number*] **Example:** (see below)	Displays detailed usage information.

Step 2 example:

```
SwitchControllerDevice# show license right-to-use usage

 Slot#  License Name     Type     usage-duration(y:m:d)  In-Use  EULA
-----------------------------------------------------------------------

1       ipservices      permanent  0 :3 :29              yes    yes
1       ipservices      evaluation 0 :0 :0               no     no
1       ipbase          permanent  0 :0 :0               no     no
1       ipbase          evaluation 0 :0 :0               no     no
1       lanbase         permanent  0 :0 :0               no     no
1       apcount         evaluation 0 :3 :11              no     no
1       apcount         base       0 :0 :0               no     yes
1       apcount         adder      0 :0 :17              yes    yes


Switch#
```

Related Topics

Monitoring and Maintaining RTU Licenses, on page 96
Right-To-Use AP-Count Licensing, on page 90
Right-to-Use AP-Count Evaluation Licenses, on page 91

Obtaining an Upgrade or Capacity Adder License

You can use the capacity adder licenses to increase the number of access points supported by the switch.

SUMMARY STEPS

1. **license right-to-use** {**activate** | **deactivate**} **apcount** {*ap-number* | **evaluation** } **slot** *slot-num* [**acceptEULA**]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**license right-to-use** {**activate** | **deactivate**} **apcount** {*ap-number* | **evaluation** } **slot** *slot-num* [**acceptEULA**] **Example:** `SwitchControllerDevice# license right to use activate apcount 5 slot 2 acceptEULA`	Activates one or more adder AP-count licenses and immediately accepts the EULA.

Related Topics

Right-to-Use AP-Count Evaluation Licenses, on page 91
Right-To-Use AP-Count Licensing, on page 90

Rehosting a License

To rehost a license, you have to deactivate the license from one switch and then activate the same license on another switch.

SUMMARY STEPS

1. **license right-to-use deactivate apcount** *ap-number* **slot** *slot-num* [**acceptEULA**]
2. **license right-to-use activate apcount** *ap-number* **slot** *slot-num* [**acceptEULA**]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**license right-to-use deactivate apcount** *ap-number* **slot** *slot-num* [**acceptEULA**] **Example:** `SwitchControllerDevice# license right to use deactivate apcount 1 slot 1 acceptEULA`	Deactivates the license on one switch.

	Command or Action	Purpose
Step 2	**license right-to-use activate apcount** *ap-number* **slot** *slot-num* [**acceptEULA**] **Example:** `SwitchControllerDevice# license right to use activate apcount 2 slot 2 acceptEULA`	Activates the license on another switch.

Related Topics

Right-To-Use AP-Count Licensing, on page 90
Right-to-Use AP-Count Evaluation Licenses, on page 91

Changing Mobility Mode

SUMMARY STEPS

1. **wireless mobility controller**
2. **write memory**
3. **reload** [*LINE* | **at** | **cancel** | **in** | **slot** *stack-member-number* | **standby-cpu**]
4. **no wireless mobility controller**
5. **write memory**
6. **reload** [*LINE* | **at** | **cancel** | **in** | **slot** *stack-member-number* | **standby-cpu**]

DETAILED STEPS

	Command or Action	Purpose

Step 1	**wireless mobility controller**
	
	Example:
	`SwitchControllerDevice(config)# wireless mobility controller`
	`%`
	`Mobility role changed to Mobility Controller.`
	`Please save config and reboot the whole stack.`
		Changes a switch in Mobility Agent mode to Mobility Controller mode.

Step 2	**write memory**
	
	Example:
	`SwitchControllerDevice# write memory`
	
	`Building configuration...`
	`Compressed configuration from 13870 bytes to 5390 bytes[OK]`
	`SwitchControllerDevice#`	

	Command or Action	Purpose

Step 3	**reload** [*LINE* | **at** | **cancel** | **in** | **slot** *stack-member-number* | **standby-cpu**]
	
	Example:
	`SwitchControllerDevice# reload slot 3`
	`Proceed with reload? [confirm] y`	

Step 4	**no wireless mobility controller**
	
	Example:
	`SwitchControllerDevice(config)# no wireless mobility controller`
	`%`
	`Mobility role changed to Mobility Agent.`
	`Please save config and reboot the whole stack.`
	`Switch(config)#`
		Changes a switch in Mobility Controller mode to Mobility Agent mode.

Step 5	**write memory**
	
	Example:
	`SwitchControllerDevice# write memory`
	
	`Building configuration...`
	`Compressed configuration from 13870 bytes to 5390 bytes[OK]`
	`SwitchControllerDevice#`	

Step 6	**reload** [*LINE* | **at** | **cancel** | **in** | **slot** *stack-member-number* | **standby-cpu**]
	
	Example:
	`SwitchControllerDevice# reload slot 3`
	`Proceed with reload? [confirm] y`	

Related Topics

Mobility Controller Mode, on page 90

Monitoring and Maintaining RTU Licenses

Command	Purpose
show license right-to-use default	Displays the default license information.
show license right-to-use detail	Displays detailed information of all the licenses in the switch stack.
show license right-to-use eula {adder | evaluation | permanent}	Displays the end user license agreement.
show license right-to-use mismatch	Displays the license information that does not match.

Command	Purpose
show license right-to-use slot *slot-number*	Displays the license information for a specific slot in a switch stack.
show license right-to-use summary	Displays a summary of the license information on the entire switch stack.
show license right-to-use usage [**slot** *slot-number*]	Displays detailed information about usage for all licenses in the switch stack.
show switch	Displays detailed information of every member in a switch stack including the state of the license.

Related Topics

Activating an Imaged Based License, on page 91
Examples: Activating RTU Image Based Licenses, on page 97
Activating an AP-Count License, on page 93

Configuration Examples for RTU Licensing

Examples: Activating RTU Image Based Licenses

This example shows how to activate an IP Services image license and accept the EULA for a specific slot:

```
Switch# license right-to-use activate ipservices slot 1 acceptEULA
% switch-1:stack-mgr:Reboot the switch to invoke the highest activated License level
```

This example shows how to activate a license for evaluation:

```
Switch# license right-to-use activate ipservices evaluation acceptEULA
% switch-1:stack-mgr:Reboot the switch to invoke the highest activated License level
```

Related Topics

Activating an Imaged Based License, on page 91
Restrictions for Configuring RTU Licenses, on page 87
Right-To-Use Licensing, on page 88
Monitoring and Maintaining RTU Licenses, on page 96

Examples: Displaying RTU Licensing Information

This example shows the consolidated RTU licensing information from the active switch on a switch stack. All of the members in the stack have the same license level. When the evaluation AP-count license is activated, the adder AP-count licenses are ignored. The maximum number of AP-count licenses are available when evaluation is enabled.

```
Switch# show license right-to-use summary

 License Name    Type           Count   Period left
-------------------------------------------------------
  ipservices     permanent        10      Lifetime
  apcount        evaluation       40        90

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

License Level In Use: ipservices
License Level on Reboot: ipbase
Evaluation AP-Count: Enabled
Total AP Count Licenses: 50
AP Count Licenses In-use: 10
AP Count Licenses Remaining: 40
```

This example shows a summary of permanent and adder licenses. The evaluation AP-count license is disabled displaying the total number of activated adder AP-count licenses in the switch stack. AP-count licenses in-use mean that they are connected.

```
Switch# show license right-to-use summary

  License Name    Type          Count      Period left
-------------------------------------------------------------
  ipservices     permanent      N/A         Lifetime
  apcount        base           0
  apcount        adder          40          Lifetime

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

License Level In Use: ipservices
License Level on Reboot: ipservices eval
Evaluation AP-Count: Disabled
Total AP Count Licenses: 40
AP Count Licenses In-use: 10
AP Count Licenses Remaining: 30
```

This example shows the RTU default licenses. Default licenses are pre-installed and cannot be removed or transferred. If no license is activated the switch uses the default license, after a reboot.

```
Switch# show license right-to-use default

 Slot#    License Name    Type           Count
----------------------------------------------------
 1        ipservices      permanent     N/A
 1        apcount         base          0
 1        apcount         adder         10

 Slot#    License Name    Type           Count
----------------------------------------------------
 2        ipservices      permanent     N/A
 2        apcount         base          0
 2        apcount         adder         10

 Slot#    License Name    Type           Count
----------------------------------------------------
 3        ipservices      permanent     N/A
```

```
3        apcount         base          0
3        apcount         adder         10
```

Example: Displaying RTU License Details

This example shows all the detailed information for the RTU licenses on slot 1:

```
Switch# show license right-to-use detail slot 1

Index 1:  License Name: ipservices
           Period left: Lifetime
           License Type: permanent
           License State: Active, In use
           License Count: Non-Counted
           License Location: Slot 1
Index 2:  License Name: ipservices
           Period left: 90
           License Type: evaluation
           License State: Not Activated
           License Count: Non-Counted
           License Location: Slot 1
Index 3:  License Name: ipbase
           Period left: Lifetime
           License Type: permanent
           License State: Active, Not In use
           License Count: Non-Counted
           License Location: Slot 1
Index 4:  License Name: ipbase
           Period left: 90
           License Type: evaluation
           License State: Not Activated
           License Count: Non-Counted
           License Location: Slot 1
           License Location: Standby Switch 1
Index 5:  License Name: lanbase
           Period left: Lifetime
           License Type: permanent
           License State: Not Activated
           License Count: Non-Counted
           License Location: Slot 1
Index 6:  License Name: apcount
           Period left: 90
           License Type: evaluation
           License State: Active, In use
           License Count: 50
           License Location: Slot 1
Index 7:  License Name: apcount
           Period left: Lifetime
           License Type: base
           License State: Active, Not In use
           License Count: 0
           License Location: Slot 1
Index 8:  License Name: apcount
           Period left: Lifetime
           License Type: adder
           License State: Active, Not In use
           License Count: 10
           License Location: Slot 1
```

Example: Displaying RTU License Mismatch

This example shows the license information of the switches in a stack and a mismatch state of a member switch. The member must match the active.

```
Switch# show switch

Switch/Stack Mac Address : 6400.f125.0c80
                                                 H/W   Current
Switch#   Role        Mac Address     Priority Version  State
-------------------------------------------------------------------------------
 1       Standby     6400.f125.1b00     1       0        Ready
*2       Active      6400.f125.0c80     1       V01      Ready
 3       Member      6400.f125.1780     1       0        Lic-Mismatch
```

Note To resolve the license mismatch, first check the RTU license summary:

```
Switch# show switch right-to-use summary
```

Then change the license level of the mismatched switched so that it is the same license level of the active switch. This example shows that the IP Base license was activated for the member switch to match the active switch.

```
Switch# license right-to-use activate ipbase slot 1 acceptEULA
```

Example: Displaying RTU Licensing Usage

This example shows the detailed licensing usage on your switch stack. The IP Services license in Slot 1 is permanent and usage is one day. An AP-count license in Slot 2 is ready for evaluation. EULA was accepted and state shows in use, but after reboot the evaluation license will be deactivated.

```
Switch# show license right-to-use usage

 Slot#  License Name     Type     usage-duration(y:m:d)  In-Use  EULA
------------------------------------------------------------------------------------------

 1      ipservices     permanent      0 :0 :1            yes     yes
 1      ipservices     evaluation     0 :0 :0            no      no
 1      ipbase         permanent      0 :0 :0            no      yes
 1      ipbase         evaluation     0 :0 :0            no      no
 1      lanbase        permanent      0 :0 :0            no      no
 1      apcount        evaluation     0 :0 :0            yes     yes
 1      apcount        base           0 :0 :0            no      yes
 1      apcount        adder          0 :0 :0            no      yes

 Slot#  License Name     Type     usage-duration(y:m:d)  In-Use  EULA
------------------------------------------------------------------------------------------

 2      ipservices     permanent       0 :0 :1           yes     no
 2      ipservices     evaluation      0 :0 :0           no      yes
 2      ipbase         permanent       0 :0 :0           no      yes
 2      ipbase         evaluation      0 :0 :0           no      no
 2      lanbase        permanent       0 :0 :0           no      no
```

```
2      apcount        evaluation      0 :0 :0          yes     yes
2      apcount        base            0 :0 :0          no      yes
2      apcount        adder           0 :0 :0          no      no

Slot#  License Name     Type     usage-duration(y:m:d)  In-Use  EULA
-----------------------------------------------------------------------------------------

3      ipservices     permanent       0 :0 :1          yes     yes
3      ipservices     evaluation      0 :0 :0          no      no
3      ipbase         permanent       0 :0 :0          no      no
3      ipbase         evaluation      0 :0 :0          no      no
3      lanbase        permanent       0 :0 :0          no      no
3      apcount        evaluation      0 :0 :0          yes     yes
3      apcount        base            0 :0 :0          no      yes
3      apcount        adder           0 :0 :0          no      no
```

Additional References for RTU Licensing

Related Documents

Related Topic	Document Title
RTU commands	*System Management Command Reference (Catalyst 3850 Switches)*
RTU AP image preload feature	*System Management Configuration Guide (Cisco WLC 5700 Series)*

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

Feature History and Information for RTU Licensing

Release	Feature Information
Cisco IOS XE 3.2SE	This feature was introduced.

CHAPTER 6

Configuring Administrator Usernames and Passwords

Finding Feature Information

Your software release may not support all of 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 Administrator Usernames and Passwords

You can configure administrator usernames and passwords to prevent unauthorized users from reconfiguring the switch and viewing configuration information. This section provides instructions for initial configuration and for password recovery.

You can also set administrator usernames and passwords to manage and configure one or more access points that are associated with the switch.

Strong Passwords

You can set strong administrator passwords such as encrypted passwords with ASCII keys for the administrator user for managing access points.

Use the following guidelines while creating strong passwords:

- There should be at least three of the following categories—lowercase letters, uppercase letters, digits, and special characters.
- The new password should not be the same as that of the associated username and the username should not be reversed.
- The characters in the password should not be repeated more than three times consecutively.
- The password should not be **cisco**, **ocsic**, **admin**, **nimda**, or any variant obtained by changing the capitalization of letters therein, or by substituting "1" "|" or "!" for i, and/or substituting "0" for "o", and/or substituting "$" for "s".
- The maximum number of characters accepted for the username and password is 32.

Encrypted Passwords

You can set three types of keys for the password:

- Randomly generated key—This key is generated randomly and it is the most secure option. To export the configuration file from one system to another, the key should also be exported.
- Static key—The simplest option is to use a fixed (static) encryption key. By using a fixed key, no key management is required, but if the key is somehow discovered, the data can be decrypted by anyone with the knowledge of that key. This is not a secure option and it is called obfuscation in the CLI.
- User defined key—You can define the key by yourself. To export the configuration file from one system to another, both systems should have the same key configured.

Configuring Administrator Usernames and Passwords

SUMMARY STEPS

1. **configure terminal**
2. **wireless security strong-password**
3. **username** *admin-username* **password** **{0** *unencrypted_password* **| 7** *hidden_password* **|** *unencrypted_text***}**
4. **username** *admin-username* **secret** **{0** *unencrypted_secret_text* **| 4** *SHA256 encrypted_secret_text* **| 5** *MD5 encrypted_secret_text* **| LINE}**
5. **ap mgmtuser username** *username* **password {0** *unencrypted password* **| 8** *AES encrypted password* **}secret {0** *unencrypted password* **| 8** *AES encrypted password* **}**
6. **ap dot1x username** *username* **password {0** *unencrypted password* **| 8** *AES encrypted password* **}**
7. **end**
8. **ap name apname mgmtuser username** *username***password** *password* **secret** *secret _text*
9. **ap name apname dot1x-user** *username* **password** *password*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `SwitchControllerDevice# configure terminal`	Enters global configuration mode.
Step 2	**wireless security strong-password** **Example:** `SwitchControllerDevice(config)# wireless security strong-password`	Enables strong password policy for the administrator user.
Step 3	**username** *admin-username* **password** **{0** *unencrypted_password* **| 7** *hidden_password* **|** *unencrypted_text***}** **Example:** `SwitchControllerDevice(config)# username adminuser1 password 0 QZsek239@`	Specifies a username and password for an administrator. The administrator can configure the switch and view the configured information.
Step 4	**username** *admin-username* **secret** **{0** *unencrypted_secret_text* **| 4** *SHA256 encrypted_secret_text* **| 5** *MD5 encrypted_secret_text* **| LINE}** **Example:** `SwitchControllerDevice(config)# username adminuser1 secret 0 QZsek239@`	Specifies the secret for the administrator.
Step 5	**ap mgmtuser username** *username* **password {0** *unencrypted password* **| 8** *AES encrypted password* **}secret {0** *unencrypted password* **| 8** *AES encrypted password* **}** **Example:** `SwitchControllerDevice(config)# ap mgmtuser username cisco password 0 Qwci12@ secret 0 Qwci14@!`	Specifies administrator username and password for managing all of the access points configured to the switch. You can also include the secret text to perform privileged access point management. **Note** If your password is not strong enough to fulfill the strong password policy, then the password is rejected with a valid error message. For example, the following password is rejected because it is not a strong password. `SwitchControllerDevice# ap mgmtuser username cisco password 0 abcd secret 0 1234`
Step 6	**ap dot1x username** *username* **password {0** *unencrypted password* **| 8** *AES encrypted password* **}** **Example:** `SwitchControllerDevice(config)# ap dot1x username cisco password 0 Qwci12@`	Specifies the 802.1X username and password for managing all of the access points configured to the switch.

	Command or Action	Purpose
Step 7	**end** **Example:** `SwitchControllerDevice(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.
Step 8	**ap name apname mgmtuser username** *username***password** *password* **secret** *secret _text* **Example:** `SwitchControllerDevice# ap name APf0f7.55c7.7b23 mgmtuser username cisco password Qne35! secret Nzep592$`	Configures the administrator username, password, and secret text for managing a specific access point that is configured to the switch.
Step 9	**ap name apname dot1x-user** *username* **password** *password* **Example:** `SwitchControllerDevice# ap name APf0f7.55c7.7b23 dot1x-user username cisco password Qne35!`	Configures the 802.1X username and password for a specific access point.

Examples: Administrator Usernames and Passwords Configuration

This example shows how to configure administrator usernames and passwords with the strong password policy in configuration mode:

```
SwitchControllerDevice# configure terminal
SwitchControllerDevice(config)# wireless security strong-password
SwitchControllerDevice(config)# username adminuser1 password 0 QZsek239@
SwitchControllerDevice(config)# ap mgmtuser username cisco password 0 Qwci12@ secret 0
Qwci14@!
SwitchControllerDevice(config)# ap dot1x username cisco password 0 Qwci12@
SwitchControllerDevice# end
```

This example shows how to configure administrator usernames and passwords for an access point in global EXEC mode:

```
SwitchControllerDevice# wireless security strong-password
SwitchControllerDevice# ap name APf0f7.55c7.7b23 mgmtuser username cisco password Qwci12@
secret Qwci14@
SwitchControllerDevice# ap name APf0f7.55c7.7b23 dot1x-user username cisco password Qwci12@
SwitchControllerDevice# end
```

Additional References for Administrator Usernames and Passwords

Related Documents

Related Topic	Document Title
System management commands	*System Management Command Reference Guide (Cisco IOS XE Release 3SE (Cisco WLC 5700 Series)*

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

Feature History and Information For Performing Administrator Usernames and Passwords Configuration

Release	Feature Information
Cisco IOS XE 3.2SE	This feature was introduced.

CHAPTER 7

Configuring 802.11 parameters and Band Selection

Finding Feature Information

Your software release may not support all of 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.

Restrictions on Band Selection, 802.11 Bands, and Parameters

- Band-selection enabled WLANs do not support time-sensitive applications like voice and video because of roaming delays.
- Band selection can be used only with Cisco Aironet 1040, 1140, 1250, 1260, 3500, and the 3600 series access points.

- Band selection operates only on access points that are connected to a controller. A FlexConnect access point without a controller connection does not perform band selection after a reboot.
- The band-selection algorithm directs dual-band clients only from the 2.4-GHz radio to the 5-GHz radio of the same access point, and it only runs on an access point when both the 2.4-GHz and 5-GHz radios are up and running.
- You can enable both band selection and aggressive load balancing on the controller. They run independently and do not impact one another.
- It is not possible to enable or disable band selection and client load balancing globally through the controller GUI or CLI. You can, however, enable or disable band selection and client load balancing for a particular WLAN. Band selection and client load balancing are enabled globally by default.

Information About Configuring Band Selection, 802.11 Bands, and Parameters

Band Selection

Band selection enables client radios that are capable of dual-band (2.4- and 5-GHz) operation to move to a less congested 5-GHz access point. The 2.4-GHz band is often congested. Clients on this band typically experience interference from Bluetooth devices, microwave ovens, and cordless phones as well as co-channel interference from other access points because of the 802.11b/g limit of three nonoverlapping channels. To prevent these sources of interference and improve overall network performance, you can configure band selection on the switch.

Band selection is enabled globally by default.

Band selection works by regulating probe responses to clients. It makes 5-GHz channels more attractive to clients by delaying probe responses to clients on 2.4-GHz channels.

802.11 Bands

You can configure the 802.11b/g/n (2.4-GHz) and 802.11a/n (5-GHz) bands for the controller to comply with the regulatory requirements in your country. By default, both 802.11b/g/n and 802.11a/n are enabled.

When a controller is configured to allow only 802.11g traffic, 802.11b client devices are able to successfully connect to an access point but cannot pass traffic. When you configure the controller for 802.11g traffic only, you must mark 11g rates as mandatory.

802.11n Parameter

This section provides instructions for managing 802.11n devices such as the Cisco Aironet 1140 and 3600 Series Access Points on your network. The 802.11n devices support the 2.4- and 5-GHz bands and offer high-throughput data rates.

The 802.11n high-throughput rates are available on all 802.11n access points for WLANs using WMM with no Layer 2 encryption or with WPA2/AES encryption enabled.

Note Some Cisco 802.11n APs may intermittently emit incorrect beacon frames, which can trigger false wIPS alarms. We recommend that you ignore these alarms. The issue is observed in the following Cisco 802.11n APs: 1140, 1250, 2600, 3500, and 3600.

802.11h Parameter

802.11h informs client devices about channel changes and can limit the transmit power of those client devices.

How to Configure 802.11 Bands and Parameters

Configuring Band Selection (CLI)

SUMMARY STEPS

1. **configure terminal**
2. **wireless client band-select cycle-count** *cycle_count*
3. **wireless client band-select cycle-threshold** *milliseconds*
4. **wireless client band-select expire suppression** *seconds*
5. **wireless client band-select expire dual-band** *seconds*
6. **wireless client band-select client-rssi** *client_rssi*
7. **end**
8. **wlan** *wlan_profile_name wlan_ID SSID_network_name* **band-select**
9. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `SwitchControllerDevice# configure terminal`	Enters global configuration mode.
Step 2	**wireless client band-select cycle-count** *cycle_count* **Example:** `SwitchControllerDevice(config)# wireless client band-select cycle-count 3`	Sets the probe cycle count for band select. You can enter a value between 1 and 10 for the *cycle_count* parameter.
Step 3	**wireless client band-select cycle-threshold** *milliseconds*	Sets the time threshold for a new scanning cycle period.

	Command or Action	Purpose
	Example: `SwitchControllerDevice(config)# wireless client band-select cycle-threshold 5000`	You can enter a value for threshold between 1 and 1000 for the *milliseconds* parameter.
Step 4	**wireless client band-select expire suppression** *seconds* **Example:** `SwitchControllerDevice(config)# wireless client band-select expire suppression 100`	Sets the suppression expire to the band select. You can enter a value for suppression between 10 to 200 for the *seconds* parameter.
Step 5	**wireless client band-select expire dual-band** *seconds* **Example:** `SwitchControllerDevice(config)# wireless client band-select expire dual-band 100`	Sets the dual band expire. You can enter a value for dual band between 10 and 300 for the *seconds* parameter.
Step 6	**wireless client band-select client-rssi** *client_rssi* **Example:** `SwitchControllerDevice(config)# wireless client band-select client-rssi 40`	Sets the client RSSI threshold. You can enter a value for minimum dBm of a client RSSI to respond to a probe between 20 and 90 for the *client_rssi* parameter.
Step 7	**end** **Example:** `SwitchControllerDevice(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Step 8	**wlan** *wlan_profile_name wlan_ID SSID_network_name* **band-select**
	Example:
	`SwitchControllerDevice(config)# wlan wlan1 25 ssid12`
	`SwitchControllerDevice(config-wlan)# band-select`
		Configures band selection on specific WLANs.
		You can enter a value between 1 and 512 for the *wlan_ID* parameter.
		You can enter the up to 32 alphanumeric characters for *SSID_network_name* parameter.

Step 9	**end** **Example:** `SwitchControllerDevice(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Configuring the 802.11 Bands (CLI)

You can configure 802.11 bands and parameters.

SUMMARY STEPS

1. **configure terminal**
2. **ap dot11 5ghz shutdown**
3. **ap dot11 24ghz shutdown**
4. **ap dot11 {5ghz | 24ghz} beaconperiod** *time_unit*
5. **ap dot11 {5ghz | 24ghz} fragmentation** *threshold*
6. **ap dot11 {5ghz | 24ghz} dtpc**
7. **wireless client association limit** *number* **interval** *milliseconds*
8. **ap dot11 {5ghz | 24ghz} rate** *rate {disable | mandatory | supported}*
9. **no ap dot11 5ghz shutdown**
10. **no ap dot11 24ghz shutdown**
11. **ap dot11 24ghz dot11g**
12. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `SwitchControllerDevice# configure terminal`	Enters global configuration mode.
Step 2	**ap dot11 5ghz shutdown** **Example:** `SwitchControllerDevice(config)# ap dot11 5ghz shutdown`	Disables the 802.11a band. **Note** You must disable the 802.11a band before configuring the 802.11a network parameters.
Step 3	**ap dot11 24ghz shutdown** **Example:** `SwitchControllerDevice(config)# ap dot11 24ghz shutdown`	Disables the 802.11b band. **Note** You must disable the 802.11b band before configuring the 802.11b network parameters.
Step 4	**ap dot11 {5ghz | 24ghz} beaconperiod** *time_unit* **Example:** `SwitchControllerDevice(config)# ap dot11 5ghz beaconperiod 500`	Specifies the rate at which the SSID is broadcast by the access point. The beacon interval is measured in time units (TUs). One TU is 1024 microseconds. You can configure the access point to send a beacon every 20 to 1000 milliseconds.
Step 5	**ap dot11 {5ghz | 24ghz} fragmentation** *threshold* **Example:** `SwitchControllerDevice(config)# ap dot11 5ghz fragmentation 300`	Specifies the size at which packets are fragmented. The threshold is a value between 256 and 2346 bytes (inclusive). Specify a low number for areas where communication is poor or where there is a great deal of radio interference.

	Command or Action	Purpose

Step 6	**ap dot11 {5ghz | 24ghz} dtpc**
	
	Example:
	`SwitchControllerDevice(config)# ap dot11 5ghz dtpc`
	
	`SwitchControllerDevice(config)# no ap dot11 24ghz dtpc`
		Enables access points to advertise their channels and transmit the power levels in beacons, and probe responses.
		
		The default value is enabled. Client devices using dynamic transmit power control (DTPC) receive the channel and power level information from the access points and adjust their settings automatically. For example, a client device used primarily in Japan could rely on DTPC to adjust its channel and power settings automatically when it travels to Italy and joins a network there.
		Note On access points that run Cisco IOS software, this feature is called world mode.
		
		The **no** form of the command disables the 802.11a or 802.11b DTPC setting.

Step 7	**wireless client association limit** *number* **interval** *milliseconds* **Example:** `SwitchControllerDevice(config)# wireless client association limit 50 interval 1000`	Specifies the maximum allowed clients that can be configured. You can configure a maximum number of association request on a single access point slot at a given interval. The range of association limit that you can configure is from one through 100. The association request limit interval is measured between 100 to 10000 milliseconds.
Step 8	**ap dot11 {5ghz | 24ghz} rate** *rate {disable | mandatory | supported}* **Example:** `SwitchControllerDevice(config)# ap dot11 5ghz rate 36 mandatory`	Specifies the rate at which data can be transmitted between the controller and the client. • *disabled*—Defines that the clients specify the data rates used for communication. • *mandatory*—Defines that the clients support this data rate in order to associate to an access point on the controller. • *supported*—Any associated clients that support this data rate may communicate with the access point using that rate. However, the clients are not required to be able to use this rate in order to associate. • *rate*—Specifies the rate at which data is transmitted. For the 802.11a and 802.11b bands, the data is transmitted at the rate of 1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, or 54 Mbps.
Step 9	**no ap dot11 5ghz shutdown** **Example:** `SwitchControllerDevice(config)# no ap dot11 5ghz shutdown`	Enables the 802.11a band. **Note** The default value is enabled.
Step 10	**no ap dot11 24ghz shutdown** **Example:** `SwitchControllerDevice(config)# no ap dot11 24ghz shutdown`	Enables the 802.11b band. **Note** The default value is enabled.

	Command or Action	Purpose
Step 11	**ap dot11 24ghz dot11g** **Example:** `SwitchControllerDevice(config)# ap dot11 24ghz dot11g`	Enables or disables 802.11g network support. The default value is enabled. You can use this command only if the 802.11b band is enabled. If you disable this feature, the 802.11b band is enabled without 802.11g support.
Step 12	**end** **Example:** `SwitchControllerDevice(config)# end`	Returns to privileged EXEC mode.

Configuring 802.11n Parameters (CLI)

SUMMARY STEPS

1. **configure terminal**
2. **ap dot11 {5ghz | 24ghz} dot11n**
3. **ap dot11 {5ghz | 24ghz} dot11n mcs tx** *rtu*
4. **wlan***wlan_profile_name wlan_ID SSID_network_name* **wmm require**
5. **ap dot11 {5ghz | 24ghz} shutdown**
6. **{ap | no ap} dot11 {5ghz | 24 ghz} dot11n a-mpdu tx priority {all | 0-7}**
7. **no ap dot11 {5ghz | 24ghz} shutdown**
8. **ap dot11 {5ghz | 24ghz} dot11n guard-interval {any | long}**
9. **ap dot11 {5ghz | 24ghz} dot11n rifs rx**
10. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `SwitchControllerDevice# configure terminal`	Enters global configuration mode.
Step 2	**ap dot11 {5ghz	24ghz} dot11n** **Example:** `SwitchControllerDevice(config)# ap dot11 5ghz dot11n`	Enables 802.11n support on the network. The **no** form of the command disables the 802.11n support on the network.

	Command or Action	Purpose
Step 3	**ap dot11 {5ghz | 24ghz} dot11n mcs tx** *rtu* **Example:** `SwitchControllerDevice(config)# ap dot11 5ghz dot11n mcs tx 20`	Specifies the modulation and coding scheme (MCS) rates at which data can be transmitted between the access point and the client. You can set a value from 0 through 23 for the **mcs tx** parameter. The **no** form of the command disables the MCS rates that is configured.

Step 4	**wlan***wlan_profile_name wlan_ID SSID_network_name* **wmm require**
	
	Example:
	`SwitchControllerDevice(config)# wlan wlan1 25 ssid12`
	`SwitchControllerDevice(config-wlan)# wmm require`
		Enables WMM on the WLAN and uses the 802.11n data rates that you configured.
		
		The **require** parameter requires client devices to use WMM. Devices that do not support WMM cannot join the WLAN.

Step 5	**ap dot11 {5ghz | 24ghz} shutdown** **Example:** `SwitchControllerDevice(config)# ap dot11 5ghz shutdown`	Disables the network.
Step 6	**{ap | no ap} dot11 {5ghz | 24 ghz} dot11n a-mpdu tx priority {all | 0-7}** **Example:** `SwitchControllerDevice(config)# ap dot11 5ghz dot11n a-mpdu tx priority all`	Specifies the aggregation method used for 802.11n packets. Aggregation is the process of grouping packet data frames together rather than transmitting them separately. Two aggregation methods are available: Aggregated MAC Protocol Data Unit (A-MPDU) and Aggregated MAC Service Data Unit (A-MSDU). Both A-MPDU and A-MSDU are performed in the software. You can specify the aggregation method for various types of traffic from the access point to the clients. The following table defines the priority levels (0-7) assigned per traffic type.

Table 9: Traffic Type Priority Levels

User Priority	Traffic Type
0	Best effort
1	Background
2	Spare
3	Excellent effort
4	Controlled load
5	Video, less than 100-ms latency and jitter

	Command or Action	Purpose
		6 — Voice, less than 100-ms latency and jitter 7 — Network control You can configure each priority level independently, or you can use the all parameter to configure all of the priority levels at once. You can configure priority levels so that the traffic uses either A-MPDU transmission or A-MSDU transmission. • When you use the **ap** command along with the other options, the traffic associated with that priority level uses A-MPDU transmission. • When you use the **no ap** command along with the other options, the traffic associated with that priority level uses A-MSDU transmission. Configure the priority levels to match the aggregation method used by the clients. By default, A-MPDU is enabled for priority level 0, 4 and 5 and the rest are disabled. By default, A-MPDU is enabled for all priorities except 6 and 7.
Step 7	**no ap dot11 {5ghz | 24ghz} shutdown** **Example:** `SwitchControllerDevice(config)# no ap dot11 5ghz shutdown`	Reenables the network.
Step 8	**ap dot11 {5ghz | 24ghz} dot11n guard-interval {any | long}** **Example:** `SwitchControllerDevice(config)# ap dot11 5ghz dot11n guard-interval long`	Configures the guard interval for the network.
Step 9	**ap dot11 {5ghz | 24ghz} dot11n rifs rx** **Example:** `SwitchControllerDevice(config)# ap dot11 5ghz dot11n rifs rx`	Configures the Reduced Interframe Space (RIFS) for the network.
Step 10	**end** **Example:** `SwitchControllerDevice(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Configuring 802.11h Parameters (CLI)

SUMMARY STEPS

1. **configure terminal**
2. **ap dot11 5ghz shutdown**
3. **{ap | no ap} dot11 5ghz channelswitch mode** *switch_mode*
4. **ap dot11 5ghz power-constraint** *value*
5. **no ap dot11 5ghz shutdown**
6. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `SwitchControllerDevice# configure terminal`	Enters global configuration mode.
Step 2	**ap dot11 5ghz shutdown** **Example:** `SwitchControllerDevice(config)# ap dot11 5ghz shutdown`	Disables the 802.11a network.
Step 3	**{ap | no ap} dot11 5ghz channelswitch mode** *switch_mode* **Example:** `SwitchControllerDevice(config)# ap dot11 5ghz channelswitch mode 0`	Enables or disables the access point to announce when it is switching to a new channel. You can enter a 0 or 1 for the **channelswitch** parameter to specify whether transmissions are restricted until the actual channel switch (0) or are not restricted (1). The default value is disabled.
Step 4	**ap dot11 5ghz power-constraint** *value* **Example:** `SwitchControllerDevice(config)# ap dot11 5ghz power-constraint 200`	Configures the 802.11h power constraint value in a range from zero through 255. The default value for the value parameter is 3 dB.
Step 5	**no ap dot11 5ghz shutdown** **Example:** `SwitchControllerDevice(config)# no ap dot11 5ghz shutdown`	Reenables the 802.11a network.
Step 6	**end** **Example:** `SwitchControllerDevice(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Monitoring Configuration Settings for Band Selection, 802.11 Bands, and Parameters

Monitoring Configuration Settings Using Band Selection and 802.11 Bands Commands

This section describes the new commands for band selection and 802.11 bands.

The following commands can be used to monitor band selection, and 802.11 bands and parameters the switch.

Table 10: Monitoring Configuration Settings Using Band Selection and 802.11 Bands Commands

Command	Purpose
show ap dot11 5ghz network	Displays 802.11a bands network parameters, 802.11a operational rates, 802.11n MCS settings, and 802.11n status information.
show ap dot11 24ghz network	Displays 802.11b bands network parameters, 802.11b/g operational rates, 802.11n MCS settings, and 802.11n status information.
show wireless dot11h	Displays 802.11h configuration parameters.
show wireless band-select	Displays band select configuration settings.

Example: Viewing the Configuration Settings for 5-GHz Band

```
SwitchControllerDevice# show ap dot11 5ghz network
802.11a Network : Enabled
11nSupport : Enabled
  802.11a Low Band : Enabled
  802.11a Mid Band : Enabled
  802.11a High Band : Enabled

802.11a Operational Rates
  802.11a 6M : Mandatory
  802.11a 9M : Supported
  802.11a 12M : Mandatory
  802.11a 18M : Supported
  802.11a 24M : Mandatory
  802.11a 36M : Supported
  802.11a 48M : Supported
  802.11a 54M : Supported
802.11n MCS Settings:
  MCS 0 : Supported
  MCS 1 : Supported
  MCS 2 : Supported
  MCS 3 : Supported
```

```
  MCS 4 : Supported
  MCS 5 : Supported
  MCS 6 : Supported
  MCS 7 : Supported
  MCS 8 : Supported
  MCS 9 : Supported
  MCS 10 : Supported
  MCS 11 : Supported
  MCS 12 : Supported
  MCS 13 : Supported
  MCS 14 : Supported
  MCS 15 : Supported
  MCS 16 : Supported
  MCS 17 : Supported
  MCS 18 : Supported
  MCS 19 : Supported
  MCS 20 : Supported
  MCS 21 : Supported
  MCS 22 : Supported
  MCS 23 : Supported
802.11n Status:
  A-MPDU Tx:
    Priority 0 : Enabled
    Priority 1 : Disabled
    Priority 2 : Disabled
    Priority 3 : Disabled
    Priority 4 : Enabled
    Priority 5 : Enabled
    Priority 6 : Disabled
    Priority 7 : Disabled
  A-MSDU Tx:
    Priority 0 : Enabled
    Priority 1 : Enabled
    Priority 2 : Enabled
    Priority 3 : Enabled
    Priority 4 : Enabled
    Priority 5 : Enabled
    Priority 6 : Disabled
    Priority 7 : Disabled
Guard Interval : Any
  Rifs Rx : Enabled
Beacon Interval : 100
CF Pollable mandatory : Disabled
CF Poll Request Mandatory : Disabled
CFP Period : 4
CFP Maximum Duration : 60
Default Channel : 36
Default Tx Power Level : 1
DTPC Status : Enabled
Fragmentation Threshold : 2346
Pico-Cell Status : Disabled
Pico-Cell-V2 Status : Disabled
TI Threshold : 0
Legacy Tx Beamforming setting : Disabled
Traffic Stream Metrics Status : Disabled
Expedited BW Request Status : Disabled
EDCA profile type check : default-wmm
Call Admision Control (CAC) configuration
Voice AC
  Voice AC - Admission control (ACM) : Disabled
  Voice Stream-Size : 84000
  Voice Max-Streams : 2
  Voice Max RF Bandwidth : 75
  Voice Reserved Roaming Bandwidth : 6
  Voice Load-Based CAC mode : Enabled
  Voice tspec inactivity timeout : Enabled
CAC SIP-Voice configuration
  SIP based CAC : Disabled
  SIP Codec Type : CODEC_TYPE_G711
  SIP call bandwidth : 64
  SIP call bandwith sample-size : 20
Video AC
  Video AC - Admission control (ACM) : Disabled
```

```
  Video max RF bandwidth : Infinite
  Video reserved roaming bandwidth : 0
```

Example: Viewing the Configuration Settings for 24-GHz Band

```
SwitchControllerDevice# show ap dot11 24ghz network
802.11b Network : Enabled
11gSupport : Enabled
11nSupport : Enabled

  802.11b/g Operational Rates
  802.11b 1M : Mandatory
  802.11b 2M : Mandatory
  802.11b 5.5M : Mandatory
  802.11g 6M : Supported
  802.11g 9M : Supported
  802.11b 11M : Mandatory
  802.11g 12M : Supported
  802.11g 18M : Supported
  802.11g 24M : Supported
  802.11g 36M : Supported
  802.11g 48M : Supported
  802.11g 54M : Supported
802.11n MCS Settings:
  MCS 0 : Supported
  MCS 1 : Supported
  MCS 2 : Supported
  MCS 3 : Supported
  MCS 4 : Supported
  MCS 5 : Supported
  MCS 6 : Supported
  MCS 7 : Supported
  MCS 8 : Supported
  MCS 9 : Supported
  MCS 10 : Supported
  MCS 11 : Supported
  MCS 12 : Supported
  MCS 13 : Supported
  MCS 14 : Supported
  MCS 15 : Supported
  MCS 16 : Supported
  MCS 17 : Supported
  MCS 18 : Supported
  MCS 19 : Supported
  MCS 20 : Supported
  MCS 21 : Supported
  MCS 22 : Supported
  MCS 23 : Supported
802.11n Status:
  A-MPDU Tx:
    Priority 0 : Enabled
    Priority 1 : Disabled
    Priority 2 : Disabled
    Priority 3 : Disabled
    Priority 4 : Enabled
    Priority 5 : Enabled
    Priority 6 : Disabled
    Priority 7 : Disabled
  A-MSDU Tx:
    Priority 0 : Enabled
    Priority 1 : Enabled
    Priority 2 : Enabled
    Priority 3 : Enabled
    Priority 4 : Enabled
    Priority 5 : Enabled
  Priority 6 : Disabled
    Priority 7 : Disabled
  Guard Interval : Any
  Rifs Rx : Enabled
```

```
Beacon Interval : 100
CF Pollable Mandatory : Disabled
CF Poll Request Mandatory : Disabled
CFP Period : 4
CFP Maximum Duration : 60
Default Channel : 11
Default Tx Power Level : 1
DTPC Status : true
Call Admission Limit : 105
G711 CU Quantum : 15
ED Threshold : -50
Fragmentation Threshold : 2346
PBCC Mandatory : Disabled
Pico-Cell Status : Disabled
Pico-Cell-V2 Status : Disabled
RTS Threshold : 2347
Short Preamble Mandatory : Enabled
Short Retry Limit : 7
Legacy Tx Beamforming setting : Disabled
Traffic Stream Metrics Status : Disabled
Expedited BW Request Status : Disabled
EDCA profile type : default-wmm
Call Admision Control (CAC) configuration
Voice AC
  Voice AC - Admission control (ACM) : Disabled
  Voice Stream-Size : 84000
  Voice Max-Streams : 2
  Voice Max RF Bandwidth : 75
  Voice Reserved Roaming Bandwidth : 6
  Voice Load-Based CAC mode : Enabled
  Voice tspec inactivity timeout : Enabled
CAC SIP-Voice configuration
  SIP based CAC : Disabled
  SIP Codec Type : CODEC_TYPE_G711
  SIP call bandwidth : 64
  SIP call bandwith sample-size : 20
Video AC
  Video AC - Admission control (ACM) : Disabled
  Video max RF bandwidth : Infinite
  Video reserved roaming bandwidth : 0
```

Example: Viewing the status of 802.11h Parameters

```
SwitchControllerDevice# show wireless dot11h
Power Constraint: 0
Channel Switch: 0
Channel Switch Mode: 0
```

Example: Verifying the Band Selection Settings

```
SwitchControllerDevice# show wireless band-select
Band Select Probe Response    : per WLAN enabling
Cycle Count                  : 2
Cycle Threshold (millisec)   : 200
Age Out Suppression (sec)    : 20
Age Out Dual Band (sec)      : 60
Client RSSI (dBm)            : 80
```

Configuration Examples for Band Selection, 802.11 Bands, and Parameters

Examples: Band Selection Configuration

This example shows how to set the probe cycle count and time threshold for a new scanning cycle period for band select:

```
SwitchControllerDevice# configure terminal
SwitchControllerDevice(config)# wireless client band-select cycle-count 3
SwitchControllerDevice(config)# wireless client band-select cycle-threshold 5000
SwitchControllerDevice(config)# end
```

This example shows how to set the suppression expire to the band select:

```
SwitchControllerDevice# configure terminal
SwitchControllerDevice(config)# wireless client band-select expire suppression 100
SwitchControllerDevice(config)# end
```

This example shows how to set the dual band expire for the band select:

```
SwitchControllerDevice# configure terminal
SwitchControllerDevice(config)# wireless client band-select expire dual-band 100
SwitchControllerDevice(config)# end
```

This example shows how to set the client RSSI threshold for the band select:

```
SwitchControllerDevice# configure terminal
SwitchControllerDevice(config)# wireless client band-select client-rssi 40
SwitchControllerDevice(config)# end
```

This example shows how to configure band selection on specific WLANs:

```
SwitchControllerDevice# configure terminal
SwitchControllerDevice(config)# wlan wlan1 25 ssid12
SwitchControllerDevice(config-wlan)# band-select
SwitchControllerDevice(config)# end
```

Examples: 802.11 Bands Configuration

This example shows how to configure 802.11 bands using beacon interval, fragmentation, and dynamic transmit power control:

```
SwitchControllerDevice# configure terminal
SwitchControllerDevice(config)# ap dot11 5ghz shutdown
SwitchControllerDevice(config)# ap dot11 24ghz shutdown
SwitchControllerDevice(config)# ap dot11 5ghz beaconperiod 500
SwitchControllerDevice(config)# ap dot11 5ghz fragmentation 300
SwitchControllerDevice(config)# ap dot11 5ghz dtpc
SwitchControllerDevice(config)# wireless client association limit 50 interval 1000
SwitchControllerDevice(config)# ap dot11 5ghz rate 36 mandatory
SwitchControllerDevice(config)# no ap dot11 5ghz shutdown
SwitchControllerDevice(config)# no ap dot11 24ghz shutdown
SwitchControllerDevice(config)# ap dot11 24ghz dot11g
SwitchControllerDevice(config)#end
```

Examples: 802.11n Configuration

This example shows how to configure 802.11n parameters for 5-GHz band using aggregation method:

```
SwitchControllerDevice# configure terminal
SwitchControllerDevice(config)# ap dot11 5ghz dot11n
SwitchControllerDevice(config)# ap dot11 5ghz dot11n mcs tx 20
SwitchControllerDevice(config)# wlan wlan1 25 ssid12
SwitchControllerDevice(config-wlan)# wmm require\
SwitchControllerDevice(config-wlan)# exit
SwitchControllerDevice(config)# ap dot11 5ghz shutdown
SwitchControllerDevice(config)# ap dot11 5ghz dot11n a-mpdu tx priority all
SwitchControllerDevice(config)# no ap dot11 5ghz shutdown
SwitchControllerDevice(config)#exit
```

This example shows how to configure the guard interval for 5-GHz band:

```
SwitchControllerDevice# configure terminal
SwitchControllerDevice(config)# ap dot11 5ghz dot11n
SwitchControllerDevice(config)# ap dot11 5ghz dot11n mcs tx 20
SwitchControllerDevice(config)# wlan wlan1 25 ssid12
SwitchControllerDevice(config-wlan)# wmm require\
SwitchControllerDevice(config-wlan)# exit
SwitchControllerDevice(config)# no ap dot11 5ghz shutdown
SwitchControllerDevice(config)# ap dot11 5ghz dot11n guard-interval long
SwitchControllerDevice(config)#end
```

This example shows how to configure the RIFS for 5-GHz band:

```
SwitchControllerDevice# configure terminal
SwitchControllerDevice(config)# ap dot11 5ghz dot11n
SwitchControllerDevice(config)# ap dot11 5ghz dot11n mcs tx 20
SwitchControllerDevice(config)# wlan wlan1 25 ssid12
SwitchControllerDevice(config-wlan)# wmm require\
SwitchControllerDevice(config-wlan)# exit
SwitchControllerDevice(config)# ap dot11 5ghz shutdown
SwitchControllerDevice(config)# ap dot11 5ghz dot11n rifs rx
SwitchControllerDevice(config)#end
```

Examples: 802.11h Configuration

This example shows how to configure the access point to announce when it is switching to a new channel using restriction transmission:

```
SwitchControllerDevice# configure terminal
SwitchControllerDevice(config)# ap dot11 5ghz shutdown
SwitchControllerDevice(config)# ap dot11 5ghz channelswitch mode 0
SwitchControllerDevice(config)# no ap dot11 5ghz shutdown
SwitchControllerDevice(config)#end
```

This example shows how to configure the 802.11h power constraint for 5-GHz band:

```
SwitchControllerDevice# configure terminal
SwitchControllerDevice(config)# ap dot11 5ghz shutdown
SwitchControllerDevice(config)# ap dot11 5ghz power-constraint 200
SwitchControllerDevice(config)# no ap dot11 5ghz shutdown
SwitchControllerDevice(config)#end
```

Additional References for 802.11 Parameters and Band Selection

Related Documents

Related Topic	Document Title
System management commands	*System Management Command Reference, Cisco IOS XE Release 3SE (Cisco WLC 5700 Series)*

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

Feature History and Information For Performing 802.11 parameters and Band Selection Configuration

Release	Feature Information
Cisco IOS XE 3.2SE	This feature was introduced.

CHAPTER 8

Configuring Client Roaming

Finding Feature Information

Your software release may not support all of 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.

Restrictions for Configuring Client Roaming

The following are the restrictions that you should be aware while configuring client roaming:

- Cisco Compatible Extensions (CCX) support is enabled automatically for every WLAN on the switch and cannot be disabled. The switch stores the CCX version of the client in its client database and uses it to generate and respond to CCX frames appropriately. Clients must support CCXv4 or v5 (or CCXv2 for access point assisted roaming) to utilize these roaming enhancements.
- Client roaming between 600 Series Access points is not supported.

Information About Client Roaming

The controllers deliver high-end wireless services to the clients roaming across wireless network. Now, the wireless services are integrated with the switches, thus delivering a value-added Cisco unified new mobility architecture. This unified architecture enables client-roaming services to both wireless and wired clients with seamless, fast- roaming services.

The new mobility architecture supports fast client roaming services using logical categorization of network into Mobility Domains (MDs), Mobility Groups (MGs), Mobility Subdomains (MSDs), and Switch Peer Groups (SPGs) using systems such as Mobility Oracle (MO), Mobility Controller (MC), and Mobility Agent (MA).

- A **Mobility Domain** is the entire domain across which client roaming is supported. It is a collection of mobility groups. For example, a campus network can be considered as a mobility domain.
- A **Mobility Group** is a collection of mobility subdomains across which fast roaming is supported. The mobility group can be one or more buildings within a campus across which frequent roaming is supported.
- A **Mobility Subdomain** is an autonomous portion of the mobility domain network. Each mobility subdomain contains one mobility controller (MC) and a collection of SPGs. A subdomain is equivalent to an 802.11r key domain.
- A **Switch Peer Group** is a collection of mobility agents.
- The **Mobility Oracle** acts as the point of contact for mobility events that occur across mobility subdomains. The mobility oracle also maintains a local database of each client in the entire mobility domain, their home and current subdomain. There is only one MO for an entire mobility domain. The Cisco WLC 5700 Series Controllers or Cisco Unified Wireless Networking Solution controller can act as MO.
- The **Mobility Controller** provides mobility management services for inter-SPG roaming events. The MC sends the configuration like SPG name and SPG peer member list to all of the mobility agents under its subdomain. The Cisco WLC 5700 Series Controllers, Cisco Catalyst 3850 Switch, or Cisco Unified Wireless Networking Solution controller can act as MC. The MC has MC functionality and MA functionality that is running internally into it.
- The **Mobility Agent** is the component that maintains client mobility state machine for a mobile client. All APs are connected to the mobility agent.

The New mobility architecture supports seamless roaming in the following scenarios:

- Intra-switch roaming—The client roaming between APs managed by same mobility agent.
- Intra-SPG roaming—The client roaming between mobility agents in the same SPG.
- Inter-SPG, Intra-subdomain roaming—The client roaming between mobility agents in different SPGs within the same subdomain.
- Inter-subdomain roaming—The client roaming between mobility agents across a subdomain.

Fast Roaming

New mobility architecture supports fast roaming when clients roam within a mobility group by eliminating the need for full authentication. Security polices should be same across the switches for fast roaming.

Local, anchor, foreign MAs and MCs

When a client joins an MA initially and its point of attachment has not changed, that MA is referred as local or associated MA. The MC to which this MA is associated is referred as local or associated MC.

When a client roams between two MAs, the MA to which the client was previously associated is the anchor MA (point of attachment) and the MA to which the client is currently associated is the foreign or associated MA (point of presence). The MCs to which these MAs are associated are referred as anchor, foreign, or associated MCs, respectively.

Inter-Subnet Roaming

Multiple-controller deployments support client roaming across access points managed by controllers in the same mobility group on different subnets. This roaming is transparent to the client because the session is sustained and a tunnel between the controllers allows the client to continue using the same DHCP-assigned or client-assigned IP address as long as the session remains active. The tunnel is torn down, and the client must reauthenticate when the client sends a DHCP Discover with a 0.0.0.0 client IP address or a 169.254.*.* client auto-IP address or when the operator-set user timeout is exceeded.

Voice-over-IP Telephone Roaming

802.11 voice-over-IP (VoIP) telephones actively seek out associations with the strongest RF signal to ensure the best quality of service (QoS) and the maximum throughput. The minimum VoIP telephone requirement of 20-millisecond or shorter latency time for the roaming handover is easily met by the Cisco Unified Wireless Network (Cisco UWN) solution, which has an average handover latency of 5 or fewer milliseconds when open authentication is used. This short latency period is controlled by controllers rather than allowing independent access points to negotiate roaming handovers.

The Cisco UWN solution supports 802.11 VoIP telephone roaming across lightweight access points managed by controllers on different subnets, as long as the controllers are in the same mobility group. This roaming is transparent to the VoIP telephone because the session is sustained and a tunnel between controllers allows the VoIP telephone to continue using the same DHCP-assigned IP address as long as the session remains active. The tunnel is torn down, and the VoIP client must reauthenticate when the VoIP telephone sends a DHCP Discover with a 0.0.0.0 VoIP telephone IP address or a 169.254.*.* VoIP telephone auto-IP address or when the operator-set user timeout is exceeded.

CCX Layer 2 Client Roaming

The controller supports five CCX Layer 2 client roaming enhancements:

- Access point assisted roaming—This feature helps clients save scanning time. When a CCXv2 client associates to an access point, it sends an information packet to the new access point listing the characteristics of its previous access point. Roaming time decreases when the client recognizes and uses an access point list built by compiling all previous access points to which each client was associated and sent (unicast) to the client immediately after association. The access point list contains the channels, BSSIDs of neighbor access points that support the client's current SSID(s), and time elapsed since disassociation.
- Enhanced neighbor list—This feature focuses on improving a CCXv4 client's roam experience and network edge performance, especially when servicing voice applications. The access point provides its associated client information about its neighbors using a neighbor-list update unicast message.

- Enhanced neighbor list request (E2E)—The End-2-End specification is a Cisco and Intel joint program that defines new protocols and interfaces to improve the overall voice and roaming experience. It applies only to Intel clients in a CCX environment. Specifically, it enables Intel clients to request a neighbor list at will. When this occurs, the access point forwards the request to the controller. The controller receives the request and replies with the current CCX roaming sublist of neighbors for the access point to which the client is associated.

Note To see whether a particular client supports E2E, choose **Wireless** > **Clients** on the controller GUI, click the **Detail** link for the desired client, and look at the E2E Version text box in the Client Properties area.

- Roam reason report—This feature enables CCXv4 clients to report the reason why they roamed to a new access point. It also allows network administrators to build and monitor a roam history.
- Directed roam request—This feature enables the controller to send directed roam requests to the client in situations when the controller can better service the client on an access point different from the one to which it is associated. In this case, the controller sends the client a list of the best access points that it can join. The client can either honor or ignore the directed roam request. Non-CCX clients and clients running CCXv3 or below must not take any action. No configuration is required for this feature.

How to Configure Layer 2 or Layer 3 Roaming

Configuring Layer 2 or Layer 3 Roaming

Before You Begin

To configure the mobility agent for Layer 2 or Layer 3 roaming, the following requisites should be considered:

- SSID and security polices should be same across MAs for Layer 2 and Layer 3 roaming.
- Client VLAN ID should be same for Layer 2 roaming and different for Layer 3 roaming.
- Bridge domain ID and client VLAN IDs should be same for Layer 2 roaming. Either one or both of the bridge domain ID and client VLAN ID should be different for Layer 3 roaming.

SUMMARY STEPS

1. **configure terminal**
2. **wlan** *wlan_profile_name wlan_ID SSID_network_name*
3. **no mobility anchor sticky**
4. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `SwitchControllerDevice# configure terminal`	Enters global configuration mode.
Step 2	**wlan** *wlan_profile_name wlan_ID SSID_network_name* **Example:** `SwitchControllerDevice(config)#wlan wlan1`	Enters WLAN configuration mode.
Step 3	**no mobility anchor sticky** **Example:** `SwitchControllerDevice(config-wlan)#no mobility anchor sticky`	(Optional) Disables Layer 2 anchoring.
Step 4	**end** **Example:** `SwitchControllerDevice(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Configuring CCX Client Roaming Parameters (CLI)

SUMMARY STEPS

1. **configure terminal**
2. **ap dot11 {5ghz | 24ghz} l2roam rf-params** {**default | custom** *min-rssi roam-hyst scan-thresh trans-time*}
3. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `SwitchControllerDevice# configure terminal`	Enters global configuration mode.
Step 2	**ap dot11 {5ghz | 24ghz} l2roam rf-params** {**default | custom** *min-rssi roam-hyst scan-thresh trans-time*}	Configures CCX Layer 2 client roaming parameters. To choose the default RF parameters, enter the **default** option. To fine-tune the RF parameters that affect client roaming, enter the **custom** option and then enter any one of the following options:

	Command or Action	Purpose
	Example: `SwitchControllerDevice#`**`ap dot11 5ghz l2roam rf-params custom -80`**	• Minimum RSSI—Indicates minimum Received Signal Strength Indicator (RSSI) required for the client to associate to an access point. If the client's average received signal power dips below this threshold, reliable communication is usually impossible. Therefore, clients must already have found and roamed to another access point with a stronger signal before the minimum RSSI value is reached. You can configure the minimum RSSI range from –80 through –90 dBm and the default is –85 dBm. • Hysteresis—Indicates how much greater the signal strength of a neighboring access point must be for the client to roam to it. This parameter is intended to reduce the amount of roaming between access points if the client is physically located on or near the border between two access points. You can configure the hysteresis range from 3 through 20 dB and the default is 3 dB. • Scan Threshold—Indicates a minimum RSSI that is allowed before the client should roam to a better access point. When the RSSI drops below the specified value, the client must be able to roam to a better access point within the specified transition time. This parameter also provides a power-save method to minimize the time that the client spends in active or passive scanning. For example, the client can scan slowly when the RSSI is above the threshold and scan more rapidly when the RSSI is below the threshold. You can configure the RSSI range from –70 through –77 dBm and the default value is –72 dBm. • Transition Time—Indicates the maximum time allowed for the client to detect a suitable neighboring access point to roam to and to complete the roam, whenever the RSSI from the client's associated access point is below the scan threshold. The Scan Threshold and Transition Time parameters guarantee a minimum level of client roaming performance. Together with the highest expected client speed and roaming hysteresis, these parameters make it possible to design a wireless LAN network that supports roaming simply by ensuring a certain minimum overlap distance between access points. You can configure the time period in the range from 1 through 10 seconds and the default time is 5 seconds.
Step 3	**end** **Example:** `SwitchControllerDevice(config)#`**`end`**	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Configuring Mobility Oracle

SUMMARY STEPS

1. **configure terminal**
2. **wireless mobility oracle**
3. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `SwitchControllerDevice# configure terminal`	Enters global configuration mode.
Step 2	**wireless mobility oracle** **Example:** `SwitchControllerDevice(config)# wireless mobility oracle`	Enables mobility oracle on the controller.
Step 3	**end** **Example:** `SwitchControllerDevice(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Configuring Mobility Controller

SUMMARY STEPS

1. **configure terminal**
2. **wireless mobility controller**
3. **wireless mobility controller peer-group** *switch-peer-group-name*
4. **wireless mobility controller peer-group** *switch-peer-group-name* **member ip** *ip-address* {**public-ip** *public-ip-address*}
5. **wireless mobility controller peer-group** *switch-peer-group-name* **multicast**
6. **wireless mobility controller peer-group** *switch-peer-group-name* **multicast ip** *peer-group-multicast-ip-addr*
7. **wireless mobility controller peer-group***switch-peer-group-name* **bridge-domain-id** *id*
8. **wireless mobility group member ip** *ip-address* [**public-ip** *public-ip-address*] [**group** *group-name*]
9. **wireless mobility dscp** *value*
10. **wireless mobility group keepalive** {*count* | *interval*}
11. **wireless mobility group name** *name*
12. **wireless mobility oracle ip***mo-ip-address*
13. **wireless management interface** *interface-name*
14. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `SwitchControllerDevice#` **`configure terminal`**	Enters global configuration mode.
Step 2	**wireless mobility controller** **Example:** `SwitchControllerDevice(config)# wireless mobility controller`	Enables wireless mobility controller.
Step 3	**wireless mobility controller peer-group** *switch-peer-group-name* **Example:** `SwitchControllerDevice(config)# wireless mobility controller peer-group SPG1`	Configures a switch peer group name. You can enter up to 31 case-sensitive ASCII printable characters for the group name. Spaces are not allowed in mobility group. **Note** The **No** form of the command deletes the switch peer group.
Step 4	**wireless mobility controller peer-group** *switch-peer-group-name* **member ip** *ip-address* {**public-ip** *public-ip-address*}	Adds a mobility group member to a switch peer group. **Note** The **No** form of the command deletes the member from the switch peer group.

	Command or Action	Purpose
	Example: `SwitchControllerDevice(config)# wireless mobility controller peer-group SPG1 member ip 10.0.0.1`	
Step 5	**wireless mobility controller peer-group** *switch-peer-group-name* **multicast** **Example:** `SwitchControllerDevice(config)# wireless mobility controller peer-group SPG1 multicast`	Configures the multicast mode within a switch peer group.
Step 6	**wireless mobility controller peer-group** *switch-peer-group-name* **multicast ip** *peer-group-multicast-ip-addr* **Example:** `SwitchControllerDevice(config)# wireless mobility controller peer-group SPG1 multicast ip 10.0.0.4`	Configures the multicast IP address for a switch peer group. **Note** The **No** form of the command deletes the multicast IP for the switch peer group.
Step 7	**wireless mobility controller peer-group***switch-peer-group-name* **bridge-domain-id** *id* **Example:** `SwitchControllerDevice(config)# wireless mobility controller peer-group SPG bridge-domain-id 10.0.0.5`	Configures the bridge domain ID for a switch peer group. The default is zero. **Note** The **No** form of command sets the bridge domain ID to the default value.
Step 8	**wireless mobility group member ip** *ip-address* [**public-ip** *public-ip-address*] [**group** *group-name*] **Example:** `SwitchControllerDevice(config)# wireless mobility group member ip 10.0.0.1`	Adds a mobility group member. **Note** The **No** form of the command removes the member from the group. The default group name is the group name of MC.
Step 9	**wireless mobility dscp** *value* **Example:** `SwitchControllerDevice(config)# wireless mobility dscp 46`	Sets the DSCP value for mobility control packet. You can configure the DSCP value in a range from 0 through 63. The default value is 46.
Step 10	**wireless mobility group keepalive** {*count* | *interval*} **Example:** `SwitchControllerDevice(config)# wireless mobility group keepalive count`	Configures the wireless mobility group keepalive count which is the number of keepalive retries before a member status is termed DOWN and keepalive interval which is interval between two keepalives.
Step 11	**wireless mobility group name** *name* **Example:** `SwitchControllerDevice(config)# wireless mobility group name group1`	Specifies the case sensitive wireless mobility group name which can be ASCII printable string up to 31 characters.

	Command or Action	Purpose
Step 12	**wireless mobility oracle ip***mo-ip-address* **Example:** `SwitchControllerDevice(config)# wireless mobility oracle ip 10.0.0.5`	Configures the mobility oracle IP address.
Step 13	**wireless management interface** *interface-name* **Example:** `SwitchControllerDevice(config)# wireless management interface Vlan21`	Configures the wireless management interface.
Step 14	**end** **Example:** `SwitchControllerDevice(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Configuring Mobility Agent

SUMMARY STEPS

1. **configure terminal**
2. **wireless mobility controller ip** *ip-address*
3. **wireless mobility load-balance**
4. **wireless mobility load-balance threshold** *threshold -value*
5. **wireless management interface** *interface-name*
6. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `SwitchControllerDevice# configure terminal`	Enters global configuration mode.
Step 2	**wireless mobility controller ip** *ip-address* **Example:** `SwitchControllerDevice(config)# wireless mobility controller ip 10.10.10.20`	Sets the IP address of the mobility controller.
Step 3	**wireless mobility load-balance**	Configures wireless mobility load balancing.

	Command or Action	Purpose
	Example: `SwitchControllerDevice(config)# wireless mobility load-balance`	
Step 4	**wireless mobility load-balance threshold** *threshold -value* **Example:** `SwitchControllerDevice(config)# wireless mobility load-balance threshold 100`	Configures the number of clients that can be local or anchored on the MA. You can configure the threshold value in a range from 100 to 2000. The default value is 1000.
Step 5	**wireless management interface** *interface-name* **Example:** `SwitchControllerDevice(config)# wireless management interface Vlan21`	Configures wireless management interface for the mobility agent.
Step 6	**end** **Example:** `SwitchControllerDevice(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Monitoring Client Roaming Parameters

This section describes the new commands for the client parameters.

The following commands can be used to monitor the client roaming parameters on the switch.

Table 11: Monitoring Client Roaming Parameters Commands

Command	Purpose
show ap dot11 {5ghz | 24ghz} l2roam rf-param	Displays the current RF parameters configured for client roaming for the 802.11a or 802.11b/g network.
show ap dot11 {5ghz | 24ghz} l2roam statistics	Displays the CCX Layer 2 client roaming statistics for the 802.11a or 802.11b/g network.
show ap dot11 {5ghz | 24ghz} l2roam mac-address *mac-address* **statistics**	Displays the CCX Layer 2 client roaming statistics for a particular access point.

Monitoring Mobility Configurations

This section describes the new commands for monitoring mobility configurations.

The following command can be used to monitor mobility configurations on the Mobility Oracle, Mobility Controller, and Mobility Agent.

Table 12: Monitoring Mobility Configuration Commands on the Mobility Controller and Mobility Agent

Command	Purpose
show wireless mobility summary	Displays the summary information for the Mobility Controller and Mobility Agent.
show wireless mobility statistics	Displays mobility statistics.
show wireless mobility dtls connections	Displays established DTLS connections.

Table 13: Monitoring Mobility Configuration Commands on the Mobility Oracle

Command	Purpose
show wireless mobility oracle summary	Displays the status of the Mobility Controllers known to the Mobility Oracle.
show wireless mobility oracle client summary	Displays the information of a list of clients in the Mobility Oracle database.
show wireless mobility oracle client detail *client -mac-address*	Displays the detailed information of a particular client in the Mobility Oracle database.
show wireless mobility oracle *mc-ip*	Displays the information of a list of clients in the Mobility Oracle database that are anchored or associated to a specified Mobility Controller.

Table 14: Monitoring Mobility Configuration Commands on the Mobility Controller

Command	Purpose
show wireless mobility controller client summary	Displays a list of clients in the subdomain.
show wireless mobility controller client *mac-address* **detail**	Displays detailed information for a client in a subdomain.
show wireless mobility agent *ma-ip* **client summary**	Displays a list of clients anchored or associated to a specified Mobility Agent.
show wireless mobility ap-list	Displays the list of Cisco APs known to the mobility group.

Table 15: Monitoring Mobility Configuration Commands on the Mobility Agent

Command	Purpose
show wireless mobility load-balance summary	Displays the summary of mobility load-balance properties.

Additional References for Configuring Client Roaming

Related Documents

Related Topic	Document Title
Mobility configuration	*Mobility Configuration Guide, Cisco IOS XE Release 3SE (Cisco WLC 5700 Series)*
Mobility-related commands	*Mobility Command Reference Guide, Cisco IOS XE Release 3SE (Cisco WLC 5700 Series)*

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

Feature History and Information For Performing Client Roaming Configuration

Release	Feature Information
Cisco IOS XE 3.2SE	This feature was introduced.

CHAPTER 9

Configuring Application Visibility and Control

Finding Feature Information

Your software release may not support all of 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 Application Visibility and Control

Application Visibility and Control (AVC) classifies applications using deep packet inspection techniques with the Network-Based Application Recognition engine, and provides application-level visibility and control (QoS) in wireless networks. After the applications are recognized, the AVC feature enables you to either drop, mark, or police the data traffic.

Using AVC, we can detect more than 1000 applications. AVC enables you to perform real-time analysis and create policies to reduce network congestion, costly network link usage, and infrastructure upgrades.

Note You can view list of 30 applications in Top Applications in Monitor Summary section of the UI.

Restrictions for Application Visibility and Control

- AVC is supported only on the following access points:
  - Cisco Aironet 1260 Series Access Points
  - Cisco Aironet 1600 Series Access Points
  - Cisco Aironet 2600 Series Access Point
  - Cisco Aironet 2600 Series Wireless Access Points
  - Cisco Aironet 2700 Series Access Point
  - Cisco Aironet 3500 Series Access Points
  - Cisco Aironet 3600 Series Access Points
- AVC is not supported on Cisco Aironet 702W, 702I (128 M memory), and 1530 Series Access Points.
- Dropping or marking of the data traffic (control part) is not supported for software Release 3.3.
- Dropping or marking of the data traffic (control part) is supported in software Release 3E.
- Multicast traffic classification is not supported.
- Only the applications that are recognized with App visibility can be used for applying QoS control.
- IPv6 including ICMPv6 traffic classifications are not supported.
- Datalink is not supported for NetFlow fields for AVC.
- The following commands are not supported for AVC flow records:
  - **collect flow username**
  - **collect interface** { **input** | **output**}
  - **collect wireless client ipv4 address**
  - **match interface** { **input** | **output**}
  - **match transport igmp type**
- The template timeout cannot be modified on exporters configured with AVC. Even if the template timeout value is configured to a different value, only the default value of 600 seconds is used.
- For the username information in the AVC-based record templates, ensure that you configure the options **records** to get the user MAC address to username mapping.
- The total number of flows for which downstream AVC QoS supported per client is 1000.
- The maximum number of flows supported for Catalyst 3850 Series Switch is 48 K.
- Google shares resources among several of their services because of which for some of the traffic it is not possible to say it is unique to one application. Therefore we added google-services for traffic that cannot be distinguished. The behavior you experience is expected.

How to Configure Application Visibility and Control

Configuring Application Visibility and Control (GUI)

Configuring Application Visibility (GUI)

You can apply the default flow record (**wireless avc basic**) to the default flow monitor (**wireless-avc-basic**).

If you are using the flow record and flow monitor you have created, then the record name and monitor name should be same. This is specific only for configuring AVC from GUI and not for the CLI configuration.

You can use the flow monitor you have created either for upstream or downstream, or both, but ensure that you use the same record name while mapping with the flow monitor.

Step 1 Choose **Configuration** > **Wireless** > **WLAN**.
The **WLAN** page appears.

Step 2 Click on the corresponding WLAN ID to open the **WLAN > Edit** page and click **AVC**.
The **Application Visibility** page appears.

a) Select the **Application Visibility Enabled** check box to enable AVC on a WLAN.
b) In the **Upstream Profile** text box, enter the name of the AVC profile.
c) In the **Downstream Profile** text box, enter the name of the AVC profile.

To enable AVC, you need to enter the profile names for the upstream and downstream profiles. The profile names are the flow monitor names. By default, the flow monitor names (**wireless-avc-basic**) appear in the **Upstream Profile** and **Downstream Profile** text boxes. For the default flow monitor, the default flow record (**wireless avc basic**) will be taken. The default flow record is generated by the system and is available.

You can change the profile names for the upstream and downstream profiles but ensure that the same flow records are available for the flow monitors.

The upstream and downstream profiles can have different profile names but there should be flow records available for the flow monitors.

Step 3 Click **Apply** to apply AVC on the WLAN.

Step 4 To disable AVC on a specific WLAN, perform the following steps:

- Choose **Configuration** > **Wireless** > **WLAN** to open the **WLAN** page.
- Click on the corresponding WLAN ID to open the **WLAN > Edit** page.
- Click **AVC** to open the **Application Visibility** page.
- Uncheck the **Application Visibility Enabled** check box.
- Click **Apply** to disable AVC on the specific WLAN.

Monitoring Application Visibility and Control

Monitoring Application Visibility and Control (CLI)

This section describes the new commands for application visibility.

The following commands can be used to monitor application visibility on the switch and access points.

Table 16: Monitoring Application Visibility Commands on the switch

Command	Purpose
show avc client *client-mac* **top** *n* **application** [**aggregate** | **upstream** | **downstream**]	Displays information about top "N" applications for the given client MAC.
show avc wlan *ssid* **top** *n* **application** [**aggregate** | **upstream** | **downstream**]	Displays information about top "N" applications for the given SSID.
avc top user[enable | disable]	Enables or disables the information about top "N" application.
show avc wlan *wlan-id* **application** *app name* **top***N* [**aggregate** | **upstream** | **downstream**]	Displays to know network usage information on a per user basis within an application. **Note** On Catalyst 4500E Supervisor Engine 8-E, in the information about top N users that is displayed, the client's MAC address and username are not displayed. This issue occurs only within 90 seconds after the client is disconnected.
show wlan id *wlan-id*	Displays information whether AVC is enabled or disabled on a particular WLAN.
show flow monitor *flow_monitor_name* **cache**	Displays information about flow monitors.
show wireless client mac-address *mac-address* **service-policy** { **input** | **output** }	Displays information about policy mapped to the wireless clients.

show ip nbar protocol-discovery[**interface***interface-type interface-number*] [**stats**{**byte-count** | **bit-rate** | **packet-count** | **max-bit-rate**}] [**protocol***protocol-name* | **top-n***number*]	Displays the statistics gathered by the NBAR Protocol Discovery feature. • (Optional) Enter keywords and arguments to fine-tune the statistics displayed. For more information on each of the keywords, refer to the **show ip nbar protocol-discovery**command in Cisco IOS Quality of Service Solutions Command Reference. **Note** When you configure NBAR, you must enable Protocol Discovery on the interface.
show policy-map target **show policy-map** **show policy-map** *policy-name* **show policy-map interface***interface-type interface-number*	Displays information about policy map.

Table 17: Clearing Application Visibility Statistics Commands

Command	Purpose
clear avc client *mac* **stats**	Clears the statistics per client.
clear avc wlan *wlan-name* **stats**	Clears the statistics per WLAN.

Monitoring Application Visibility and Control (GUI)

You can view AVC information on a WLAN in a single shot using a **AVC on WLAN** pie chart on the **Home** page of the switch. The pie chart displays the AVC data (Aggregate - Application Cumulative usage %) of the first WLAN. In addition, the top 5 WLANs based on clients are displayed first. Click on any one of the WLANs to view the corresponding pie chart information. If AVC is not enabled on the first WLAN, then the **Home** page does not display the AVC pie chart.

Step 1 Choose **Monitor** > **Controller** > **AVC** > **WLANs**.
The **WLANs** page appears.

Step 2 Click the corresponding WLAN profile.
The **Application Statistics** page appears.

From the **Top Applications** drop-down list, choose the number of top applications you want to view and click **Apply**. The valid range is between 5 to 30, in multiples of 5.

a) On the Aggregate, Upstream, and Downstream tabs, you can view the application cumulative and last 90 seconds statistics and usage percent with the following fields:

- Application name
- Packet count
- Byte count
- Average packet size
- usage (%)

Step 3 Choose **Monitor** > **Clients** > **Client Details** > **Clients**.
The **Clients** page appears.

Step 4 Click **Client MAC Address** and then click **AVC Statistics** tab.
The **Application Visibility** page appears.

a) On the Aggregate, Upstream, and Downstream tabs, you can view the application cumulative and last 90 seconds statistics and usage percent with the following fields:

- Application name
- Packet count
- Byte count
- Average packet size
- usage (%)

Examples: Application Visibility and Control

Examples: Application Visibility Configuration

This example shows how to create a flow record, create a flow monitor, apply the flow record to the flow monitor, and apply the flow monitor on a WLAN:

```
SwitchControllerDevice# configure terminal
SwitchControllerDevice(config)# flow record fr_v4
SwitchControllerDevice(config-flow-record)# match ipv4 protocol
SwitchControllerDevice(config-flow-record)# match ipv4 source address
SwitchControllerDevice(config-flow-record)# match ipv4 destination address
SwitchControllerDevice(config-flow-record)# match transport destination-port
SwitchControllerDevice(config-flow-record)# match flow direction
SwitchControllerDevice(config-flow-record)# match application name
SwitchControllerDevice(config-flow-record)# match wireless ssid
SwitchControllerDevice(config-flow-record)# collect counter bytes long
SwitchControllerDevice(config-flow-record)# collect counter packets long
SwitchControllerDevice(config-flow-record)# collect wireless ap mac address
SwitchControllerDevice(config-flow-record)# collect wireless client mac address
```

```
SwitchControllerDevice(config)#end
```

```
SwitchControllerDevice# configure terminal
SwitchControllerDevice# flow monitor fm_v4
SwitchControllerDevice(config-flow-monitor)# record fr_v4
SwitchControllerDevice(config-flow-monitor)# cache timeout active 1800
SwitchControllerDevice(config)#end
```

```
SwitchControllerDevice(config)#wlan wlan1
SwitchControllerDevice(config-wlan)#ip flow monitor fm_v4 input
SwitchControllerDevice(config-wlan)#ip flow mon fm-v4 output
SwitchControllerDevice(config)#end
```

Additional References for Application Visibility and Control

Related Documents

Related Topic	Document Title
System management commands	*System Management Command Reference Guide, Cisco IOS XE Release 3SE (Cisco WLC 5700 Series)*
Flexible NetFlow configuration	*Flexible NetFlow Configuration Guide, Cisco IOS XE Release 3SE (Cisco WLC 5700 Series)*
Flexible NetFlow commands	*Flexible NetFlow Command Reference, Cisco IOS XE Release 3SE (Cisco WLC 5700 Series)*
QoS configuration	*QoS Configuration Guide, Cisco IOS XE Release 3E (Cisco WLC 5700 Series)*
QoS commands	*QoS Command Reference, Cisco IOS XE Release 3E (Cisco WLC 5700 Series)*

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

Feature History and Information For Application Visibility and Control

Release	Feature Information
Cisco IOS XE 3.3SE	This feature was introduced.
Cisco IOS XE 3E	AVC control with QoS was introduced.

CHAPTER 10

Configuring Voice and Video Parameters

Finding Feature Information

Your software release may not support all of 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 Voice and Video Parameters

You can confirm the following points before configuring voice and video parameters:

- Ensure that the switch has access points connected to it.
- Configure SSID.

Restrictions for Voice and Video Parameters

The following are the restrictions that you should keep in mind while configuring voice and video parameters:

- SIP CAC can be used for the 9971 Cisco phones that support TSPEC-based admission control. You can also use the phones that support Status code 17.
- SIP snooping is supported for providing voice priority to the non-TSPEC SIP phones.
- TSPEC for video CAC is not supported.

Information About Configuring Voice and Video Parameters

Three parameters on the switch affect voice and/or video quality:

- Call Admission Control
- Expedited bandwidth requests
- Unscheduled automatic power save delivery

Call Admission Control (CAC) and UAPSD are supported on Cisco Compatible Extensions (CCX) v4 and v5; however, these parameters are also supported even without CCX but on any device implementing WMM (that supports 802.1e). Expedited bandwidth requests are supported only on CCXv5.

Traffic stream metrics (TSM) can be used to monitor and report issues with voice quality.

Call Admission Control

Call Admission Control (CAC) enables an access point to maintain controlled quality of service (QoS) when the wireless LAN is experiencing congestion. The WMM protocol deployed in CCXv4 maintains QoS under differing network loads.

Two types of Over The Air (OTA) CAC are available: static-based CAC and load-based CAC.

The switch supports the following QoS policies:

- User-defined policies: You can define your own QoS policies. You can have more control over these policies than the existing metal policies.
- System-defined precious metal policies: To support backward compatibility.
    - Platinum: Used for VoIP clients.
    - Gold: Used for video clients.
    - Silver: Used for best effort traffic.
    - Bronze: Used for NRT traffic.

Static-Based CAC

Voice over WLAN applications supporting WMM and TSPEC can specify how much bandwidth or shared medium time is required to initiate a call. Bandwidth-based, or static, CAC enables the access point to determine whether it is capable of accommodating a particular call. The access point rejects the call if necessary in order to maintain the maximum allowed number of calls with acceptable quality.

The QoS setting for a WLAN determines the level of bandwidth-based CAC support. To use bandwidth-based CAC with voice applications, the WLAN must be configured for Platinum QoS. With bandwidth-based CAC, the access point bandwidth availability is determined based on the amount of bandwidth currently used by the access point clients, to which the bandwidth requested by the Voice over WLAN applications is added. If this total exceeds a configured bandwidth threshold, the new call is rejected.

Note You must enable admission control (ACM) for CCXv4 clients that have WMM enabled. Otherwise, bandwidth-based CAC does not operate properly for these CCXv4 clients.

Load-Based CAC

Load-based CAC incorporates a measurement scheme that takes into account the bandwidth consumed by all traffic types (including that from clients), cochannel access point loads, and coallocated channel interference, for voice and video applications. Load-based CAC also covers the additional bandwidth consumption resulting from PHY and channel impairment.

In load-based CAC, the access point continuously measures and updates the utilization of the RF channel (that is, the mean time of bandwidth that has been exhausted), channel interference, and the additional calls that the access point can admit. The access point admits a new call only if the channel has enough unused bandwidth to support that call. By doing so, load-based CAC prevents oversubscription of the channel and maintains QoS under all conditions of WLAN loading and interference.

Note If you disable load-based CAC, the access points start using bandwidth-based CAC.

IOSd Call Admission Control

IOSd Call Admission Control (CAC) controls bandwidth availability from switch to access point.

You can configure class-based, unconditional packet marking features on your switch for CAC.

CAC is a concept that applies to voice and video traffic only—not data traffic. If an influx of data traffic oversubscribes a particular link in the network, queueing, buffering, and packet drop decisions resolve the congestion. The extra traffic is simply delayed until the interface becomes available to send the traffic, or, if traffic is dropped, the protocol or the end user initiates a timeout and requests a retransmission of the information.

Network congestion cannot be resolved in this manner when real-time traffic, sensitive to both latency and packet loss, is present, without jeopardizing the quality of service (QoS) expected by the users of that traffic. For real-time delay-sensitive traffic such as voice, it is better to deny network access under congestion conditions than to allow traffic onto the network to be dropped and delayed, causing intermittent impaired QoS and resulting in customer dissatisfaction.

CAC is therefore a deterministic and informed decision that is made before a voice call is established and is based on whether the required network resources are available to provide suitable QoS for the new call.

Based on the admit CAC CLI configuration in addition to the existing CAC algorithm, switch allows either voice or video with TSPEC or SIP snooping. The **admit cac** CLI is mandatory for the voice call to pass through.

If the BSSID policer is configured for the voice or video traffic, then additional checks are performed on the packets.

Expedited Bandwidth Requests

The expedited bandwidth request feature enables CCXv5 clients to indicate the urgency of a WMM traffic specifications (TSPEC) request (for example, an e911 call) to the WLAN. When the controller receives this request, it attempts to facilitate the urgency of the call in any way possible without potentially altering the quality of other TSPEC calls that are in progress.

You can apply expedited bandwidth requests to both bandwidth-based and load-based CAC. Expedited bandwidth requests are disabled by default. When this feature is disabled, the controller ignores all expedited requests and processes TSPEC requests as normal TSPEC requests.

The following table lists examples of TSPEC request handling for normal TSPEC requests and expedited bandwidth requests.

Table 18: TSPEC Request Handling Examples

CAC Mode	Reserved bandwidth for voice calls[1]	Usage[2]	Normal TSPEC Request	TSPEC with Expedited Bandwidth Request
Bandwidth-based CAC	75% (default setting)	Less than 75%	Admitted	Admitted
		Between 75% and 90% (reserved bandwidth for voice calls exhausted)	Rejected	Admitted
		More than 90%	Rejected	Rejected
Load-based CAC		Less than 75%	Admitted	Admitted
		Between 75% and 85% (reserved bandwidth for voice calls exhausted)	Rejected	Admitted
		More than 85%	Rejected	Rejected

1 For bandwidth-based CAC, the voice call bandwidth usage is per access point radio and does not take into account cochannel access points. For load-based CAC, the voice call bandwidth usage is measured for the entire channel.
2 Bandwidth-based CAC (consumed voice and video bandwidth) or load-based CAC (channel utilization [Pb]).

Note Admission control for TSPEC G711-20ms and G711-40 ms codec types are supported.

U-APSD

Unscheduled automatic power save delivery (U-APSD) is a QoS facility defined in IEEE 802.11e that extends the battery life of mobile clients. In addition to extending battery life, this feature reduces the latency of traffic flow delivered over the wireless media. Because U-APSD does not require the client to poll each individual packet buffered at the access point, it allows delivery of multiple downlink packets by sending a single uplink trigger packet. U-APSD is enabled automatically when WMM is enabled.

Traffic Stream Metrics

In a voice-over-wireless LAN (VoWLAN) deployment, traffic stream metrics (TSM) can be used to monitor voice-related metrics on the client-access point air interface. It reports both packet latency and packet loss. You can isolate poor voice quality issues by studying these reports.

The metrics consist of a collection of uplink (client side) and downlink (access point side) statistics between an access point and a client device that supports CCX v4 or later releases. If the client is not CCX v4 or CCXv5 compliant, only downlink statistics are captured. The client and access point measure these metrics. The access point also collects the measurements every 5 seconds, prepares 90-second reports, and then sends the reports to the controller. The controller organizes the uplink measurements on a client basis and the downlink measurements on an access point basis and maintains an hour's worth of historical data. To store this data, the controller requires 32 MB of additional memory for uplink metrics and 4.8 MB for downlink metrics.

TSM can be configured through either the GUI or the CLI on a per radio-band basis (for example, all 802.11a radios). The controller saves the configuration in flash memory so that it persists across reboots. After an access point receives the configuration from the controller, it enables TSM on the specified radio band.

This table shows the upper limit for TSM entries in different controller series.

TSM Entries	5700
MAX AP TSM entries	100
MAX Client TSM entries	250
MAX TSM entries	100*250=25000

Note Once the upper limit is reached, additional TSM entries cannot be stored and sent to WCS or NCS. If client TSM entries are full and AP TSM entries are available, then only the AP entries are stored, and viceversa. This leads to partial output. TSM cleanup occurs every one hour. Entries are removed only for those APs and clients that are not in the system.

Information About Configuring Voice Prioritization Using Preferred Call Numbers

You can configure a switch to provide support for SIP calls from VoWLAN clients that do not support TSPEC-based calls. This feature is known as SIP CAC support. If bandwidth is available in the configured voice pool, the SIP call uses the normal flow and the switch allocates the bandwidth to those calls.

You can also prioritize up to six preferred call numbers. When a call comes to one of the configured preferred numbers, the switch does not check the configured maximum voice bandwidth. The switch allocates the bandwidth needed for the call, even if it exceeds the maximum bandwidth for voice configured for voice CAC. The preferred call will be rejected if bandwidth allocation exceeds 85% of the radio bandwidth. The bandwidth allocation is 85 percent of the entire bandwidth pool, not just from the maximum configured voice pool. The bandwidth allocation is the same even for roaming calls.

You must configure the following parameters before configuring voice prioritization:

- Set WLAN QoS to allow voice calls to pass through.
- Enable ACM for the radio.
- Enable SIP call snooping on the WLAN.

Information About EDCA Parameters

Enhanced distributed channel access (EDCA) parameters are designed to provide preferential wireless channel access for voice, video, and other quality-of-service (QoS) traffic.

How to Configure Voice and Video Parameters

Configuring Voice Parameters (CLI)

Before You Begin

Ensure that you have configured SIP-based CAC.

You should have created a class map for CAC before beginning this procedure.

SUMMARY STEPS

1. **show wlan summary**
2. **show wlan** *wlan_id*
3. **configure terminal**
4. **policy-map** *policy-map name*
5. **class** {*class-name* | **class-default**}
6. **admit cac wmm-tspec**
7. **service-policy** *policy-map name*
8. **end**
9. **wlan** *wlan_profile_name wlan_ID SSID_network_name* **wlan shutdown**
10. **wlan** *wlan_profile_name wlan_ID SSID_network_name*
11. **wlan** *wlan_name* **call-snoop**
12. **wlan** *wlan_name* **service-policy input** *input_policy_name*
13. **wlan** *wlan_name* **service-policy output** *ouput_policy_name*
14. **wlan** *wlan_name* **service-policy input** *ingress_policy_name*
15. **wlan** *wlan_name* **service-policy output** *egress_policy_name*
16. **ap dot11 {5ghz | 24ghz} shutdown**
17. **ap dot11 {5ghz | 24ghz} cac voice sip**
18. **ap dot11 {5ghz | 24ghz} cac voice acm**
19. **ap dot11 {5ghz | 24ghz} cac voice max-bandwidth** *bandwidth*
20. **ap dot11 {5ghz | 24ghz} cac voice roam-bandwidth** *bandwidth*
21. **no wlan shutdown**
22. **no ap dot11 {5ghz | 24ghz} shutdown**
23. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**show wlan summary** **Example:** `SwitchControllerDevice# show wlan summary`	Specifies all of the WLANs configured on the switch.
Step 2	**show wlan** *wlan_id* **Example:** `SwitchControllerDevice# show wlan 25`	Specifies the WLAN that you plan to modify. For voice over WLAN, ensure that the WLAN is configured for WMM and the QoS level is set to Platinum.
Step 3	**configure terminal** **Example:** `SwitchControllerDevice# configure terminal`	Enters global configuration mode.
Step 4	**policy-map** *policy-map name*	Enters policy map configuration mode.

	Command or Action	Purpose

	Example:
	`SwitchControllerDevice(config)# policy-map test_2000`
	`SwitchControllerDevice(config-pmap)#`
		Creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy.
		In WLAN, you need to configure service-policy for these commands to take effect.

Step 5	**class** {*class-name* | **class-default**}
	Example:
	`SwitchControllerDevice(config-pmap)# class test_1000`
	`SwitchControllerDevice(config-pmap-c)#`
		Enters policy class map configuration mode. Specifies the name of the class whose policy you want to create or change.
		Specifies the name of the class whose policy you want to create or change.
		You can also create a system default class for unclassified packets.

Step 6	**admit cac wmm-tspec**
	Example:
	`SwitchControllerDevice(config-pmap-c)# admit cac wmm-tspec`
	`SwitchControllerDevice(config-pmap-c)#`
		(Optional) Admits the request for Call Admission Control (CAC) for policy map.

Step 7	**service-policy** *policy-map name*
	Example:
	`SwitchControllerDevice(config-pmap-c)# service-policy test_2000`
	`SwitchControllerDevice(config-pmap-c)#`
		Configures the QoS service policy.

Step 8	**end** **Example:** `SwitchControllerDevice(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Step 9	**wlan** *wlan_profile_name wlan_ID SSID_network_name* **wlan shutdown**
	Example:
	`SwitchControllerDevice(config)# wlan wlan1`
	`SwitchControllerDevice(config-wlan)# wlan shutdown`
		Disables all WLANs with WMM enabled prior to changing the video parameters.

Step 10	**wlan** *wlan_profile_name wlan_ID SSID_network_name*
	Example:
	`SwitchControllerDevice(config)# wlan wlan1`
	`SwitchControllerDevice(config-wlan)# wlan shutdown`
		Disables all WLANs with WMM enabled prior to changing the voice parameters.

Step 11	**wlan** *wlan_name* **call-snoop** **Example:** `SwitchControllerDevice(config)# wlan wlan1 call-snoop`	Enables the call-snooping on a particular WLAN.

	Command or Action	Purpose

Step 12	**wlan** *wlan_name* **service-policy input** *input_policy_name*
	
	Example:
	`SwitchControllerDevice(config)# wlan wlan1`
	`SwitchControllerDevice(config-wlan)#`
	`service-policy input platinum-up`
		Configures input SSID policy on a particular WLAN to voice.

Step 13	**wlan** *wlan_name* **service-policy output** *ouput_policy_name*
	
	Example:
	`SwitchControllerDevice(config)# wlan wlan1`
	`SwitchControllerDevice(config-wlan)#`
	`service-policy output platinum`
		Configures output SSID policy on a particular WLAN to voice.

Step 14	**wlan** *wlan_name* **service-policy input** *ingress_policy_name*
	
	Example:
	`SwitchControllerDevice(config)# wlan wlan1`
	`SwitchControllerDevice(config-wlan)#`
	`service-policy input policy1`
		Configures ingress SSID policy on a particular WLAN as user-defined policy.

Step 15	**wlan** *wlan_name* **service-policy output** *egress_policy_name*
	
	Example:
	`SwitchControllerDevice(config)# wlan wlan1`
	`SwitchControllerDevice(config-wlan)#`
	`service-policy output policy2`
		Configures egress SSID policy on a particular WLAN as user-defined policy.

Step 16	**ap dot11 {5ghz | 24ghz} shutdown** **Example:**	Disables the radio network. `SwitchControllerDevice(config)# ap dot11 5ghz shutdown`
Step 17	**ap dot11 {5ghz | 24ghz} cac voice sip** **Example:** `SwitchControllerDevice(config)# ap dot11 5ghz cac voice sip`	Enables or disables SIP IOSd CAC for the 802.11a or 802.11b/g network.
Step 18	**ap dot11 {5ghz | 24ghz} cac voice acm** **Example:** `SwitchControllerDevice(config)# ap dot11 5ghz cac voice acm`	Enables or disables bandwidth-based voice CAC for the 802.11a or 802.11b/g network.
Step 19	**ap dot11 {5ghz | 24ghz} cac voice max-bandwidth** *bandwidth* **Example:** `SwitchControllerDevice(config)# ap dot11 5ghz cac voice max-bandwidth 85`	Sets the percentage of maximum bandwidth allocated to clients for voice applications on the 802.11a or 802.11b/g network. The bandwidth range is 5 to 85%, and the default value is 75%. Once the client reaches the value specified, the access point rejects new videos on this network.

	Command or Action	Purpose
Step 20	**ap dot11 {5ghz | 24ghz} cac voice roam-bandwidth** *bandwidth* **Example:** `SwitchControllerDevice(config)# ap dot11 5ghz cac voice roam-bandwidth 10`	Sets the percentage of maximum allocated bandwidth reserved for roaming voice clients. The bandwidth range is 0 to 25%, and the default value is 6%. The switch reserves this much bandwidth from the maximum allocated bandwidth for roaming voice clients.
Step 21	**no wlan shutdown** **Example:** `SwitchControllerDevice(config-wlan)# no wlan shutdown`	Reenables all WLANs with WMM enabled.
Step 22	**no ap dot11 {5ghz | 24ghz} shutdown** **Example:** `SwitchControllerDevice(config)# no ap dot11 5ghz shutdown`	Reenables the radio network.
Step 23	**end** **Example:** `SwitchControllerDevice(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Configuring Video Parameters (CLI)

SUMMARY STEPS

1. **show wlan summary**
2. **show wlan** *wlan_id*
3. **configure terminal**
4. **policy-map** *policy-map name*
5. **class** {*class-name* | **class-default**}
6. **admit cac wmm-tspec**
7. **service-policy** *policy-map name*
8. **end**
9. **wlan***wlan_profile_name*
10. **ap dot11 {5ghz | 24ghz} shutdown**
11. **ap dot11 {5ghz | 24ghz} cac video acm**
12. **ap dot11 {5ghz | 24ghz} cac video load-based**
13. **ap dot11 {5ghz | 24ghz} cac video max-bandwidth** *bandwidth*
14. **ap dot11 {5ghz | 24ghz} cac video roam-bandwidth** *bandwidth*
15. **no wlan shutdown** *wlan_id*
16. **no ap dot11 {5ghz | 24ghz} shutdown**
17. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**show wlan summary** **Example:** `SwitchControllerDevice# show wlan summary`	Specifies all of the WLANs configured on the switch.
Step 2	**show wlan** *wlan_id* **Example:** `SwitchControllerDevice# show wlan 25`	Specifies the WLAN that you plan to modify.
Step 3	**configure terminal** **Example:** `SwitchControllerDevice# configure terminal`	Enters global configuration mode.

Step 4	**policy-map** *policy-map name*
	
	Example:
	`SwitchControllerDevice(config)# policy-map test_2000`
	`SwitchControllerDevice(config-pmap)#`
		Enters policy map configuration mode.
		Creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy.
		In WLAN, you need to configure service-policy for these commands to take effect.

	Command or Action	Purpose

Step 5	**class** {*class-name* | **class-default**}
	
	Example:
	`SwitchControllerDevice(config-pmap)# class test_1000`
	`SwitchControllerDevice(config-pmap-c)#`
		Enters policy class map configuration mode. Specifies the name of the class whose policy you want to create or change.
		Specifies the name of the class whose policy you want to create or change.
		You can also create a system default class for unclassified packets.

Step 6	**admit cac wmm-tspec**
	
	Example:
	`SwitchControllerDevice(config-pmap-c)# admit cac wmm-tspec`
	`SwitchControllerDevice(config-pmap-c)#`
		(Optional) Admits the request for Call Admission Control (CAC) for policy map.

Step 7	**service-policy** *policy-map name*
	
	Example:
	`SwitchControllerDevice(config-pmap-c)# service-policy test_2000`
	`SwitchControllerDevice(config-pmap-c)#`
		Configures the QoS service policy.

Step 8	**end** **Example:** `SwitchControllerDevice(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Step 9	**wlan***wlan_profile_name*
	
	Example:
	`SwitchControllerDevice(config)# wlan wlan1`
	`SwitchControllerDevice(config-wlan)# wlan shutdown`
		Disables all WLANs with WMM enabled prior to changing the video parameters.

Step 10	**ap dot11 {5ghz | 24ghz} shutdown** **Example:** `SwitchControllerDevice(config)# ap dot11 5ghz shutdown`	Disables the radio network.
Step 11	**ap dot11 {5ghz | 24ghz} cac video acm** **Example:** `SwitchControllerDevice(config)# ap dot11 5ghz cac video acm`	Enables or disables bandwidth-based video CAC for the 802.11a or 802.11b/g network.
Step 12	**ap dot11 {5ghz | 24ghz} cac video load-based** **Example:** `SwitchControllerDevice(config)# ap dot11 5ghz cac video load-based`	Configures the load-based CAC method. If you do not enter this command, then the default static CAC is applied.

	Command or Action	Purpose
Step 13	**ap dot11 {5ghz | 24ghz} cac video max-bandwidth** *bandwidth* **Example:** `SwitchControllerDevice(config)#` **`ap dot11 5ghz cac video max-bandwidth 20`**	Sets the percentage of maximum bandwidth allocated to clients for video applications on the 802.11a or 802.11b/g network. The bandwidth range is 5 to 85%, and the default value is 75%. The default value is 0, which means no bandwidth request control. The sum of the voice bandwidth and video bandwidth should not exceed 85% or configured maximum media bandwidth.
Step 14	**ap dot11 {5ghz | 24ghz} cac video roam-bandwidth** *bandwidth* **Example:** `SwitchControllerDevice(config)#` **`ap dot11 5ghz cac video roam-bandwidth 9`**	Sets the percentage of maximum allocated bandwidth reserved for roaming clients for video. The bandwidth range is 0 to 25%, and the default value is 0%.
Step 15	**no wlan shutdown** *wlan_id* **Example:** `SwitchControllerDevice(config-wlan)#` **`no wlan shutdown 25`**	Reenables all WLANs with WMM enabled.
Step 16	**no ap dot11 {5ghz | 24ghz} shutdown** **Example:** `SwitchControllerDevice(config)#` **`no ap dot11 5ghz shutdown`**	Reenables the radio network.
Step 17	**end** **Example:** `SwitchControllerDevice(config)#` **`end`**	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Configuring SIP-Based CAC (CLI)

SIP CAC controls the total number of SIP calls that can be made.

SUMMARY STEPS

1. **configure terminal**
2. **wlan** *wlan-name*
3. **call-snoop**
4. **service-policy** [**client**] **input** *policy-map name*
5. **service-policy** [**client**] **output** *policy-map name*
6. **end**
7. **show wlan** {*wlan-id* | *wlan-name*}
8. **configure terminal**
9. **ap dot11 {5ghz | 24ghz} cac {voice | video} acm**
10. **ap dot11 {5ghz | 24ghz} cac voice sip**
11. **end**

DETAILED STEPS

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

Step 2	**wlan** *wlan-name*
	
	Example:
	`SwitchControllerDevice(config)# wlan qos-wlan`
	`SwitchControllerDevice(config-wlan)#`
		Enters WLAN configuration submode.

Step 3	**call-snoop** **Example:** `SwitchControllerDevice(config-wlan)# call-snoop`	Enables the call-snooping feature for a particular WLAN.

Step 4	**service-policy** [**client**] **input** *policy-map name*
	
	Example:
	`SwitchControllerDevice(config-wlan)#`
	`service-policy input platinum-up`
		Assigns a policy map to WLAN input traffic. Ensure that you provide QoS policy to voice for input traffic.

Step 5	**service-policy** [**client**] **output** *policy-map name*
	
	Example:
	`SwitchControllerDevice(config-wlan)#`
	`service-policy output platinum`
		Assigns policy map to WLAN output traffic. Ensure that you provide QoS policy to voice for output traffic.

Step 6	**end** **Example:** `SwitchControllerDevice(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.
Step 7	**show wlan** {*wlan-id* | *wlan-name*}	Verifies the configured QoS policy on the WLAN.

	Command or Action	Purpose
	Example: `SwitchControllerDevice#` **`show wlan qos-wlan`**	
Step 8	**configure terminal** **Example:** `SwitchControllerDevice#` **`configure terminal`**	Enters global configuration mode.
Step 9	**ap dot11 {5ghz | 24ghz} cac {voice | video} acm** **Example:** `SwitchControllerDevice(config)#` **`ap dot11 5ghz cac voice acm`**	Enables the ACM static on the radio. When enabling SIP snooping, use the static CAC, not the load-based CAC.
Step 10	**ap dot11 {5ghz | 24ghz} cac voice sip** **Example:** `SwitchControllerDevice(config)#` **`ap dot11 5ghz cac voice sip`**	Configures SIP-based CAC.
Step 11	**end** **Example:** `SwitchControllerDevice(config)#` **`end`**	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Configuring a Preferred Call Number (CLI)

Before You Begin

You must set the following parameters before configuring a preferred call number.

- Set WLAN QoS to voice.
- Enable ACM for the radio.
- Enable SIP call snooping on the WLAN.
- Enable SIP-based CAC.

SUMMARY STEPS

1. **configure terminal**
2. **wlan** *wlan-name* **qos platinum**
3. **ap dot11 {5ghz | 24ghz} cac {voice | video} acm**
4. **wlan** *wlan-name*
5. **wireless sip preferred-call-no** *call_index call_number*
6. **no wireless sip preferred-call-no** *call_index*
7. **end**

DETAILED STEPS

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

Step 2	**wlan** *wlan-name* **qos platinum**
	
	Example:
	`SwitchControllerDevice(config)# wlan wlan1`
	`SwitchControllerDevice(config-wlan)# qos platinum`
		Sets QoS to voice on a particular WLAN.

Step 3	**ap dot11 {5ghz | 24ghz} cac {voice | video} acm** **Example:** `SwitchControllerDevice(config)# ap dot11 5ghz cac voice acm`	Enables the static ACM on the radio. When enabling SIP snooping, use the static CAC, not the load-based CAC.

Step 4	**wlan** *wlan-name*
	
	Example:
	`SwitchControllerDevice(config)# wlan wlan1`
	`SwitchControllerDevice(config-wlan)# call-snoop`
		Enables the call-snooping feature for a particular WLAN.

Step 5	**wireless sip preferred-call-no** *call_index call_number* **Example:** `SwitchControllerDevice(config)# wireless sip preferred-call-no 1 555333`	Adds a new preferred call.
Step 6	**no wireless sip preferred-call-no** *call_index* **Example:** `SwitchControllerDevice(config)# no wireless sip preferred-call-no 1`	Removes a preferred call.
Step 7	**end** **Example:** `SwitchControllerDevice(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Configuring EDCA Parameters (CLI)

SUMMARY STEPS

1. **configure terminal**
2. **ap dot11 {5ghz | 24ghz } shutdown**
3. **ap dot11 {5ghz | 24ghz} edca-parameters {custom-voice | optimized-video-voice | optimized-voice | svp-voice | wmm-default}**
4. **show ap dot11 {5ghz | 24ghz} network**
5. **no ap dot11 {5ghz | 24ghz} shutdown**
6. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `SwitchControllerDevice# `**`configure terminal`**	Enters global configuration mode.
Step 2	**ap dot11 {5ghz	24ghz } shutdown** **Example:** `SwitchControllerDevice(config)# `**`ap dot11 5ghz shutdown`**	Disables the radio network.
Step 3	**ap dot11 {5ghz	24ghz} edca-parameters {custom-voice	optimized-video-voice	optimized-voice	svp-voice	wmm-default}** **Example:** `SwitchControllerDevice(config)# `**`ap dot11 5ghz edca-parameters optimized-voice`**	Enables a specific EDCA parameters for the 802.11a or 802.11b/g network. • custom-voice—Enables custom voice parameters for the 802.11a or 802.11b/g network. • optimized-video-voice—Enables EDCA voice- and video-optimized parameters for the 802.11a or 802.11b/g network. Choose this option when both voice and video services are deployed on your network. • optimized-voice—Enables non-SpectraLink voice-optimized profile parameters for the 802.11a or 802.11b/g network. Choose this option when voice services other than SpectraLink are deployed on your network. • svp-voice—Enables SpectraLink voice priority parameters for the 802.11a or 802.11b/g network.

	Command or Action	Purpose
		Choose this option if SpectraLink phones are deployed on your network to improve the quality of calls. • wmm-default—Enables the Wi-Fi Multimedia (WMM) default parameters for the 802.11a or 802.11b/g network. This is the default value. Choose this option when voice or video services are not deployed on your network.
Step 4	**show ap dot11 {5ghz | 24ghz} network** **Example:** `SwitchControllerDevice(config)# show ap dot11 5ghz network`	Displays the current status of MAC optimization for voice.
Step 5	**no ap dot11 {5ghz | 24ghz} shutdown** **Example:** `SwitchControllerDevice(config)# no ap dot11 5ghz shutdown`	Reenables the radio network.
Step 6	**end** **Example:** `SwitchControllerDevice(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Monitoring Voice and Video Parameters

This section describes the new commands for the voice and video parameters.

The following commands can be used to monitor voice and video parameters.

Table 19: Monitoring Voice Parameters Commands

Command	Purpose
show ap dot11 {5ghz | 24ghz} network	Displays the radio-based statistics for voice.
show ap name *ap_name* **dot11 24ghz tsm all**	Displays the TSM voice metrics and current status of MAC optimization for voice.
show ap name *apname* **cac voice**	Displays the information about CAC for a particular access point.
show client detail *client_mac*	Displays the U-APSD status for a particular client.
show policy-map interface wireless client	Displays the video client policy details.

show access-list	Displays the video client dynamic access-list from the switch.
show wireless client voice diag status	Displays information about whether voice diagnostics are enabled or disabled. If enabled, this also displays information about the clients in the watch list and the time remaining for the diagnostics of the voice call. **Note** To work on voice diagnostics CLIs, you need to enter the following command: **debug voice-diagnostic mac-addr** *client_mac_01 client_mac_02*
show wireless client voice diag tspec	Displays the TSPEC information sent from the clients that are enabled for voice diagnostics.
show wireless client voice diag qos-map	Displays information about the QoS/DSCP mapping and packet statistics in each of the four queues: VO, VI, BE, BK. The different DSCP values are also displayed.
show wireless client voice diag rssi	Display the client's RSSI values in the last 5 seconds when voice diagnostics is enabled.
show client voice-diag roam-history	Displays information about the last three roaming calls. The output contains the timestamp, access point associated with roaming, roaming reason, and if there is a roaming failure, reason for roaming-failure.
show policy-map interface wireless mac *mac-address*	Displays information about the voice and video data packet statistics.
show wireless media-stream client summary	Displays a summary of the media stream and video client information.
show controllers d0 | b queue	Displays which queue the packets are going through on an access point.
show platform qos queue stats *interface*	Displays which queue packets are going through from the switch.

You can monitor the video parameters using the following commands.

Table 20: Monitoring Video Parameters Commands

Command	Purpose
show ap join stats summary *ap_mac*	Displays the last join error detail for a specific access point.

show ip igmp snooping wireless mgid	Displays the TSM voice metrics and current status of MAC optimization for voice.
show wireless media-stream multicast-direct state	Displays the media stream multicast-direct parameters.
show wireless media-stream group summary	Displays the summary of the media stream and client information.
show wireless media-stream group detail *group_name*	Displays the details of a specific media-stream group.
show wireless media-stream client summary	Displays the details for a set of media-stream clients.
show wireless media-stream client detail *group_name*	Displays the details for a set of media-stream clients.
show ap dot11 {5ghz | 24ghz) media-stream rrc	Display the details of media stream.
show wireless media-stream message details	Displays information about the message configuration.
show ap name *ap-name* **auto-rf dot11 5ghz | i Util**	Displays the details of channel utilization.
show controllers d0 | b queue	Displays which queue the packets are going through on an access point based on 2.4- and 5-GHz bands.
show controllers d1 | b queue	Displays which queue the packets are going through on an access point based on 2.4- and 5-GHz bands.
show cont d1 | b Media	Displays the video metric details on the band A or B.
show capwap mcast mgid all	Displays information about all of the multicast groups and their corresponding multicast group identifications (MGIDs) associated to the access point.
show capwap mcast mgid id *id*	Displays information about all of the video clients joined to the multicast group in a specific MGID.

Additional References for Voice and Video Parameters

Related Documents

Related Topic	Document Title
Multicast configuration	*Multicast Configuration Guide, Cisco IOS XE Release 3SE (Cisco WLC 5700 Series)*

Related Topic	Document Title
VideoStream configuration	*VideoStream Configuration Guide, Cisco IOS XE Release 3SE (Cisco WLC 5700 Series)*

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

Feature History and Information For Performing Voice and Video Parameters Configuration

Release	Feature Information
Cisco IOS XE 3.2SE	This feature was introduced.

CHAPTER 11

Configuring RFID Tag Tracking

Finding Feature Information

Your software release may not support all of 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 RFID Tag Tracking

The SwitchControllerDevice enables you to configure radio-frequency identification (RFID) tag tracking. RFID tags are small wireless devices that are affixed to assets for real-time location tracking. They operate by advertising their location using special 802.11 packets, which are processed by access points, the controller, and the location appliance.

How to Configure RFID Tag Tracking

Configuring RFID Tag Tracking (CLI)

SUMMARY STEPS

1. **location rfid status**
2. (Optional) **no location rfid status**
3. **location rfid timeout** *seconds*
4. **location rfid mobility vendor-name** *name*
5. (Optional) **no location rfid mobility** *name*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**location rfid status** **Example:** `SwitchControllerDevice(config)# location rfid status`	Enables RFID tag tracking. By default, RFID tag tracking is enabled.
Step 2	(Optional) **no location rfid status** **Example:** `SwitchControllerDevice(config)# no location rfid status`	Disables RFID tag tracking.
Step 3	**location rfid timeout** *seconds* **Example:** `SwitchControllerDevice(config)# location rfid timeout 1500`	Specifies a static timeout value (between 60 and 7200 seconds). The static timeout value is the amount of time that the switch maintains tags before expiring them. For example, if a tag is configured to beacon every 30 seconds, we recommend that you set the timeout value to 90 seconds (approximately three times the beacon value). The default value is 1200 seconds.
Step 4	**location rfid mobility vendor-name** *name* **Example:** `SwitchControllerDevice(config)# location rfid mobility vendor-name Aerosct`	Enables RFID tag mobility for specific tags. When you enter the **location rfid mobility vendor-name** command, tags are unable to obtain a DHCP address for client mode when attempting to select and/or download a configuration. **Note** These commands can be used only for Pango tags. Therefore, the only valid entry for **vendor_name** is “pango” in all lowercase letters.
Step 5	(Optional) **no location rfid mobility** *name* **Example:** `SwitchControllerDevice(config)# no location rfid mobility test`	Disables RFID tag mobility for specific tags. When you enter the **no location rfid mobility** command , tags can obtain a DHCP address. If a tag roams from one subnet to another, it obtains a new address rather than retaining the anchor state.

Monitoring RFID Tag Tracking Information

This section describes the new commands for the RFID tag tracking Information.

The following commands can be used to monitor the RFID tag tracking Information on the switch.

Table 21: Monitoring RFID Tag Tracking Information Commands

Command	Purpose
show location rfid config	Displays the current configuration for RFID tag tracking.
show location rfid detail *mac_address*	Displays the detailed information for a specific RFID tag.
show location rfid summary	Displays a list of all RFID tags currently connected to the switch.
show location rfid client	Displays a list of RFID tags that are associated to the switch as clients.

Additional References RFID Tag Tracking

Related Documents

Related Topic	Document Title
System management commands	*System Management Command Reference, Cisco IOS XE Release 3SE (Cisco WLC 5700 Series)*

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

Feature History and Information For Performing RFID Tag Tracking Configuration

Release	Feature Information
Cisco IOS XE 3.2SE	This feature was introduced.

CHAPTER 12

Configuring Location Settings

Finding Feature Information

Your software release may not support all of 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 Location Settings

The switch determines the location of client devices by gathering Received Signal Strength Indication (RSSI) measurements from access points all around the client of interest. The switch can obtain location reports from up to 16 access points for clients, RFID tags, and rogue access points.

You can configure the path loss measurement (S60) request for normal clients or calibrating clients to improve location accuracy.

How to Configure Location Settings

Configuring Location Settings (CLI)

SUMMARY STEPS

1. **configure terminal**
2. **location plm** {**calibrating** [**multiband** | **uniband**] | **client** *burst_interval*
3. **location rssi-half-life** {**calibrating-client** | **client** | **rogue-aps** | **tags** } *seconds*
4. **location expiry** {**calibrating-client** | **client** | **rogue-aps** | **tags** } *timeout*
5. **location algorithm** {**rssi-average** | **simple**}
6. **location admin-tag** *string*
7. **location civic-location identifier** {*identifier* | **host**}
8. **location custom-location identifier** {*identifier* | **host**}
9. **location geo-location identifier** {*identifier* | **host**}
10. **location prefer** {**cdp** | **lldp-med** | **static**} **weight** *priority_value*
11. **location rfid** {**status** | **timeout** | **vendor-name**}
12. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `SwitchControllerDevice# configure terminal`	Enters global configuration mode.
Step 2	**location plm** {**calibrating** [**multiband** | **uniband**] | **client** *burst_interval* **Example:** `SwitchControllerDevice(config)# location plm client 100`	Configures the path loss measurement (S60) request for calibrating clients or non-calibrating. The path loss measurement request improves the location accuracy. You can configure the **burst_interval** parameter for the normal, noncalibrating client from zero through 3600 seconds, and the default value is 60 seconds. You can configure the path loss measurement request for calibrating clients on the associated 802.11a or 802.11b/g radio or on the associated 802.11a/b/g radio. If a client does not send probes often or sends them only on a few channels, its location cannot be updated or cannot be updated accurately. The **location plm** command forces clients to send more packets on all channels. When a CCXv4 (or higher) client associates, the SwitchControllerDevice sends it a path loss measurement request, which instructs the client to transmit on the bands and channels that the access points are on (typically, channels 1,

	Command or Action	Purpose
		6, and 11 for 2.4-GHz-only access points) at a configurable interval (such as 60 seconds) indefinitely.
Step 3	**location rssi-half-life** {**calibrating-client** | **client** | **rogue-aps** | **tags** } *seconds* **Example:** `SwitchControllerDevice(config)#` **`location rssi-half-life calibrating-client 60`**	Configures the RSSI half life for the clients, calibrating clients, RFID tags, and rogue access points. You can enter the **location rssi-half-life** parameter value for the clients, calibrating clients, RFID tags, and rogue access points as 0, 1, 2, 5, 10, 20, 30, 60, 90, 120, 180, or 300 seconds, and the default value is 0 seconds. Some client devices transmit at reduced power immediately after changing channels, and RF is variable, so RSSI values might vary considerably from packet to packet. The **location rssi-half-life** command increases accuracy by averaging nonuniformly arriving data using a configurable forget period (or half life). **Note** We recommend that you do not use or modify the **location rssi-half-life** command.
Step 4	**location expiry** {**calibrating-client** | **client** | **rogue-aps** | **tags** } *timeout* **Example:** `SwitchControllerDevice(config)#` **`location expiry calibrating-client 50`**	Configures the RSSI timeout value for the clients, calibrating clients, RFID tags, and rogue access points. You can enter the RSSI timeout value for the clients, RFID tags, and rogue access points from 5 through 3600 seconds, and the default value is 5 seconds. For the calibrating clients, you can enter the RSSI timeout value from 0 through 3600 seconds, and the default value is 5 seconds. Ensuring that recent, strong RSSIs are retained by the CPU is critical to location accuracy. The **location expiry** command enables you to specify the length of time after which old RSSI averages expire. **Note** We recommend that you do not use or modify the **location expiry** command.
Step 5	**location algorithm** {**rssi-average** | **simple**} **Example:** `SwitchControllerDevice(config)#` **`location algorithm rssi-average`**	Configures the algorithm used to average RSSI and signal-to-noise ratio (SNR) values. You can enter the **location algorithm rssi-average** command to specify a more accurate algorithm but requires more CPU overhead or the **location algorithm simple** command to specify a faster algorithm that requires low CPU overhead but provides less accuracy. **Note** We recommend that you do not use or modify the **location algorithm** command.
Step 6	**location admin-tag** *string* **Example:** `SwitchControllerDevice(config)#` **`location admin-tag`**	Sets administrative tag or site information for the location of client devices.
Step 7	**location civic-location identifier** {*identifier* | **host**}	Specifies civic location information. You can set the civic location identifier either as a string or host.

	Command or Action	Purpose
	Example: `SwitchControllerDevice(config)#` **`location civic-location identifier host`**	
Step 8	**location custom-location identifier** {*identifier* | **host**} **Example:** `SwitchControllerDevice(config)#` **`location custom-location identifier host`**	Specifies custom location information. You can set the custom location identifier either as a string or host.
Step 9	**location geo-location identifier** {*identifier* | **host**} **Example:** `SwitchControllerDevice(config)#` **`location geo-location identifier host`**	Specifies geographical location information of the client devices. You can set the location identifier either as a string or host.
Step 10	**location prefer** {**cdp** | **lldp-med** | **static**} **weight** *priority_value* **Example:** `SwitchControllerDevice(config)#` **`location prefer weight cdp 50`**	Sets location information source priority. You can enter the priority weight from zero through 255.
Step 11	**location rfid** {**status** | **timeout** | **vendor-name**} **Example:** `SwitchControllerDevice(config)#` **`location rfid timeout 100`**	Configures RFID tag tracking options such as RFID tag status, RFID timeout value, and RFID tag vendor name. You can enter the RFID timeout value in a range from 60 and 7200 seconds.
Step 12	**end** **Example:** `SwitchControllerDevice(config)#` **`end`**	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Modifying the NMSP Notification Interval for Clients, RFID Tags, and Rogues (CLI)

The Network Mobility Services Protocol (NMSP) manages communication between the mobility services engine and the controller for incoming and outgoing traffic. If your application requires more frequent location updates, you can modify the NMSP notification interval (to a value between 1 and 180 seconds) for clients, active RFID tags, and rogue access points and clients.

Note The TCP port (16113) that the controller and mobility services engine communicate over must be open (not blocked) on any firewall that exists between the controller and the mobility services engine for NMSP to function.

SUMMARY STEPS

1. **configure terminal**
2. **nmsp notification interval** {**attachment** *seconds* | **location** *seconds* | **rssi** [**clients** *interval* | **rfid** *interval* | **rogues** [**ap** | **client**] *interval*]}
3. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `SwitchControllerDevice# configure terminal`	Enters global configuration mode.
Step 2	**nmsp notification interval** {**attachment** *seconds* | **location** *seconds* | **rssi** [**clients** *interval* | **rfid** *interval* | **rogues** [**ap** | **client**] *interval*]} **Example:** `SwitchControllerDevice(config)# nmsp notification interval rssi rfid 50`	Sets the NMSP notification interval value for clients, RFID tags, and rogue clients and access points. You can enter the NMSP notification interval value for RSSI measurement from 1 through 180 seconds.
Step 3	**end** **Example:** `SwitchControllerDevice(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Modifying the NMSP Notification threshold for Clients, RFID Tags, and Rogues (CLI)

SUMMARY STEPS

1. **configure terminal**
2. **location notify-threshold** {**clients** | **rogues ap** | **tags** } *threshold*
3. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `SwitchControllerDevice# configure terminal`	Enters global configuration mode.
Step 2	**location notify-threshold** {**clients** | **rogues ap** | **tags** } *threshold* **Example:** `SwitchControllerDevice(config)# location notify-threshold clients 5`	Configures the NMSP notification threshold for clients, RFID tags, and rogue clients and access points. You can enter the RSSI threshold value from zero through 10 db.
Step 3	**end** **Example:** `SwitchControllerDevice(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Monitoring Location Settings and NMSP Settings

Monitoring Location Settings (CLI)

This section describes the new commands for location settings.

The following commands can be used to monitor location settings on the switch.

Table 22: Monitoring Location Settings Commands

Command	Purpose
show location summary	Displays the current location configuration values.
show location statistics rfid	Displays the location-based RFID statistics.
show location detail *client_mac_addr*	Displays the RSSI table for a particular client.

Monitoring NMSP Settings (CLI)

This section describes the new commands for NMSP settings.

The following commands can be used to monitor NMSP settings on the switch.

Table 23: Monitoring NMSP Settings Commands

Command	Purpose
show nmsp attachment suppress interfaces	Displays the attachment suppress interfaces.
show nmsp capability	Displays the NMSP capabilities.
show nmsp notification interval	Displays the NMSP notification intervals.
show nmsp statistics connection	Displays the connection-specific NMSP counters.
show nmsp statistics summary	Displays the common NMSP counters.
show nmsp status	Displays the status of active NMSP connections.
show nmsp subscription detail	Displays all of the mobility services to which the switch is subscribed.
show nmsp subscription detail *ip_addr*	Displays details only for the mobility services subscribed to by a specific IP address.
show nmsp subscription summary	Displays details for all of the mobility services to which the switch is subscribed.

Examples: Location Settings Configuration

This example shows how to configure the path loss measurement (S60) request for calibrating client on the associated 802.11a or 802.11b/g radio:

```
SwitchControllerDevice# configure terminal
SwitchControllerDevice(config)# location plm calibrating uniband
SwitchControllerDevice(config)# end
SwitchControllerDevice# show location summary
```

This example shows how to configure the RSSI half life for a rouge access point:

```
SwitchControllerDevice# configure terminal
SwitchControllerDevice(config)# location rssi-half-life rogue-aps 20
SwitchControllerDevice(config)# end
SwitchControllerDevice# show location summary
```

Examples: NMSP Settings Configuration

This example shows how to configure the NMSP notification interval for RFID tags:

```
SwitchControllerDevice# configure terminal
SwitchControllerDevice(config)# nmsp notification interval rssi rfid 50
```

```
SwitchControllerDevice(config)# end
SwitchControllerDevice# show nmsp notification interval
```

This example shows how to configure the NMSP notification threshold for clients:

```
SwitchControllerDevice# configure terminal
SwitchControllerDevice(config)# nmsp notify-threshold 5
SwitchControllerDevice(config)# end
SwitchControllerDevice# show nmsp statistics summary
```

Additional References for Location Settings

Related Documents

Related Topic	Document Title
System management commands	*System Management Command Reference, Cisco IOS XE Release 3SE (Cisco WLC 5700 Series)*

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

Feature History and Information For Performing Location Settings Configuration

Release	Feature Information
Cisco IOS XE 3.2SE	This feature was introduced.

CHAPTER 13

Monitoring Flow Control

Finding Feature Information

Your software release may not support all of 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 Flow Control

Flow control is enabled by default on the switch.

Flow control provides shim layers between WCM and Cisco IOS for a reliable IPC. Every component in WCM has a dedicated channel. Few of the components in WCM have leveraged flow control in that. There is no configuration of flow control from CLI. You can monitor the flow control for any channel.

Monitoring Flow Control

This section describes the new commands for flow control.

The following commands can be used to monitor flow control on the switch.

Table 24: Monitoring Flow Control

Command	Purpose
show wireless flow-control *channel -id*	Displays information about flow control on a particular channel.
show wireless flow-control *channel-id* **statistics**	Displays statistical information about flow control on a particular channel.

Examples: Monitoring Flow Control

This example shows how to view information pertaining to any channel:

```
SwitchControllerDevice# show wireless flow-control 3
SwitchControllerDevice#

Channel Name        : CAPWAP
FC State            : Disabled
Remote Server State : Enabled
Pass-thru Mode      : Disabled
EnQ Disabled        : Disabled
Queue Depth         : 2048
Max Retries         : 5
Min Retry Gap (mSec): 3
```

This example shows how to view flow control for a particular channel:

```
SwitchControllerDevice# show wireless flow-control 3
SwitchControllerDevice#

Channel Name                                : CAPWAP
# of times channel went into FC             : 0
# of times channel came out of FC           : 0
Total msg count received by the FC Infra    : 1
Pass-thru msgs send count                   : 0
Pass-thru msgs fail count                   : 0
# of msgs successfully queued               : 0
# of msgs for which queuing failed          : 0
# of msgs sent thru after queuing           : 0
# of msgs sent w/o queuing                  : 1
# of msgs for which send failed             : 0
# of invalid EAGAINS received               : 0
Highest watermark reached                   : 0
# of times Q hit max capacity               : 0
Avg time channel stays in FC (mSec)         : 0
```

Additional References for Monitoring Flow Control

Related Documents

Related Topic	Document Title
System management commands	*System Management Command Reference Guide, Cisco IOS XE Release 3SE (Cisco WLC 5700 Series)*

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

Feature History and Information For Monitoring Flow Control

Release	Feature Information
Cisco IOS XE 3.3SE	This feature was introduced.

CHAPTER 14

Configuring SDM Templates

Finding Feature Information

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

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

Related Topics

Feature History and Information for Troubleshooting Software Configuration, on page 336

Information About Configuring SDM Templates

SDM Templates

You can use SDM templates to configure system resources to optimize support for specific features, depending on how your device is used in the network. You can select a template to provide maximum system usage for some functions.

These templates are supported on your device:

- Advanced—The advanced template is available on all supported images for this release. It maximizes system resources for features like netflow, multicast groups, security ACEs, QoS ACEs, and so on.
- VLAN—The VLAN template is available only on the LAN Base license. The VLAN template disables routing and supports the maximum number of unicast MAC addresses. It would typically be selected for a Layer 2 device.

After you change the template and the system reboots, you can use the **show sdm prefer** privileged EXEC command to verify the new template configuration. If you enter the **show sdm prefer** command before you enter the **reload** privileged EXEC command, the **show sdm prefer** command shows the template currently in use and the template that will become active after a reload.

The default is the advanced template.

Table 25: Approximate Number of Feature Resources Allowed by Templates

Resource	Advanced	VLAN
Number of VLANs	4094	4094
Unicast MAC addresses	32 K	32 K
Overflow unicast MAC addresses	512	512
IGMP groups and multicast routes	4 K	4 K
Overflow IGMP groups and multicast routes	512	512
• Directly connected routes	32 K	32 K
• Indirectly connected IP hosts	8 K	8 K
Policy-based routing ACEs	1024	0
QoS classification ACEs	3 K	3 K
Security ACEs	3 K	3 K

Resource	Advanced	VLAN
Netflow ACEs	1024	1024
Input Microflow policer ACEs:	256 K	0
Output Microflow policer ACEs:	256 K	0
FSPAN ACEs	256	256
Control Plane Entries:	512	512
Input Netflow flows:	8 K	8 K
Output Netflow flows:	16 K	16 K

Note When the switch is used as a Wireless Mobility Agent, the only template allowed is the advanced template.

The tables represent approximate hardware boundaries set when a template is selected. If a section of a hardware resource is full, all processing overflow is sent to the CPU, seriously impacting switch performance.

SDM Templates and Switch Stacks

In a switch stack, all stack members must use the same SDM template that is stored on the active switch. When a new switch is added to a stack, the SDM configuration that is stored on the active switch overrides the template configured on an individual switch.

How to Configure SDM Templates

Configuring SDM Templates

Configuring the Switch SDM Template

Setting the SDM Template

SUMMARY STEPS

1. **configure terminal**
2. **sdm prefer** { **advanced** | **vlan** }
3. **end**
4. **reload**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch> configure terminal`	Enters global configuration mode.
Step 2	**sdm prefer** { **advanced** | **vlan** } **Example:** `SwitchControllerDevice(config)# sdm prefer advanced`	Specifies the SDM template to be used on the switch. The keywords have these meanings: • **advanced** —Supports advanced features such as Netflow. • **vlan** —Maximizes VLAN configuration on the switch with no routing supported in hardware. **Note** The **no sdm prefer** command and a default template is not supported.
Step 3	**end** **Example:** `SwitchControllerDevice(config)# end`	Returns to privileged EXEC mode.
Step 4	**reload** **Example:** `SwitchControllerDevice# reload`	Reloads the operating system.

Monitoring and Maintaining SDM Templates

Command	Purpose
show sdm prefer	Displays the SDM template in use.
reload	Reloads the switch to activate the newly configured SDM template.
no sdm prefer	Sets the default SDM template.

Configuration Examples for Configuring SDM Templates

Examples: Configuring SDM Templates

This example shows how to configure the VLAN template:

```
SwitchControllerDevice(config)# sdm prefer vlan
SwitchControllerDevice(config)# exit
SwitchControllerDevice# reload
  Proceed with reload? [confirm]
```

Examples: Displaying SDM Templates

This is an example output showing the advanced template information:

```
SwitchControllerDevice# show sdm prefer

Showing SDM Template Info

This is the Advanced template.
  Number of VLANs:                                  4094
  Unicast MAC addresses:                            32768
  Overflow Unicast MAC addresses:                   512
  IGMP and Multicast groups:                        8192
  Overflow IGMP and Multicast groups:               512
  Directly connected routes:                        32768
  Indirect routes:                                  8192
  Security Access Control Entries:                  3072
  QoS Access Control Entries:                       2816
  Policy Based Routing ACEs:                        1024
  Netflow ACEs:                                     1024
  Input Microflow policer ACEs:                     256
  Output Microflow policer ACEs:                    256
  Flow SPAN ACEs:                                   256
  Tunnels:                                          256
  Control Plane Entries:                            512
  Input Netflow flows:                              8192
  Output Netflow flows:                             16384
These numbers are typical for L2 and IPv4 features.
Some features such as IPv6, use up double the entry size;
so only half as many entries can be created.


SwitchControllerDevice#
```

This is an example output showing the VLAN template information:

```
SwitchControllerDevice# show sdm prefer vlan

Showing SDM Template Info

This is the VLAN template for a typical Layer 2 network.
  Number of VLANs:                                  4094
  Unicast MAC addresses:                            32768
  Overflow Unicast MAC addresses:                   512
  IGMP and Multicast groups:                        8192
  Overflow IGMP and Multicast groups:               512
  Directly connected routes:                        32768
```

```
  Indirect routes:                                  8192
  Security Access Control Entries:                  3072
  QoS Access Control Entries:                       3072
  Policy Based Routing ACEs:                        0
  Netflow ACEs:                                     1024
  Input Microflow policer ACEs:                     0
  Output Microflow policer ACEs:                    0
  Flow SPAN ACEs:                                   256
  Tunnels:                                          0
  Control Plane Entries:                            512
  Input Netflow flows:                              16384
  Output Netflow flows:                             8192
These numbers are typical for L2 and IPv4 features.
Some features such as IPv6, use up double the entry size;
so only half as many entries can be created.

SwitchControllerDevice#
```

Additional References for SDM Templates

Related Documents

Related Topic	Document Title
SDM command reference	*System Management Command Reference (Catalyst 3850 Switches)*
VLAN configuration guide	*VLAN Configuration Guide (Catalyst 3850 Switches)*

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

Feature History and Information for Configuring SDM Templates

Release	Modification
Cisco IOS XE 3.2SE	This feature was introduced.

CHAPTER 15

Configuring System Message Logs

Finding Feature Information

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

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

Related Topics

Feature History and Information for Troubleshooting Software Configuration, on page 336

Information About Configuring System Message Logs

System Messsage Logging

By default, a switch sends the output from system messages and **debug** privileged EXEC commands to a logging process. Stack members can trigger system messages. A stack member that generates a system message appends its hostname in the form of hostname-n, where n is a switch range from 1 to 4, and redirects the output to the logging process on the active switch. Though the active switch is a stack member, it does not append its hostname to system messages. The logging process controls the distribution of logging messages to various destinations, such as the logging buffer, terminal lines, or a UNIX syslog server, depending on your configuration. The process also sends messages to the console.

When the logging process is disabled, messages are sent only to the console. The messages are sent as they are generated, so message and debug output are interspersed with prompts or output from other commands. Messages appear on the active consoles after the process that generated them has finished.

You can set the severity level of the messages to control the type of messages displayed on the consoles and each of the destinations. You can time-stamp log messages or set the syslog source address to enhance real-time debugging and management. For information on possible messages, see the system message guide for this release.

You can access logged system messages by using the switch command-line interface (CLI) or by saving them to a properly configured syslog server. The switch software saves syslog messages in an internal buffer on a standalone switch, and in the case of a switch stack, on the active switch. If a standalone switch or the stack master fails, the log is lost unless you had saved it to flash memory.

You can remotely monitor system messages by viewing the logs on a syslog server or by accessing the switch through Telnet, through the console port, or through the Ethernet management port. In a switch stack, all stack member consoles provide the same console output.

Note The syslog format is compatible with 4.3 BSD UNIX.

System Log Message Format

System log messages can contain up to 80 characters and a percent sign (%), which follows the optional sequence number or time-stamp information, if configured. Depending on the switch, messages appear in one of these formats:

- *seq no:timestamp: %facility-severity-MNEMONIC:description (hostname-n)*
- *seq no:timestamp: %facility-severity-MNEMONIC:description*

The part of the message preceding the percent sign depends on the setting of these global configuration commands:

- **service sequence-numbers**
- **service timestamps log datetime**
- **service timestamps log datetime** [**localtime**] [**msec**] [**show-timezone**]
- **service timestamps log uptime**

Table 26: System Log Message Elements

Element	Description
seq no:	Stamps log messages with a sequence number only if the **service sequence-numbers** global configuration command is configured.
timestamp formats: *mm/dd h h:mm:ss* or *hh:mm:ss* (short uptime) or *d h* (long uptime)	Date and time of the message or event. This information appears only if the **service timestamps log** [**datetime** | **log**] global configuration command is configured.
facility	The facility to which the message refers (for example, SNMP, SYS, and so forth).
severity	Single-digit code from 0 to 7 that is the severity of the message.
MNEMONIC	Text string that uniquely describes the message.
description	Text string containing detailed information about the event being reported.
hostname-n	Hostname of a stack member and its switch number in the stack. Though the active switch is a stack member, it does *not* append its hostname to system messages.

Default System Message Logging Settings

Table 27: Default System Message Logging Settings

Feature	Default Setting
System message logging to the console	Enabled.
Console severity	Debugging.
Logging file configuration	No filename specified.
Logging buffer size	4096 bytes.
Logging history size	1 message.

Feature	Default Setting
Time stamps	Disabled.
Synchronous logging	Disabled.
Logging server	Disabled.
Syslog server IP address	None configured.
Server facility	Local7
Server severity	Informational.

Syslog Message Limits

If you enabled syslog message traps to be sent to an SNMP network management station by using the **snmp-server enable trap** global configuration command, you can change the level of messages sent and stored in the switch history table. You also can change the number of messages that are stored in the history table.

Messages are stored in the history table because SNMP traps are not guaranteed to reach their destination. By default, one message of the level **warning** and numerically lower levels are stored in the history table even if syslog traps are not enabled.

When the history table is full (it contains the maximum number of message entries specified with the **logging history size** global configuration command), the oldest message entry is deleted from the table to allow the new message entry to be stored.

The history table lists the level keywords and severity level. For SNMP usage, the severity level values increase by 1. For example, *emergencies* equal 1, not 0, and *critical* equals 3, not 2.

How to Configure System Message Logs

Setting the Message Display Destination Device

If message logging is enabled, you can send messages to specific locations in addition to the console.

This task is optional.

SUMMARY STEPS

1. **configure terminal**
2. **logging buffered** [*size*]
3. **logging** *host*
4. **logging file flash:** *filename* [*max-file-size* [*min-file-size*]] [*severity-level-number* | *type*]
5. **end**
6. **terminal monitor**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `SwitchControllerDevice# configure terminal`	Enters global configuration mode.
Step 2	**logging buffered** [*size*] **Example:** `SwitchControllerDevice(config)# logging buffered 8192`	Logs messages to an internal buffer on the switch or on a standalone switch or, in the case of a switch stack, on the active switch. The range is 4096 to 2147483647 bytes. The default buffer size is 4096 bytes. If a standalone switch or the active switch fails, the log file is lost unless you previously saved it to flash memory. See Step 4. **Note** Do not make the buffer size too large because the switch could run out of memory for other tasks. Use the **show memory** privileged EXEC command to view the free processor memory on the switch. However, this value is the maximum available, and the buffer size should *not* be set to this amount.
Step 3	**logging** *host* **Example:** `SwitchControllerDevice(config)# logging 125.1.1.100`	Logs messages to a UNIX syslog server host. *host* specifies the name or IP address of the host to be used as the syslog server. To build a list of syslog servers that receive logging messages, enter this command more than once.
Step 4	**logging file flash:** *filename* [*max-file-size* [*min-file-size*]] [*severity-level-number* | *type*] **Example:** `SwitchControllerDevice(config)# logging file flash:log_msg.txt 40960 4096 3`	Stores log messages in a file in flash memory on a standalone switch or, in the case of a switch stack, on the active switch. • *filename*—Enters the log message filename. • (Optional) **max-file-size** —Specifies the maximum logging file size. The range is 4096 to 2147483647. The default is 4096 bytes. • (Optional) *min-file-size*—Specifies the minimum logging file size. The range is 1024 to 2147483647. The default is 2048 bytes. • (Optional) *severity-level-number* | *type*—Specifies either the logging severity level or the logging type. The severity range is 0 to 7.

	Command or Action	Purpose
Step 5	**end** **Example:** `SwitchControllerDevice(config)# end`	Returns to privileged EXEC mode.
Step 6	**terminal monitor** **Example:** `SwitchControllerDevice# terminal monitor`	Logs messages to a nonconsole terminal during the current session. Terminal parameter-setting commands are set locally and do not remain in effect after the session has ended. You must perform this step for each session to see the debugging messages.

Synchronizing Log Messages

You can synchronize unsolicited messages and **debug** privileged EXEC command output with solicited device output and prompts for a specific console port line or virtual terminal line. You can identify the types of messages to be output asynchronously based on the level of severity. You can also configure the maximum number of buffers for storing asynchronous messages for the terminal after which messages are dropped.

When synchronous logging of unsolicited messages and **debug** command output is enabled, unsolicited device output appears on the console or printed after solicited device output appears or is printed. Unsolicited messages and **debug** command output appears on the console after the prompt for user input is returned. Therefore, unsolicited messages and **debug** command output are not interspersed with solicited device output and prompts. After the unsolicited messages appear, the console again displays the user prompt.

This task is optional.

SUMMARY STEPS

1. **configure terminal**
2. **line** [**console** | **vty**] *line-number* [*ending-line-number*]
3. **logging synchronous** [**level** [*severity-level* | **all**] | **limit** *number-of-buffers*]
4. **end**

DETAILED STEPS

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

	Command or Action	Purpose
	`terminal`	
Step 2	**line** [**console** | **vty**] *line-number* [*ending-line-number*] **Example:** `SwitchControllerDevice(config)#` **`line console`**	Specifies the line to be configured for synchronous logging of messages. • **console** —Specifies configurations that occur through the switch console port or the Ethernet management port. • **line vty** *line-number*—Specifies which vty lines are to have synchronous logging enabled. You use a vty connection for configurations that occur through a Telnet session. The range of line numbers is from 0 to 15. You can change the setting of all 16 vty lines at once by entering: line vty 0 15 You can also change the setting of the single vty line being used for your current connection. For example, to change the setting for vty line 2, enter: line vty 2 When you enter this command, the mode changes to line configuration.
Step 3	**logging synchronous** [**level** [*severity-level* | **all**] | **limit** *number-of-buffers*] **Example:** `SwitchControllerDevice(config)#` **`logging synchronous level 3 limit 1000`**	Enables synchronous logging of messages. • (Optional) **level** *severity-level*—Specifies the message severity level. Messages with a severity level equal to or higher than this value are printed asynchronously. Low numbers mean greater severity and high numbers mean lesser severity. The default is 2. • (Optional) **level all**—Specifies that all messages are printed asynchronously regardless of the severity level. • (Optional) **limit** *number-of-buffers*—Specifies the number of buffers to be queued for the terminal after which new messages are dropped. The range is 0 to 2147483647. The default is 20.
Step 4	**end** **Example:** `SwitchControllerDevice(config)#` **`end`**	Returns to privileged EXEC mode.

Disabling Message Logging

Message logging is enabled by default. It must be enabled to send messages to any destination other than the console. When enabled, log messages are sent to a logging process, which logs messages to designated locations asynchronously to the processes that generated the messages.

Disabling the logging process can slow down the switch because a process must wait until the messages are written to the console before continuing. When the logging process is disabled, messages appear on the console as soon as they are produced, often appearing in the middle of command output.

The **logging synchronous** global configuration command also affects the display of messages to the console. When this command is enabled, messages appear only after you press **Return**.

To reenable message logging after it has been disabled, use the **logging on** global configuration command.

This task is optional.

SUMMARY STEPS

1. **configure terminal**
2. **no logging console**
3. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `SwitchControllerDevice# configure terminal`	Enters global configuration mode.
Step 2	**no logging console** **Example:** `SwitchControllerDevice(config)# no logging console`	Disables message logging.
Step 3	**end** **Example:** `SwitchControllerDevice(config)# end`	Returns to privileged EXEC mode.

Enabling and Disabling Time Stamps on Log Messages

By default, log messages are not time-stamped.

This task is optional.

SUMMARY STEPS

1. **configure terminal**
2. Use one of these commands:
   - **service timestamps log uptime**
   - **service timestamps log datetime**[**msec** | **localtime** | **show-timezone**]
3. **end**

DETAILED STEPS

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

Step 2	Use one of these commands:
	• **service timestamps log uptime**
	• **service timestamps log datetime**[**msec** | **localtime** | **show-timezone**]
	
	Example:
	`SwitchControllerDevice(config)# service timestamps log uptime`
	or
	`SwitchControllerDevice(config)# service timestamps log datetime`
		Enables log time stamps.
		• **log uptime**—Enables time stamps on log messages, showing the time since the system was rebooted.
		• **log datetime**—Enables time stamps on log messages. Depending on the options selected, the time stamp can include the date, time in milliseconds relative to the local time zone, and the time zone name.

Step 3	**end** **Example:** `SwitchControllerDevice(config)# end`	Returns to privileged EXEC mode.

Enabling and Disabling Sequence Numbers in Log Messages

If there is more than one log message with the same time stamp, you can display messages with sequence numbers to view these messages. By default, sequence numbers in log messages are not displayed.

This task is optional.

SUMMARY STEPS

1. **configure terminal**
2. **service sequence-numbers**
3. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `SwitchControllerDevice# configure terminal`	Enters global configuration mode.
Step 2	**service sequence-numbers** **Example:** `SwitchControllerDevice(config)# service sequence-numbers`	Enables sequence numbers.
Step 3	**end** **Example:** `SwitchControllerDevice(config)# end`	Returns to privileged EXEC mode.

Defining the Message Severity Level

Limit messages displayed to the selected device by specifying the severity level of the message.

This task is optional.

SUMMARY STEPS

1. **configure terminal**
2. **logging console** *level*
3. **logging monitor** *level*
4. **logging trap** *level*
5. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `SwitchControllerDevice# configure terminal`	Enters global configuration mode.
Step 2	**logging console** *level* **Example:** `SwitchControllerDevice(config)# logging console 3`	Limits messages logged to the console. By default, the console receives debugging messages and numerically lower levels.
Step 3	**logging monitor** *level* **Example:** `SwitchControllerDevice(config)# logging monitor 3`	Limits messages logged to the terminal lines. By default, the terminal receives debugging messages and numerically lower levels.
Step 4	**logging trap** *level* **Example:** `SwitchControllerDevice(config)# logging trap 3`	Limits messages logged to the syslog servers. By default, syslog servers receive informational messages and numerically lower levels.
Step 5	**end** **Example:** `SwitchControllerDevice(config)# end`	Returns to privileged EXEC mode.

Limiting Syslog Messages Sent to the History Table and to SNMP

This task explains how to limit syslog messages that are sent to the history table and to SNMP.

This task is optional.

SUMMARY STEPS

1. **configure terminal**
2. **logging history** *level*
3. **logging history size** *number*
4. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `SwitchControllerDevice# configure terminal`	Enters global configuration mode.
Step 2	**logging history** *level* **Example:** `SwitchControllerDevice(config)# logging history 3`	Changes the default level of syslog messages stored in the history file and sent to the SNMP server. By default, **warnings**, **errors**, **critical**, **alerts**, and **emergencies** messages are sent.
Step 3	**logging history size** *number* **Example:** `SwitchControllerDevice(config)# logging history size 200`	Specifies the number of syslog messages that can be stored in the history table. The default is to store one message. The range is 0 to 500 messages.
Step 4	**end** **Example:** `SwitchControllerDevice(config)# end`	Returns to privileged EXEC mode.

Logging Messages to a UNIX Syslog Daemon

This task is optional.

Note Some recent versions of UNIX syslog daemons no longer accept by default syslog packets from the network. If this is the case with your system, use the UNIX **man syslogd** command to decide what options must be added to or removed from the syslog command line to enable logging of remote syslog messages.

Before You Begin

- Log in as root.
- Before you can send system log messages to a UNIX syslog server, you must configure the syslog daemon on a UNIX server.

SUMMARY STEPS

1. Add a line to the file /etc/syslog.conf.
2. Enter these commands at the UNIX shell prompt.
3. Make sure the syslog daemon reads the new changes.

DETAILED STEPS

	Command or Action	Purpose
Step 1	Add a line to the file /etc/syslog.conf. **Example:** `local7.debug /usr/adm/logs/`*cisco.log*	• **local7**—Specifies the logging facility. • **debug**—Specifies the syslog level. The file must already exist, and the syslog daemon must have permission to write to it.
Step 2	Enter these commands at the UNIX shell prompt. **Example:** `$ touch /var/log/`*cisco.log* `$ chmod 666 /var/log/`*cisco.log*	Creates the log file. The syslog daemon sends messages at this level or at a more severe level to this file.
Step 3	Make sure the syslog daemon reads the new changes. **Example:** ``$ kill -HUP `cat /etc/syslog.pid` ``	For more information, see the **man syslog.conf** and **man syslogd** commands on your UNIX system.

Monitoring and Maintaining System Message Logs

Monitoring Configuration Archive Logs

Command	Purpose
show archive log config {**all** | **number** [*end-number*] | **user** *username* [**session** *number*] *number* [*end-number*] | **statistics**} [**provisioning**]	Displays the entire configuration log or the log for specified parameters.

Configuration Examples for System Message Logs

Example: Stacking System Message

This example shows a partial switch system message for active switch and a stack member (hostname *Switch-2*):

```
00:00:46: %LINK-3-UPDOWN: Interface Port-channel1, changed state to up
00:00:47: %LINK-3-UPDOWN: Interface GigabitEthernet1/0/1, changed state to up
00:00:47: %LINK-3-UPDOWN: Interface GigabitEthernet1/0/2, changed state to up
00:00:48: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to down
00:00:48: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/1, changed
state to down 2
*Mar  1 18:46:11: %SYS-5-CONFIG_I: Configured from console by vty2 (10.34.195.36)
18:47:02: %SYS-5-CONFIG_I: Configured from console by vty2 (10.34.195.36)
*Mar  1 18:48:50.483 UTC: %SYS-5-CONFIG_I: Configured from console by vty2 (10.34.195.36)

00:00:46: %LINK-3-UPDOWN: Interface Port-channel1, changed state to up (Switch-2)
00:00:47: %LINK-3-UPDOWN: Interface GigabitEthernet2/0/1, changed state to up (Switch-2)
00:00:47: %LINK-3-UPDOWN: Interface GigabitEthernet2/0/2, changed state to up (Switch-2)
00:00:48: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to down
(Switch-2)
00:00:48: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet2/0/1, changed
state to down 2 (Switch-2)
```

Example: Switch System Message

This example shows a partial switch system message on a switch:

```
00:00:46: %LINK-3-UPDOWN: Interface Port-channel1, changed state to up
00:00:47: %LINK-3-UPDOWN: Interface GigabitEthernet0/1, changed state to up
00:00:47: %LINK-3-UPDOWN: Interface GigabitEthernet0/2, changed state to up
00:00:48: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to down
00:00:48: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state
 to down 2
*Mar  1 18:46:11: %SYS-5-CONFIG_I: Configured from console by vty2 (10.34.195.36)
18:47:02: %SYS-5-CONFIG_I: Configured from console by vty2 (10.34.195.36)
```

```
*Mar  1 18:48:50.483 UTC: %SYS-5-CONFIG_I: Configured from console by vty2 (10.34.195.36)
```

Additional References for System Message Logs

Related Documents

Related Topic	Document Title
System management commands	*System Management Command Reference (Catalyst 3850 Switches)*
Platform-independent command references	*Configuration Fundamentals Command Reference, Cisco IOS XE Release 3S (Catalyst 3850 Switches)*
Platform-independent configuration information	*Configuration Fundamentals Configuration Guide, Cisco IOS XE Release 3S (Catalyst 3850 Switches)* *IP Addressing Configuration Guide Library, Cisco IOS XE Release 3S (Catalyst 3850 Switches)*

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

Feature History and Information For System Message Logs

Release	Modification
Cisco IOS XE 3.2SE	This feature was introduced.

CHAPTER 16

Configuring Online Diagnostics

Finding Feature Information

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

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

Related Topics

Feature History and Information for Troubleshooting Software Configuration, on page 336

Information About Configuring Online Diagnostics

Online Diagnostics

With online diagnostics, you can test and verify the hardware functionality of the switch while the switch is connected to a live network.

The online diagnostics contain packet switching tests that check different hardware components and verify the data path and the control signals.

The online diagnostics detect problems in these areas:

- Hardware components
- Interfaces (Ethernet ports and so forth)
- Solder joints

Online diagnostics are categorized as on-demand, scheduled, or health-monitoring diagnostics. On-demand diagnostics run from the CLI; scheduled diagnostics run at user-designated intervals or at specified times when the switch is connected to a live network; and health-monitoring runs in the background with user-defined intervals. By default, the health-monitoring test runs for every 30 seconds.

After you configure online diagnostics, you can manually start diagnostic tests or display the test results. You can also see which tests are configured for the switch or switch stack and the diagnostic tests that have already run.

How to Configure Online Diagnostics

Starting Online Diagnostic Tests

After you configure diagnostic tests to run on the switch, use the **diagnostic start** privileged EXEC command to begin diagnostic testing.

After starting the tests, you cannot stop the testing process.

Use this privileged EXEC command to manually start online diagnostic testing:

SUMMARY STEPS

1. **diagnostic start switch** *number* **test** {*name* | *test-id* | *test-id-range* | **all** | **basic** | **complete** | **minimal** | **non-disruptive** | **per-port**}

DETAILED STEPS

	Command or Action	Purpose
Step 1	**diagnostic start switch** *number* **test** {*name* | *test-id* | *test-id-range* | **all** | **basic** | **complete** | **minimal** | **non-disruptive** | **per-port**} **Example:** `SwitchControllerDevice# diagnostic start switch 2 test basic`	Starts the diagnostic tests. The **switch** *number* keyword is supported only on stacking switches. The range is from 1 to 4. You can specify the tests by using one of these options: • *name*—Enters the name of the test. • *test-id*—Enters the ID number of the test. • *test-id-range*—Enters the range of test IDs by using integers separated by a comma and a hyphen.

	Command or Action	Purpose
		• **all—**Starts all of the tests. • **basic—** Starts the basic test suite. • **complete—**Starts the complete test suite. • **minimal—**Starts the minimal bootup test suite. • **non-disruptive—**Starts the non-disruptive test suite. • **per-port—**Starts the per-port test suite.

Configuring Online Diagnostics

You must configure the failure threshold and the interval between tests before enabling diagnostic monitoring.

Scheduling Online Diagnostics

You can schedule online diagnostics to run at a designated time of day or on a daily, weekly, or monthly basis for a switch. Use the **no** form of this command to remove the scheduling.

SUMMARY STEPS

1. **configure terminal**
2. **diagnostic schedule switch** *number* **test** {*name* | *test-id* | *test-id-range* | **all** | **basic** | **complete** | **minimal** | **non-disruptive** | **per-port**} {**daily** | **on** *mm dd yyyy hh:mm* | **port** *inter-port-number port-number-list* | **weekly** *day-of-week hh:mm*}

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `SwitchControllerDevice# configure terminal`	Enters global configuration mode.
Step 2	**diagnostic schedule switch** *number* **test** {*name* | *test-id* | *test-id-range* | **all** | **basic** | **complete** | **minimal** | **non-disruptive** | **per-port**} {**daily** | **on** *mm dd yyyy hh:mm* | **port** *inter-port-number port-number-list* | **weekly** *day-of-week hh:mm*}	Schedules on-demand diagnostic tests for a specific day and time. The **switch** *number* keyword is supported only on stacking switches. The range is from 1 to 4. When specifying the tests to be scheduled, use these options:

	Command or Action	Purpose
	Example: `SwitchControllerDevice(config)#` **`diagnostic schedule switch 3 test 1-5 on July 3 2013 23:10`**	• *name*—Name of the test that appears in the **show diagnostic content** command output. • *test-id*—ID number of the test that appears in the **show diagnostic content** command output. • *test-id-range*—ID numbers of the tests that appear in the **show diagnostic content** command output. • **all—**All test IDs. • **basic—**Starts the basic on-demand diagnostic tests. • **complete—**Starts the complete test suite. • **minimal—**Starts the minimal bootup test suite. • **non-disruptive—**Starts the non-disruptive test suite. • **per-port—**Starts the per-port test suite. You can schedule the tests as follows: • Daily—Use the **daily** *hh:mm* parameter. • Specific day and time—Use the **on** *mm dd yyyy hh:mm* parameter. • Weekly—Use the **weekly** *day-of-week hh:mm* parameter.

Configuring Health-Monitoring Diagnostics

You can configure health-monitoring diagnostic testing on a switch while it is connected to a live network. You can configure the execution interval for each health-monitoring test, enable the switch to generate a syslog message because of a test failure, and enable a specific test.

By default, health monitoring is disabled, but the switch generates a syslog message when a test fails.

SUMMARY STEPS

1. **configure terminal**
2. **diagnostic monitor interval switch** *number* **test** {*name* | *test-id* | *test-id-range* | **all**} *hh:mm:ss milliseconds day*
3. **diagnostic monitor syslog**
4. **diagnostic monitor threshold switch** *number* **test** {*name* | *test-id* | *test-id-range* | **all**} **failure count** *count*
5. **diagnostic monitor switch** *number* **test** {*name* | *test-id* | *test-id-range* | **all**}
6. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `SwitchControllerDevice# configure terminal`	Enters global configuration mode.
Step 2	**diagnostic monitor interval switch** *number* **test** {*name* | *test-id* | *test-id-range* | **all**} *hh:mm:ss milliseconds day* **Example:** `SwitchControllerDevice(config)# diagnostic monitor interval switch 2 test 1 12:30:00 750 5`	Configures the health-monitoring interval of the specified tests. The **switch** *number* keyword is supported only on stacking switches. The range is from 1 to 9. When specifying the tests, use one of these parameters: • *name*—Name of the test that appears in the **show diagnostic content** command output. • *test-id*—ID number of the test that appears in the **show diagnostic content** command output. • *test-id-range*—ID numbers of the tests that appear in the **show diagnostic content** command output. • **all**—All of the diagnostic tests. When specifying the interval, set these parameters: • *hh:mm:ss*—Monitoring interval in hours, minutes, and seconds. The range for *hh* is 0 to 24, and the range for *mm* and *ss* is 0 to 60. • *milliseconds*—Monitoring interval in milliseconds (ms). The range is from 0 to 999. • *day*—Monitoring interval in the number of days. The range is from 0 to 20.
Step 3	**diagnostic monitor syslog** **Example:** `SwitchControllerDevice(config)# diagnostic monitor syslog`	(Optional) Configures the switch to generate a syslog message when a health-monitoring test fails.
Step 4	**diagnostic monitor threshold switch** *number* **test** {*name* | *test-id* | *test-id-range* | **all**} **failure count** *count* **Example:** `SwitchControllerDevice(config)# diagnostic monitor threshold switch 2 test 1 failure count 20`	(Optional) Sets the failure threshold for the health-monitoring tests. The **switch** *number* keyword is supported only on stacking switches. The range is from 1 to 9. When specifying the tests, use one of these parameters: • *name*—Name of the test that appears in the **show diagnostic content** command output.

	Command or Action	Purpose
		• *test-id*—ID number of the test that appears in the **show diagnostic content** command output. • *test-id-range*—ID numbers of the tests that appear in the **show diagnostic content** command output. • **all**—All of the diagnostic tests. The range for the failure threshold *count* is 0 to 99.
Step 5	**diagnostic monitor switch** *number* **test** {*name* | *test-id* | *test-id-range* | **all**} **Example:** `SwitchControllerDevice(config)#` **`diagnostic monitor switch 2 test 1`**	Enables the specified health-monitoring tests. The **switch** *number* keyword is supported only on stacking switches. The range is from 1 to 9. When specifying the tests, use one of these parameters: • *name*—Name of the test that appears in the **show diagnostic content** command output. • *test-id*—ID number of the test that appears in the **show diagnostic content** command output. • *test-id-range*—ID numbers of the tests that appear in the **show diagnostic content** command output. • **all**—All of the diagnostic tests.
Step 6	**end** **Example:** `SwitchControllerDevice(config)#` **`end`**	Returns to privileged EXEC mode.

Monitoring and Maintaining Online Diagnostics

Displaying Online Diagnostic Tests and Test Results

You can display the online diagnostic tests that are configured for the switch ro switch stack and check the test results by using the privileged EXEC **show** commands in this table:

Table 28: Commands for Diagnostic Test Configuration and Results

Command	Purpose
show diagnostic content switch [*number* | **all**]	Displays the online diagnostics configured for a switch. The **switch** [*number* | **all**] parameter is supported only on stacking switches.
show diagnostic status	Displays the currently running diagnostic tests.
show diagnostic result switch [*number* | **all**] [**detail** | **test** {*name* | *test-id* | *test-id-range* | **all**} [**detail**]]	Displays the online diagnostics test results. The **switch** [*number* | **all**] parameter is supported only on stacking switches.
show diagnostic switch [*number* | **all**] [**detail**]	Displays the online diagnostics test results. The **switch** [*number* | **all**] parameter is supported only on stacking switches.
show diagnostic schedule switch [*number* | **all**]	Displays the online diagnostics test schedule. The **switch** [*number* | **all**] parameter is supported only on stacking switches.
show diagnostic post	Displays the POST results. (The output is the same as the **show post** command output.)

Configuration Examples for Online Diagnostic Tests

Examples: Start Diagnostic Tests

This example shows how to start a diagnostic test by using the test name:

```
SwitchControllerDevice# diagnostic start switch 2 test TestInlinePwrCtlr
```

This example shows how to start all of the basic diagnostic tests:

```
SwitchControllerDevice# diagnostic start switch 1 test all
```

Example: Configure a Health Monitoring Test

This example shows how to configure a health-monitoring test:

```
SwitchControllerDevice(config)# diagnostic monitor threshold switch 1 test 1 failure count
```

```
 50
SwitchControllerDevice(config)# diagnostic monitor interval switch 1 test
TestPortAsicStackPortLoopback
```

Examples: Schedule Diagnostic Test

This example shows how to schedule diagnostic testing for a specific day and time on a specific switch:

```
SwitchControllerDevice(config)# diagnostic schedule test DiagThermalTest on June 3 2013
22:25
```

This example shows how to schedule diagnostic testing to occur weekly at a certain time on a specific switch:

```
SwitchControllerDevice(config)# diagnostic schedule switch 1 test 1,2,4-6 weekly saturday
10:30
```

Examples: Displaying Online Diagnostics

This example shows how to display on demand diagnostic settings:

```
SwitchControllerDevice# show diagnostic ondemand settings

Test iterations = 1
Action on test failure = continue
```

This example shows how to display diagnostic events for errors:

```
SwitchControllerDevice# show diagnostic events event-type error

Diagnostic events (storage for 500 events, 0 events recorded)
Number of events matching above criteria = 0

No diagnostic log entry exists.
```

This example shows how to display the description for a diagnostic test:

```
SwitchControllerDevice# show diagnostic description switch 1 test all

DiagGoldPktTest :
        The GOLD packet Loopback test verifies the MAC level loopback
        functionality. In this test, a GOLD packet, for which doppler
        provides the support in hardware, is sent. The packet loops back
        at MAC level and is matched against the stored packet. It is a non
        -disruptive test.

DiagThermalTest :
        This test verifies the temperature reading from the sensor is below the yellow
        temperature threshold. It is a non-disruptive test and can be run as a health
monitoring test.

DiagFanTest :
        This test verifies all fan modules have been inserted and working properly on the
board
        It is a non-disruptive test and can be run as a health monitoring test.

DiagPhyLoopbackTest :
        The PHY Loopback test verifies the PHY level loopback
        functionality. In this test, a packet is sent which loops back
        at PHY level and is matched against the stored packet. It is a
```

```
        disruptive test and cannot be run as a health monitoring test.

DiagScratchRegisterTest :
        The Scratch Register test monitors the health of application-specific
        integrated circuits (ASICs) by writing values into registers and reading
        back the values from these registers. It is a non-disruptive test and can
        be run as a health monitoring test.

DiagPoETest :
        This test checks the PoE controller functionality. This is a disruptive test
        and should not be performed during normal switch operation.

DiagStackCableTest :
        This test verifies the stack ring loopback functionality
        in the stacking environment. It is a disruptive test and
        cannot be run as a health monitoring test.

DiagMemoryTest :
        This test runs the exhaustive ASIC memory test during normal switch operation
        NG3K utilizes mbist for this test. Memory test is very disruptive
        in nature and requires switch reboot after the test.

SwitchControllerDevice#
```

This example shows how to display the boot up level:

```
SwitchControllerDevice# show diagnostic bootup level

Current bootup diagnostic level: minimal

SwitchControllerDevice#
```

Additional References for Online Diagnostics

Related Documents

Related Topic	Document Title
System management commands	*System Management Command Reference (Catalyst 3850 Switches)*
Platform-independent command reference	*Configuration Fundamentals Command Reference, Cisco IOS XE Release 3S (Catalyst 3850 Switches)*
Platform-independent configuration information	*Configuration Fundamentals Configuration Guide, Cisco IOS XE Release 3S (Catalyst 3850 Switches)*

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

Feature History and Information for Configuring Online Diagnostics

Release	Modification
Cisco IOS XE 3.2SE	This feature was introduced.

CHAPTER 17

Managing Configuration Files

Prerequisites for Managing Configuration Files

- You should have at least a basic familiarity with the Cisco IOS environment and the command-line interface.
- You should have at least a minimal configuration running on your system. You can create a basic configuration file using the **setup** command.

Restrictions for Managing Configuration Files

- Many of the Cisco IOS commands described in this document are available and function only in certain configuration modes on the switch.
- Some of the Cisco IOS configuration commands are only available on certain switch platforms, and the command syntax may vary on different platforms.

Information About Managing Configuration Files

Types of Configuration Files

Configuration files contain the Cisco IOS software commands used to customize the functionality of your Cisco switch. Commands are parsed (translated and executed) by the Cisco IOS software when the system is booted (from the startup-config file) or when you enter commands at the CLI in a configuration mode.

Startup configuration files (startup-config) are used during system startup to configure the software. Running configuration files (running-config) contain the current configuration of the software. The two configuration files can be different. For example, you may want to change the configuration for a short time period rather than permanently. In this case, you would change the running configuration using the **configure terminal** EXEC command but not save the configuration using the **copy running-config startup-config** EXEC command.

To change the running configuration, use the **configure terminal** command, as described in the Modifying the Configuration File (CLI) section. As you use the Cisco IOS configuration modes, commands generally are executed immediately and are saved to the running configuration file either immediately after you enter them or when you exit a configuration mode.

To change the startup configuration file, you can either save the running configuration file to the startup configuration using the **copy running-config startup-config** EXEC command or copy a configuration file from a file server to the startup configuration (see the Copying a Configuration File from a TFTP Server to the Switch (CLI) section for more information).

Configuration Mode and Selecting a Configuration Source

To enter configuration mode on the switch, enter the **configure** command at the privileged EXEC prompt. The Cisco IOS software responds with the following prompt asking you to specify the terminal, memory, or a file stored on a network server (network) as the source of configuration commands:

```
Configuring from terminal, memory, or network [terminal]?
```

Configuring from the terminal allows you to enter configuration commands at the command line, as described in the following section. See the Re-executing the Configuration Commands in the Startup Configuration File (CLI) section for more information.

Configuring from the network allows you to load and execute configuration commands over the network. See the Copying a Configuration File from a TFTP Server to the Switch (CLI) section for more information.

Configuration File Changes Using the CLI

The Cisco IOS software accepts one configuration command per line. You can enter as many configuration commands as you want. You can add comments to a configuration file describing the commands you have entered. Precede a comment with an exclamation point (!). Because comments are *not* stored in NVRAM or in the active copy of the configuration file, comments do not appear when you list the active configuration with the **show running-config** or **more system:running-config** EXEC command. Comments are not displayed when you list the startup configuration with the **show startup-config** or **more nvram:startup-config** EXEC mode command. Comments are stripped out of the configuration file when it is loaded onto the switch.

However, you can list the comments in configuration files stored on a File Transfer Protocol (FTP), Remote Copy Protocol (RCP), or Trivial File Transfer Protocol (TFTP) server. When you configure the software using the CLI, the software executes the commands as you enter them.

Location of Configuration Files

Configuration files are stored in the following locations:

- The running configuration is stored in RAM.
- On all platforms except the Class A Flash file system platforms, the startup configuration is stored in nonvolatile random-access memory (NVRAM).
- On Class A Flash file system platforms, the startup configuration is stored in the location specified by the CONFIG_FILE environment variable (see the Specifying the CONFIG_FILE Environment Variable on Class A Flash File Systems (CLI) section). The CONFIG_FILE variable defaults to NVRAM and can be a file in the following file systems:
    - **nvram:** (NVRAM)
    - **bootflash:** (internal flash memory)
    - **usbflash0:** (flash file system)

Copy Configuration Files from a Network Server to the Switch

You can copy configuration files from a TFTP, rcp, or FTP server to the running configuration or startup configuration of the switch. You may want to perform this function for one of the following reasons:

- To restore a backed-up configuration file.
- To use the configuration file for another switch. For example, you may add another switch to your network and want it to have a similar configuration to the original switch. By copying the file to the new switch, you can change the relevant parts rather than recreating the whole file.
- To load the same configuration commands on to all of the switches in your network so that all of the switches have similar configurations.

The **copy**{**ftp:** | **rcp:** | **tftp:system:running-config**} EXEC command loads the configuration files into the switch as if you were typing the commands on the command line. The switch does not erase the existing running configuration before adding the commands. If a command in the copied configuration file replaces a command in the existing configuration file, the existing command is erased. For example, if the copied configuration file contains a different IP address in a particular command than the existing configuration, the IP address in the copied configuration is used. However, some commands in the existing configuration may not be replaced or negated. In this case, the resulting configuration file is a mixture of the existing configuration file and the copied configuration file, with the copied configuration file having precedence.

To restore a configuration file to an exact copy of a file stored on a server, you need to copy the configuration file directly to the startup configuration (using the **copy ftp:**| **rcp:**| **tftp:**} **nvram:startup-config** command) and reload the switch.

To copy configuration files from a server to a switch, perform the tasks described in the following sections.

The protocol that you use depends on which type of server you are using. The FTP and rcp transport mechanisms provide faster performance and more reliable delivery of data than TFTP. These improvements are possible because the FTP and rcp transport mechanisms are built on and use the TCP/IP stack, which is connection-oriented.

Copying a Configuration File from the SwitchControllerDevice to a TFTP Server

In some implementations of TFTP, you must create a dummy file on the TFTP server and give it read, write, and execute permissions before copying a file over it. Refer to your TFTP documentation for more information.

Copying a Configuration File from the Switch to an RCP Server

You can copy a configuration file from the switch to an RCP server.

One of the first attempts to use the network as a resource in the UNIX community resulted in the design and implementation of the remote shell protocol, which included the remote shell (rsh) and remote copy (rcp) functions. Rsh and rcp give users the ability to execute commands remotely and copy files to and from a file system residing on a remote host or server on the network. The Cisco implementation of rsh and rcp interoperates with standard implementations.

The rcp **copy** commands rely on the rsh server (or daemon) on the remote system. To copy files using rcp, you need not create a server for file distribution, as you do with TFTP. You need only to have access to a server that supports the remote shell (rsh). (Most UNIX systems support rsh.) Because you are copying a file from one place to another, you must have read permission on the source file and write permission on the destination file. If the destination file does not exist, rcp creates it for you.

Although the Cisco rcp implementation emulates the functions of the UNIX rcp implementation—copying files among systems on the network—the Cisco command syntax differs from the UNIX rcp command syntax. The Cisco rcp support offers a set of **copy** commands that use rcp as the transport mechanism. These rcp **copy** commands are similar in style to the Cisco TFTP **copy** commands, but they offer an alternative that provides faster performance and reliable delivery of data. These improvements are possible because the rcp transport mechanism is built on and uses the TCP/IP stack, which is connection-oriented. You can use rcp commands to copy system images and configuration files from the switch to a network server and vice versa.

You also can enable rcp support to allow users on remote systems to copy files to and from the switch.

To configure the Cisco IOS software to allow remote users to copy files to and from the switch, use the **ip rcmd rcp-enable** global configuration command.

Restrictions

The RCP protocol requires a client to send a remote username on each RCP request to a server. When you copy a configuration file from the switch to a server using RCP, the Cisco IOS software sends the first valid username it encounters in the following sequence:

1. The username specified in the **copy** EXEC command, if a username is specified.
2. The username set by the **ip rcmd remote-username** global configuration command, if the command is configured.
3. The remote username associated with the current tty (terminal) process. For example, if the user is connected to the switch through Telnet and was authenticated through the **username** command, the switch software sends the Telnet username as the remote username.

4 The switch host name.

For the RCP copy request to execute successfully, an account must be defined on the network server for the remote username. If the server has a directory structure, the configuration file or image is written to or copied from the directory associated with the remote username on the server. For example, if the system image resides in the home directory of a user on the server, you can specify that user name as the remote username.

Use the **ip rcmd remote-username** command to specify a username for all copies. (Rcmd is a UNIX routine used at the super-user level to execute commands on a remote machine using an authentication scheme based on reserved port numbers. Rcmd stands for "remote command"). Include the username in the **copy** command if you want to specify a username for that copy operation only.

If you are writing to the server, the RCP server must be properly configured to accept the RCP write request from the user on the switch. For UNIX systems, you must add an entry to the .rhosts file for the remote user on the RCP server. For example, suppose the switch contains the following configuration lines:

```
hostname SwitchControllerDevice1
ip rcmd remote-username User0
```

If the switch IP address translates to switch1.example.com, then the .rhosts file for User0 on the RCP server should contain the following line:

```
SwitchControllerDevice1.example.com SwitchControllerDevice1
```

Requirements for the RCP Username

The RCP protocol requires a client to send a remote username on each RCP request to a server. When you copy a configuration file from the switch to a server using RCP, the Cisco IOS software sends the first valid username it encounters in the following sequence:

1. The username specified in the **copy** EXEC command, if a username is specified.
2. The username set by the **ip rcmd remote-username** global configuration command, if the command is configured.
3. The remote username associated with the current tty (terminal) process. For example, if the user is connected to the switch through Telnet and is authenticated through the **username** command, the switch software sends the Telnet username as the remote username.
4. The switch host name.

For the RCP copy request to execute, an account must be defined on the network server for the remote username. If the server has a directory structure, the configuration file or image is written to or copied from the directory associated with the remote username on the server. For example, if the system image resides in the home directory of a user on the server, specify that user name as the remote username.

Refer to the documentation for your RCP server for more information.

Copying a Configuration File from the Switch to an FTP Server

You can copy a configuration file from the switch to an FTP server.

Understanding the FTP Username and Password

The FTP protocol requires a client to send a remote username and password on each FTP request to a server. When you copy a configuration file from the switch to a server using FTP, the Cisco IOS software sends the first valid username it encounters in the following sequence:

1. The username specified in the **copy** EXEC command, if a username is specified.
2. The username set by the **ip ftp username** global configuration command, if the command is configured.
3. Anonymous.

The switch sends the first valid password it encounters in the following sequence:

1. The password specified in the **copy** command, if a password is specified.
2. The password set by the **ip ftp password** command, if the command is configured.
3. The switch forms a password *username @switchname.domain* . The variable *username* is the username associated with the current session, *switchname* is the configured host name, and *domain* is the domain of the switch.

The username and password must be associated with an account on the FTP server. If you are writing to the server, the FTP server must be properly configured to accept the FTP write request from the user on the switch.

If the server has a directory structure, the configuration file or image is written to or copied from the directory associated with the username on the server. For example, if the system image resides in the home directory of a user on the server, specify that user name as the remote username.

Refer to the documentation for your FTP server for more information.

Use the **ip ftp username** and **ip ftp password** global configuration commands to specify a username and password for all copies. Include the username in the **copy** EXEC command if you want to specify a username for that copy operation only.

Configuration Files Larger than NVRAM

To maintain a configuration file that exceeds the size of NVRAM, you should be aware of the information in the following sections.

Compressing the Configuration File

The **service compress-config** global configuration command specifies that the configuration file be stored compressed in NVRAM. Once the configuration file has been compressed, the switch functions normally. When the system is booted, it recognizes that the configuration file is compressed, expands it, and proceeds normally. The **more nvram:startup-config** EXEC command expands the configuration before displaying it.

Before you compress configuration files, refer to the appropriate hardware installation and maintenance publication. Verify that your system's ROMs support file compression. If not, you can install new ROMs that support file compression.

The size of the configuration must not exceed three times the NVRAM size. For a 128-KB size NVRAM, the largest expanded configuration file size is 384 KB.

The **service compress-config** global configuration command works only if you have Cisco IOS software Release 10.0 or later release boot ROMs. Installing new ROMs is a one-time operation and is necessary only if you do not already have Cisco IOS Release 10.0 in ROM. If the boot ROMs do not recognize a compressed configuration, the following message is displayed:

```
Boot ROMs do not support NVRAM compression Config NOT written to NVRAM
```

Storing the Configuration in Flash Memory on Class A Flash File Systems

On class A Flash file system switches, you can store the startup configuration in flash memory by setting the CONFIG_FILE environment variable to a file in internal flash memory or flash memory in a PCMCIA slot.

See the Specifying the CONFIG_FILE Environment Variable on Class A Flash File Systems (CLI) section for more information.

Care must be taken when editing or changing a large configuration. Flash memory space is used every time a **copy system:running-config nvram:startup-config** EXEC command is issued. Because file management for flash memory (such as optimizing free space) is not done automatically, you must pay close attention to available flash memory. Use the **squeeze** command to reclaim used space. We recommend that you use a large-capacity Flash card of at least 20 MB.

Loading the Configuration Commands from the Network

You can also store large configurations on FTP, RCP, or TFTP servers and download them at system startup. To use a network server to store large configurations, see the Copying a Configuration File from the SwitchControllerDevice to a TFTP Server (CLI) and Configuring the Switch to Download Configuration Files sections for more information on these commands.

Configuring the Switch to Download Configuration Files

You can configure the switch to load one or two configuration files at system startup. The configuration files are loaded into memory and read in as if you were typing the commands at the command line. Thus, the configuration for the switch is a mixture of the original startup configuration and the one or two downloaded configuration files.

Network Versus Host Configuration Files

For historical reasons, the first file the switch downloads is called the network configuration file. The second file the switch downloads is called the host configuration file. Two configuration files can be used when all of the switches on a network use many of the same commands. The network configuration file contains the standard commands used to configure all of the switches. The host configuration files contain the commands specific to one particular host. If you are loading two configuration files, the host configuration file should be the configuration file you want to have precedence over the other file. Both the network and host configuration files must reside on a network server reachable via TFTP, RCP, or FTP, and must be readable.

How to Manage Configuration File Information

Displaying Configuration File Information (CLI)

To display information about configuration files, complete the tasks in this section:

SUMMARY STEPS

1. **enable**
2. **show boot**
3. **more** *file-url*
4. **show running-config**
5. **show startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `SwitchControllerDevice> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**show boot** **Example:** `SwitchControllerDevice# show boot`	Lists the contents of the BOOT environment variable (if set), the name of the configuration file pointed to by the CONFIG_FILE environment variable, and the contents of the BOOTLDR environment variable.
Step 3	**more** *file-url* **Example:** `SwitchControllerDevice# more 10.1.1.1`	Displays the contents of a specified file.
Step 4	**show running-config** **Example:** `SwitchControllerDevice# show running-config`	Displays the contents of the running configuration file. (Command alias for the **more system:running-config** command.)
Step 5	**show startup-config** **Example:** `SwitchControllerDevice# show startup-config`	Displays the contents of the startup configuration file. (Command alias for the **more nvram:startup-config** command.) On all platforms except the Class A Flash file system platforms, the default startup-config file usually is stored in NVRAM.

	Command or Action	Purpose
		On the Class A Flash file system platforms, the CONFIG_FILE environment variable points to the default startup-config file. The CONFIG_FILE variable defaults to NVRAM.

Modifying the Configuration File (CLI)

The Cisco IOS software accepts one configuration command per line. You can enter as many configuration commands as you want. You can add comments to a configuration file describing the commands you have entered. Precede a comment with an exclamation point (!). Because comments are *not* stored in NVRAM or in the active copy of the configuration file, comments do not appear when you list the active configuration with the **show running-config** or **more system:running-config** EXEC commands. Comments do not display when you list the startup configuration with the **show startup-config** or **more nvram:startup-config** EXEC mode commands. Comments are stripped out of the configuration file when it is loaded onto the switch. However, you can list the comments in configuration files stored on a File Transfer Protocol (FTP), Remote Copy Protocol (RCP), or Trivial File Transfer Protocol (TFTP) server. When you configure the software using the CLI, the software executes the commands as you enter them. To configure the software using the CLI, use the following commands in privileged EXEC mode:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **configuration command**
4. Do one of the following:
   - **end**
   - **^Z**
5. **copy system:running-config nvram:startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `SwitchControllerDevice> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `SwitchControllerDevice# configure terminal`	Enters global configuration mode.
Step 3	**configuration command** **Example:** `SwitchControllerDevice(config)# configuration command`	Enter the necessary configuration commands. The Cisco IOS documentation set describes configuration commands organized by technology.
Step 4	Do one of the following: • **end** • **^Z** **Example:** `SwitchControllerDevice(config)# end`	Ends the configuration session and exits to EXEC mode. **Note** When you press the Ctrl and Z keys simultaneously, ^Z is displayed to the screen.
Step 5	**copy system:running-config nvram:startup-config** **Example:** `SwitchControllerDevice# copy system:running-config nvram:startup-config`	Saves the running configuration file as the startup configuration file. You may also use the **copy running-config startup-config** command alias, but you should be aware that this command is less precise. On most platforms, this command saves the configuration to NVRAM. On the Class A Flash file system platforms, this step saves the configuration to the location specified by the CONFIG_FILE environment variable (the default CONFIG_FILE variable specifies that the file should be saved to NVRAM).

Examples

In the following example, the switch prompt name of the switch is configured. The comment line, indicated by the exclamation mark (!), does not execute any command. The **hostname** command is used to change the switch name from switch to new_name. By pressing Ctrl-Z (^Z) or entering the **end** command, the user quits configuration mode. The **copy system:running-config nvram:startup-config** command saves the current configuration to the startup configuration.

```
SwitchControllerDevice# configure terminal
SwitchControllerDevice(config)# !The following command provides the switch host name.
SwitchControllerDevice(config)# hostname new_name
new_name(config)# end
new_name# copy system:running-config nvram:startup-config
```

When the startup configuration is NVRAM, it stores the current configuration information in text format as configuration commands, recording only non-default settings. The memory is checksummed to guard against corrupted data.

Note Some specific commands might not get saved to NVRAM. You need to enter these commands again if you reboot the machine. These commands are noted in the documentation. We recommend that you keep a list of these settings so that you can quickly reconfigure your switch after rebooting.

Copying a Configuration File from the SwitchControllerDevice to a TFTP Server (CLI)

To copy configuration information on a TFTP network server, complete the tasks in this section:

SUMMARY STEPS

1. **enable**
2. **copy system:running-config tftp:** [[[//*location*]/*directory*]/*filename*]
3. **copy nvram:startup-config tftp:** [[[//*location*]/*directory*]/*filename*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `SwitchControllerDevice> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**copy system:running-config tftp:** [[[//*location*]/*directory*]/*filename*] **Example:** `SwitchControllerDevice# copy system:running-config tftp: //server1/topdir/file10`	Copies the running configuration file to a TFTP server.
Step 3	**copy nvram:startup-config tftp:** [[[//*location*]/*directory*]/*filename*] **Example:** `SwitchControllerDevice# copy nvram:startup-config tftp: //server1/1stdir/file10`	Copies the startup configuration file to a TFTP server.

Examples

The following example copies a configuration file from a switch to a TFTP server:

```
SwitchControllerDevice# copy system:running-config tftp://172.16.2.155/tokyo-confg
Write file tokyo-confg on host 172.16.2.155? [confirm] Y
Writing tokyo-confg!!! [OK]
```

What to Do Next

After you have issued the **copy** command, you may be prompted for additional information or for confirmation of the action. The prompt displayed depends on how much information you provide in the **copy** command and the current setting of the **file prompt** global configuration command.

Copying a Configuration File from the SwitchControllerDevice to an RCP Server (CLI)

To copy a startup configuration file or a running configuration file from the switch to an RCP server, use the following commands beginning in privileged EXEC mode:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip rcmd remote-username** *username*
4. **end**
5. Do one of the following:
    - **copy system:running-config rcp:** [[[//[*username@*]*location*]/*directory*]/*filename*]
    - **copy nvram:startup-config rcp:** [[[//[*username@*]*location*]/*directory*]/*filename*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `SwitchControllerDevice> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `SwitchControllerDevice# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 3	**ip rcmd remote-username** *username* **Example:** `SwitchControllerDevice(config)# ip rcmd remote-username NetAdmin1`	(Optional) Changes the default remote username.
Step 4	**end** **Example:** `SwitchControllerDevice(config)# end`	(Optional) Exits global configuration mode.
Step 5	Do one of the following: • **copy system:running-config rcp:** [[[//[*username@*]*location*]/*directory*]/*filename*] • **copy nvram:startup-config rcp:** [[[//[*username@*]*location*]/*directory*]/*filename*] **Example:** `SwitchControllerDevice# copy system:running-config rcp: //NetAdmin1@example.com/dir-files/file1`	• Specifies that the switch running configuration file is to be stored on an RCP server or • Specifies that the switch startup configuration file is to be stored on an RCP server

Examples

Storing a Running Configuration File on an RCP Server

The following example copies the running configuration file named runfile2-confg to the netadmin1 directory on the remote host with an IP address of 172.16.101.101:

```
SwitchControllerDevice# copy system:running-config
rcp://netadmin1@172.16.101.101/runfile2-confg
Write file runfile2-confg on host 172.16.101.101?[confirm]
Building configuration...[OK]
Connected to 172.16.101.101
SwitchControllerDevice#
```

Storing a Startup Configuration File on an RCP Server

The following example shows how to store a startup configuration file on a server by using RCP to copy the file:

```
SwitchControllerDevice# configure terminal

SwitchControllerDevice(config)# ip rcmd remote-username netadmin2
```

```
SwitchControllerDevice(config)# end

SwitchControllerDevice# copy nvram:startup-config rcp:

Remote host[]? 172.16.101.101

Name of configuration file to write [start-confg]?
Write file start-confg on host 172.16.101.101?[confirm]
![OK]
```

What to Do Next

After you have issued the **copy** EXEC command, you may be prompted for additional information or for confirmation of the action. The prompt displayed depends on how much information you provide in the **copy** command and the current setting of the **file prompt** global configuration command.

Copying a Configuration File from the Switch to the FTP Server (CLI)

To copy a startup configuration file or a running configuration file from the switch to an FTP server, complete the following tasks:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip ftp username** *username*
4. **ip ftp password** *password*
5. **end**
6. Do one of the following:
   - **copy system:running-config ftp:** [[[//[*username* [**:***password*]**@**]*location*]/*directory*]/*filename*] or
   - **copy nvram:startup-config ftp:** [[[//[*username* [**:***password*]**@**]*location*]/*directory*]/*filename*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `SwitchControllerDevice> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `SwitchControllerDevice# configure terminal`	Enters global configuration mode on the switch.

	Command or Action	Purpose
Step 3	**ip ftp username** *username* **Example:** `SwitchControllerDevice(config)# ip ftp username NetAdmin1`	(Optional) Specifies the default remote username.
Step 4	**ip ftp password** *password* **Example:** `SwitchControllerDevice(config)# ip ftp password adminpassword`	(Optional) Specifies the default password.
Step 5	**end** **Example:** `SwitchControllerDevice(config)# end`	(Optional) Exits global configuration mode. This step is required only if you override the default remote username or password (see Steps 2 and 3).
Step 6	Do one of the following: • **copy system:running-config ftp:** [[[//[*username* [**:***password*]**@**]*location*]/*directory*]/*filename*] or • **copy nvram:startup-config ftp:** [[[//[*username* [**:***password*]**@**]*location*]/*directory*]/*filename*] **Example:** `SwitchControllerDevice# copy system:running-config ftp:`	Copies the running configuration or startup configuration file to the specified location on the FTP server.

Examples

Storing a Running Configuration File on an FTP Server

The following example copies the running configuration file named runfile-confg to the netadmin1 directory on the remote host with an IP address of 172.16.101.101:

```
SwitchControllerDevice# copy system:running-config
ftp://netadmin1:mypass@172.16.101.101/runfile-confg
Write file runfile-confg on host 172.16.101.101?[confirm]
Building configuration...[OK]
Connected to 172.16.101.101
SwitchControllerDevice#
```

Storing a Startup Configuration File on an FTP Server

The following example shows how to store a startup configuration file on a server by using FTP to copy the file:

```
SwitchControllerDevice# configure terminal

SwitchControllerDevice(config)# ip ftp username netadmin2

SwitchControllerDevice(config)# ip ftp password mypass

SwitchControllerDevice(config)# end

SwitchControllerDevice# copy nvram:startup-config ftp:

Remote host[]? 172.16.101.101

Name of configuration file to write [start-confg]?
Write file start-confg on host 172.16.101.101?[confirm]
![OK]
```

What to Do Next

After you have issued the **copy** EXEC command, you may be prompted for additional information or for confirmation of the action. The prompt displayed depends on how much information you provide in the **copy** command and the current setting of the **file prompt** global configuration command.

Copying a Configuration File from a TFTP Server to the Switch (CLI)

To copy a configuration file from a TFTP server to the switch, complete the tasks in this section:

SUMMARY STEPS

1. **enable**
2. **copy tftp:** [[[//*location*]/*directory*]/*filename*] **system:running-config**
3. **copy tftp:** [[[//*location*]/*directory*]/*filename*] **nvram:startup-config**
4. **copy tftp:** [[[//*location*]/*directory*]/*filename*]**flash-[n]:/directory/startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `SwitchControllerDevice> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**copy tftp:** [[[//*location*]/*directory*]/*filename*] **system:running-config** **Example:** `SwitchControllerDevice# copy tftp://server1/dir10/datasource system:running-config`	Copies a configuration file from a TFTP server to the running configuration.
Step 3	**copy tftp:** [[[//*location*]/*directory*]/*filename*] **nvram:startup-config** **Example:** `SwitchControllerDevice# copy tftp://server1/dir10/datasource nvram:startup-config`	Copies a configuration file from a TFTP server to the startup configuration.
Step 4	**copy tftp:** [[[//*location*]/*directory*]/*filename*]**flash-[n]:/directory/startup-config** **Example:** `SwitchControllerDevice# copy tftp://server1/dir10/datasource flash:startup-config`	Copies a configuration file from a TFTP server to the startup configuration.

Examples

In the following example, the software is configured from the file named tokyo-confg at IP address 172.16.2.155:

```
SwitchControllerDevice# copy tftp://172.16.2.155/tokyo-confg system:running-config

Configure using tokyo-confg from 172.16.2.155? [confirm] Y

Booting tokyo-confg from 172.16.2.155:!!! [OK - 874/16000 bytes]
```

What to Do Next

After you have issued the **copy** EXEC command, you may be prompted for additional information or for confirmation of the action. The prompt displayed depends on how much information you provide in the **copy** command and the current setting of the **file prompt** global configuration command.

Copying a Configuration File from the rcp Server to the Switch (CLI)

To copy a configuration file from an rcp server to the running configuration or startup configuration, complete the following tasks:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip rcmd remote-username** *username*
4. **end**
5. Do one of the following:
    - **copy rcp:**[[[//[*username@*]*location*]/*directory*]/*filename*]**system:running-config**
    - **copy rcp:**[[[//[*username@*]*location*]/*directory*]/*filename*]**nvram:startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `SwitchControllerDevice> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `SwitchControllerDevice# configure terminal`	(Optional) Enters configuration mode from the terminal. This step is required only if you override the default remote username (see Step 3).
Step 3	**ip rcmd remote-username** *username* **Example:** `SwitchControllerDevice(config)# ip rcmd remote-username NetAdmin1`	(Optional) Specifies the remote username.
Step 4	**end** **Example:** `SwitchControllerDevice(config)# end`	(Optional) Exits global configuration mode. This step is required only if you override the default remote username (see Step 2).
Step 5	Do one of the following: • **copy rcp:**[[[//[*username@*]*location*]/*directory*]/*filename*]**system:running-config** • **copy rcp:**[[[//[*username@*]*location*]/*directory*]/*filename*]**nvram:startup-config**	Copies the configuration file from an rcp server to the running configuration or startup configuration.

	Command or Action	Purpose
	Example: `SwitchControllerDevice# copy rcp://[user1@example.com/dir10/fileone] nvram:startup-config`	

Examples

Copy RCP Running-Config

The following example copies a configuration file named host1-confg from the netadmin1 directory on the remote server with an IP address of 172.16.101.101, and loads and runs the commands on the switch:

```
SwitchControllerDevice# copy rcp://netadmin1@172.16.101.101/host1-confg system:running-config
Configure using host1-confg from 172.16.101.101? [confirm]
Connected to 172.16.101.101
Loading 1112 byte file host1-confg:![OK]
SwitchControllerDevice#
%SYS-5-CONFIG: Configured from host1-config by rcp from 172.16.101.101
```

Copy RCP Startup-Config

The following example specifies a remote username of netadmin1. Then it copies the configuration file named host2-confg from the netadmin1 directory on the remote server with an IP address of 172.16.101.101 to the startup configuration.

```
SwitchControllerDevice# configure terminal
SwitchControllerDevice(config)# ip rcmd remote-username netadmin1
SwitchControllerDevice(config)# end
SwitchControllerDevice# copy rcp: nvram:startup-config
Address of remote host [255.255.255.255]? 172.16.101.101
Name of configuration file[rtr2-confg]? host2-confg
Configure using host2-confg from 172.16.101.101?[confirm]
Connected to 172.16.101.101
Loading 1112 byte file host2-confg:![OK]
[OK]
SwitchControllerDevice#
%SYS-5-CONFIG_NV:Non-volatile store configured from host2-config by rcp from 172.16.101.101
```

What to Do Next

After you have issued the **copy** EXEC command, you may be prompted for additional information or for confirmation of the action. The prompt displayed depends on how much information you provide in the **copy** command and the current setting of the **file prompt** global configuration command.

Copying a Configuration File from an FTP Server to the Switch (CLI)

To copy a configuration file from an FTP server to the running configuration or startup configuration, complete the tasks in this section:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip ftp username** *username*
4. **ip ftp password** *password*
5. **end**
6. Do one of the following:
   - **copy ftp:** [[[//[*username*[**:***password*]**@**]*location*] /*directory*]/*filename*]**system:running-config**
   - **copy ftp:** [[[//[*username*[**:***password*]**@**]*location*]/*directory*]/*filename*]**nvram:startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `SwitchControllerDevice> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `SwitchControllerDevice# configure terminal`	(Optional) Allows you to enter global configuration mode. This step is required only if you want to override the default remote username or password (see Steps 3 and 4).
Step 3	**ip ftp username** *username* **Example:** `SwitchControllerDevice(config)# ip ftp username NetAdmin1`	(Optional) Specifies the default remote username.
Step 4	**ip ftp password** *password* **Example:** `SwitchControllerDevice(config)# ip ftp password adminpassword`	(Optional) Specifies the default password.

	Command or Action	Purpose
Step 5	**end** **Example:** `SwitchControllerDevice(config)# end`	(Optional) Exits global configuration mode. This step is required only if you override the default remote username or password (see Steps 3 and 4).
Step 6	Do one of the following: • **copy ftp:** [[[//[*username*[**:***password*]**@**]*location*] /*directory*]/*filename*]**system:running-config** • **copy ftp:** [[[//[*username*[**:***password*]**@**]*location*]/*directory*]/*filename*]**nvram:startup-config** **Example:** `SwitchControllerDevice# copy ftp:nvram:startup-config`	Using FTP copies the configuration file from a network server to running memory or the startup configuration.

Examples

Copy FTP Running-Config

The following example copies a host configuration file named host1-confg from the netadmin1 directory on the remote server with an IP address of 172.16.101.101, and loads and runs the commands on the switch:

```
SwitchControllerDevice# copy ftp://netadmin1:mypass@172.16.101.101/host1-confg
system:running-config
Configure using host1-confg from 172.16.101.101? [confirm]
Connected to 172.16.101.101
Loading 1112 byte file host1-confg:![OK]
SwitchControllerDevice#
%SYS-5-CONFIG: Configured from host1-config by ftp from 172.16.101.101
```

Copy FTP Startup-Config

The following example specifies a remote username of netadmin1. Then it copies the configuration file named host2-confg from the netadmin1 directory on the remote server with an IP address of 172.16.101.101 to the startup configuration:

```
SwitchControllerDevice# configure terminal
SwitchControllerDevice(config)# ip ftp username netadmin1
SwitchControllerDevice(config)# ip ftp password mypass
SwitchControllerDevice(config)# end
SwitchControllerDevice# copy ftp: nvram:startup-config
Address of remote host [255.255.255.255]? 172.16.101.101
Name of configuration file[host1-confg]? host2-confg
Configure using host2-confg from 172.16.101.101?[confirm]
Connected to 172.16.101.101
Loading 1112 byte file host2-confg:![OK]
```

```
[OK]
SwitchControllerDevice#
%SYS-5-CONFIG_NV:Non-volatile store configured from host2-config by ftp from 172.16.101.101
```

What to Do Next

After you have issued the **copy** EXEC command, you may be prompted for additional information or for confirmation of the action. The prompt displayed depends on how much information you provide in the **copy** command and the current setting of the **file prompt** global configuration command.

Maintaining Configuration Files Larger than NVRAM

To maintain a configuration file that exceeds the size of NVRAM, perform the tasks described in the following sections:

Compressing the Configuration File (CLI)

To compress configuration files, complete the tasks in this section:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **service compress-config**
4. **end**
5. Do one of the following:
   - Use FTP, RCP, or TFTP to copy the new configuration.
   - **configure terminal**
6. **copy system:running-config nvram:startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `SwitchControllerDevice> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `SwitchControllerDevice# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 3	**service compress-config** **Example:** `SwitchControllerDevice(config)# service compress-config`	Specifies that the configuration file be compressed.
Step 4	**end** **Example:** `SwitchControllerDevice(config)# end`	Exits global configuration mode.
Step 5	Do one of the following: • Use FTP, RCP, or TFTP to copy the new configuration. • **configure terminal** **Example:** `SwitchControllerDevice# configure terminal`	Enters the new configuration: • If you try to load a configuration that is more than three times larger than the NVRAM size, the following error message is displayed: "[buffer overflow - *file-size* /*buffer-size* bytes]."
Step 6	**copy system:running-config nvram:startup-config** **Example:** `SwitchControllerDevice(config)# copy system:running-config nvram:startup-config`	When you have finished changing the running-configuration, save the new configuration.

Examples

The following example compresses a 129-KB configuration file to 11 KB:

```
SwitchControllerDevice# configure terminal

SwitchControllerDevice(config)# service compress-config

SwitchControllerDevice(config)# end

SwitchControllerDevice# copy tftp://172.16.2.15/tokyo-confg system:running-config

Configure using tokyo-confg from 172.16.2.155? [confirm] y

Booting tokyo-confg from 172.16.2.155:!!! [OK - 874/16000 bytes]
SwitchControllerDevice# copy system:running-config nvram:startup-config

Building configuration...
Compressing configuration from 129648 bytes to 11077 bytes
[OK]
```

Storing the Configuration in Flash Memory on Class A Flash File Systems (CLI)

To store the startup configuration in flash memory, complete the tasks in this section:

SUMMARY STEPS

1. **enable**
2. **copy nvram:startup-config** *flash-filesystem:filename*
3. **configure terminal**
4. **boot config flash-filesystem:** *filename*
5. **end**
6. Do one of the following:
   - Use FTP, RCP, or TFTP to copy the new configuration. If you try to load a configuration that is more than three times larger than the NVRAM size, the following error message is displayed: "[buffer overflow - *file-size* /*buffer-size* bytes]. "
   - **configure terminal**
7. **copy system:running-config nvram:startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `SwitchControllerDevice> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**copy nvram:startup-config** *flash-filesystem:filename* **Example:** `SwitchControllerDevice# copy nvram:startup-config usbflash0:switch-config`	Copies the current startup configuration to the new location to create the configuration file.
Step 3	**configure terminal** **Example:** `SwitchControllerDevice# configure terminal`	Enters global configuration mode.
Step 4	**boot config flash-filesystem:** *filename* **Example:** `SwitchControllerDevice(config)# boot config usbflash0:switch-config`	Specifies that the startup configuration file be stored in flash memory by setting the CONFIG_FILE variable.

	Command or Action	Purpose
Step 5	**end** **Example:** `SwitchControllerDevice(config)# end`	Exits global configuration mode.
Step 6	Do one of the following: • Use FTP, RCP, or TFTP to copy the new configuration. If you try to load a configuration that is more than three times larger than the NVRAM size, the following error message is displayed: “[buffer overflow - *file-size* /*buffer-size* bytes]. ” • **configure terminal** **Example:** `SwitchControllerDevice# configure terminal`	Enters the new configuration.
Step 7	**copy system:running-config nvram:startup-config** **Example:** `SwitchControllerDevice(config)# copy system:running-config nvram:startup-config`	When you have finished changing the running-configuration, save the new configuration.

Examples

The following example stores the configuration file in usbflash0:

```
SwitchControllerDevice# copy nvram:startup-config usbflash0:switch-config

SwitchControllerDevice# configure terminal

SwitchControllerDevice(config)# boot config usbflash0:switch-config

SwitchControllerDevice(config)# end

SwitchControllerDevice# copy system:running-config nvram:startup-config
```

Loading the Configuration Commands from the Network (CLI)

To use a network server to store large configurations, complete the tasks in this section:

SUMMARY STEPS

1. **enable**
2. **copy system:running-config** {**ftp:** | **rcp:** | **tftp:**}
3. **configure terminal**
4. **boot network** {**ftp:**[[[//[*username* [**:***password*]**@**]*location*]/*directory*]/*filename*] | **rcp:**[[[//[*username***@**]*location*]/*directory*]/*filename*] | **tftp:**[[[//*location*]/*directory*]/*filename*]}
5. **service config**
6. **end**
7. **copy system:running-config nvram:startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `SwitchControllerDevice> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**copy system:running-config** {**ftp:** | **rcp:** | **tftp:**} **Example:** `SwitchControllerDevice# copy system:running-config ftp:`	Saves the running configuration to an FTP, RCP, or TFTP server.
Step 3	**configure terminal** **Example:** `SwitchControllerDevice# configure terminal`	Enters global configuration mode.
Step 4	**boot network** {**ftp:**[[[//[*username* [**:***password*]**@**]*location*]/*directory*]/*filename*] | **rcp:**[[[//[*username***@**]*location*]/*directory*]/*filename*] | **tftp:**[[[//*location*]/*directory*]/*filename*]} **Example:** `SwitchControllerDevice(config)# boot network ftp://user1:guessme@example.com/dir10/file1`	Specifies that the startup configuration file be loaded from the network server at startup.
Step 5	**service config** **Example:** `SwitchControllerDevice(config)# service config`	Enables the switch to download configuration files at system startup.

	Command or Action	Purpose
Step 6	**end** **Example:** `SwitchControllerDevice(config)# end`	Exits global configuration mode.
Step 7	**copy system:running-config nvram:startup-config** **Example:** `SwitchControllerDevice# copy system:running-config nvram:startup-config`	Saves the configuration.

Copying Configuration Files from Flash Memory to the Startup or Running Configuration (CLI)

To copy a configuration file from flash memory directly to your startup configuration in NVRAM or your running configuration, enter one of the commands in Step 2:

SUMMARY STEPS

1. **enable**
2. Do one of the following:
   - **copy** *filesystem*: [*partition-number*:][*filename*] **nvram:startup-config**
   - **copy** *filesystem*: [*partition-number*:][*filename*] **system:running-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `SwitchControllerDevice> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	Do one of the following: • **copy** *filesystem*: [*partition-number*:][*filename*] **nvram:startup-config** • **copy** *filesystem*: [*partition-number*:][*filename*] **system:running-config**	• Loads a configuration file directly into NVRAM or • Copies a configuration file to your running configuration

	Command or Action	Purpose
	Example: `SwitchControllerDevice# copy usbflash0:4:ios-upgrade-1 nvram:startup-config`	

Examples

The following example copies the file named ios-upgrade-1 from partition 4 of the flash memory PC Card in usbflash0 to the switch startup configurations:

```
SwitchControllerDevice# copy usbflash0:4:ios-upgrade-1 nvram:startup-config

Copy 'ios-upgrade-1' from flash device as 'startup-config' ? [yes/no] yes

[OK]
```

Copying Configuration Files Between Flash Memory File Systems (CLI)

On platforms with multiple flash memory file systems, you can copy files from one flash memory file system, such as internal flash memory to another flash memory file system. Copying files to different flash memory file systems lets you create backup copies of working configurations and duplicate configurations for other switchs. To copy a configuration file between flash memory file systems, use the following commands in EXEC mode:

SUMMARY STEPS

1. **enable**
2. **show** *source-filesystem*:
3. **copy** *source-filesystem*: [*partition-number*:][*filename*] *dest-filesystem*:[*partition-number*:][*filename*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `SwitchControllerDevice> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**show** *source-filesystem*: **Example:** `SwitchControllerDevice# show flash:`	Displays the layout and contents of flash memory to verify the filename.

	Command or Action	Purpose
Step 3	**copy** *source-filesystem*: [*partition-number***:**][*filename*] *dest-filesystem***:**[*partition-number***:**][*filename*] **Example:** `SwitchControllerDevice# copy flash: usbflash0:`	Copies a configuration file between flash memory devices. • The source device and the destination device cannot be the same. For example, the **copy usbflash0: usbflash0:** command is invalid.

Example

The following example copies the file named running-config from partition 1 on internal flash memory to partition 1 of usbflash0 on a switch. In this example, the source partition is not specified, so the switch prompts for the partition number:

```
SwitchControllerDevice# copy flash: usbflash0:

System flash
Partition   Size    Used      Free      Bank-Size  State          Copy Mode
  1         4096K   3070K     1025K     4096K      Read/Write     Direct
  2        16384K   1671K    14712K     8192K      Read/Write     Direct
[Type ?<no> for partition directory; ? for full directory; q to abort]
Which partition? [default = 1]
System flash directory, partition 1:
File  Length   Name/status
  1   3142748  dirt/network/mars-test/c3600-j-mz.latest
  2   850      running-config
[3143728 bytes used, 1050576 available, 4194304 total]
usbflash0 flash directory:
File  Length   Name/status
  1   1711088  dirt/gate/c3600-i-mz
  2   850      running-config
[1712068 bytes used, 2482236 available, 4194304 total]
Source file name? running-config

Destination file name [running-config]?
Verifying checksum for 'running-config' (file # 2)...  OK
Erase flash device before writing? [confirm]
Flash contains files. Are you sure you want to erase? [confirm]
Copy 'running-config' from flash: device
  as 'running-config' into usbflash0: device WITH erase? [yes/no] yes

Erasing device... eeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeee ...erased!

 [OK - 850/4194304 bytes]
Flash device copy took 00:00:30 [hh:mm:ss]
Verifying checksum...  OK (0x16)
```

Copying a Configuration File from an FTP Server to Flash Memory Devices (CLI)

To copy a configuration file from an FTP server to a flash memory device, complete the task in this section:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip ftp username** *username*
4. **ip ftp password** *password*
5. **end**
6. **copy ftp:** [[//*location*]/*directory*]/*bundle_name* **flash:**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `SwitchControllerDevice> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `SwitchControllerDevice# configure terminal`	(Optional) Enters global configuration mode. This step is required only if you override the default remote username or password (see Steps 3 and 4).
Step 3	**ip ftp username** *username* **Example:** `SwitchControllerDevice(config)# ip ftp username Admin01`	(Optional) Specifies the remote username.
Step 4	**ip ftp password** *password* **Example:** `SwitchControllerDevice(config)# ip ftp password adminpassword`	(Optional) Specifies the remote password.
Step 5	**end** **Example:** `SwitchControllerDevice(config)# end`	(Optional) Exits configuration mode. This step is required only if you override the default remote username (see Steps 3 and 4).
Step 6	**copy ftp:** [[//*location*]/*directory*]/*bundle_name* **flash:** **Example:** `SwitchControllerDevice>copy ftp:/cat3k_caa-universalk9.SSA.03.12.02.EZP.150-12.02.EZP.150-12.02.EZP.bin flash:`	Copies the configuration file from a network server to the flash memory device using FTP.

What to Do Next

After you have issued the **copy** EXEC command, you may be prompted for additional information or for confirmation of the action. The prompt displayed depends on how much information you provide in the **copy** command and the current setting of the **file prompt** global configuration command.

Copying a Configuration File from an RCP Server to Flash Memory Devices (CLI)

To copy a configuration file from an RCP server to a flash memory device, complete the tasks in this section:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip rcmd remote-username** *username*
4. **end**
5. **copy rcp:** [[[//[*username@*]*location*]/*directory*] /*bundle_name*] **flash:**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `SwitchControllerDevice> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `SwitchControllerDevice# configure terminal`	(Optional) Enters global configuration mode. This step is required only if you override the default remote username or password (see Step 3).
Step 3	**ip rcmd remote-username** *username* **Example:** `SwitchControllerDevice(config)# ip rcmd remote-username Admin01`	(Optional) Specifies the remote username.

	Command or Action	Purpose
Step 4	**end** **Example:** `SwitchControllerDevice(config)# end`	(Optional) Exits configuration mode. This step is required only if you override the default remote username or password (see Step 3).
Step 5	**copy rcp:** [[[//[*username@*]*location*]/*directory*] /*bundle_name*] **flash:** **Example:** `SwitchControllerDevice# copy rcp://netadmin@172.16.101.101/bundle1 flash:`	Copies the configuration file from a network server to the flash memory device using RCP. Respond to any switch prompts for additional information or confirmation. Prompting depends on how much information you provide in the **copy** command and the current setting of the **file prompt** command.

Copying a Configuration File from a TFTP Server to Flash Memory Devices (CLI)

To copy a configuration file from a TFTP server to a flash memory device, complete the tasks in this section:

SUMMARY STEPS

1. **enable**
2. **copy tftp:** [[[//*location*]/*directory*]/bundle_name **flash:**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `SwitchControllerDevice> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**copy tftp:** [[[//*location*]/*directory*]/bundle_name **flash:** **Example:** `SwitchControllerDevice# copy tftp:/cat3k_caa-universalk9.SSA.03.12.02.EZP.150-12.02.EZP.150-12.02.EZP.bin flash:`	Copies the file from a TFTP server to the flash memory device. Reply to any switch prompts for additional information or confirmation. Prompting depends on how much information you provide in the **copy** command and the current setting of the **file prompt** command.

	Command or Action	Purpose

Examples

The following example shows the copying of the configuration file named switch-config from a TFTP server to the flash memory card inserted in usbflash0. The copied file is renamed new-config.

```
SwitchControllerDevice#
copy tftp:switch-config usbflash0:new-config
```

Re-executing the Configuration Commands in the Startup Configuration File (CLI)

To re-execute the commands located in the startup configuration file, complete the task in this section:

SUMMARY STEPS

1. **enable**
2. **configure memory**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `SwitchControllerDevice> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure memory** **Example:** `SwitchControllerDevice# configure memory`	Re-executes the configuration commands located in the startup configuration file.

Clearing the Startup Configuration (CLI)

You can clear the configuration information from the startup configuration. If you reboot the switch with no startup configuration, the switch enters the Setup command facility so that you can configure the switch from scratch. To clear the contents of your startup configuration, complete the task in this section:

SUMMARY STEPS

1. **enable**
2. **erase nvram**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `SwitchControllerDevice> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**erase nvram** **Example:** `SwitchControllerDevice# erase nvram`	Clears the contents of your startup configuration. **Note** For all platforms except the Class A Flash file system platforms, this command erases NVRAM. The startup configuration file cannot be restored once it has been deleted. On Class A Flash file system platforms, when you use the **erase startup-config** EXEC command, the switch erases or deletes the configuration pointed to by the CONFIG_FILE environment variable. If this variable points to NVRAM, the switch erases NVRAM. If the CONFIG_FILE environment variable specifies a flash memory device and configuration filename, the switch deletes the configuration file. That is, the switch marks the file as “deleted,” rather than erasing it. This feature allows you to recover a deleted file.

Deleting a Specified Configuration File (CLI)

To delete a specified configuration on a specific flash device, complete the task in this section:

SUMMARY STEPS

1. **enable**
2. **delete** *flash-filesystem*:*filename*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `SwitchControllerDevice> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**delete** *flash-filesystem***:***filename* **Example:** `SwitchControllerDevice# delete usbflash0:myconfig`	Deletes the specified configuration file on the specified flash device. **Note** On Class A and B Flash file systems, when you delete a specific file in flash memory, the system marks the file as deleted, allowing you to later recover a deleted file using the **undelete** EXEC command. Erased files cannot be recovered. To permanently erase the configuration file, use the **squeeze** EXEC command. On Class C Flash file systems, you cannot recover a file that has been deleted. If you attempt to erase or delete the configuration file specified by the CONFIG_FILE environment variable, the system prompts you to confirm the deletion.

Specifying the CONFIG_FILE Environment Variable on Class A Flash File Systems (CLI)

On Class A flash file systems, you can configure the Cisco IOS software to load the startup configuration file specified by the CONFIG_FILE environment variable. The CONFIG_FILE variable defaults to NVRAM. To change the CONFIG_FILE environment variable, complete the tasks in this section:

SUMMARY STEPS

1. **enable**
2. **copy** [*flash-url* | *ftp-url* | *rcp-url* | *tftp-url* | **system:running-config** | **nvram:startup-config**] *dest-flash-url*
3. **configure terminal**
4. **boot config** *dest-flash-url*
5. **end**
6. **copy system:running-config nvram:startup-config**
7. **show boot**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `SwitchControllerDevice> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**copy** [*flash-url* | *ftp-url* | *rcp-url* | *tftp-url* | **system:running-config** | **nvram:startup-config**] *dest-flash-url*	Copies the configuration file to the flash file system from which the switch loads the file on restart.

	Command or Action	Purpose
	Example: `SwitchControllerDevice# copy system:running-config nvram:startup-config`	
Step 3	**configure terminal** **Example:** `SwitchControllerDevice# configure terminal`	Enters global configuration mode.
Step 4	**boot config** *dest-flash-url* **Example:** `SwitchControllerDevice(config)# boot config 172.16.1.1`	Sets the CONFIG_FILE environment variable. This step modifies the runtime CONFIG_FILE environment variable.
Step 5	**end** **Example:** `SwitchControllerDevice(config)# end`	Exits global configuration mode.
Step 6	**copy system:running-config nvram:startup-config** **Example:** `SwitchControllerDevice# copy system:running-config nvram:startup-config`	Saves the configuration performed in Step 3 to the startup configuration.
Step 7	**show boot** **Example:** `SwitchControllerDevice# show boot`	(Optional) Allows you to verify the contents of the CONFIG_FILE environment variable.

Examples

The following example copies the running configuration file to the switch. This configuration is then used as the startup configuration when the system is restarted:

```
SwitchControllerDevice# copy system:running-config usbflash0:config2
SwitchControllerDevice# configure terminal
SwitchControllerDevice(config)# boot config usbflash0:config2
SwitchControllerDevice(config)# end
SwitchControllerDevice# copy system:running-config nvram:startup-config
[ok]
SwitchControllerDevice# show boot
BOOT variable = usbflash0:rsp-boot-m
CONFIG_FILE variable = nvram:
```

```
Current CONFIG_FILE variable = usbflash0:config2
Configuration register is 0x010F
```

What to Do Next

After you specify a location for the startup configuration file, the **nvram:startup-config** command is aliased to the new location of the startup configuration file. The **more nvram:startup-config** EXEC command displays the startup configuration, regardless of its location. The **erase nvram:startup-config** EXEC command erases the contents of NVRAM and deletes the file pointed to by the CONFIG_FILE environment variable.

When you save the configuration using the **copy system:running-config nvram:startup-config** command, the switch saves a complete version of the configuration file to the location specified by the CONFIG_FILE environment variable and a distilled version to NVRAM. A distilled version is one that does not contain access list information. If NVRAM contains a complete configuration file, the switch prompts you to confirm your overwrite of the complete version with the distilled version. If NVRAM contains a distilled configuration, the switch does not prompt you for confirmation and proceeds with overwriting the existing distilled configuration file in NVRAM.

Note If you specify a file in a flash device as the CONFIG_FILE environment variable, every time you save your configuration file with the **copy system:running-config nvram:startup-config** command, the old configuration file is marked as "deleted," and the new configuration file is saved to that device. Eventually, Flash memory fills up as the old configuration files still take up memory. Use the **squeeze** EXEC command to permanently delete the old configuration files and reclaim the space.

Configuring the Switch to Download Configuration Files

You can specify an ordered list of network configuration and host configuration filenames. The Cisco IOS XE software scans this list until it loads the appropriate network or host configuration file.

To configure the switch to download configuration files at system startup, perform at least one of the tasks described in the following sections:

- Configuring the Switch to Download the Network Configuration File (CLI)
- Configuring the Switch to Download the Host Configuration File (CLI)

If the switch fails to load a configuration file during startup, it tries again every 10 minutes (the default setting) until a host provides the requested files. With each failed attempt, the switch displays the following message on the console terminal:

```
Booting host-confg... [timed out]
```

If there are any problems with the startup configuration file, or if the configuration register is set to ignore NVRAM, the switch enters the Setup command facility.

Configuring the Switch to Download the Network Configuration File (CLI)

To configure the Cisco IOS software to download a network configuration file from a server at startup, complete the tasks in this section:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **boot network** {**ftp:**[[[//[*username* [**:***password*]**@**]*location*]/*directory*]/*filename*] | **rcp:**[[[//[*username@*]*location*]/*directory*]/*filename*] | **tftp:**[[[//*location*]/*directory*]/*filename*]}
4. **service config**
5. **end**
6. **copy system:running-config nvram:startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `SwitchControllerDevice> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `SwitchControllerDevice# configure terminal`	Enters global configuration mode.
Step 3	**boot network** {**ftp:**[[[//[*username* [**:***password*]**@**]*location*]/*directory*]/*filename*] | **rcp:**[[[//[*username@*]*location*]/*directory*]/*filename*] | **tftp:**[[[//*location*]/*directory*]/*filename*]} **Example:** `SwitchControllerDevice(config)# boot network tftp:hostfile1`	Specifies the network configuration file to download at startup, and the protocol to be used (TFTP, RCP, or FTP). • If you do not specify a network configuration filename, the Cisco IOS software uses the default filename network-confg. If you omit the address, the switch uses the broadcast address. • You can specify more than one network configuration file. The software tries them in order entered until it loads one. This procedure can be useful for keeping files with different configuration information loaded on a network server.
Step 4	**service config** **Example:** `SwitchControllerDevice(config)# service config`	Enables the system to automatically load the network file on restart.
Step 5	**end** **Example:** `SwitchControllerDevice(config)# end`	Exits global configuration mode.

	Command or Action	Purpose
Step 6	**copy system:running-config nvram:startup-config** **Example:** `SwitchControllerDevice# copy system:running-config nvram:startup-config`	Saves the running configuration to the startup configuration file.

Configuring the Switch to Download the Host Configuration File (CLI)

To configure the Cisco IOS software to download a host configuration file from a server at startup, complete the tasks in this section:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **boot host** {**ftp:**[[[//[*username* [**:***password*]**@**]*location*]/*directory*]/*filename*] | **rcp:**[[[//[*username***@**]*location*]/*directory*]/*filename*] | **tftp:**[[[//*location*]/*directory*]/*filename*] }
4. **service config**
5. **end**
6. **copy system:running-config nvram:startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `SwitchControllerDevice> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `SwitchControllerDevice# configure terminal`	Enters global configuration mode.
Step 3	**boot host** {**ftp:**[[[//[*username* [**:***password*]**@**]*location*]/*directory*]/*filename*] | **rcp:**[[[//[*username***@**]*location*]/*directory*]/*filename*] | **tftp:**[[[//*location*]/*directory*]/*filename*] }	Specifies the host configuration file to download at startup, and the protocol to be used (FTP, RCP, or TFTP): • If you do not specify a host configuration filename, the switch uses its own name to form a host configuration filename by

	Command or Action	Purpose
	Example: `SwitchControllerDevice(config)# boot host tftp:hostfile1`	converting the name to all lowercase letters, removing all domain information, and appending "-confg." If no host name information is available, the software uses the default host configuration filename switch-confg. If you omit the address, the switch uses the broadcast address. • You can specify more than one host configuration file. The Cisco IOS software tries them in order entered until it loads one. This procedure can be useful for keeping files with different configuration information loaded on a network server.
Step 4	**service config** **Example:** `SwitchControllerDevice(config)# service config`	Enables the system to automatically load the host file upon restart.
Step 5	**end** **Example:** `SwitchControllerDevice(config)# end`	Exits global configuration mode.
Step 6	**copy system:running-config nvram:startup-config** **Example:** `SwitchControllerDevice# copy system:running-config nvram:startup-config`	Saves the running configuration to the startup configuration file.

Example

In the following example, a switch is configured to download the host configuration file named hostfile1 and the network configuration file named networkfile1. The switch uses TFTP and the broadcast address to obtain the file:

```
SwitchControllerDevice# configure terminal
SwitchControllerDevice(config)# boot host tftp:hostfile1
SwitchControllerDevice(config)# boot network tftp:networkfile1
SwitchControllerDevice(config)# service config
SwitchControllerDevice(config)# end
SwitchControllerDevice# copy system:running-config nvram:startup-config
```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
Cisco IOS configuration commands	*Cisco IOS Configuration Fundamentals Command Reference*

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

Standard	Title
No new or modified standards are supported, and support for existing standards has not been modified	--

MIBs

MIB	MIBs Link
• No new or modified MIBs are supported, and support for existing MIBs has not been modified.	To locate and download MIBs for selected platforms, Cisco software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
No new or modified RFCs are supported, and support for existing RFCs has not been modified.	--

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

CHAPTER 18

Configuration Replace and Configuration Rollback

Prerequisites for Configuration Replace and Configuration Rollback

The format of the configuration files used as input by the Configuration Replace and Configuration Rollback feature must comply with standard Cisco software configuration file indentation rules as follows:

- Start all commands on a new line with no indentation, unless the command is within a configuration submode.
- Indent commands within a first-level configuration submode one space.
- Indent commands within a second-level configuration submode two spaces.
- Indent commands within subsequent submodes accordingly.

These indentation rules describe how the software creates configuration files for such commands as **show running-config** or **copy running-config** *destination-url*. Any configuration file generated on a Cisco device complies with these rules.

Free memory larger than the combined size of the two configuration files (the current running configuration and the saved replacement configuration) is required.

Restrictions for Configuration Replace and Configuration Rollback

If the device does not have free memory larger than the combined size of the two configuration files (the current running configuration and the saved replacement configuration), the configuration replace operation is not performed.

Certain Cisco configuration commands such as those pertaining to physical components of a networking device (for example, physical interfaces) cannot be added or removed from the running configuration. For example, a configuration replace operation cannot remove the **interface ethernet 0** command line from the current running configuration if that interface is physically present on the device. Similarly, the **interface ethernet 1** command line cannot be added to the running configuration if no such interface is physically present on the device. A configuration replace operation that attempts to perform these types of changes results in error messages indicating that these specific command lines failed.

In very rare cases, certain Cisco configuration commands cannot be removed from the running configuration without reloading the device. A configuration replace operation that attempts to remove this type of command results in error messages indicating that these specific command lines failed.

Information About Configuration Replace and Configuration Rollback

Configuration Archive

The Cisco IOS configuration archive is intended to provide a mechanism to store, organize, and manage an archive of Cisco IOS configuration files to enhance the configuration rollback capability provided by the **configure replace** command. Before this feature was introduced, you could save copies of the running configuration using the **copy running-config** *destination-url* command, storing the replacement file either locally or remotely. However, this method lacked any automated file management. On the other hand, the Configuration Replace and Configuration Rollback feature provides the capability to automatically save copies of the running configuration to the Cisco IOS configuration archive. These archived files serve as checkpoint configuration references and can be used by the **configure replace** command to revert to previous configuration states.

The **archive config** command allows you to save Cisco IOS configurations in the configuration archive using a standard location and filename prefix that is automatically appended with an incremental version number (and optional timestamp) as each consecutive file is saved. This functionality provides a means for consistent identification of saved Cisco IOS configuration files. You can specify how many versions of the running configuration are kept in the archive. After the maximum number of files are saved in the archive, the oldest file is automatically deleted when the next, most recent file is saved. The **show archive** command displays information for all configuration files saved in the Cisco IOS configuration archive.

The Cisco IOS configuration archive, in which the configuration files are stored and available for use with the **configure replace** command, can be located on the following file systems: FTP, HTTP, RCP, TFTP.

Configuration Replace

The **configure replace** privileged EXEC command provides the capability to replace the current running configuration with any saved Cisco IOS configuration file. This functionality can be used to revert to a previous configuration state, effectively rolling back any configuration changes that were made since the previous configuration state was saved.

When using the **configure replace** command, you must specify a saved Cisco IOS configuration as the replacement configuration file for the current running configuration. The replacement file must be a complete configuration generated by a Cisco IOS device (for example, a configuration generated by the **copy running-config** *destination-url* command), or, if generated externally, the replacement file must comply with the format of files generated by Cisco IOS devices. When the **configure replace** command is entered, the current running configuration is compared with the specified replacement configuration and a set of diffs is generated. The algorithm used to compare the two files is the same as that employed by the **show archive config differences** command. The resulting diffs are then applied by the Cisco IOS parser to achieve the replacement configuration state. Only the diffs are applied, avoiding potential service disruption from reapplying configuration commands that already exist in the current running configuration. This algorithm effectively handles configuration changes to order-dependent commands (such as access lists) through a multiple pass process. Under normal circumstances, no more than three passes are needed to complete a configuration replace operation, and a limit of five passes is performed to preclude any looping behavior.

The Cisco IOS **copy** *source-url* **running-config** privileged EXEC command is often used to copy a stored Cisco IOS configuration file to the running configuration. When using the **copy** *source-url* **running-config** command as an alternative to the **configure replace** *target-url* privileged EXEC command, the following major differences should be noted:

- The **copy** *source-url* **running-config** command is a merge operation and preserves all of the commands from both the source file and the current running configuration. This command does not remove commands from the current running configuration that are not present in the source file. In contrast, the **configure replace** *target-url* command removes commands from the current running configuration that are not present in the replacement file and adds commands to the current running configuration that need to be added.
- The **copy** *source-url* **running-config** command applies every command in the source file, whether or not the command is already present in the current running configuration. This algorithm is inefficient and, in some cases, can result in service outages. In contrast, the **configure replace** *target-url* command only applies the commands that need to be applied**—**no existing commands in the current running configuration are reapplied.
- A partial configuration file may be used as the source file for the **copy** *source-url* **running-config** command, whereas a complete Cisco IOS configuration file must be used as the replacement file for the **configure replace** *target-url* command.

A locking feature for the configuration replace operation was introduced. When the **configure replace** command is used, the running configuration file is locked by default for the duration of the configuration replace operation. This locking mechanism prevents other users from changing the running configuration while the replacement operation is taking place, which might otherwise cause the replacement operation to terminate unsuccessfully. You can disable the locking of the running configuration by using the **no lock** keyword when issuing the **configure replace** command.

The running configuration lock is automatically cleared at the end of the configuration replace operation. You can display any locks that may be currently applied to the running configuration using the **show configuration lock** command.

Configuration Rollback

The concept of rollback comes from the transactional processing model common to database operations. In a database transaction, you might make a set of changes to a given database table. You then must choose whether to commit the changes (apply the changes permanently) or to roll back the changes (discard the changes and revert to the previous state of the table). In this context, rollback means that a journal file containing a log of the changes is discarded, and no changes are applied. The result of the rollback operation is to revert to the previous state, before any changes were applied.

The **configure replace** command allows you to revert to a previous configuration state, effectively rolling back changes that were made since the previous configuration state was saved. Instead of basing the rollback operation on a specific set of changes that were applied, the Cisco IOS configuration rollback capability uses the concept of reverting to a specific configuration state based on a saved Cisco IOS configuration file. This concept is similar to the database idea of saving a checkpoint (a saved version of the database) to preserve a specific state.

If the configuration rollback capability is desired, you must save the Cisco IOS running configuration before making any configuration changes. Then, after entering configuration changes, you can use that saved configuration file to roll back the changes (using the **configure replace** *target-url* command). Furthermore, because you can specify any saved Cisco IOS configuration file as the replacement configuration, you are not limited to a fixed number of rollbacks, as is the case in some rollback models.

Configuration Rollback Confirmed Change

The Configuration Rollback Confirmed Change feature allows configuration changes to be performed with an optional requirement that they be confirmed. If this confirmation is not received, the configuration is returned to the state prior to the changes being applied. The mechanism provides a safeguard against inadvertent loss of connectivity between a network device and the user or management application due to configuration changes.

Benefits of Configuration Replace and Configuration Rollback

- Allows you to revert to a previous configuration state, effectively rolling back configuration changes.
- Allows you to replace the current running configuration file with the startup configuration file without having to reload the switch or manually undo CLI changes to the running configuration file, therefore reducing system downtime.
- Allows you to revert to any saved Cisco IOS configuration state.
- Simplifies configuration changes by allowing you to apply a complete configuration file to the switch, where only the commands that need to be added or removed are affected.
- When using the **configure replace** command as an alternative to the **copy** *source-url* **running-config** command, increases efficiency and prevents risk of service outages by not reapplying existing commands in the current running configuration.

How to Use Configuration Replace and Configuration Rollback

Creating a Configuration Archive (CLI)

No prerequisite configuration is needed to use the **configure replace** command. Using the **configure replace** command in conjunction with the Cisco IOS configuration archive and the **archive config** command is optional but offers significant benefit for configuration rollback scenarios. Before using the **archive config** command, the configuration archive must be configured. Perform this task to configure the characteristics of the configuration archive.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **archive**
4. **path** *url*
5. **maximum** *number*
6. **time-period** *minutes*
7. **end**
8. **archive config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `SwitchControllerDevice> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `SwitchControllerDevice# configure terminal`	Enters global configuration mode.
Step 3	**archive** **Example:** `SwitchControllerDevice(config)# archive`	Enters archive configuration mode.

	Command or Action	Purpose
Step 4	**path** *url* **Example:** `SwitchControllerDevice(config-archive)# path flash:myconfiguration`	Specifies the location and filename prefix for the files in the Cisco IOS configuration archive. **Note** If a directory is specified in the path instead of file, the directory name must be followed by a forward slash as follows: path flash:/directory/. The forward slash is not necessary after a filename; it is only necessary when specifying a directory.
Step 5	**maximum** *number* **Example:** `SwitchControllerDevice(config-archive)# maximum 14`	(Optional) Sets the maximum number of archive files of the running configuration to be saved in the Cisco IOS configuration archive. • The *number* argument is the maximum number of archive files of the running configuration to be saved in the Cisco IOS configuration archive. Valid values are from 1 to 14. The default is 10. **Note** Before using this command, you must configure the **path** command to specify the location and filename prefix for the files in the Cisco IOS configuration archive.
Step 6	**time-period** *minutes* **Example:** `SwitchControllerDevice(config-archive)# time-period 1440`	(Optional) Sets the time increment for automatically saving an archive file of the current running configuration in the Cisco IOS configuration archive. • The *minutes* argument specifies how often, in minutes, to automatically save an archive file of the current running configuration in the Cisco IOS configuration archive. **Note** Before using this command, you must configure the **path** command to specify the location and filename prefix for the files in the Cisco IOS configuration archive.
Step 7	**end** **Example:** `SwitchControllerDevice(config-archive)# end`	Exits to privileged EXEC mode.
Step 8	**archive config** **Example:** `SwitchControllerDevice# archive config`	Saves the current running configuration file to the configuration archive. **Note** The **path** command must be configured before using this command.

Performing a Configuration Replace or Configuration Rollback Operation (CLI)

Perform this task to replace the current running configuration file with a saved Cisco IOS configuration file.

Note You must create a configuration archive before performing this procedure. See Creating a Configuration Archive (CLI) for detailed steps. The following procedure details how to return to that archived configuration in the event of a problem with the current running configuration.

SUMMARY STEPS

1. **enable**
2. **configure replace** *target-url* [**nolock**] [**list**] [**force**] [**ignore case**] [**revert trigger** [**error**][**timer** *minutes*] | **time** *minutes*]]
3. **configure revert** { **now** | **timer** {*minutes* | **idle** *minutes*} }
4. **configure confirm**
5. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `SwitchControllerDevice> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure replace** *target-url* [**nolock**] [**list**] [**force**] [**ignore case**] [**revert trigger** [**error**][**timer** *minutes*] | **time** *minutes*]] **Example:** `SwitchControllerDevice# configure replace flash: startup-config time 120`	Replaces the current running configuration file with a saved Cisco IOS configuration file. • The *target - url* argument is a URL (accessible by the Cisco IOS file system) of the saved Cisco IOS configuration file that is to replace the current running configuration, such as the configuration file created using the **archive config** command. • The **list** keyword displays a list of the command lines applied by the Cisco IOS software parser during each pass of the configuration replace operation. The total number of passes performed is also displayed. • The **force** keyword replaces the current running configuration file with the specified saved Cisco IOS configuration file without prompting you for confirmation. • The **time** *minutes* keyword and argument specify the time (in minutes) within which you must enter the **configure confirm** command to confirm replacement of the current running configuration file. If the **configure confirm** command is not entered within the specified time limit, the configuration replace operation is automatically reversed (in other words, the current running configuration file is restored to the configuration state that existed prior to entering the **configure replace** command). • The **nolock** keyword disables the locking of the running configuration file that prevents other users from changing the running configuration during a configuration replace operation.

	Command or Action	Purpose

		• The **revert trigger** keywords set the following triggers for reverting to the original configuration:
		  • **error** —Reverts to the original configuration upon error.
		  • **timer** *minutes* —Reverts to the original configuration if specified time elapses.
		• The **ignore case** keyword allows the configuration to ignore the case of the confirmation command.

Step 3	**configure revert** { **now** | **timer** {*minutes* | **idle** *minutes*} }
	
	Example:
	`SwitchControllerDevice# configure revert now`
		(Optional) To cancel the timed rollback and trigger the rollback immediately, or to reset parameters for the timed rollback, use the **configure revert**command in privileged EXEC mode.
		• **now** —Triggers the rollback immediately.
		• **timer** —Resets the configuration revert timer.
		  • Use the *minutes* argument with the **timer** keyword to specify a new revert time in minutes.
		  • Use the **idle** keyword along with a time in minutes to set the maximum allowable time period of no activity before reverting to the saved configuration.

Step 4	**configure confirm** **Example:** `SwitchControllerDevice# configure confirm`	(Optional) Confirms replacement of the current running configuration file with a saved Cisco IOS configuration file. **Note** Use this command only if the **time** *seconds* keyword and argument of the **configure replace** command are specified.
Step 5	**exit** **Example:** `SwitchControllerDevice# exit`	Exits to user EXEC mode.

Monitoring and Troubleshooting the Feature (CLI)

Perform this task to monitor and troubleshoot the Configuration Replace and Configuration Rollback feature.

SUMMARY STEPS

1. **enable**
2. **show archive**
3. **debug archive versioning**
4. **debug archive config timestamp**
5. **exit**

DETAILED STEPS

Step 1 **enable**

Use this command to enable privileged EXEC mode. Enter your password if prompted.

Example:

```
SwitchControllerDevice> enable
SwitchControllerDevice#
```

Step 2 **show archive**

Use this command to display information about the files saved in the Cisco IOS configuration archive.

Example:

```
SwitchControllerDevice# show archive
There are currently 1 archive configurations saved.
The next archive file will be named flash:myconfiguration-2
 Archive #  Name
   0
   1       flash:myconfiguration-1 <- Most Recent
   2
   3
   4
   5
   6
   7
   8
   9
   10
   11
   12
   13
   14
```

The following is sample output from the **show archive** command after several archive files of the running configuration have been saved. In this example, the maximum number of archive files to be saved is set to three.

Example:

```
SwitchControllerDevice# show archive
There are currently 3 archive configurations saved.
The next archive file will be named flash:myconfiguration-8
 Archive #  Name
   0
   1       :Deleted
   2       :Deleted
   3       :Deleted
   4       :Deleted
```

```
5       flash:myconfiguration-5
6       flash:myconfiguration-6
7       flash:myconfiguration-7 <- Most Recent
8
9
10
11
12
13
14
```

Step 3 **debug archive versioning**

Use this command to enable debugging of the Cisco IOS configuration archive activities to help monitor and troubleshoot configuration replace and rollback.

Example:

```
SwitchControllerDevice# debug archive versioning
Jan  9 06:46:28.419:backup_running_config
Jan  9 06:46:28.419:Current = 7
Jan  9 06:46:28.443:Writing backup file flash:myconfiguration-7
Jan  9 06:46:29.547: backup worked
```

Step 4 **debug archive config timestamp**

Use this command to enable debugging of the processing time for each integral step of a configuration replace operation and the size of the configuration files being handled.

Example:

```
SwitchControllerDevice# debug archive config timestamp
SwitchControllerDevice# configure replace flash:myconfiguration force
Timing Debug Statistics for IOS Config Replace operation:
       Time to read file usbflash0:sample_2.cfg = 0 msec (0 sec)
       Number of lines read:55
       Size of file        :1054
Starting Pass 1
       Time to read file system:running-config = 0 msec (0 sec)
       Number of lines read:93
       Size of file        :2539
       Time taken for positive rollback pass = 320 msec (0 sec)
       Time taken for negative rollback pass = 0 msec (0 sec)
       Time taken for negative incremental diffs pass = 59 msec (0 sec)
       Time taken by PI to apply changes = 0 msec (0 sec)
       Time taken for Pass 1 = 380 msec (0 sec)
Starting Pass 2
       Time to read file system:running-config = 0 msec (0 sec)
       Number of lines read:55
       Size of file        :1054
       Time taken for positive rollback pass = 0 msec (0 sec)
       Time taken for negative rollback pass = 0 msec (0 sec)
       Time taken for Pass 2 = 0 msec (0 sec)
Total number of passes:1
Rollback Done
```

Step 5 **exit**

Use this command to exit to user EXEC mode.

Example:

```
SwitchControllerDevice# exit
SwitchControllerDevice>
```

Configuration Examples for Configuration Replace and Configuration Rollback

Creating a Configuration Archive

The following example shows how to perform the initial configuration of the Cisco IOS configuration archive. In this example, flash:myconfiguration is specified as the location and filename prefix for the files in the configuration archive and a value of 10 is set as the maximum number of archive files to be saved.

```
configure terminal
!
archive
 path flash:myconfiguration
 maximum 10
end
```

Replacing the Current Running Configuration with a Saved Cisco IOS Configuration File

The following example shows how to replace the current running configuration with a saved Cisco IOS configuration file named flash:myconfiguration. The **configure replace** command interactively prompts you to confirm the operation.

```
SwitchControllerDevice# configure replace flash:myconfiguration
This will apply all necessary additions and deletions
to replace the current running configuration with the
contents of the specified configuration file, which is
assumed to be a complete configuration, not a partial
configuration. Enter Y if you are sure you want to proceed. ? [no]: Y
Total number of passes: 1
Rollback Done
```

In the following example, the **list** keyword is specified in order to display the command lines that were applied during the configuration replace operation:

```
SwitchControllerDevice# configure replace flash:myconfiguration list
This will apply all necessary additions and deletions
to replace the current running configuration with the
contents of the specified configuration file, which is
assumed to be a complete configuration, not a partial
configuration. Enter Y if you are sure you want to proceed. ? [no]: Y
!Pass 1
!List of Commands:
no snmp-server community public ro
snmp-server community mystring ro

end
Total number of passes: 1
Rollback Done
```

Reverting to the Startup Configuration File

The following example shows how to revert to the Cisco IOS startup configuration file using the **configure replace** command. This example also shows the use of the optional **force** keyword to override the interactive user prompt:

```
SwitchControllerDevice# configure replace flash:startup-config force
Total number of passes: 1
Rollback Done
```

Performing a Configuration Replace Operation with the configure confirm Command

The following example shows the use of the **configure replace** command with the **time** *minutes* keyword and argument. You must enter the **configure confirm** command within the specified time limit to confirm replacement of the current running configuration file. If the **configure confirm** command is not entered within the specified time limit, the configuration replace operation is automatically reversed (in other words, the current running configuration file is restored to the configuration state that existed prior to entering the **configure replace** command).

```
SwitchControllerDevice# configure replace flash:startup-config time 120
This will apply all necessary additions and deletions
to replace the current running configuration with the
contents of the specified configuration file, which is
assumed to be a complete configuration, not a partial
configuration. Enter Y if you are sure you want to proceed. ? [no]: Y
Total number of passes: 1
Rollback Done
SwitchControllerDevice# configure confirm
```

The following example shows the use of the **configure revert** command with the **timer** keyword. You must enter the **configure revert** command to cancel the timed rollback and trigger the rollback immediately, or to reset parameters for the timed rollback.

```
SwitchControllerDevice# configure revert timer 100
```

Performing a Configuration Rollback Operation

The following example shows how to make changes to the current running configuration and then roll back the changes. As part of the configuration rollback operation, you must save the current running configuration before making changes to the file. In this example, the **archive config** command is used to save the current running configuration. The generated output of the **configure replace** command indicates that only one pass was performed to complete the rollback operation.

Note Before using the **archive config** command, you must configure the **path** command to specify the location and filename prefix for the files in the Cisco IOS configuration archive.

You first save the current running configuration in the configuration archive as follows:

```
archive config
```

You then enter configuration changes as shown in the following example:

```
configure terminal
!
user netops2 password rain
user netops3 password snow
exit
```

After having made changes to the running configuration file, assume you now want to roll back these changes and revert to the configuration that existed before the changes were made. The **show archive** command is used to verify the version of the configuration to be used as a replacement file. The **configure replace** command is then used to revert to the replacement configuration file as shown in the following example:

```
SwitchControllerDevice# show archive
There are currently 1 archive configurations saved.
The next archive file will be named flash:myconfiguration-2
 Archive #  Name
   0
   1       flash:myconfiguration-1 <- Most Recent
   2
   3
   4
   5
   6
   7
   8
   9
   10
SwitchControllerDevice# configure replace flash:myconfiguration-1
Total number of passes: 1
Rollback Done
```

Additional References

Related Documents

Related Topic	Document Title
Configuration Locking	*Exclusive Configuration Change Access and Access Session Locking*
Commands for managing configuration files	*Cisco IOS Configuration Fundamentals Command Reference*
Information about managing configuration files	*Managing Configuration Files*

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

Standards	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	--

MIBs

MIBs	MIBs Link
No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature.	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

RFCs

RFCs	Title
No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature.	--

Technical Assistance

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

CHAPTER 19

Working with the Flash File System

Information About the Flash File System

The flash file system is a single flash device on which you can store files. It also provides several commands to help you manage software bundles and configuration files. The default flash file system on the switch is named flash:.

As viewed from the active switch, or any stack member, flash: refers to the local flash device, which is the device attached to the same switch on which the file system is being viewed. In a switch stack, each of the flash devices from the various stack members can be viewed from the active switch. The names of these flash file systems include the corresponding switch member numbers. For example, flash-3:, as viewed from the active switch, refers to the same file system as does flash: on stack member 3. Use the **show file systems** privileged EXEC command to list all file systems, including the flash file systems in the switch stack.

Only one user at a time can manage the software bundles and configuration files for a switch stack.

Displaying Available File Systems

To display the available file systems on your switch, use the **show file systems** privileged EXEC command as shown in this example for a standalone switch:

```
SwitchControllerDevice# show file systems
File Systems:
     Size(b)     Free(b)       Type    Flags   Prefixes
*   15998976     5135872      flash     rw     flash:
           -           -     opaque     rw     bs:
           -           -     opaque     rw     vb:
      524288      520138      nvram     rw     nvram:
           -           -    network     rw     tftp:
           -           -     opaque     rw     null:
           -           -     opaque     rw     system:
           -           -     opaque     ro     xmodem:
           -           -     opaque     ro     ymodem:
```

This example shows a switch stack. In this example, the active switch is stack member 1; the file system on stack member 2 is displayed as flash-2:, the file system on stack member 3 is displayed as flash-3: and so on up to stack member 9, displayed as flash-9: for a 9-member stack. The example also shows the crashinfo directories and a USB flash drive plugged into the active switch:

```
SwitchControllerDevice# show file systems
File Systems:
      Size(b)        Free(b)      Type   Flags   Prefixes
     145898496      5479424       disk     rw    crashinfo:crashinfo-1:
     248512512      85983232      disk     rw    crashinfo-2:stby-crashinfo:
     146014208      17301504      disk     rw    crashinfo-3:
     146014208             0      disk     rw    crashinfo-4:
     146014208       1572864      disk     rw    crashinfo-5:
     248512512      30932992      disk     rw    crashinfo-6:
     146014208       6291456      disk     rw    crashinfo-7:
     146276352      15728640      disk     rw    crashinfo-8:
     146276352      73400320      disk     rw    crashinfo-9:
*    741621760     481730560      disk     rw    flash:flash-1:
    1622147072    1360527360      disk     rw    flash-2:stby-flash:
     729546752     469762048      disk     rw    flash-3:
     729546752     469762048      disk     rw    flash-4:
     729546752     469762048      disk     rw    flash-5:
    1622147072    1340604416      disk     rw    flash-6:
     729546752     469762048      disk     rw    flash-7:
    1749549056    1487929344      disk     rw    flash-8:
    1749549056    1487929344      disk     rw    flash-9:
             0             0      disk     rw    unix:
             -             -      disk     rw    usbflash0:usbflash0-1:
             -             -      disk     rw    usbflash0-2: stby-usbflash0:
             -             -      disk     rw    usbflash0-3:
             -             -      disk     rw    usbflash0-4:
             -             -      disk     rw    usbflash0-5:
             -             -      disk     rw    usbflash0-6:
             -             -      disk     rw    usbflash0-7:
             -             -      disk     rw    usbflash0-8:
             -             -      disk     rw    usbflash0-9:
             0             0      disk     ro    webui:
             -             -    opaque     rw    system:
             -             -    opaque     rw    tmpsys:
       2097152       2055643     nvram     rw    stby-nvram:
             -             -     nvram     rw    stby-rcsf:
             -             -    opaque     rw    null:
             -             -    opaque     ro    tar:
             -             -   network     rw    tftp:
       2097152       2055643     nvram     rw    nvram:
             -             -    opaque     wo    syslog:
             -             -   network     rw    rcp:
             -             -   network     rw    http:
```

```
       -              -   network     rw    ftp:
       -              -   network     rw    scp:
       -              -   network     rw    https:
       -              -    opaque     ro    cns:
       -              -    opaque     rw    revrcsf:
```

Table 29: show file systems Field Descriptions

Field	Value
Size(b)	Amount of memory in the file system in bytes.
Free(b)	Amount of free memory in the file system in bytes.
Type	Type of file system. **disk**—The file system is for a flash memory device, USB flash, and crashinfo file. **network**—The file system for network devices; for example, an FTP server or and HTTP server. **nvram**—The file system is for a NVRAM device. **opaque**—The file system is a locally generated pseudo file system (for example, the system) or a download interface, such as brimux. **unknown**—The file system is an unknown type.
Flags	Permission for file system. **ro**—read-only. **rw**—read/write. **wo**—write-only.

Field	Value
Prefixes	Alias for file system. **crashinfo:—**Crashinfo file. **flash:—**Flash file system. **ftp:—**FTP server. **http:—**HTTP server. **https:—**Secure HTTP server. **nvram:—**NVRAM. **null:—**Null destination for copies. You can copy a remote file to null to find its size. **rcp:—**Remote Copy Protocol (RCP) server. **scp:—**Session Control Protocol (SCP) server. **system:—**Contains the system memory, including the running configuration. **tftp:—**TFTP network server. **usbflash0:—**USB flash memory. **xmodem:—**Obtain the file from a network machine by using the Xmodem protocol. **ymodem:—**Obtain the file from a network machine by using the Ymodem protocol.

Setting the Default File System

You can specify the file system or directory that the system uses as the default file system by using the **cd** *filesystem:* privileged EXEC command. You can set the default file system to omit the *filesystem:* argument from related commands. For example, for all privileged EXEC commands that have the optional *filesystem:* argument, the system uses the file system specified by the **cd** command.

By default, the default file system is *flash:*.

You can display the current default file system as specified by the **cd** command by using the **pwd** privileged EXEC command.

Displaying Information About Files on a File System

You can view a list of the contents of a file system before manipulating its contents. For example, before copying a new configuration file to flash memory, you might want to verify that the file system does not already contain a configuration file with the same name. Similarly, before copying a flash configuration file to another location, you might want to verify its filename for use in another command. To display information about files on a file system, use one of the privileged EXEC commands listed in the following table.

Table 30: Commands for Displaying Information About Files

Command	Description
dir [/all] **[***filesystem:filename***]**	Displays a list of files on a file system.
show file systems	Displays more information about each of the files on a file system.
show file information *file-url*	Displays information about a specific file.
show file descriptors	Displays a list of open file descriptors. File descriptors are the internal representations of open files. You can use this command to see if another user has a file open.

For example, to display a list of all files in a file system, use the **dir** privileged EXEC command:

```
switch# dir flash:
Directory of flash:/
7386  -rwx     2097152 Jan 23 2013 14:06:49 +00:00 nvram_config
7378  drwx        4096 Jan 23 2013 09:35:11 +00:00 mnt
7385  -rw-   221775876 Jan 23 2013 14:15:13 +00:00
cat3k_caa-universalk9.SSA.03.12.02.EZP.150-12.02.EZP.150-12.02.EZP.bin
7389  -rwx         556 Jan 21 2013 20:47:30 +00:00 vlan.dat
712413184 bytes total (445063168 bytes free)
switch#
```

Changing Directories and Displaying the Working Directory (CLI)

Beginning in privileged EXEC mode, follow these steps to change directories and to display the working directory:

SUMMARY STEPS

1. **dir** *filesystem:*
2. **cd** *directory_name*
3. **pwd**
4. **cd**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**dir** *filesystem:*	Displays the directories on the specified file system.

	Command or Action	Purpose
	Example: `SwitchControllerDevice# dir flash:`	For *filesystem:*, use flash: for the system board flash device. To access flash partitions of switch members in a stack, use flash-*n* where *n* is the stack member number. For example, flash-4.
Step 2	**cd** *directory_name* **Example:** `SwitchControllerDevice# cd new_configs`	Navigates to the specified directory. The command example shows how to navigate to the directory named *new_configs*.
Step 3	**pwd** **Example:** `SwitchControllerDevice# pwd`	Displays the working directory.
Step 4	**cd** **Example:** `SwitchControllerDevice# cd`	Navigates to the default directory.

Creating Directories (CLI)

Beginning in privileged EXEC mode, follow these steps to create a directory:

SUMMARY STEPS

1. **dir** *filesystem:*
2. **mkdir** *directory_name*
3. **dir** *filesystem:*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**dir** *filesystem:* **Example:** `SwitchControllerDevice# dir flash:`	Displays the directories on the specified file system. For *filesystem:*, use flash: for the system board flash device.

	Command or Action	Purpose
Step 2	**mkdir** *directory_name* **Example:** `SwitchControllerDevice# mkdir new_configs`	Creates a new directory. Directory names are case sensitive and are limited to 45 characters between the slashes (/); the name cannot contain control characters, spaces, slashes, quotes, semicolons, or colons.
Step 3	**dir** *filesystem:* **Example:** `SwitchControllerDevice# dir flash:`	Verifies your entry.

Removing Directories

To remove a directory with all its files and subdirectories, use the **delete /force /recursive** *filesystem:/file-url* privileged EXEC command.

Use the **/recursive** keyword to delete the named directory and all subdirectories and the files contained in it. Use the **/force** keyword to suppress the prompting that confirms a deletion of each file in the directory. You are prompted only once at the beginning of this deletion process.

For *filesystem*, use **flash:** for the system board flash device. For *file-url*, enter the name of the directory to be deleted. All of the files in the directory and the directory are removed.

Caution When directories are deleted, their contents cannot be recovered.

Copying Files

To copy a file from a source to a destination, use the **copy** *source-url destination-url* privileged EXEC command. For the source and destination URLs, you can use **running-config** and **startup-config** keyword shortcuts. For example, the **copy running-config startup-config** command saves the currently running configuration file to the NVRAM section of flash memory to be used as the configuration during system initialization.

You can also copy from special file systems (**xmodem:**, **ymodem:**) as the source for the file from a network machine that uses the Xmodem or Ymodem protocol.

Network file system URLs include ftp:, rcp:, and tftp: and have these syntaxes:

- FTP—ftp:[[//username [:password]@location]/directory]/filename
- RCP—rcp:[[//username@location]/directory]/filename
- TFTP—tftp:[[//location]/directory]/filename

Local writable file systems include flash:.

Some invalid combinations of source and destination exist. Specifically, you cannot copy these combinations:

- From a running configuration to a running configuration
- From a startup configuration to a startup configuration
- From a device to the same device (for example, the **copy flash: flash:** command is invalid)

Copying Files from One SwitchControllerDevice in a Stack to Another SwitchControllerDevice in the Same Stack

To copy a file from one switch in a stack to another switch in the same stack, use the **flash-X:** notation, where **X** is the switch number.

To view all switches in a stack, use the **show switch** command in privileged EXEC mode, as in the following example of a 9-member switch stack:

```
SwitchControllerDevice# show switch
Switch/Stack Mac Address : 0006.f6b9.b580 - Local Mac Address Mac persistency wait time:
Indefinite
                                             H/W   Current
Switch#   Role    Mac Address     Priority Version  State
------------------------------------------------------------
*1       Active   0006.f6b9.b580     15     P3B     Ready
 2       Standby  0006.f6ba.0c80     14     P3B     Ready
 3       Member   0006.f6ba.3300     7      P3B     Ready
 4       Member   0006.f6b9.df80     6      P3B     Ready
 5       Member   0006.f6ba.3880     13     P1A     Ready
 6       Member   1ce6.c7b6.ef00     4      PP      Ready
 7       Member   2037.06ce.2580     3      P2A     Ready
 8       Member   2037.0653.7e00     2      P5A     Ready
 9       Member   2037.0653.9280     1      P5B     Ready
```

To view all file systems available to copy on a specific switch, use the **copy** command as in the following example of a 5-member stack:

```
SwitchControllerDevice# copy flash: ?
  crashinfo-1:     Copy to crashinfo-1: file system
  crashinfo-2:     Copy to crashinfo-2: file system
  crashinfo-3:     Copy to crashinfo-3: file system
  crashinfo-4:     Copy to crashinfo-4: file system
  crashinfo-5:     Copy to crashinfo-5: file system
  crashinfo:       Copy to crashinfo: file system
  flash-1:         Copy to flash-1: file system
  flash-2:         Copy to flash-2: file system
  flash-3:         Copy to flash-3: file system
  flash-4:         Copy to flash-4: file system
  flash-5:         Copy to flash-5: file system
  flash:           Copy to flash: file system
  ftp:             Copy to ftp: file system
  http:            Copy to http: file system
  https:           Copy to https: file system
  null:            Copy to null: file system
  nvram:           Copy to nvram: file system
  rcp:             Copy to rcp: file system
  revrcsf:         Copy to revrcsf: file system
  running-config   Update (merge with) current system configuration
  scp:             Copy to scp: file system
  startup-config   Copy to startup configuration
  stby-crashinfo:  Copy to stby-crashinfo: file system
  stby-flash:      Copy to stby-flash: file system
  stby-nvram:      Copy to stby-nvram: file system
  stby-rcsf:       Copy to stby-rcsf: file system
```

```
  stby-usbflash0:  Copy to stby-usbflash0: file system
  syslog:          Copy to syslog: file system
  system:          Copy to system: file system
  tftp:            Copy to tftp: file system
  tmpsys:          Copy to tmpsys: file system
  usbflash0-1:     Copy to usbflash0-1: file system
  usbflash0-2:     Copy to usbflash0-2: file system
  usbflash0-3:     Copy to usbflash0-3: file system
  usbflash0-4:     Copy to usbflash0-4: file system
  usbflash0-5:     Copy to usbflash0-5: file system
  usbflash0:       Copy to usbflash0: file system

SwitchControllerDevice#
```

This example shows how to copy a config file stored in the flash partition of switch 2 to the flash partition of switch 4. It assumes that switch 2 and switch 4 are in the same stack.

```
SwitchControllerDevice# copy flash-2:config.txt flash-4:config.txt
```

Deleting Files

When you no longer need a file on a flash memory device, you can permanently delete it. To delete a file or directory from a specified flash device, use the **delete** [/**force**] [/**recursive**] [*filesystem:*]/*file-url* privileged EXEC command.

Use the **/recursive** keyword for deleting a directory and all subdirectories and the files contained in it. Use the **/force** keyword to suppress the prompting that confirms a deletion of each file in the directory. You are prompted only once at the beginning of this deletion process. Use the **/force** and **/recursive** keywords for deleting old software images that were installed by using the **archive download-sw** command but are no longer needed.

If you omit the *filesystem:* option, the switch uses the default device specified by the **cd** command. For *file-url*, you specify the path (directory) and the name of the file to be deleted.

When you attempt to delete any files, the system prompts you to confirm the deletion.

Caution When files are deleted, their contents cannot be recovered.

This example shows how to delete the file *myconfig* from the default flash memory device:

```
SwitchControllerDevice# delete myconfig
```

Creating, Displaying and Extracting Files (CLI)

You can create a file and write files into it, list the files in a file, and extract the files from a file as described in the next sections.

Beginning in privileged EXEC mode, follow these steps to create a file, display the contents, and extract it:

SUMMARY STEPS

1. **archive tar /create** *destination-url* **flash:** */file-url*
2. **archive tar /table** *source-url*
3. **archive tar /xtract** *source-url* **flash:**/*file-url* [*dir/file...*]
4. **more** [/**ascii** | /**binary** | /**ebcdic**] /*file-url*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**archive tar /create** *destination-url* **flash:** */file-url* **Example:** `switch# archive tar /create tftp:172.20.10.30/saved. flash:/new-configs`	Creates a file and adds files to it. For destination-url, specify the destination URL alias for the local or network file system and the name of the file to create: • Local flash file system syntax: **flash:** • FTP syntax: **ftp**:[[//*username*[:*password*]@*location*]/*directory*]/*-filename*. • RCP syntax: **rcp**:[[//*username@location*]/*directory*]/*-filename*. • TFTP syntax: **tftp**:[[//*location*]/*directory*]/*-filename*. For **flash:**/*file-url*, specify the location on the local flash file system in which the new file is created. You can also specify an optional list of files or directories within the source directory to add to the new file. If none are specified, all files and directories at this level are written to the newly created file.
Step 2	**archive tar /table** *source-url* **Example:** `switch# archive tar /table flash: /new_configs`	Displays the contents of a file. For *source-url*, specify the source URL alias for the local or network file system. The *-filename.* is the file to display. These options are supported: • Local flash file system syntax: **flash:** • FTP syntax: **ftp**:[[//*username*[:*password*]@*location*]/*directory*]/*-filename*. • RCP syntax: **rcp**:[[//*username@location*]/*directory*]/*-filename*. • TFTP syntax: **tftp**:[[//*location*]/*directory*]/*-filename*.

	Command or Action	Purpose
		You can also limit the file displays by specifying a list of files or directories after the file. Only those files appear. If none are specified, all files and directories appear.
Step 3	**archive tar /xtract** *source-url* **flash:**/*file-url* [*dir/file...*] **Example:** `switch# archive tar /xtract tftp:/172.20.10.30/saved. flash:/new-configs`	Extracts a file into a directory on the flash file system. For *source-url*, specify the source URL alias for the local file system. The *-filename.* is the file from which to extract files. These options are supported: • Local flash file system syntax: **flash:** • FTP syntax: **ftp**:[[//*username*[:*password*]@*location*]/*directory*]/*-filename*. • RCP syntax: **rcp**:[[//*username*@*location*]/*directory*]/*-filename*. • TFTP syntax: **tftp**:[[//*location*]/*directory*]/*-filename*. For **flash:**/*file-url* [*dir/file...*], specify the location on the local flash file system from which the file is extracted. Use the *dir/file...* option to specify a list of files or directories within the file to be extracted. If none are specified, all files and directories are extracted.
Step 4	**more** [/**ascii** | /**binary** | /**ebcdic**] /*file-url* **Example:** `switch# more flash:/new-configs`	Displays the contents of any readable file, including a file on a remote file system.

Additional References

Related Documents

Related Topic	Document Title
Commands for managing flash: file systems	*Cisco IOS Configuration Fundamentals Command Reference*

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

Standards	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	--

MIBs

MIBs	MIBs Link
No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature.	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

RFCs

RFCs	Title
No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature.	--

Technical Assistance

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

CHAPTER 20

Working with Cisco IOS XE Software Bundles

About Software Bundles and Packages

Cisco IOS XE software bundles include a set of Cisco IOS XE package (.pkg) files. You can install the package files on the switch or you can boot the switch from the IOS XE bundle itself.

To display information about the contents of a Cisco IOS XE bundle (.bin file), use the **show software package** command in privileged EXEC mode. Use the command to display information about an individual IOS XE package (.pkg) file as well.

Bundle and Package File Location on the Switch

When the switch is running in installed mode, the Cisco IOS XE package (.pkg) files and provisioning file (packages.conf) are stored in the system board flash memory (flash:). When the switch is running in bundle mode, the booted Cisco IOS XE software bundle (.bin) file is stored in the system board flash memory (flash:) or USB flash memory (usbflash0:).

To display information about the provisioning software that is currently running on the switch, use the **show version** privileged EXEC command. In the display, check the line that begins with

```
System bundle file is....
```

When the switch is running in installed mode, this line displays the name and location of the booted Cisco IOS XE provisioning file, typically flash:packages.conf.

When the switch is running in bundle mode, this line displays the name and location of the booted Cisco IOS XE bundle file.

To display information about the Cisco IOS XE package files that are running on the switch, use the **show version running** privileged EXEC command.

When the switch is running in installed mode, this command displays information about the set of package files contained in the booted provisioning file.

When the switch is running in bundle mode, this command displays information about the set of package files contained in the booted Cisco IOS XE software bundle.

Note For usbflash0:, the default format is FAT16, while FAT32 format is also supported.

```
SwitchControllerDevice# format usbflash0: ?
  FAT16   FAT16  filesystem type
  FAT32   FAT32  filesystem type
```

Upgrading Cisco IOS XE Software

The method that you use to upgrade Cisco IOS XE software depends on whether the switch is running in installed mode or in bundle mode.

Upgrading Cisco IOS XE Software: Install Mode

To upgrade the Cisco IOS XE software when the switch is running in installed mode, use the **software install** privileged EXEC command to install the packages from a new software bundle file. The software bundle can be installed from the local storage media or it can be installed over the network using TFTP or FTP.

The **software install** command expands the package files from the specified source bundle file and copies them to the local flash: storage device. When the source bundle is specified as a tftp: or ftp: URL, the bundle file is first downloaded into the switch's memory (RAM); the bundle file is not copied to local storage media.

After the package files are expanded and copied to flash: the running provisioning file (flash:packages.conf) is updated to reflect the newly installed packages, and the switch displays a reload prompt.

Note The **software install** command is not supported when the switch is running in bundle mode. Use the **software expand** privileged EXEC command to convert the switch from bundle mode to installed mode.

Upgrading Cisco IOS XE Software Install Mode Example

This example shows the **software install file** command being used to expand and copy the packages from a Cisco IOS XE bundle located on a TFTP server in order to upgrade to a new image:

```
SwitchControllerDevice#
software install file
tftp://172.19.211.47/cat3k_caa-universalk9.SSA.03.12.02.EZP.150-12.02.EZP.150-12.02.EZP.bin
Preparing install operation ...
[1]: Downloading file
tftp://172.19.211.47/cat3k_caa-universalk9.SSA.03.12.02.EZP.150-12.02.EZP.150-12.02.EZP.bin
 to active switch 1
[1]: Finished downloading file
tftp://172.19.211.47/cat3k_caa-universalk9.SSA.03.12.02.EZP.150-12.02.EZP.150-12.02.EZP.bin
 to active switch 1
[1]: Starting install operation
[1]: Expanding bundle cat3k_caa-universalk9.SSA.03.12.02.EZP.150-12.02.EZP.150-12.02.EZP.bin
[1]: Copying package files
```

```
[1]: Package files copied
[1]: Finished expanding bundle
cat3k_caa-universalk9.SSA.03.12.02.EZP.150-12.02.EZP.150-12.02.EZP.bin
[1]: Verifying and copying expanded package files to flash:
[1]: Verified and copied expanded package files to flash:
[1]: Starting compatibility checks
[1]: Finished compatibility checks
[1]: Starting application pre-installation processing
[1]: Finished application pre-installation processing
[1]: Old files list:
Removed cat3k_caa-base.SSA.03.09.17.EMP.pkg
Removed cat3k_caa-drivers.SSA.03.09.17.EMP.pkg
Removed cat3k_caa-infra.SSA.03.09.17.EMP.pkg
Removed cat3k_caa-iosd-universalk9.SSA.150-9.17.EMP.pkg
Removed cat3k_caa-platform.SSA.03.09.17.EMP.pkg
Removed cat3k_caa-wcm.SSA.03.09.17.EMP.pkg
[1]: New files list:
Added cat3k_caa-base.SPA.03.02.00.SE.pkg
Added cat3k_caa-drivers.SPA.03.02.00.SE.pkg
Added cat3k_caa-infra.SPA.03.02.00SE.pkg
Added cat3k_caa-iosd-universalk9.SPA.150-1.EX.pkg
Added cat3k_caa-platform.SPA.03.02.00.SE.pkg
Added cat3k_caa-wcm.SPA.03.02.00.SE.pkg
[1]: Creating pending provisioning file
[1]: Finished installing software. New software will load on reboot.
[1]: Setting rollback timer to 45 minutes
[1]: Do you want to proceed with reload? [yes/no]:
```

Upgrading Cisco IOS XE Software: Bundle Mode

To upgrade the Cisco IOS XE software when the switch is running in bundle mode, follow these steps:

1. Download the bundle file to local storage media.
2. Configure the **boot system** global configuration command to point to the bundle file.
3. Reload the switch.

Upgrading Cisco IOS XE Software Bundle Mode Example

This example shows the steps to upgrade the Cisco IOS XE software on a switch that is running in bundle mode. It shows using the **copy** command to copy the bundle file to flash:, configuring the boot system variable to point to the bundle file, saving a copy of the running configuration, and finally, reloading the switch.

```
SwitchControllerDevice#
copy
tftp://172.19.211.47/cat3k_caa-universalk9.SSA.03.12.02.EZP.150-12.02.EZP.150-12.02.EZP.bin
 flash:
Destination filename [cat3k_caa-universalk9.SSA.03.12.02.EZP.150-12.02.EZP.150-12.02.EZP.bin]?
Accessing
tftp://172.19.211.47/cat3k_caa-universalk9.SSA.03.12.02.EZP.150-12.02.EZP.150-12.02.EZP.bin...Loading
/tftpboot/cstohs/cat3k_caa-universalk9.SSA.03.12.02.EZP.150-12.02.EZP.150-12.02.EZP.bin
from 172.19.211.47 (via GigabitEthernet0/0):
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!! [OK - 220766688 bytes]
220766688 bytes copied in 124.330 secs (1775651 bytes/sec)

SwitchControllerDevice#
SwitchControllerDevice#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SwitchControllerDevice(config)# boot system switch all
flash:cat3k_caa-universalk9.SSA.03.12.02.EZP.150-12.02.EZP.150-12.02.EZP.bin
SwitchControllerDevice(config)# end
SwitchControllerDevice#
```

```
*Nov 19 14:02:42.441: %SYS-5-CONFIG_I: Configured from console by console

SwitchControllerDevice#
SwitchControllerDevice# write memory
Building configuration...
Compressed configuration from 4941 bytes to 2236 bytes[OK]

SwitchControllerDevice# reload
Reload command is being issued on Active unit, this will reload the whole stack
Proceed with reload? [confirm]
```

Converting from the Bundle Running Mode to the Install Running Mode

To convert the running mode of a switch from bundle mode to installed mode, use the **software expand running** privileged EXEC command. This command expands the packages from the booted IOS XE software bundle and copies them and the provisioning file to the specified to destination.

When you use the **software expand running** command to convert the switch from bundle mode to installed mode, specify the **to** destination as **flash:**. After you execute the command, configure the **boot system** command to point to the expanded provisioning file (flash:packages.conf), then reload the switch to boot in installed mode.

Note The **software expand running** command is not supported when the switch is running in installed mode.

Converting from the Bundle Running Mode to the Install Running Mode Example

This example shows using the **software expand running to** command to convert the active switch in a switch stack from the bundle running mode to the installed running mode:

```
SwitchControllerDevice# dir flash:
Directory of flash:/
 7386 -rwx     2097152 Jan 23 2013 14:06:49 +00:00 nvram_config
 7378 drwx        4096 Jan 23 2013 09:35:11 +00:00 mnt
 7385 -rw-   221775876 Jan 23 2013 14:15:13 +00:00
cat3k_caa-universalk9.SSA.03.12.02.EZP.150-12.02.EZP.150-12.02.EZP.bin
 7389 -rwx         556 Jan 21 2013 20:47:30 +00:00 vlan.dat
712413184 bytes total (445063168 bytes free)

SwitchControllerDevice#
SwitchControllerDevice# software expand running to flash:
Preparing expand operation ...
[2]: Expanding the running bundle
[2]: Copying package files
[2]: Package files copied
[2]: Finished expanding the running bundle
SwitchControllerDevice#
SwitchControllerDevice# dir flash:
Directory of flash:/
 7386 -rwx     2097152 Jan 23 2013 14:06:49 +00:00 nvram_config
 7378 drwx        4096 Jan 23 2013 09:35:11 +00:00 mnt
 7385 -rw-   221775876 Jan 23 2013 14:15:13 +00:00
cat3k_caa-universalk9.SSA.03.12.02.EZP.150-12.02.EZP.150-12.02.EZP.bin
 7391 -rw-    74410468 Jan 23 2013 14:16:57 +00:00 cat3k_caa-base.SPA.03.02.00SE.pkg
 7392 -rw-     2773680 Jan 23 2013 14:16:57 +00:00 cat3k_caa-drivers.SPA.03.02.00.SE.pkg
 7393 -rw-    32478044 Jan 23 2013 14:16:57 +00:00 cat3k_caa-infra.SPA.03.02.00SE.pkg
 7394 -rw-    30393116 Jan 23 2013 14:16:57 +00:00 cat3k_caa-iosd-universalk9.SPA.150-1.EX.pkg

 7389 -rwx         556 Jan 21 2013 20:47:30 +00:00 vlan.dat
```

```
 7395 -rw-    18313952 Jan 23 2013 14:16:57 +00:00 cat3k_caa-platform.SPA.03.02.00.SE.pkg
 7396 -rw-    63402700 Jan 23 2013 14:16:57 +00:00 cat3k_caa-wcm.SPA.10.0.100.0.pkg
 7388 -rw-        1218 Jan 23 2013 14:17:43 +00:00 packages.conf
712413184 bytes total (223019008 bytes free)

SwitchControllerDevice#
SwitchControllerDevice# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SwitchControllerDevice(config)# boot system switch all flash:packages.conf
SwitchControllerDevice(config)# end
SwitchControllerDevice#

*Jan 23 14:28:47.722: %SYS-5-CONFIG_I: Configured from console by console

SwitchControllerDevice# write memory
Building configuration...
Compressed configuration from 4851 bytes to 2187 bytes[OK]

SwitchControllerDevice#
SwitchControllerDevice# reload
Reload command is being issued on Active unit, this will reload the whole stack
Proceed with reload? [confirm]
```

Copying IOS XE Package and Bundle Files from One Stack Member to Another

For switch stacks running in installed mode, use the **software install source switch** privileged EXEC command to install the running software packages from an existing stack member to one or more other stack members that are running different (but compatible) software packages.

Copying IOS XE Package and Bundle Files from One Stack Member to Another Example

This example shows a 2-member stack where each switch is running a different (but compatible) software package. The **software install source switch** command is used to install the packages that are currently running on the standby switch (switch 1) onto the active switch (switch 2):

```
SwitchControllerDevice# show version running
Package: Base, version: 03.02.00SE, status: active
File: cat3k_caa-base.SPA.03.02.00SE.pkg, on: Switch1
Built: Wed Jan 09 21:59:52 PST 2013, by: gereddy

Package: Drivers, version: 03.02.00.SE, status: active
File: cat3k_caa-drivers.SPA.03.02.00.SE.pkg, on: Switch1
Built: Wed Jan 09 22:03:41 PST 2013, by: gereddy

Package: Infra, version: 03.02.00SE, status: active
File: cat3k_caa-infra.SPA.03.02.00SE.pkg, on: Switch1
Built: Wed Jan 09 22:00:56 PST 2013, by: gereddy

Package: IOS, version: 150-1.EX, status: active
File: cat3k_caa-iosd-universalk9.SPA.150-1.EX.pkg, on: Switch1
Built: Wed Jan 09 22:02:23 PST 2013, by: gereddy

Package: Platform, version: 03.02.00.SE, status: active
File: cat3k_caa-platform.SPA.03.02.00.SE.pkg, on: Switch1
Built: Wed Jan 09 22:01:46 PST 2013, by: gereddy

Package: WCM, version: 10.0.100.0, status: active
File: cat3k_caa-wcm.SPA.10.0.100.0.pkg, on: Switch1
Built: Wed Jan 09 22:03:05 PST 2013, by: gereddy

SwitchControllerDevice#
SwitchControllerDevice# software install source switch 1
Preparing install operation ...
[2]: Copying software from source switch 1 to switch 2
[2]: Finished copying software to switch 2
```

```
[2]: Starting install operation
[2]: Starting compatibility checks
[2]: Finished compatibility checks
[2]: Starting application pre-installation processing
[2]: Finished application pre-installation processing
[2]: Old files list:
Removed cat3k_caa-base.SSA.03.09.17.EMP.pkg
Removed cat3k_caa-drivers.SSA.03.09.17.EMP.pkg
Removed cat3k_caa-infra.SSA.03.09.17.EMP.pkg
Removed cat3k_caa-iosd-universalk9.SSA.150-9.17.EMP.pkg
Removed cat3k_caa-platform.SSA.03.09.17.EMP.pkg
Removed cat3k_caa-wcm.SSA.03.09.17.EMP.pkg
[2]: New files list:
Added cat3k_caa-base.SPA.03.02.00.SE.pkg
Added cat3k_caa-drivers.SPA.03.02.00.SE.pkg
Added cat3k_caa-infra.SPA.03.02.00.SE.pkg
Added cat3k_caa-iosd-universalk9.SPA.150-1.EX.pkg
Added cat3k_caa-platform.SPA.03.02.00.SE.pkg
Added cat3k_caa-wcm.SPA.10.0.100.0.pkg
[2]: Creating pending provisioning file
[2]: Finished installing software. New software will load on reboot.
[2]: Committing provisioning file
[2]: Do you want to proceed with reload? [yes/no]:
```

For switch stacks running in bundle mode, follow these steps to copy the bundle file from one stack member to another:

1. Use the **copy** privileged EXEC command to copy the running bundle from one switch in the stack to the other.
2. Configure the **boot system** global configuration command to point to the bundle file.
3. Reload the switch.

This example shows a 2-member stack where each switch is running a different (but compatible) software packages:

```
SwitchControllerDevice# copy
flash:cat3k_caa-universalk9.SSA.03.12.02.EZP.150-12.02.EZP.150-12.02.EZP.bin flash-1:
Destination filename [cat3k_caa-universalk9.SSA.03.12.02.EZP.150-12.02.EZP.150-12.02.EZP.bin]?
Copy in progress...
...
220766688 bytes copied in 181.700 secs (1215007 bytes/sec)
SwitchControllerDevice#
SwitchControllerDevice# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.

SwitchControllerDevice(config)# boot system switch 1
flash:cat3k_caa-universalk9.SSA.03.12.02.EZP.150-12.02.EZP.150-12.02.EZP.bin
SwitchControllerDevice(config)# end
SwitchControllerDevice#
```

Upgrading a SwitchControllerDevice Running Incompatible Software

To upgrade a switch that is running in installed mode with software packages that are incompatible with the switch stack (also running in installed mode), use the **software auto-upgrade** privileged EXEC command to install the software packages from an existing stack member to the stack member that is running incompatible software. Upon completion of the auto-upgrade installation, the incompatible switch automatically reloads and joins the stack as a fully functioning member.

Note If you configure the global **software auto-upgrade enable** command, the auto-upgrade functionality is initiated automatically when a switch with incompatible software running in installed mode joins the stack that is running in installed mode. For more information, see *Cisco IOS Configuration Fundamentals Command Reference, Cisco IOS XE Release 3SE (Catalyst 3850 Switches)*.

Upgrading a SwitchControllerDevice Running Incompatible Software Example

This example shows a 2-member switch stack; switch 2 is the active switch and switch 1 is running incompatible software:

```
SwitchControllerDevice# show switch
Switch/Stack Mac Address : 6400.f125.1100 - Local Mac Address
Mac persistency wait time: Indefinite
H/W Current
Switch# Role Mac Address Priority Version State
------------------------------------------------------------
1 Member 6400.f125.1a00 1 0 V-Mismatch
*2 Active 6400.f125.1100 1 V01 Ready
SwitchControllerDevice#
SwitchControllerDevice# software auto-upgrade
% Auto upgrade has been initiated for the following incompatible switches: 1

INFO level system messages will be generated to provide status information during
the auto upgrade process

SwitchControllerDevice#
*Oct 19 06:59:14.521: %INSTALLER-6-AUTO_UPGRADE_SW_INITIATED: 2 installer: Auto upgrade
initiated for switch 1
*Oct 19 06:59:14.522: %INSTALLER-6-AUTO_UPGRADE_SW: 2 installer: Searching stack for software
 to upgrade switch 1
*Oct 19 06:59:14.523: %INSTALLER-6-AUTO_UPGRADE_SW: 2 installer: Found donor switch 2 to
auto upgrade switch 1
*Oct 19 06:59:14.523: %INSTALLER-6-AUTO_UPGRADE_SW: 2 installer: Upgrading switch 1 with
software from switch 2
*Oct 19 07:00:47.829: %INSTALLER-6-AUTO_UPGRADE_SW: 2 installer: Finished installing software
 on switch 1
*Oct 19 07:00:47.829: %INSTALLER-6-AUTO_UPGRADE_SW: 2 installer: Reloading switch 1 to
complete the auto upgrade
```

To upgrade a switch that is running in bundle mode with a software bundle that is incompatible with the switch stack (also running in bundle mode), follow these steps:

1. Use the **copy** privileged EXEC command to copy the running bundle from one switch in the stack to the other.
2. Configure the **boot system** global configuration command to point to the bundle file.
3. Reload the switch.

This example shows a 2-member switch stack running in bundle mode; switch 2 is the active switch and switch 1 is running an incompatible bundle:

```
SwitchControllerDevice# show switch
Switch/Stack Mac Address : 6400.f125.1100 - Local Mac Address
Mac persistency wait time: Indefinite
H/W Current
Switch# Role Mac Address Priority Version State
------------------------------------------------------------
1 Member 6400.f125.1a00 1 0 V-Mismatch
*2 Active 6400.f125.1100 1 V01 Ready
```

```
SwitchControllerDevice#
SwitchControllerDevice# copy
flash:cat3k_caa-universalk9.SSA.03.12.02.EZP.150-12.02.EZP.150-12.02.EZP.bin flash-1:
Destination filename [cat3k_caa-universalk9.SSA.03.12.02.EZP.150-12.02.EZP.150-12.02.EZP.bin]?
Copy in progress...
...
220766688 bytes copied in 181.700 secs (1215007 bytes/sec)

SwitchControllerDevice#
SwitchControllerDevice# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SwitchControllerDevice(config)# boot system switch 1
flash:cat3k_caa-universalk9.SSA.03.12.02.EZP.150-12.02.EZP.150-12.02.EZP.bin
SwitchControllerDevice(config)# end
SwitchControllerDevice#
*Nov 19 16:08:14.857: %SYS-5-CONFIG_I: Configured from console by console
SwitchControllerDevice# reload slot 1
Stack is in Half ring setup; Reloading a switch might cause stack split
Proceed with reload? [confirm]
```

Upgrading a Switch Running in Incompatible Running Mode

When a switch running in bundle mode tries to join a stack running in installed mode, use the **software auto-upgrade** privileged EXEC command to install the incompatible switch's running packages and convert the switch to installed mode. Upon completion of the auto-upgrade running mode conversion, the incompatible switch automatically reloads and attempts to join the stack in installed mode.

Note If you configure the global **software auto-upgrade enable** command, the auto-upgrade functionality is initiated automatically when a switch with incompatible software running in installed mode joins the stack that is running in installed mode. For more information, see *Cisco IOS Configuration Fundamentals Command Reference, Cisco IOS XE Release 3SE (Catalyst 3850 Switches)*.

Upgrading a SwitchControllerDevice Running in Incompatible Running Mode Example

This example shows a 2-member switch stack running in installed mode; switch 2 is the active switch and switch1 is running in bundle mode:

```
SwitchControllerDevice# show switch
Switch/Stack Mac Address : 6400.f125.1100 - Local Mac Address
Mac persistency wait time: Indefinite
H/W Current
Switch# Role Mac Address Priority Version State
------------------------------------------------------------
1 Member 6400.f125.1a00 1 0 V-Mismatch
*2 Active 6400.f125.1100 1 V01 Ready

SwitchControllerDevice#
SwitchControllerDevice# software auto-upgrade
% Auto upgrade has been initiated for the following incompatible switches: 1

INFO level system messages will be generated to provide status information during the auto
 upgrade process

SwitchControllerDevice#
*Oct 19 07:17:16.694: %INSTALLER-6-AUTO_UPGRADE_SW_INITIATED: 2 installer: Auto upgrade
initiated for switch 1
*Oct 19 07:17:16.694: %INSTALLER-6-AUTO_UPGRADE_SW: 2 installer: Converting switch 1 to
installed mode by
*Oct 19 07:17:16.694: %INSTALLER-6-AUTO_UPGRADE_SW: 2 installer: installing its running
software
```

```
*Oct 19 07:18:50.488: %INSTALLER-6-AUTO_UPGRADE_SW: 2 installer: Setting the boot var on
switch 1
*Oct 19 07:18:51.553: %INSTALLER-6-AUTO_UPGRADE_SW: 2 installer: Finished installing the
running software on switch 1
*Oct 19 07:18:51.553: %INSTALLER-6-AUTO_UPGRADE_SW: 2 installer: Reloading switch 1 to boot
 in installed mode
```

Note When you use the **software auto-upgrade** command to convert an incompatible switch to installed mode, the command installs the packages from the incompatible switch's running bundle. If, after you reload and boot the incompatible switch in installed mode, the switch's installed packages are found to be incompatible with the stack, you can use the **software auto-upgrade** command again. For more information, see *Cisco IOS Configuration Fundamentals Command Reference, Cisco IOS XE Release 3SE (Catalyst 3850 Switches)*.

To convert a switch that is running in installed mode and joining a stack that is running in bundle mode, follow these steps:

1. Use the **copy** privileged EXEC command to copy the running bundle from one switch in the stack to the other.
2. Configure the **boot system** global configuration command to point to the bundle file.
3. Reload the switch.

After reloading, the incompatible switch boots in bundle mode and joins the stack as a fully functioning member.

This example shows a 2-member switch stack running in bundle mode; switch 2 is the active switch and switch 1 is running in installed mode:

```
SwitchControllerDevice#
SwitchControllerDevice# copy
flash:cat3k_caa-universalk9.SSA.03.12.02.EZP.150-12.02.EZP.150-12.02.EZP.bin flash-1:
Destination filename [cat3k_caa-universalk9.SSA.03.12.02.EZP.150-12.02.EZP.150-12.02.EZP.bin]?
Copy in progress...
....
220766688 bytes copied in 181.700 secs (1215007 bytes/sec)
SwitchControllerDevice#
SwitchControllerDevice# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SwitchControllerDevice(config)# boot system switch 1
flash:cat3k_caa-universalk9.SSA.03.12.02.EZP.150-12.02.EZP.150-12.02.EZP.bin
SwitchControllerDevice(config)# end
SwitchControllerDevice#
*Nov 19 16:08:14.857: %SYS-5-CONFIG_I: Configured from console by console
SwitchControllerDevice# reload slot 1
Stack is in Half ring setup; Reloading a switch might cause stack split
Proceed with reload? [confirm]
```

Additional References

Related Documents

Related Topic	Document Title
Commands for managing software bundles and packages	*Cisco IOS Configuration Fundamentals Command Reference*

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

Standards	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	--

MIBs

MIBs	MIBs Link
No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature.	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

RFCs

RFCs	Title
No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature.	--

Technical Assistance

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

CHAPTER 21

Troubleshooting the Software Configuration

This chapter describes how to identify and resolve software problems related to the Cisco IOS software on the switch. Depending on the nature of the problem, you can use the command-line interface (CLI), Device Manager, or Network Assistant to identify and solve problems.

Additional troubleshooting information, such as LED descriptions, is provided in the hardware installation guide.

Finding Feature Information

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

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

Related Topics

Feature History and Information for Troubleshooting Software Configuration, on page 336

Information About Troubleshooting the Software Configuration

Software Failure on a Switch

Switch software can be corrupted during an upgrade by downloading the incorrect file to the switch, and by deleting the image file. In all of these cases, the switch does not pass the power-on self-test (POST), and there is no connectivity.

Related Topics

Recovering from a Software Failure, on page 315

Lost or Forgotten Password on a Switch

The default configuration for the switch allows an end user with physical access to the switch to recover from a lost password by interrupting the boot process during power-on and by entering a new password. These recovery procedures require that you have physical access to the switch.

Note On these switches, a system administrator can disable some of the functionality of this feature by allowing an end user to reset a password only by agreeing to return to the default configuration. If you are an end user trying to reset a password when password recovery has been disabled, a status message reminds you to return to the default configuration during the recovery process.

Related Topics

Recovering from a Lost or Forgotten Password, on page 317

Power over Ethernet Ports

A Power over Ethernet (PoE) switch port automatically supplies power to one of these connected devices if the switch detects 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 detect the real-time power consumption of the device by monitoring and policing the power usage.

For more information, see the "Configuring PoE" chapter in the *Interface and Hardware Component Configuration Guide (Catalyst 3850 Switches)* .

Related Topics

Scenarios to Troubleshoot Power over Ethernet (PoE), on page 330

Disabled Port Caused by Power Loss

If a powered device (such as a Cisco IP Phone 7910) that is connected to a PoE switch port and powered by an AC power source loses power from the AC power source, the device might enter an error-disabled state. To recover from an error-disabled state, enter the **shutdown** interface configuration command, and then enter the **no shutdown** interface command. You can also configure automatic recovery on the switch to recover from the error-disabled state.

On a switch, the **errdisable recovery cause loopback** and the **errdisable recovery interval** *seconds* global configuration commands automatically take the interface out of the error-disabled state after the specified period of time.

Disabled Port Caused by False Link-Up

If a Cisco powered device is connected to a port and you configure the port by using the **power inline never** interface configuration command, a false link-up can occur, placing the port into an error-disabled state. To take the port out of the error-disabled state, enter the **shutdown** and the **no shutdown** interface configuration commands.

You should not connect a Cisco powered device to a port that has been configured with the **power inline never** command.

Ping

The switch supports IP ping, which you can use to test connectivity to remote hosts. Ping sends an echo request packet to an address and waits for a reply. Ping returns one of these responses:

- Normal response—The normal response (hostname is alive) occurs in 1 to 10 seconds, depending on network traffic.
- Destination does not respond—If the host does not respond, a no-answer message is returned.
- Unknown host—If the host does not exist, an unknown host message is returned.
- Destination unreachable—If the default gateway cannot reach the specified network, a destination-unreachable message is returned.
- Network or host unreachable—If there is no entry in the route table for the host or network, a network or host unreachable message is returned.

Related Topics

Executing Ping, on page 324

Example: Pinging an IP Host, on page 333

Layer 2 Traceroute

The Layer 2 traceroute feature allows the switch to identify the physical path that a packet takes from a source device to a destination device. Layer 2 traceroute supports only unicast source and destination MAC addresses. Traceroute finds the path by using the MAC address tables of the switches in the path. When the switch detects a device in the path that does not support Layer 2 traceroute, the switch continues to send Layer 2 trace queries and lets them time out.

The switch can only identify the path from the source device to the destination device. It cannot identify the path that a packet takes from source host to the source device or from the destination device to the destination host.

Layer 2 Traceroute Guidelines

- Cisco Discovery Protocol (CDP) must be enabled on all the devices in the network. For Layer 2 traceroute to function properly, do not disable CDP.

  If any devices in the physical path are transparent to CDP, the switch cannot identify the path through these devices.

- A switch is reachable from another switch when you can test connectivity by using the **ping** privileged EXEC command. All switches in the physical path must be reachable from each other.
- The maximum number of hops identified in the path is ten.
- You can enter the **traceroute mac** or the **traceroute mac ip** privileged EXEC command on a switch that is not in the physical path from the source device to the destination device. All switches in the path must be reachable from this switch.
- The **traceroute mac** command output shows the Layer 2 path only when the specified source and destination MAC addresses belong to the same VLAN. If you specify source and destination MAC addresses that belong to different VLANs, the Layer 2 path is not identified, and an error message appears.
- If you specify a multicast source or destination MAC address, the path is not identified, and an error message appears.
- If the source or destination MAC address belongs to multiple VLANs, you must specify the VLAN to which both the source and destination MAC addresses belong. If the VLAN is not specified, the path is not identified, and an error message appears.
- The **traceroute mac ip** command output shows the Layer 2 path when the specified source and destination IP addresses belong to the same subnet. When you specify the IP addresses, the switch uses the Address Resolution Protocol (ARP) to associate the IP addresses with the corresponding MAC addresses and the VLAN IDs.
    - If an ARP entry exists for the specified IP address, the switch uses the associated MAC address and identifies the physical path.
    - If an ARP entry does not exist, the switch sends an ARP query and tries to resolve the IP address. If the IP address is not resolved, the path is not identified, and an error message appears.

- When multiple devices are attached to one port through hubs (for example, multiple CDP neighbors are detected on a port), the Layer 2 traceroute feature is not supported. When more than one CDP neighbor is detected on a port, the Layer 2 path is not identified, and an error message appears.
- This feature is not supported in Token Ring VLANs.

IP Traceroute

You can use IP traceroute to identify the path that packets take through the network on a hop-by-hop basis. The command output displays all network layer (Layer 3) devices, such as routers, that the traffic passes through on the way to the destination.

Your switches can participate as the source or destination of the **traceroute** privileged EXEC command and might or might not appear as a hop in the **traceroute** command output. If the switch is the destination of the traceroute, it is displayed as the final destination in the traceroute output. Intermediate switches do not show up in the traceroute output if they are only bridging the packet from one port to another within the same VLAN. However, if the intermediate switch is a multilayer switch that is routing a particular packet, this switch shows up as a hop in the traceroute output.

The **traceroute** privileged EXEC command uses the Time To Live (TTL) field in the IP header to cause routers and servers to generate specific return messages. Traceroute starts by sending a User Datagram Protocol (UDP) datagram to the destination host with the TTL field set to 1. If a router finds a TTL value of 1 or 0, it drops the datagram and sends an Internet Control Message Protocol (ICMP) time-to-live-exceeded message to the sender. Traceroute finds the address of the first hop by examining the source address field of the ICMP time-to-live-exceeded message.

To identify the next hop, traceroute sends a UDP packet with a TTL value of 2. The first router decrements the TTL field by 1 and sends the datagram to the next router. The second router sees a TTL value of 1, discards the datagram, and returns the time-to-live-exceeded message to the source. This process continues until the TTL is incremented to a value large enough for the datagram to reach the destination host (or until the maximum TTL is reached).

To learn when a datagram reaches its destination, traceroute sets the UDP destination port number in the datagram to a very large value that the destination host is unlikely to be using. When a host receives a datagram destined to itself containing a destination port number that is unused locally, it sends an ICMP *port-unreachable* error to the source. Because all errors except port-unreachable errors come from intermediate hops, the receipt of a port-unreachable error means that this message was sent by the destination port.

Related Topics

Executing IP Traceroute, on page 325

Example: Performing a Traceroute to an IP Host, on page 333

Time Domain Reflector Guidelines

You can use the Time Domain Reflector (TDR) feature to diagnose and resolve cabling problems. When running TDR, a local device sends a signal through a cable and compares the reflected signal to the initial signal.

TDR is supported on 10/100/1000 copper Ethernet ports and on Multigigabit Ethernet (100Mbps/1/2.5/5/10 Gbps) ports. It is not supported on SFP module ports.

TDR can detect these cabling problems:

- Open, broken, or cut twisted-pair wires—The wires are not connected to the wires from the remote device.
- Shorted twisted-pair wires—The wires are touching each other or the wires from the remote device. For example, a shorted twisted pair can occur if one wire of the twisted pair is soldered to the other wire.

  If one of the twisted-pair wires is open, TDR can find the length at which the wire is open.

Note When using the feature with Multigigabit Ethernet ports, the cable length is displayed only when an open or short condition is detected.

Use TDR to diagnose and resolve cabling problems in these situations:

- Replacing a Switch
- Setting up a wiring closet
- Troubleshooting a connection between two devices when a link cannot be established or when it is not operating properly

When you run TDR, the Switch reports accurate information in these situations:

- The cable for the gigabit link is a solid-core cable.
- The open-ended cable is not terminated.

When you run TDR, the Switch does not report accurate information in these situations:

- The cable for the gigabit link is a twisted-pair cable or is in series with a solid-core cable.
- The link is a 10-megabit or a 100-megabit link.
- The cable is a stranded cable.
- The link partner is a Cisco IP Phone.
- The link partner is not IEEE 802.3 compliant.

Debug Commands

Caution Because debugging output is assigned high priority in the CPU process, it can render the system unusable. For this reason, use **debug** commands only to troubleshoot specific problems or during troubleshooting sessions with Cisco technical support staff. It is best to use **debug** commands during periods of lower network traffic and fewer users. Debugging during these periods decreases the likelihood that increased **debug** command processing overhead will affect system use.

All **debug** commands are entered in privileged EXEC mode, and most **debug** commands take no arguments.

Related Topics

Redirecting Debug and Error Message Output, on page 326
Example: Enabling All System Diagnostics, on page 334

Crashinfo Files

The crashinfo files save information that helps Cisco technical support representatives to debug problems that caused the Cisco IOS image to fail (crash). The switch generates two files at the time of the failure: full core and crashinfo.

The information in the crashinfo file includes the Cisco IOS image name and version that failed, a list of the processor registers, and a stack trace. You can provide this information to the Cisco technical support representative by using the **show tech-support** privileged EXEC command.

The file names have the following format:

```
[fullcore | crashinfo]_[process that crashed]_[date]-[timestamp]-UTC
```

From IOS, you can view the crashinfo files on each switch by using the following command:

```
SwitchControllerDevice#  dir crashinfo?
crashinfo-1: crashinfo-2: crashinfo-3: crashinfo:
SwitchControllerDevice#
```

For example, to access the crashinfo directory for switch 1, enter

```
SwitchControllerDevice dir crashinfo-1
```

From the ROMMON prompt, you can view the crashinfo files by using the **dir** command:

```
SwitchControllerDevice: dir sda1
```

The following is sample output of a crashinfo file

```
SwitchControllerDevice# dir crashinfo:

Directory of crashinfo:/

   12  -rwx        2768  Dec 31 1969 16:00:15 -08:00  koops.dat
   15  -rwx           0  Jan 12 2000 22:53:40 -08:00  deleted_crash_files
   16  -rwx    4246576  Jan 12 2000 22:53:40 -08:00  crashinfo_stack-mgr_20000113-065250-UTC

   17  -rwx          50   Oct 2 2012 03:18:42 -08:00  last_crashinfo
   26  -rwx          39  Jan 22 2013 14:14:14 -08:00  last_systemreport
   18  -rwx     2866565  Jan 12 2000 22:53:41 -08:00  fullcore_stack-mgr_20000113-065250-UTC

   20  -rwx    4391796   Feb 1 2000 17:50:44 -08:00  crashinfo_stack-mgr_20000202-014954-UTC

   21  -rwx     2920325   Feb 1 2000 17:50:45 -08:00  fullcore_stack-mgr_20000202-014954-UTC
34817  -rw-     1050209  Jan 10 2013 20:26:23 -08:00  system-report_1_20130111-042535-UTC.gz
18434  -rw-     1016913  Jan 11 2013 10:35:28 -08:00  system-report_1_20130111-183440-UTC.gz
18435  -rw-     1136167  Jan 22 2013 14:14:11 -08:00  system-report_1_20130122-221322-UTC.gz
34821  -rw-     1094631   Jan 2 2013 17:59:23 -08:00  system-report_1_20130103-015835-UTC.gz

 6147  -rw-      967429   Jan 3 2013 10:32:44 -08:00  system-report_1_20130103-183156-UTC.gz
34824  -rwx          50  Jan 22 2013 14:14:14 -08:00  deleted_sysreport_files
6155  -rwx         373  Jan 22 2013 14:14:13 -08:00  last_systemreport_log

145898496 bytes total (18569216 bytes free)
stack3#

The file name of the most recent crashinfo file is stored in last_crashinfo.
The file name of the most recent system report is stored in last_systemreport.


SwitchControllerDevice#
```

System Reports

When a switch crashes, a system report is automatically generated for each switch in the switch stack. The system report file captures all the trace buffers, and other system-wide logs found on the switch. System reports are located in the crashinfo directory in the following format:

```
system-report_[switch number]_[date]-[timestamp]-UTC.gz
```

After a switch crash, you should check if a system report file was generated. The name of the most recently generated system report file is stored in the last_systemreport file under the crashinfo directory. The system report and crashinfo files assist TAC when troubleshooting your issue.

Onboard Failure Logging on the Switch

You can use the onboard failure logging (OBFL) feature to collect information about the switch. The information includes uptime, temperature, and voltage information and helps Cisco technical support representatives to troubleshoot switch problems. We recommend that you keep OBFL enabled and do not erase the data stored in the flash memory.

By default, OBFL is enabled. It collects information about the switch and small form-factor pluggable (SFP) modules. The switch stores this information in the flash memory:

- CLI commands—Record of the OBFL CLI commands that are entered on a standalone switch or a switch stack member.
- Environment data—Unique device identifier (UDI) information for a standalone switch or a stack member and for all the connected FRU devices: the product identification (PID), the version identification (VID), and the serial number.
- Message—Record of the hardware-related system messages generated by a standalone switch or a stack member.
- Power over Ethernet (PoE)—Record of the power consumption of PoE ports on a standalone switch or a stack member.
- Temperature—Temperature of a standalone switch or a stack member.
- Uptime data—Time when a standalone switch or a stack member starts, the reason the switch restarts, and the length of time the switch has been running since it last restarted.
- Voltage—System voltages of a standalone switch or a stack member.

You should manually set the system clock or configure it by using Network Time Protocol (NTP).

When the switch is running, you can retrieve the OBFL data by using the **show logging onboard** privileged EXEC commands. If the switch fails, contact your Cisco technical support representative to find out how to retrieve the data.

Related Topics

Configuring OBFL, on page 326

Displaying OBFL Information, on page 327

Fan Failures

By default, the feature is disabled. When more than one of the fans fails in a field-replaceable unit (FRU) or in a power supply, the switch does not shut down, and this error message appears:

```
Multiple fan(FRU/PS) failure detected. System may get overheated. Change fan quickly.
```

The switch might overheat and shut down.

To enable the fan failures feature, enter the **system env fan-fail-action shut** privileged EXEC command. If more than one fan in the switch fails, the switch automatically shuts down, and this error message appears:

```
Faulty (FRU/PS) fans detected, shutting down system!
```

After the first fan shuts down, if the switch detects a second fan failure, the switch waits for 20 seconds before it shuts down.

To restart the switch, it must be power cycled.

Possible Symptoms of High CPU Utilization

Excessive CPU utilization might result in these symptoms, but the symptoms might also result from other causes:

- Spanning tree topology changes
- EtherChannel links brought down due to loss of communication
- Failure to respond to management requests (ICMP ping, SNMP timeouts, slow Telnet or SSH sessions)
- UDLD flapping
- IP SLAs failures because of SLAs responses beyond an acceptable threshold
- DHCP or IEEE 802.1x failures if the switch does not forward or respond to requests

How to Troubleshoot the Software Configuration

Recovering from a Software Failure

Before You Begin

This recovery procedure requires that you have physical access to the switch.

This procedure uses boot loader commands and TFTP to recover from a corrupted or incorrect image file.

Step 1 From your PC, download the software image file (*image.bin*) from Cisco.com.

Step 2 Load the software image to your TFTP server.

Step 3 Connect your PC to the switch Ethernet management port.

Step 4 Unplug the switch power cord.

Step 5 Press the **Mode** button, and at the same time, reconnect the power cord to the switch.

Step 6 From the bootloader (ROMMON) prompt, ensure that you can ping your TFTP server.

a) Set the IP address **switch: set IP_ADDR** *ip_address subnet_mask*

Example:
```
switch: set IP_ADDR 192.0.2.123/255.255.255.0
```

b) Set the default router IP address **switch: set DEFAULT_ROUTER** *ip_address*

Example:
```
switch: set DEFAULT_ROUTER 192.0.2.1
```

c) Verify that you can ping the TFTP server **switch: ping** *ip_address_of_TFTP_server*

Example:
```
switch: ping 192.0.2.15
ping 192.0.2.1 with 32 bytes of data...
Host 192.0.2.1 is alive.
switch:
```

Step 7 Verify that you have a recovery image in your recovery partition (sda9:).
This recovery image is required for recovery using the emergency-install feature.

Example:

```
switch: dir sda9:
Directory of sda9:/

    2  drwx  1024       .
    2  drwx  1024       ..
   11  -rw-  18923068   c3850-recovery.bin

36939776 bytes available (20830208 bytes used)
switch:
```

Step 8 From the bootloader (ROMMON) prompt, initiate the emergency-install feature that assists you in recovering the software image on your switch.
WARNING: The emergency install command will erase your entire boot flash!

Example:
```
Switch#
emergency-install
tftp://192.0.2.47/cat3k_caa-universalk9.SSA.03.12.02.EZP.150-12.02.EZP.150-12.02.EZP.bin

The bootflash will be erased during install operation, continue (y/n)?y
Starting emergency recovery
(tftp://192.0.2.47/cat3k/cat3k_caa-universalk9.SPA.03.02.00.SE.150-1.EX.bin)...
```

```
Reading full image into memory......................done
Nova Bundle Image
--------------------------------------
Kernel Address : 0x6042e5cc
Kernel Size : 0x318261/3244641
Initramfs Address : 0x60746830
Initramfs Size : 0xdb0fb9/14356409
Compression Format: .mzip

Bootable image at @ ram:0x6042e5cc
Bootable image segment 0 address range [0x81100000, 0x81b80000] is in range [0x80180000, 0x90000000].
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
File "sda9:c3850-recovery.bin" uncompressed and installed, entry point: 0x811060f0
Loading Linux kernel with entry point 0x811060f0 ...
Bootloader: Done loading app on core_mask: 0xf

### Launching Linux Kernel (flags = 0x5)



Initiating Emergency Installation of bundle
tftp://192.0.2.47/cat3k/cat3k_caa-universalk9.SSA.03.12.02.EZP.150-12.02.EZP.150-12.02.EZP.bin


Downloading bundle
tftp://192.0.2.47/cat3k/cat3k_caa-universalk9.SSA.03.12.02.EZP.150-12.02.EZP.150-12.02.EZP.bin...
Validating bundle
tftp://192.0.2.47/cat3k/cat3k_caa-universalk9.SSA.03.12.02.EZP.150-12.02.EZP.150-12.02.EZP.bin...
Installing bundle
tftp://192.0.2.47/cat3k/cat3k_caa-universalk9.SSA.03.12.02.EZP.150-12.02.EZP.150-12.02.EZP.bin...
Verifying bundle
tftp://192.0.2.47/cat3k/cat3k_caa-universalk9.SSA.03.12.02.EZP.150-12.02.EZP.150-12.02.EZP.bin...
Package cat3k_caa-base..pkg is Digitally Signed
Package cat3k_caa-drivers.SPA.03.02.00.SE.pkg is Digitally Signed
Package cat3k_caa-infra.SPA.03.02.00.SE.pkg is Digitally Signed
Package cat3k_caa-iosd-universalk9.SPA.03.02.00.SE.pkg is Digitally Signed
Package cat3k_caa-platform.SPA.03.02.00.SE.pkg is Digitally Signed
Package cat3k_caa-wcm.SPA.03.02.00.SE.pkg is Digitally Signed
Preparing flash...
Syncing device...
Emergency Install successful... Rebooting
Restarting system.


Booting...(use DDR clock 667 MHz)Initializing and Testing RAM +++@@@@####...++@@++@@++@@++@
```

Related Topics

Software Failure on a Switch, on page 308

Recovering from a Lost or Forgotten Password

The default configuration for the switch allows an end user with physical access to the switch to recover from a lost password by interrupting the boot process during power-on and by entering a new password. These recovery procedures require that you have physical access to the switch.

Note On these switches, a system administrator can disable some of the functionality of this feature by allowing an end user to reset a password only by agreeing to return to the default configuration. If you are an end user trying to reset a password when password recovery has been disabled, a status message shows this during the recovery process.

SUMMARY STEPS

1. Connect a terminal or PC to the switch.
2. Set the line speed on the emulation software to 9600 baud.
3. Power off the standalone switch or the entire switch stack.
4. Reconnect the power cord to the or the active switch. Within 15 seconds, press the **Mode** button while the System LED is still flashing green. Continue pressing the **Mode** button until all the system LEDs turn on and remain solid; then release the **Mode** button.
5. After recovering the password, reload the switch or the active switch .
6. Power on the remaining switches in the stack.

DETAILED STEPS

Step 1 Connect a terminal or PC to the switch.

- Connect a terminal or a PC with terminal-emulation software to the switch console port. If you are recovering the password for a switch stack, connect to the console port of the active switch or
- Connect a PC to the Ethernet management port. If you are recovering the password for a switch stack, connect to the Ethernet management port of a stack member .

Step 2 Set the line speed on the emulation software to 9600 baud.

Step 3 Power off the standalone switch or the entire switch stack.

Step 4 Reconnect the power cord to the or the active switch. Within 15 seconds, press the **Mode** button while the System LED is still flashing green. Continue pressing the **Mode** button until all the system LEDs turn on and remain solid; then release the **Mode** button.

-

```
Switch:
Xmodem file system is available.
Base ethernet MAC Address: 20:37:06:4d:e9:80
Verifying bootloader digital signature.


The system has been interrupted prior to loading the operating
system software, console will be reset to 9600 baud rate.
```

proceed to the *Procedure with Password Recovery Enabled* section, and follow the steps.

Step 5 After recovering the password, reload the switch or the active switch .

On a switch:

```
Switch> reload
Proceed with reload? [confirm] y
```

On the active switch:

```
Switch> reload slot <stack-active-member-number>
Proceed with reload? [confirm] y
```

Step 6 Power on the remaining switches in the stack.

Related Topics

Lost or Forgotten Password on a Switch, on page 308

Procedure with Password Recovery Enabled

If the password-recovery operation is enabled, this message appears:

Step 1 Initialize the flash file system.

```
SwitchControllerDevice: flash_init
```

Step 2 Ignore the startup configuration with the following command:

```
SwitchControllerDevice: SWITCH_IGNORE_STARTUP_CFG=1
```

Step 3 Boot the switch with the *packages.conf* file from flash.

```
SwitchControllerDevice: boot flash:packages.conf
```

Step 4 Terminate the initial configuration dialog by answering **No**.

```
Would you like to enter the initial configuration dialog? [yes/no]: No
```

Step 5 At the switch prompt, enter privileged EXEC mode.

```
SwitchControllerDevice> enable
Switch#
```

Step 6 Copy the startup configuration to running configuration.

```
SwitchControllerDevice# copy startup-config running-config Destination filename [running-config]?
```

Press Return in response to the confirmation prompts. The configuration file is now reloaded, and you can change the password.

Step 7 Enter global configuration mode and change the **enable** password.

```
SwitchControllerDevice# configure terminal
SwitchControllerDevice(config)#
```

Step 8 Write the running configuration to the startup configuration file.

```
SwitchControllerDevice# copy running-config startup-config
```

Step 9 Confirm that manual boot mode is enabled.

```
SwitchControllerDevice# show boot

 BOOT variable = flash:packages.conf;
 Manual Boot = yes
 Enable Break = yes
```

Step 10 Reload the switch.

```
SwitchControllerDevice# reload
```

Step 11 Return the Bootloader parameters (previously changed in Steps 2 and 3) to their original values.

```
SwitchControllerDevice: switch: SWITCH_IGNORE_STARTUP_CFG=0
```

Step 12 Boot the switch with the *packages.conf* file from flash.

```
SwitchControllerDevice: boot flash:packages.conf
```

Step 13 After the switch boots up, disable manual boot on the switch.

```
SwitchControllerDevice(config)# no boot manual
```

Procedure with Password Recovery Disabled

If the password-recovery mechanism is disabled, this message appears:

```
The password-recovery mechanism has been triggered, but
is currently disabled.  Access to the boot loader prompt
through the password-recovery mechanism is disallowed at
this point.  However, if you agree to let the system be
reset back to the default system configuration, access
```

```
to the boot loader prompt can still be allowed.
Would you like to reset the system back to the default configuration (y/n)?
```

Caution Returning the switch to the default configuration results in the loss of all existing configurations. We recommend that you contact your system administrator to verify if there are backup switch and VLAN configuration files.

- If you enter **n** (no), the normal boot process continues as if the **Mode** button had not been pressed; you cannot access the boot loader prompt, and you cannot enter a new password. You see the message:

  ```
  Press Enter to continue........
  ```

- If you enter **y** (yes), the configuration file in flash memory and the VLAN database file are deleted. When the default configuration loads, you can reset the password.

Step 1 Choose to continue with password recovery and delete the existing configuration:

```
Would you like to reset the system back to the default configuration (y/n)? Y
```

Step 2 Display the contents of flash memory:

```
SwitchControllerDevice: dir flash:
```

The switch file system appears.

```
Directory of flash:/
.
.
.i'
15494  drwx        4096   Jan 1 2000 00:20:20 +00:00  kirch
15508  -rw-   258065648   Sep 4 2013 14:19:03 +00:00
cat3k_caa-universalk9.SSA.03.12.02.EZP.150-12.02.EZP.150-12.02.EZP.bin
162196684
```

Step 3 Boot up the system:

```
SwitchControllerDevice: boot
```

You are prompted to start the setup program. To continue with password recovery, enter **N** at the prompt:

```
Continue with the configuration dialog? [yes/no]: N
```

Step 4 At the switch prompt, enter privileged EXEC mode:

```
SwitchControllerDevice> enable
```

Step 5 Enter global configuration mode:

```
SwitchControllerDevice# configure terminal
```

Step 6 Change the password:

```
SwitchControllerDevice(config)# enable secret password
```

The secret password can be from 1 to 25 alphanumeric characters, can start with a number, is case sensitive, and allows spaces but ignores leading spaces.

Step 7 Return to privileged EXEC mode:

```
SwitchControllerDevice(config)# exit
SwitchControllerDevice#
```

Note Before continuing to Step 9, power on any connected stack members and wait until they have completely initialized.

Step 8 Write the running configuration to the startup configuration file:

```
SwitchControllerDevice# copy running-config startup-config
```

The new password is now in the startup configuration.

Step 9 You must now reconfigure the switch. If the system administrator has the backup switch and VLAN configuration files available, you should use those.

Preventing Switch Stack Problems

To prevent switch stack problems, you should do the following:

- Make sure that the switches that you add to or remove from the switch stack are powered off. For all powering considerations in switch stacks, see the "Switch Installation" chapter in the hardware installation guide.
- Press the **Mode** button on a stack member until the Stack mode LED is on. The last two port LEDs on the switch should be green. Depending on the switch model, the last two ports are either 10/100/1000 ports or small form-factor pluggable (SFP) module. If one or both of the last two port LEDs are not green, the stack is not operating at full bandwidth.
- We recommend using only one CLI session when managing the switch stack. Be careful when using multiple CLI sessions to the active switch . Commands that you enter in one session are not displayed in the other sessions. Therefore, it is possible that you might not be able to identify the session from which you entered a command.
- Manually assigning stack member numbers according to the placement of the switches in the stack can make it easier to remotely troubleshoot the switch stack. However, you need to remember that the switches have manually assigned numbers if you add, remove, or rearrange switches later. Use the **switch** *current-stack-member-number* **renumber** *new-stack-member-number* global configuration command to manually assign a stack member number.

If you replace a stack member with an identical model, the new switch functions with the exact same configuration as the replaced switch. This is also assuming the new switch is using the same member number as the replaced switch.

Removing powered-on stack members causes the switch stack to divide (partition) into two or more switch stacks, each with the same configuration. If you want the switch stacks to remain separate, change the IP address or addresses of the newly created switch stacks. To recover from a partitioned switch stack, follow these steps:

1. Power off the newly created switch stacks.
2. Reconnect them to the original switch stack through their StackWise Plus ports.
3. Power on the switches.

Preventing Autonegotiation Mismatches

The IEEE 802.3ab autonegotiation protocol manages the switch settings for speed (10 Mb/s, 100 Mb/s, and 1000 Mb/s, excluding SFP module ports) and duplex (half or full). There are situations when this protocol can incorrectly align these settings, reducing performance. A mismatch occurs under these circumstances:

- A manually set speed or duplex parameter is different from the manually set speed or duplex parameter on the connected port.
- A port is set to autonegotiate, and the connected port is set to full duplex with no autonegotiation.

To maximize switch performance and ensure a link, follow one of these guidelines when changing the settings for duplex and speed:

- Let both ports autonegotiate both speed and duplex.
- Manually set the speed and duplex parameters for the ports on both ends of the connection.

Note If a remote device does not autonegotiate, configure the duplex settings on the two ports to match. The speed parameter can adjust itself even if the connected port does not autonegotiate.

Troubleshooting SFP Module Security and Identification

Cisco small form-factor pluggable (SFP) modules have a serial EEPROM that contains the module serial number, the vendor name and ID, a unique security code, and cyclic redundancy check (CRC). When an SFP module is inserted in the switch, the switch software reads the EEPROM to verify the serial number, vendor name and vendor ID, and recompute the security code and CRC. If the serial number, the vendor name or vendor ID, the security code, or CRC is invalid, the software generates a security error message and places the interface in an error-disabled state.

Note The security error message references the GBIC_SECURITY facility. The switch supports SFP modules and does not support GBIC modules. Although the error message text refers to GBIC interfaces and modules, the security messages actually refer to the SFP modules and module interfaces.

If you are using a non-Cisco SFP module, remove the SFP module from the switch, and replace it with a Cisco module. After inserting a Cisco SFP module, use the **errdisable recovery cause gbic-invalid** global configuration command to verify the port status, and enter a time interval for recovering from the error-disabled state. After the elapsed interval, the switch brings the interface out of the error-disabled state and retries the operation.

If the module is identified as a Cisco SFP module, but the system is unable to read vendor-data information to verify its accuracy, an SFP module error message is generated. In this case, you should remove and reinsert the SFP module. If it continues to fail, the SFP module might be defective.

Monitoring SFP Module Status

You can check the physical or operational status of an SFP module by using the **show interfaces transceiver** privileged EXEC command. This command shows the operational status, such as the temperature and the current for an SFP module on a specific interface and the alarm status. You can also use the command to check the speed and the duplex settings on an SFP module.

Executing Ping

If you attempt to ping a host in a different IP subnetwork, you must define a static route to the network or have IP routing configured to route between those subnets.

IP routing is disabled by default on all switches.

Note Though other protocol keywords are available with the **ping** command, they are not supported in this release.

Use this command to ping another device on the network from the switch:

Command	Purpose
ping ip *host* | *address* `SwitchControllerDevice# ping 172.20.52.3`	Pings a remote host through IP or by supplying the hostname or network address.

Related Topics

Ping, on page 309
Example: Pinging an IP Host, on page 333

Monitoring Temperature

The switch monitors the temperature conditions and uses the temperature information to control the fans.

Use the **show env temperature status** privileged EXEC command to display the temperature value, state, and thresholds. The temperature value is the temperature in the switch (not the external temperature).You can configure only the yellow threshold level (in Celsius) by using the **system env temperature threshold yellow** *value* global configuration command to set the difference between the yellow and red thresholds. You cannot configure the green or red thresholds.

Monitoring the Physical Path

You can monitor the physical path that a packet takes from a source device to a destination device.

Table 31: Monitoring the Physical Path

Command	Purpose
tracetroute mac [**interface** *interface-id*] {*source-mac-address*} [**interface** *interface-id*] {*destination-mac-address*} [**vlan** *vlan-id*] [**detail**]	Displays the Layer 2 path taken by the packets from the specified source MAC address to the specified destination MAC address.
tracetroute mac ip {*source-ip-address* | *source-hostname*}{*destination-ip-address* | *destination-hostname*} [**detail**]	Displays the Layer 2 path taken by the packets from the specified source IP address or hostname to the specified destination IP address or hostname.

Executing IP Traceroute

Note Though other protocol keywords are available with the **traceroute** privileged EXEC command, they are not supported in this release.

Command	Purpose
traceroute ip *host* `SwitchControllerDevice# traceroute ip 192.51.100.1`	Traces the path that packets take through the network.

Related Topics

IP Traceroute , on page 311
Example: Performing a Traceroute to an IP Host, on page 333

Running TDR and Displaying the Results

When you run TDR on an interface, you can run it on the active switch or a stack member.

To run TDR, enter the **test cable-diagnostics tdr interface** *interface-id* privileged EXEC command.

To display the results, enter the **show cable-diagnostics tdr interface** *interface-id* privileged EXEC command.

Redirecting Debug and Error Message Output

By default, the network server sends the output from **debug** commands and system error messages to the console. If you use this default, you can use a virtual terminal connection to monitor debug output instead of connecting to the console port or the Ethernet management port.

Possible destinations include the console, virtual terminals, internal buffer, and UNIX hosts running a syslog server. The syslog format is compatible with 4.3 Berkeley Standard Distribution (BSD) UNIX and its derivatives.

Note Be aware that the debugging destination you use affects system overhead. When you log messages to the console, very high overhead occurs. When you log messages to a virtual terminal, less overhead occurs. Logging messages to a syslog server produces even less, and logging to an internal buffer produces the least overhead of any method.

Related Topics

Debug Commands, on page 312

Using the show platform forward Command

The output from the **show platform forward** privileged EXEC command provides some useful information about the forwarding results if a packet entering an interface is sent through the system. Depending upon the parameters entered about the packet, the output provides lookup table results and port maps used to calculate forwarding destinations, bitmaps, and egress information.

Most of the information in the output from the command is useful mainly for technical support personnel, who have access to detailed information about the switch application-specific integrated circuits (ASICs). However, packet forwarding information can also be helpful in troubleshooting.

Configuring OBFL

Caution We recommend that you do not disable OBFL and that you do not remove the data stored in the flash memory.

- To enable OBFL, use the **hw-switch switch** [*switch-number*] **logging onboard** [**message level** *level*] global configuration command. On switches, the range for *switch-number* is from 1 to 9. Use the **message level** *level* parameter to specify the severity of the hardware-related messages that the switch generates and stores in the flash memory.
- To copy the OBFL data to the local network or a specific file system, use the **copy onboard switch** *switch-number* **url** *url-destination* privileged EXEC command.
- To disable OBFL, use the **no hw-switch switch** [*switch-number*] **logging onboard** [**message level**] global configuration command.
- To clear all the OBFL data in the flash memory except for the uptime and CLI command information, use the **clear onboard switch** *switch-number* privileged EXEC command.
- In a switch stack, you can enable OBFL on a standalone switch or on all stack members by using the **hw-switch switch** [*switch-number*] **logging onboard** [**message level** *level*] global configuration command.
- You can enable or disable OBFL on a member switch from the active switch.

Related Topics

Onboard Failure Logging on the Switch, on page 314
Displaying OBFL Information, on page 327

Verifying Troubleshooting of the Software Configuration

Displaying OBFL Information

Table 32: Commands for Displaying OBFL Information

Command	Purpose
show onboard switch *switch-number* **clilog** `SwitchControllerDevice# show onboard switch 1 clilog`	Displays the OBFL CLI commands that were entered on a standalone switch or the specified stack members.
show onboard switch *switch-number* **environment** `SwitchControllerDevice# show onboard switch 1 environment`	Displays the UDI information for a standalone switch or the specified stack members and for all the connected FRU devices: the PID, the VID, and the serial number.
show onboard switch *switch-number* **message** `SwitchControllerDevice# show onboard switch 1 message`	Displays the hardware-related messages generated by a standalone switch or the specified stack members.
show onboard switch *switch-number* **counter** `SwitchControllerDevice# show onboard switch 1 counter`	Displays the counter information on a standalone switch or the specified stack members.

Command	Purpose
show onboard switch *switch-number* **temperature** `SwitchControllerDevice# show onboard switch 1 temperature`	Displays the temperature of a standalone switch or the specified switch stack members.
show onboard switch *switch-number* **uptime** `SwitchControllerDevice# show onboard switch 1 uptime`	Displays the time when a standalone switch or the specified stack members start, the reason the standalone switch or specified stack members restart, and the length of time that the standalone switch or specified stack members have been running since they last restarted.
show onboard switch *switch-number* **voltage** `SwitchControllerDevice# show onboard switch 1 voltage`	Displays the system voltages of a standalone switch or the specified stack members.
show onboard switch *switch-number* **status** `SwitchControllerDevice# show onboard switch 1 status`	Displays the status of a standalone switch or the specified stack members.

Related Topics

Onboard Failure Logging on the Switch, on page 314
Configuring OBFL, on page 326

Example: Verifying the Problem and Cause for High CPU Utilization

To determine if high CPU utilization is a problem, enter the **show processes cpu sorted** privileged EXEC command. Note the underlined information in the first line of the output example.

```
SwitchControllerDevice# show processes cpu sorted
CPU utilization for five seconds: 8%/0%; one minute: 7%; five minutes: 8%
PID Runtime(ms) Invoked uSecs 5Sec 1Min 5Min TTY Process
309 42289103 752750 56180 1.75% 1.20% 1.22% 0 RIP Timers
140 8820183 4942081 1784 0.63% 0.37% 0.30% 0 HRPC qos request
100 3427318 16150534 212 0.47% 0.14% 0.11% 0 HRPC pm-counters
192 3093252 14081112 219 0.31% 0.14% 0.11% 0 Spanning Tree
143 8 37 216 0.15% 0.01% 0.00% 0 Exec
...
<output truncated>
```

This example shows normal CPU utilization. The output shows that utilization for the last 5 seconds is 8%/0%, which has this meaning:

- The total CPU utilization is 8 percent, including both time running Cisco IOS processes and time spent handling interrupts.
- The time spent handling interrupts is zero percent.

Table 33: Troubleshooting CPU Utilization Problems

Type of Problem	Cause	Corrective Action
Interrupt percentage value is almost as high as total CPU utilization value.	The CPU is receiving too many packets from the network.	Determine the source of the network packet. Stop the flow, or change the switch configuration. See the section on “Analyzing Network Traffic.”
Total CPU utilization is greater than 50% with minimal time spent on interrupts.	One or more Cisco IOS process is consuming too much CPU time. This is usually triggered by an event that activated the process.	Identify the unusual event, and troubleshoot the root cause. See the section on “Debugging Active Processes.”

Scenarios for Troubleshooting the Software Configuration

Scenarios to Troubleshoot Power over Ethernet (PoE)

Table 34: Power over Ethernet Troubleshooting Scenarios

Symptom or Problem	Possible Cause and Solution
Only one port does not have PoE. Trouble is on only one switch port. PoE and non-PoE devices do not work on this port, but do on other ports.	Verify that the powered device works on another PoE port. Use the **show run**, or **show interface status** user EXEC commands to verify that the port is not shut down or error-disabled. **Note** Most switches turn off port power when the port is shut down, even though the IEEE specifications make this optional. Verify that the Ethernet cable from the powered device to the switch port is good: Connect a known good non-PoE Ethernet device to the Ethernet cable, and make sure that the powered device establishes a link and exchanges traffic with another host. Verify that the total cable length from the switch front panel to the powered device is not more than 100 meters. Disconnect the Ethernet cable from the switch port. Use a short Ethernet cable to connect a known good Ethernet device directly to this port on the switch front panel (not on a patch panel). Verify that it can establish an Ethernet link and exchange traffic with another host, or ping the port VLAN SVI. Next, connect a powered device to this port, and verify that it powers on. If a powered device does not power on when connected with a patch cord to the switch port, compare the total number of connected powered devices to the switch power budget (available PoE). Use the **show inline power** command to verify the amount of available power.

Symptom or Problem	Possible Cause and Solution
No PoE on all ports or a group of ports. Trouble is on all switch ports. Nonpowered Ethernet devices cannot establish an Ethernet link on any port, and PoE devices do not power on.	If there is a continuous, intermittent, or reoccurring alarm related to power, replace the power supply if possible it is a field-replaceable unit. Otherwise, replace the switch. If the problem is on a consecutive group of ports but not all ports, the power supply is probably not defective, and the problem could be related to PoE regulators in the switch. Use the **show log** privileged EXEC command to review alarms or system messages that previously reported PoE conditions or status changes. If there are no alarms, use the **show interface status** command to verify that the ports are not shut down or error-disabled. If ports are error-disabled, use the **shut** and **no shut** interface configuration commands to reenable the ports. Use the **show env power** and **show power inline** privileged EXEC commands to review the PoE status and power budget (available PoE). Review the running configuration to verify that **power inline never** is not configured on the ports. Connect a nonpowered Ethernet device directly to a switch port. Use only a short patch cord. Do not use the existing distribution cables. Enter the **shut** and **no shut** interface configuration commands, and verify that an Ethernet link is established. If this connection is good, use a short patch cord to connect a powered device to this port and verify that it powers on. If the device powers on, verify that all intermediate patch panels are correctly connected. Disconnect all but one of the Ethernet cables from switch ports. Using a short patch cord, connect a powered device to only one PoE port. Verify the powered device does not require more power than can be delivered by the switch port. Use the **show power inline** privileged EXEC command to verify that the powered device can receive power when the port is not shut down. Alternatively, watch the powered device to verify that it powers on. If a powered device can power on when only one powered device is connected to the switch, enter the **shut** and **no shut** interface configuration commands on the remaining ports, and then reconnect the Ethernet cables one at a time to the switch PoE ports. Use the **show interface status** and **show power inline** privileged EXEC commands to monitor inline power statistics and port status. If there is still no PoE at any port, a fuse might be open in the PoE section of the power supply. This normally produces an alarm. Check the log again for alarms reported earlier by system messages.

Symptom or Problem	Possible Cause and Solution
Cisco IP Phone disconnects or resets. After working normally, a Cisco phone or wireless access point intermittently reloads or disconnects from PoE.	Verify all electrical connections from the switch to the powered device. Any unreliable connection results in power interruptions and irregular powered device functioning such as erratic powered device disconnects and reloads. Verify that the cable length is not more than 100 meters from the switch port to the powered device. Notice what changes in the electrical environment at the switch location or what happens at the powered device when the disconnect occurs. Notice whether any error messages appear at the same time a disconnect occurs. Use the **show log** privileged EXEC command to review error messages. Verify that an IP phone is not losing access to the Call Manager immediately before the reload occurs. (It might be a network problem and not a PoE problem.) Replace the powered device with a non-PoE device, and verify that the device works correctly. If a non-PoE device has link problems or a high error rate, the problem might be an unreliable cable connection between the switch port and the powered device.
Non-Cisco powered device does not work on Cisco PoE switch. A non-Cisco powered device is connected to a Cisco PoE switch, but never powers on or powers on and then quickly powers off. Non-PoE devices work normally.	Use the **show power inline** command to verify that the switch power budget (available PoE) is not depleted before or after the powered device is connected. Verify that sufficient power is available for the powered device type before you connect it. Use the **show interface status** command to verify that the switch detects the connected powered device. Use the **show log** command to review system messages that reported an overcurrent condition on the port. Identify the symptom precisely: Does the powered device initially power on, but then disconnect? If so, the problem might be an initial surge-in (or *inrush*) current that exceeds a current-limit threshold for the port.

Related Topics

Power over Ethernet Ports, on page 308

Configuration Examples for Troubleshooting Software

Example: Pinging an IP Host

This example shows how to ping an IP host:

```
SwitchControllerDevice# ping 172.20.52.3

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echoes to 172.20.52.3, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
SwitchControllerDevice#
```

Table 35: Ping Output Display Characters

Character	Description
!	Each exclamation point means receipt of a reply.
.	Each period means the network server timed out while waiting for a reply.
U	A destination unreachable error PDU was received.
C	A congestion experienced packet was received.
I	User interrupted test.
?	Unknown packet type.
&	Packet lifetime exceeded.

To end a ping session, enter the escape sequence (**Ctrl-^ X** by default). Simultaneously press and release the **Ctrl**, **Shift**, and **6** keys and then press the **X** key.

Related Topics

Ping, on page 309
Executing Ping, on page 324

Example: Performing a Traceroute to an IP Host

This example shows how to perform a **traceroute** to an IP host:

```
SwitchControllerDevice# traceroute ip 192.0.2.10

Type escape sequence to abort.
Tracing the route to 192.0.2.10
```

```
1 192.0.2.1 0 msec 0 msec 4 msec
2 192.0.2.203 12 msec 8 msec 0 msec
3 192.0.2.100 4 msec 0 msec 0 msec
4 192.0.2.10 0 msec 4 msec 0 msec
```

The display shows the hop count, the IP address of the router, and the round-trip time in milliseconds for each of the three probes that are sent.

Table 36: Traceroute Output Display Characters

Character	Description
*	The probe timed out.
?	Unknown packet type.
A	Administratively unreachable. Usually, this output means that an access list is blocking traffic.
H	Host unreachable.
N	Network unreachable.
P	Protocol unreachable.
Q	Source quench.
U	Port unreachable.

To end a trace in progress, enter the escape sequence (**Ctrl-^ X** by default). Simultaneously press and release the **Ctrl**, **Shift**, and **6** keys and then press the **X** key.

Related Topics

IP Traceroute , on page 311
Executing IP Traceroute, on page 325

Example: Enabling All System Diagnostics

Caution Because debugging output takes priority over other network traffic, and because the **debug all** privileged EXEC command generates more output than any other **debug** command, it can severely diminish switch performance or even render it unusable. In virtually all cases, it is best to use more specific **debug** commands.

This command disables all-system diagnostics:

```
SwitchControllerDevice# debug all
```

The **no debug all** privileged EXEC command disables all diagnostic output. Using the **no debug all** command is a convenient way to ensure that you have not accidentally left any **debug** commands enabled.

Related Topics

Debug Commands, on page 312

Additional References for Troubleshooting Software Configuration

Related Documents

Related Topic	Document Title
System management commands	*System Management Command Reference (Catalyst 3850 Switches)*
Platform-independent command reference	*Configuration Fundamentals Command Reference, Cisco IOS XE Release 3S (Catalyst 3850 Switches)*
Platform_independent configuration information	*Configuration Fundamentals Configuration Guide, Cisco IOS XE Release 3S (Catalyst 3850 Switches)*

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

Feature History and Information for Troubleshooting Software Configuration

Release	Modification
Cisco IOS XE 3.2SE	This feature was introduced.

Related Topics

Finding Feature Information, on page 21

INDEX

D

E

F

G

H

I

L

M

N

O