# Overview

This document describes the Cisco IOS command-line interface, the Cisco IOS Configuration Engine, and how to work with the Cisco IOS file system, configuration files, and software images. This document also describes how to identify and resolve software problems related to the Cisco IOS software on the Cisco Industrial Ethernet 2000U Series Switches, hereafter referred to as IE 2000U or switch.

## Features

This chapter provides a summary of the following features:


- Cisco IOS Command Line Interface, page 1-1
- Cisco IOS Configuration Engine, page 1-1
- Cisco IOS File System, Configuration Files, and Software Images, page 1-2
- Troubleshooting, page 1-2


## Cisco IOS Command Line Interface

The Cisco IOS command-line interface (CLI) is the primary user interface used for configuring, monitoring, and maintaining Cisco devices. This user interface allows you to directly and simply execute Cisco IOS commands, whether using a switch console or terminal, or using remote access methods.

Basic features of the Cisco IOS CLI include Cisco IOS command modes, navigation and editing features, help features, and command history features.

#### Related Topics

Chapter 2, “Using the Command-Line Interface”

## Cisco IOS Configuration Engine

The Cisco Configuration Engine is network management software that acts as a configuration service for automating the deployment and management of network devices and services. Each Configuration Engine manages a group of Cisco devices (switches and routers) and the services that they deliver, storing their configurations and delivering them as needed. The Configuration Engine automates initial configurations and configuration updates by generating device-specific configuration changes, sending them to the device, executing the configuration change, and logging the results.

The Configuration Engine supports standalone and server modes and has these Cisco Networking Services (CNS) components:

- Configuration service (web server, file manager, and namespace mapping server)
- Event service (event gateway)
- Data service directory (data models and schema)

#### Related Topics

Chapter 3, "Configuring Cisco IOS Configuration Engine"

## Cisco IOS File System, Configuration Files, and Software Images

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 image and configuration files. The default flash file system on the switch is named *flash:*.

Configuration files contain commands entered to customize the function of the Cisco IOS software. You can create a basic configuration file by using the setup program or by entering the **setup** privileged EXEC command. You can copy (*download*) configuration files from a TFTP, FTP, or RCP server to the running configuration or startup configuration of the switch. For example, you might want to restore a backed-up configuration file or download the same configuration file to several switches that have the same hardware configuration.You can copy (*upload*) configuration files from the switch to a file server by using TFTP, FTP, or RCP. You might perform this task to back up a current configuration file to a server before changing its contents so that you can later restore the original configuration file from the server.

Software image files contain the system software, the Cisco IOS code, and the embedded device manager software. You can download a switch image file from a TFTP, FTP, or RCP server to upgrade the switch software. You can replace the current image with the new one or keep the current image in flash memory after a download. You upload a switch image file to a TFTP, FTP, or RCP server for backup purposes. You can use this uploaded image for future downloads to the same switch or to another of the same type.

#### Related Topics

Chapter 4, "Working with the Cisco IOS File System, Configuration Files, and Software Images"

## Troubleshooting

You can use the command-line interface (CLI) to identify and solve the following problems related to the Cisco IOS software on the Cisco IE 2000U switch:

- Software failure due to a corrupted or incorrect image file
- Lost or forgotten password
- Autonegotiation mismatches
- Disabled Power over Ethernet (PoE) ports
- Small form-factor pluggable (SFP) module security and identification errors
- Power supply temperature problems
- Connectivity problems
- Cabling problems

Debugging, crashinfo, and on-board-failure logging (OBFL) features enable you to collect information about the switch that helps Cisco technical support representatives to troubleshoot switch problems.

### Related Topics

Chapter 5, “Troubleshooting”

# Using the Command-Line Interface

This chapter describes the Cisco IOS command-line interface (CLI) and how to use it to configure your Cisco Industrial Ethernet 2000U Series Switches, hereafter referred to as IE 2000U or switch.


- Information About Command Modes, page 2-1
- Information About the Help System, page 2-3
- Information About Abbreviated Commands, page 2-4
- Information About no and default Forms of Commands, page 2-4
- Information About CLI Error Messages, page 2-4
- Using Command History, page 2-5
- Using Editing Features, page 2-6
- Searching and Filtering Output of show and more Commands, page 2-9
- Accessing the CLI, page 2-9
- Related Documents, page 2-10


## Information About Command Modes

The Cisco IOS user interface is divided into many different modes. The commands available to configure the system vary by operating mode. Enter a question mark (?) at the system prompt to obtain a list of commands available for each command mode.

When you start a session on the switch, 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. When you save the configuration, the switch stores these commands for use after a reboot. 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.

Table 2-1 describes the main command modes, how to access each one, the prompt you see in that mode, and how to exit the mode. The examples in the table use the hostname *Switch*.

*Table 2-1 Command Mode Summary*

| Mode | Access Method | Prompt | Exit Method | About This Mode |
|---|---|---|---|---|
| User EXEC | Begin a session with your switch. | `Switch>` | Enter **logout** or **quit**. | Use this mode to<br>• Change terminal settings.<br>• Perform basic tests.<br>• Display system information. |
| Privileged EXEC | While in user EXEC mode, enter the **enable** command. | `Switch#` | Enter **disable** to exit. | Use this mode to verify commands that you have entered. Use a password to protect access to this mode. |
| Global configuration | While in privileged EXEC mode, enter the **configure** command. | `Switch(config)#` | To exit to privileged EXEC mode, enter **exit** or **end**, or press **Ctrl-Z**. | Use this mode to configure parameters that apply to the entire switch. |
| VLAN configuration | While in global configuration mode, enter the **vlan** *vlan-id* command. | `Switch(config-vlan)#` | To exit to global configuration mode, enter the **exit** command.<br>To return to privileged EXEC mode, press **Ctrl-Z** or enter **end**. | Use this mode to configure VLAN parameters. |

*Table 2-1 Command Mode Summary (continued)*

| Mode | Access Method | Prompt | Exit Method | About This Mode |
|---|---|---|---|---|
| Interface configuration | While in global configuration mode, enter the **interface** command (with a specific interface). | `Switch(config-if)#` | To exit to global configuration mode, enter **exit**.<br>To return to privileged EXEC mode, press **Ctrl-Z** or enter **end**. | Use this mode to configure parameters for the Ethernet ports.<br>For information about defining interfaces, see the "Using Interface Configuration Mode" section in the *Cisco Connected Grid Switches Interfaces Software Configuration Guide*.<br>To configure multiple interfaces with the same parameters, see the "Configuring a Range of Interfaces" section in the *Cisco Connected Grid Switches Interfaces Software Configuration Guide*. |
| Line configuration | While in global configuration mode, specify a line with the **line vty** or **line console** command. | `Switch(config-line)#` | To exit to global configuration mode, enter **exit**.<br>To return to privileged EXEC mode, press **Ctrl-Z** or enter **end**. | Use this mode to configure parameters for the terminal line. |

# Information About 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, as shown in Table 2-2.

*Table 2-2 Help Summary*

| Command | Purpose |
|---|---|
| **help** | Obtain a brief description of the help system in any command mode. |
| *abbreviated-command-entry*<**?**> | Obtain a list of commands that begin with a particular character string.<br>For example:<br>`Switch# di?`<br>`dir disable disconnect` |
| *abbreviated-command-entry*<**Tab**> | Complete a partial command name.<br>For example:<br>`Switch# sh conf<tab>`<br>`Switch# show configuration` |

*Table 2-2 Help Summary (continued)*

| Command | Purpose |
|---|---|
| **?** | List all commands available for a particular command mode.<br>For example:<br>`Switch> ?` |
| *command* **?** | List the associated keywords for a command.<br>For example:<br>`Switch> show ?` |
| *command keyword* **?** | List the associated arguments for a keyword.<br>For example:<br>`Switch(config)# cdp holdtime ?`<br>`  <10-255> Length of time (in sec) that receiver must keep this packet` |

# Information About Abbreviated Commands

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

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

```
Switch# show conf
```

# Information About 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 re-enable 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.

# Information About CLI Error Messages

Table 2-3 lists some error messages that you might encounter while using the CLI to configure your switch.

*Table 2-3 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. | Re-enter the command followed by a question mark (?) with a space between the command and the question mark.<br>The possible keywords that you can enter with the command appear. |
| `% Incomplete command.` | You did not enter all the keywords or values required by this command. | Re-enter the command followed by a question mark (?) with a space between the command and the question mark.<br>The possible keywords that you can enter with the command appear. |
| `% Invalid input detected at '^' marker.` | You entered the command incorrectly. The caret (^) marks the point of the error. | Enter a question mark (?) to display all the commands that are available in this command mode.<br>The possible keywords that you can enter with the command appear. |

# Using 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 as described in these sections:

- Changing the Command History Buffer Size, page 2-5 (optional)
- Recalling Commands, page 2-6 (optional)
- Disabling the Command History Feature, page 2-6 (optional)

## 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. These procedures are optional.

Beginning in privileged EXEC mode, enter this command to change the number of command lines that the switch records during the current terminal session:

```
Switch# terminal history [size number-of-lines]
```

The range is from 0 to 256.

Beginning in line configuration mode, enter this command to configure the number of command lines the switch records for all sessions on a particular line:

```
Switch(config-line)# history [size number-of-lines]
```

The range is from 0 to 256.

## Recalling Commands

To recall commands from the history buffer, perform one of the actions listed in Table 2-4. These actions are optional.

*Table 2-4 Recalling Commands*

| Action[1] | Result |
|---|---|
| Press **Ctrl-P** or the up arrow key. | Recall commands in the history buffer, beginning with the most recent command. Repeat the key sequence to recall successively older commands. |
| Press **Ctrl-N** or the down arrow key. | Return 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. |
| **show history** | While in privileged EXEC mode, list the last several commands that you just entered. The number of commands that appear is controlled by the setting of the **terminal history** global configuration command and the **history** line configuration command. |

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

## 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. These procedures are optional.

To disable the feature during the current terminal session, enter the **terminal no history** privileged EXEC command.

To disable command history for the line, enter the **no history** line configuration command.

# Using Editing Features

This section describes the editing features that can help you manipulate the command line.

- Enabling and Disabling Editing Features, page 2-6 (optional)
- Editing Commands through Keystrokes, page 2-7 (optional)
- Editing Command Lines that Wrap, page 2-8 (optional)

## Enabling and Disabling Editing Features

Although enhanced editing mode is automatically enabled, you can disable it, re-enable it, or configure a specific line to have enhanced editing. These procedures are optional.

To globally disable enhanced editing mode, enter this command in line configuration mode:

```
Switch (config-line)# no editing
```

To re-enable the enhanced editing mode for the current terminal session, enter this command in privileged EXEC mode:

```
Switch# terminal editing
```

To reconfigure a specific line to have enhanced editing mode, enter this command in line configuration mode:

```
Switch(config-line)# editing
```

# Editing Commands through Keystrokes

Table 2-5 shows the keystrokes that you need to edit command lines. These keystrokes are optional.

*Table 2-5 Editing Commands through Keystrokes*

| Capability | Keystroke[1] | Purpose |
|---|---|---|
| Move around the command line to make changes or corrections. | Press **Ctrl-B**, or press the left arrow key. | Move the cursor back one character. |
| | Press **Ctrl-F**, or press the right arrow key. | Move the cursor forward one character. |
| | Press **Ctrl-A**. | Move the cursor to the beginning of the command line. |
| | Press **Ctrl-E**. | Move the cursor to the end of the command line. |
| | Press **Esc B**. | Move the cursor back one word. |
| | Press **Esc F**. | Move the cursor forward one word. |
| | Press **Ctrl-T**. | Transpose the character to the left of the cursor with the character located at the cursor. |
| Recall commands from the buffer and paste them in the command line. The switch provides a buffer with the last ten items that you deleted. | Press **Ctrl-Y.** | Recall the most recent entry in the buffer. |
| | Press **Esc Y**. | Recall the next buffer entry.<br>The buffer contains only the last 10 items that you have deleted or cut. If you press **Esc Y** more than ten times, you cycle to the first buffer entry. |
| Delete entries if you make a mistake or change your mind. | Press the **Delete** or **Backspace** key. | Erase the character to the left of the cursor. |
| | Press **Ctrl-D**. | Delete the character at the cursor. |
| | Press **Ctrl-K**. | Delete all characters from the cursor to the end of the command line. |
| | Press **Ctrl-U** or **Ctrl-X**. | Delete all characters from the cursor to the beginning of the command line. |
| | Press **Ctrl-W**. | Delete the word to the left of the cursor. |
| | Press **Esc D**. | Delete from the cursor to the end of the word. |
| Capitalize or lowercase words or capitalize a set of letters. | Press **Esc C**. | Capitalize at the cursor. |
| | Press **Esc L**. | Change the word at the cursor to lowercase. |
| | Press **Esc U**. | Capitalize letters from the cursor to the end of the word. |
| Designate a particular keystroke as an executable command, perhaps as a shortcut. | Press **Ctrl-V** or **Esc Q**. | |

*Table 2-5 Editing Commands through Keystrokes (continued)*

| Capability | Keystroke[1] | Purpose |
|---|---|---|
| Scroll down a line or screen on displays that are longer than the terminal screen can display.<br>**Note** The More prompt is used for any output that has more lines than can be displayed on the terminal screen, including **show** command output. You can use the **Return** and **Space** bar keystrokes whenever you see the More prompt. | Press the **Return** key. | Scroll down one line. |
| | Press the **Space** bar. | Scroll down one screen. |
| Redisplay the current command line if the switch suddenly sends a message to your screen. | Press **Ctrl-L** or **Ctrl-R.** | Redisplay the current command line. |

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

# 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.

In this example, the **access-list** global configuration command entry 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.

```
Switch(config)# access-list 101 permit tcp 131.108.2.5 255.255.255.0 131.108.1
Switch(config)# $ 101 permit tcp 131.108.2.5 255.255.255.0 131.108.1.20 255.25
Switch(config)# $t tcp 131.108.2.5 255.255.255.0 131.108.1.20 255.255.255.0 eq
Switch(config)# $108.2.5 255.255.255.0 131.108.1.20 255.255.255.0 eq 45
```

After you complete the entry, press **Ctrl-A** to check the complete syntax before pressing the **Return** key to execute the command. The dollar sign ($) appears at the end of the line to show that the line has been scrolled to the right:

```
Switch(config)# access-list 101 permit tcp 131.108.2.5 255.255.255.0 131.108.1$
```

The software assumes you have a terminal screen that is 80 columns wide. If you have a width other than that, 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. For information about recalling previous command entries, see the "Editing Commands through Keystrokes" section on page 2-7.

# 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.

To use this functionality, enter a **show** or **more** command followed by the *pipe* character (|), one of the keywords **begin**, **include**, or **exclude**, and an expression that you want to search for or filter out:

*command* **|** {**begin** | **include** | **exclude**} *regular-expression*

Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* do not appear, but the lines that contain *Output* do appear.

This example shows how to include in the output display only lines where the expression *protocol* appears:

```
Switch# show interfaces | include protocol
Vlan1 is up, line protocol is up
Vlan10 is up, line protocol is down
GigabitEthernet0/1 is up, line protocol is down
GigabitEthernet0/2 is up, line protocol is up
```

# Accessing the CLI

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

## Accessing the CLI through a Console Connection or through Telnet

Before you can access the CLI, you must connect a terminal or PC to the switch console port and power on the switch as described in the hardware installation guide. Then, to understand the boot process and the options available for assigning IP information, see the "Assigning the Switch IP Address and Default Gateway" chapter in the *Cisco Connected Grid Switches System Management Software Configuration Guide*.

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. For more information, see the "Setting a Telnet Password for a Terminal Line" section in the *Cisco Connected Grid Switches Security Software Configuration Guide*.

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. For information about connecting to the console 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.

For information about configuring the switch for Telnet access, see the “Setting a Telnet Password for a Terminal Line” section in the *Cisco Connected Grid Switches Security Software Configuration Guide*. The switch supports up to 16 simultaneous Telnet sessions. Changes made by one Telnet user are reflected in all other Telnet sessions.

For information about configuring the switch for SSH, see the “Configuring SSH” section in the *Cisco Connected Grid Switches Security Software Configuration Guide*. The switch supports up to five simultaneous secure SSH sessions.

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

# Related Documents

- Cisco IOS Master Command List, All Releases
- Cisco Connected Grid Switches Interfaces Software Configuration Guide
- Cisco Connected Grid Switches System Management Software Configuration Guide
- Cisco Connected Grid Switches Security Software Configuration Guide

# Configuring Cisco IOS Configuration Engine

This chapter describes how to configure the Cisco IOS Configuration Engine on the Cisco Industrial Ethernet 2000U Series Switches, hereafter referred to as IE 2000U or switch.

**Note** For complete configuration information for the Cisco Configuration Engine, go to http://www.cisco.com/en/US/products/sw/netmgtsw/ps4617/tsd_products_support_series_home.html

For complete syntax and usage information for the commands used in this chapter, see the documents listed in the "Related Documents" section on page 3-17.


- Information About Cisco Configuration Engine Software, page 3-1
- Information About Cisco IOS Agents, page 3-5
- Prerequisites, page 3-6
- Guidelines and Limitations, page 3-7
- Default Settings, page 3-7
- Configuring Cisco IOS Agents, page 3-7
- Verifying Configuration, page 3-15
- Configuration Example, page 3-16
- Related Documents, page 3-17


## Information About Cisco Configuration Engine Software

The Cisco Configuration Engine is network management software that acts as a configuration service for automating the deployment and management of network devices and services (see Figure 3-1). Each Configuration Engine manages a group of Cisco devices (switches and routers) and the services that they deliver, storing their configurations and delivering them as needed. The Configuration Engine automates initial configurations and configuration updates by generating device-specific configuration changes, sending them to the device, executing the configuration change, and logging the results.

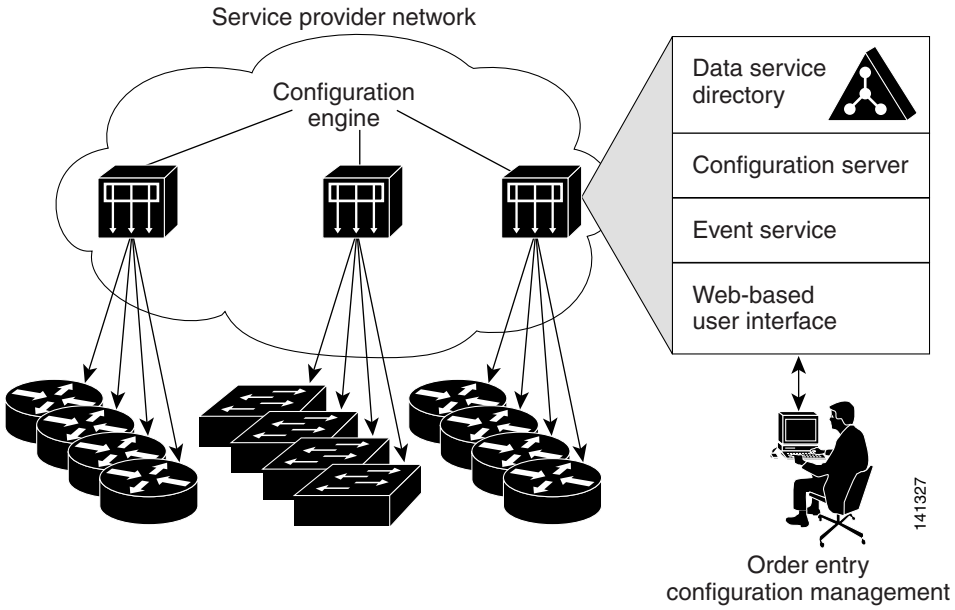
The Configuration Engine supports standalone and server modes and has these Cisco Networking Services (CNS) components:

- Configuration service (web server, file manager, and namespace mapping server)
- Event service (event gateway)

- Data service directory (data models and schema)

In standalone mode, the Configuration Engine supports an embedded Directory Service. In this mode, no external directory or other data store is required. In server mode, the Configuration Engine supports the use of a user-defined external directory.

***Figure 3-1 Configuration Engine Architectural Overview***




This section includes the following topics:

- Configuration Service, page 3-2
- Event Service, page 3-3
- What You Should Know About the CNS IDs and Device Hostnames, page 3-3

# Configuration Service

The Configuration Service is the core component of the Cisco Configuration Engine. It consists of a configuration server that works with Cisco IOS CNS agents on the switch. The Configuration Service delivers device and service configurations to the switch for initial configuration and mass reconfiguration by logical groups. Switches receive their initial configuration from the Configuration Service when they start up on the network for the first time.

The Configuration Service uses the CNS Event Service to send and receive configuration change events and to send success and failure notifications.

The configuration server is a web server that uses configuration templates and the device-specific configuration information stored in the embedded (standalone mode) or remote (server mode) directory.

Configuration templates are text files containing static configuration information in the form of CLI commands. In the templates, variables are specified using Lightweight Directory Access Protocol (LDAP) URLs that reference the device-specific configuration information stored in a directory.

The Cisco IOS agent can perform a syntax check on received configuration files and publish events to show the success or failure of the syntax check. The configuration agent can either apply configurations immediately or delay the application until receipt of a synchronization event from the configuration server.

# Event Service

The Cisco Configuration Engine uses the Event Service for receipt and generation of configuration events. The event agent is on the switch and facilitates the communication between the switch and the event gateway on the Configuration Engine.

The Event Service is a highly capable publish-and-subscribe communication method. The Event Service uses subject-based addressing to send messages to their destinations. Subject-based addressing conventions define a simple, uniform namespace for messages and their destinations.

## NameSpace Mapper

The Configuration Engine includes the NameSpace Mapper (NSM) that provides a lookup service for managing logical groups of devices based on application, device or group ID, and event.

Cisco IOS devices recognize only event subject-names that match those configured in Cisco IOS software; for example, cisco.cns.config.load. You can use the namespace mapping service to designate events by using any desired naming convention. When you have populated your data store with your subject names, NSM changes your event subject-name strings to those known by Cisco IOS.

For a subscriber, when given a unique device ID and event, the namespace mapping service returns a set of events to which to subscribe. Similarly, for a publisher, when given a unique group ID, device ID, and event, the mapping service returns a set of events on which to publish.

# What You Should Know About the CNS IDs and Device Hostnames

The Configuration Engine assumes that a unique identifier is associated with each configured switch. This unique identifier can take on multiple synonyms, where each synonym is unique within a particular namespace. The event service uses namespace content for subject-based addressing of messages.

The Configuration Engine intersects two namespaces, one for the event bus and the other for the configuration server. Within the scope of the configuration server namespace, the term *ConfigID* is the unique identifier for a device. Within the scope of the event bus namespace, the term *DeviceID* is the CNS unique identifier for a device.

Because the Configuration Engine uses both the event bus and the configuration server to provide configurations to devices, you must define both ConfigID and Device ID for each configured switch.

Within the scope of a single instance of the configuration server, no two configured switches can share the same value for ConfigID. Within the scope of a single instance of the event bus, no two configured switches can share the same value for DeviceID.

## ConfigID

Each configured switch has a unique ConfigID, which serves as the key into the Configuration Engine directory for the corresponding set of switch CLI attributes. The ConfigID defined on the switch must match the ConfigID for the corresponding switch definition on the Configuration Engine.

The ConfigID is fixed at startup time and cannot be changed until the device restarts, even if the switch hostname is reconfigured.

## DeviceID

Each configured switch participating on the event bus has a unique DeviceID, which is analogous to the switch source address so that the switch can be targeted as a specific destination on the bus. All switches configured with the **cns config partial** global configuration command must access the event bus. Therefore, the DeviceID, as originated on the switch, must match the DeviceID of the corresponding switch definition in the Configuration Engine.

The origin of the DeviceID is defined by the Cisco IOS hostname of the switch. However, the DeviceID variable and its usage reside within the event gateway adjacent to the switch.

The logical Cisco IOS termination point on the event bus is embedded in the event gateway, which in turn functions as a proxy on behalf of the switch. The event gateway represents the switch and its corresponding DeviceID to the event bus.

The switch declares its hostname to the event gateway immediately after the successful connection to the event gateway. The event gateway couples the DeviceID value to the Cisco IOS hostname each time this connection is established. The event gateway caches this DeviceID value for the duration of its connection to the switch.

## Hostname and DeviceID

The DeviceID is fixed at the time of the connection to the event gateway and does not change even when the switch hostname is reconfigured.

When changing the switch hostname on the switch, the only way to refresh the DeviceID is to break the connection between the switch and the event gateway. Enter the **no cns event** global configuration command followed by the **cns event** global configuration command.

When the connection is re-established, the switch sends its modified hostname to the event gateway. The event gateway redefines the DeviceID to the new value.

**Caution** When using the Configuration Engine user interface, you must first set the DeviceID field to the hostname value that the switch acquires *after*–not *before*–you use the **cns config initial** global configuration command at the switch. Otherwise, subsequent **cns config partial** global configuration command operations malfunction.

## Using Hostname, DeviceID, and ConfigID

In standalone mode, when a hostname value is set for a switch, the configuration server uses the hostname as the DeviceID when an event is sent on hostname. If the hostname has not been set, the event is sent on the cn=<*value*> of the device.

In server mode, the hostname is not used. In this mode, the unique DeviceID attribute is always used for sending an event on the bus. If this attribute is not set, you cannot update the switch.

These and other associated attributes (tag value pairs) are set when you run **Setup** on the Configuration Engine.

For more information about running the setup program on the Configuration Engine, see the *Cisco Configuration Engine Installation and Configuration Guide*.

# Information About Cisco IOS Agents

The CNS event agent feature allows the switch to publish and subscribe to events on the event bus and works with the Cisco IOS agent. The Cisco IOS agent feature supports the switch by providing these features:


- Initial Configuration, page 3-5
- Incremental (Partial) Configuration, page 3-6
- Synchronized Configuration, page 3-6


## Initial Configuration

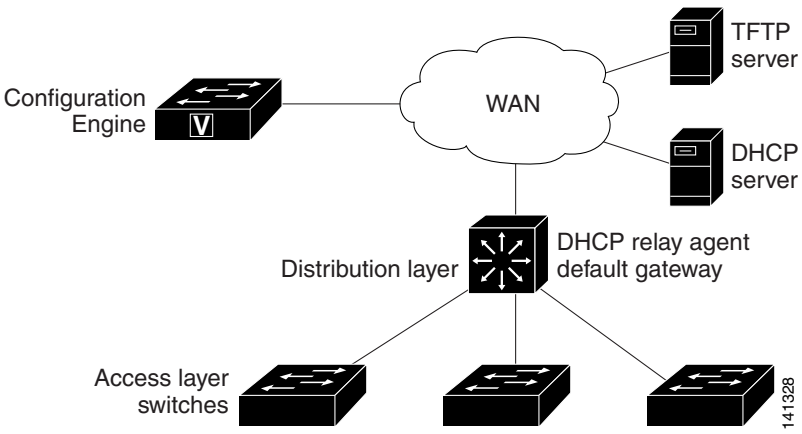
When the switch first comes up, it attempts to get an IP address by broadcasting a DHCP request on the network. Assuming there is no DHCP server on the subnet, the distribution switch acts as a DHCP relay agent and forwards the request to the DHCP server. Upon receiving the request, the DHCP server assigns an IP address to the new switch and includes the TFTP server IP address, the path to the bootstrap configuration file, and the default gateway IP address in a unicast reply to the DHCP relay agent. The DHCP relay agent forwards the reply to the switch.

The switch automatically configures the assigned IP address on interface VLAN 1 (the default) and downloads the bootstrap configuration file from the TFTP server. Upon successful download of the bootstrap configuration file, the switch loads the file in its running configuration.

The Cisco IOS agents initiate communication with the Configuration Engine by using the appropriate ConfigID and EventID. The Configuration Engine maps the Config ID to a template and downloads the full configuration file to the switch.

Figure 3-2 shows a sample network configuration for retrieving the initial bootstrap configuration file by using DHCP-based autoconfiguration.

***Figure 3-2 Initial Configuration Overview***



## Incremental (Partial) Configuration

After the network is running, new services can be added by using the Cisco IOS agent. Incremental (partial) configurations can be sent to the switch. The actual configuration can be sent as an event payload by way of the event gateway (push operation) or as a signal event that triggers the switch to initiate a pull operation.

The switch can check the syntax of the configuration before applying it. If the syntax is correct, the switch applies the incremental configuration and publishes an event that signals success to the configuration server. If the switch does not apply the incremental configuration, it publishes an event showing an error status. When the switch has applied the incremental configuration, it can write it to NVRAM or wait until signaled to do so.

## Synchronized Configuration

When the switch receives a configuration, it can defer application of the configuration upon receipt of a write-signal event. The write-signal event tells the switch not to save the updated configuration into its NVRAM. The switch uses the updated configuration as its running configuration. This ensures that the switch configuration is synchronized with other network activities before saving the configuration in NVRAM for use at the next reboot.

# Prerequisites

To enable automated CNS configuration of the switch, you must first complete the prerequisites in Table 3-1. When you complete them, power on the switch. At the **setup** prompt, do nothing: The switch begins the initial configuration as described in the "Initial Configuration" section on page 3-5. When the full configuration file is loaded on your switch, you do not need to do anything else.

***Table 3-1 Prerequisites for Enabling Automatic Configuration***

| Device | Required Configuration |
|---|---|
| Access switch | Factory default (no configuration file) |
| Distribution switch | • IP helper address<br>• Enable DHCP relay agent<br>• IP routing (if used as default gateway) |
| DHCP server | • IP address assignment<br>• TFTP server IP address<br>• Path to bootstrap configuration file on the TFTP server<br>• Default gateway IP address |

*Table 3-1 Prerequisites for Enabling Automatic Configuration (continued)*

| Device | Required Configuration |
|---|---|
| TFTP server | • A bootstrap configuration file that includes the CNS configuration commands that enable the switch to communicate with the Configuration Engine<br>• The switch configured to use either the switch MAC address or the serial number (instead of the default hostname) to generate the ConfigID and EventID<br>• The CNS event agent configured to push the configuration file to the switch |
| CNS Configuration Engine | One or more templates for each type of device, with the ConfigID of the device mapped to the template. |

**Note** For more information about running the setup program and creating templates on the Configuration Engine, see the *Cisco Configuration Engine Installation and Configuration Guide*.

# Guidelines and Limitations

These restrictions apply to the image agent running on the switch:

- You can only download the tar image file. Downloading the bin image file is not supported.
- Only the immediate download option is supported. You cannot schedule a download to occur at a specified date and time.
- The Destination field in the Associate Image with Device window of the Cisco Configuration Engine GUI is not supported.

# Default Settings

- CNS Event Agent: Disabled
- CNS Configuration Agent: Disabled

# Configuring Cisco IOS Agents

The Cisco IOS agents embedded in the switch Cisco IOS software allow the switch to be connected and automatically configured as described in the "Prerequisites" section on page 3-6. If you want to change the configuration or install a custom configuration, see these sections for instructions:

- Enabling the CNS Event Agent, page 3-8
- Enabling the Cisco IOS CNS Agent, page 3-9
- Upgrading Devices with Cisco IOS Image Agent, page 3-14

# Enabling the CNS Event Agent

You must enable the CNS event agent on the switch before you enable the CNS configuration agent.

## BEFORE YOU BEGIN

Review the "Information About Cisco IOS Agents" section on page 3-5.

## DETAILED STEPS

| | Command | Purpose |
|---|---|---|
| Step 1 | **configure terminal** | Enter global configuration mode. |
| Step 2 | **cns event** {*hostname* \| *ip-address*} [*port-number*] [**backup**] [**failover-time** *seconds*] [**keepalive** *seconds retry-count*] [**reconnect** *time*] [**source** *ip-address*] | Enable the event agent, and enter the gateway parameters.<br>• For {*hostname* \| *ip-address*}, enter either the hostname or the IP address of the event gateway.<br>• (Optional) For *port number*, enter the port number for the event gateway. The default port number is 11011.<br>• (Optional) Enter **backup** to show that this is the backup gateway. (If omitted, this is the primary gateway.)<br>• (Optional) For **failover-time** *seconds*, enter how long the switch waits for the primary gateway route after the route to the backup gateway is established.<br>• (Optional) For **keepalive** *seconds*, enter how often the switch sends keepalive messages. For *retry-count*, enter the number of unanswered keepalive messages that the switch sends before the connection is terminated. The default for each is 0.<br>• (Optional) For **reconnect** *time*, enter the maximum time interval that the switch waits before trying to reconnect to the event gateway.<br>• (Optional) For **source** *ip-address*, enter the source IP address of this device.<br>**Note** Though visible in the command-line help string, the **encrypt** and the **clock-timeout** *time* keywords are not supported. |
| Step 3 | **end** | Return to privileged EXEC mode. |
| Step 4 | **show cns event connections** | Verify information about the event agent. |

| | Command | Purpose |
|---|---|---|
| Step 5 | **show running-config** | Verify your entries. |
| Step 6 | **copy running-config startup-config** | (Optional) Save your entries in the configuration file. |

To disable the CNS event agent, use the **no cns event** {*ip-address* | *hostname*} global configuration command.

### EXAMPLE

This example shows how to enable the CNS event agent, set the IP address gateway to 10.180.1.27, set 120 seconds as the keepalive interval, and set 10 as the retry count:

```
Switch(config)# cns event 10.180.1.27 keepalive 120 10
```

# Enabling the Cisco IOS CNS Agent

After enabling the CNS event agent, start the Cisco IOS CNS agent on the switch. You can enable the Cisco IOS agent with these commands:

- The **cns config initial** global configuration command enables the Cisco IOS agent and initiates an initial configuration on the switch.
- The **cns config partial** global configuration command enables the Cisco IOS agent and initiates a partial configuration on the switch. You can then use the Configuration Engine to remotely send incremental configurations to the switch.

## Enabling an Initial Configuration

### BEFORE YOU BEGIN

Complete the "Enabling the CNS Event Agent" procedure on page 3-8.

### DETAILED STEPS

| | Command | Purpose |
|---|---|---|
| Step 1 | **configure terminal** | Enter global configuration mode. |
| Step 2 | **cns template connect** *name* | Enter CNS template connect configuration mode, and specify the name of the CNS connect template. |
| Step 3 | **cli** *config-text* | Enter a command line for the CNS connect template. Repeat this step for each command line in the template. |
| Step 4 | | Repeat Steps 2 to 3 to configure another CNS connect template. |
| Step 5 | **exit** | Return to global configuration mode. |

| | Command | Purpose |
|---|---|---|
| Step 6 | **cns connect** *name* [**retries** *number*] [**retry-interval** *seconds*] [**sleep** *seconds*] [**timeout** *seconds*] | Enter CNS connect configuration mode, specify the name of the CNS connect profile, and define the profile parameters. The switch uses the CNS connect profile to connect to the Configuration Engine.<br>• Enter the name of the CNS connect profile.<br>• (Optional) For **retries** *number*, enter the number of connection retries. The range is 1 to 30. The default is 3.<br>• (Optional) For **retry-interva**l *seconds*, enter the interval between successive connection attempts to the Configuration Engine. The range is 1 to 40 seconds. The default is 10 seconds.<br>• (Optional) For **sleep** *seconds*, enter the amount of time before which the first connection attempt occurs. The range is 0 to 250 seconds. The default is 0.<br>• (Optional) For **timeout** *seconds*, enter the amount of time after which the connection attempts end. The range is 10 to 2000 seconds. The default is 120. |
| Step 7 | **discover** {**controller** *controller-type* \| **dlci** [**subinterface** *subinterface-number*] \| **interface** [*interface-type*] \| **line** *line-type*} | Specify the interface parameters in the CNS connect profile.<br>• For **controller** *controller-type*, enter the controller type.<br>• For **dlci**, enter the active data-link connection identifiers (DLCIs).<br>(Optional) For **subinterface** *subinterface-number*, specify the point-to-point subinterface number that is used to search for active DLCIs.<br>• For **interface** [*interface-type*], enter the type of interface.<br>• For **line** *line-type*, enter the line type. |
| Step 8 | **template** *name* [ ... *name*] | Specify the list of CNS connect templates in the CNS connect profile to be applied to the switch configuration. You can specify more than one template. |
| Step 9 | | Repeat Steps 7 to 8 to specify more interface parameters and CNS connect templates in the CNS connect profile. |
| Step 10 | **exit** | Return to global configuration mode. |
| Step 11 | **hostname** *name* | Enter the hostname for the switch. |
| Step 12 | **ip route** *network-number* | (Optional) Establish a static route to the Configuration Engine whose IP address is *network-number*. |

| | Command | Purpose |
|---|---|---|
| **Step 13** | **cns id** *interface num* {**dns-reverse** \| **ipaddress** \| **mac-address**} [**event**] [**image**]<br><br>or<br><br>**cns id** {**hardware-serial** \| **hostname** \| **string** *string* \| **udi**} [**event**] [**image**] | (Optional) Set the unique EventID or ConfigID used by the Configuration Engine.<br>• For *interface num*, enter the type of interface–for example, ethernet, group-async, loopback, or virtual-template. This setting specifies from which interface the IP or MAC address should be retrieved to define the unique ID.<br>• For {**dns-reverse** \| **ipaddress** \| **mac-address**}, enter **dns-reverse** to retrieve the hostname and assign it as the unique ID, enter **ipaddress** to use the IP address, or enter **mac-address** to use the MAC address as the unique ID.<br>• (Optional) Enter **event** to set the ID to be the event-id value used to identify the switch.<br>• (Optional) Enter **image** to set the ID to be the image-id value used to identify the switch.<br>**Note** If both the **event** and **image** keywords are omitted, the image-id value is used to identify the switch.<br>• For {**hardware-serial** \| **hostname**\| **string** *string* \| **udi**}, enter **hardware-serial** to set the switch serial number as the unique ID, enter **hostname** (the default) to select the switch hostname as the unique ID, enter an arbitrary text string for **string** *string* as the unique ID, or enter **udi** to set the unique device identifier (UDI) as the unique ID. |

| | Command | Purpose |
|---|---|---|
| Step 14 | **cns config initial** {*hostname* \| *ip-address*} [*port-number*] [**event**] [**no-persist**] [**page** *page*] [**source** *ip-address*] [**syntax-check**] | Enable the Cisco IOS agent, and initiate an initial configuration.<br>• For {*hostname* \| *ip-address*}, enter the hostname or the IP address of the configuration server.<br>• (Optional) For *port-number*, enter the port number of the configuration server. The default port number is 80.<br>• (Optional) Enable **event** for configuration success, failure, or warning messages when the configuration is finished.<br>• (Optional) Enable **no-persist** to suppress the automatic writing to NVRAM of the configuration pulled as a result of entering the **cns config initial** global configuration command. If the **no-persist** keyword is not entered, using the **cns config initial** command causes the resultant configuration to be automatically written to NVRAM.<br>• (Optional) For **page** *page*, enter the web page of the initial configuration. The default is /Config/config/asp.<br>• (Optional) Enter **source** *ip-address* to use for source IP address.<br>• (Optional) Enable **syntax-check** to check the syntax when this parameter is entered.<br>**Note** Though visible in the command-line help string, the **encrypt**, **status** *url*, and **inventory** keywords are not supported. |
| Step 15 | **end** | Return to privileged EXEC mode. |
| Step 16 | **show cns config connections** | Verify information about the configuration agent. |
| Step 17 | **show running-config** | Verify your entries. |

To disable the CNS Cisco IOS agent, use the **no cns config initial** {*ip-address* | *hostname*} global configuration command.

## EXAMPLE

This example shows how to configure an initial configuration on a remote switch when the switch configuration is unknown (the CNS Zero Touch feature):

```
Switch(config)# cns template connect template-dhcp
Switch(config-tmpl-conn)# cli ip address dhcp
Switch(config-tmpl-conn)# exit
Switch(config)# cns template connect ip-route
Switch(config-tmpl-conn)# cli ip route 0.0.0.0 0.0.0.0 ${next-hop}
Switch(config-tmpl-conn)# exit
Switch(config)# cns connect dhcp
```

```
Switch(config-cns-conn)# discover interface gigabitethernet
Switch(config-cns-conn)# template template-dhcp
Switch(config-cns-conn)# template ip-route
Switch(config-cns-conn)# exit
Switch(config)# hostname RemoteSwitch
RemoteSwitch(config)# cns config initial 10.1.1.1 no-persist
```

This example shows how to configure an initial configuration on a remote switch when the switch IP address is known. The Configuration Engine IP address is 172.28.129.22.

```
Switch(config)# cns template connect template-dhcp
Switch(config-tmpl-conn)# cli ip address dhcp
Switch(config-tmpl-conn)# exit
Switch(config)# cns template connect ip-route
Switch(config-tmpl-conn)# cli ip route 0.0.0.0 0.0.0.0 ${next-hop}
Switch(config-tmpl-conn)# exit
Switch(config)# cns connect dhcp
Switch(config-cns-conn)# discover interface gigabitethernet
Switch(config-cns-conn)# template template-dhcp
Switch(config-cns-conn)# template ip-route
Switch(config-cns-conn)# exit
Switch(config)# hostname RemoteSwitch
RemoteSwitch(config)# ip route 172.28.129.22 255.255.255.255 11.11.11.1
RemoteSwitch(config)# cns id ethernet 0 ipaddress
RemoteSwitch(config)# cns config initial 172.28.129.22 no-persist
```

## Enabling a Partial Configuration

### BEFORE YOU BEGIN

Complete the "Enabling the CNS Event Agent" procedure on page 3-8.

### DETAILED STEPS

| | Command | Purpose |
|---|---|---|
| Step 1 | **configure terminal** | Enter global configuration mode. |
| Step 2 | **cns config partial** {*ip-address* \| *hostname*} [*port-number*] [**source** *ip-address*] | Enable the configuration agent, and initiate a partial configuration.<br>• For {*ip-address* \| *hostname*}, enter the IP address or the hostname of the configuration server.<br>• (Optional) For *port-number*, enter the port number of the configuration server. The default port number is 80.<br>• (Optional) Enter **source** *ip-address* to use for the source IP address.<br>**Note** Though visible in the command-line help string, the **encrypt** keyword is not supported. |
| Step 3 | **end** | Return to privileged EXEC mode. |

| | Command | Purpose |
|---|---|---|
| Step 4 | **show cns config stats**<br>or<br>**show cns config outstanding** | Verify information about the configuration agent. |
| Step 5 | **show running-config** | Verify your entries. |
| Step 6 | **copy running-config startup-config** | (Optional) Save your entries in the configuration file. |

To disable the Cisco IOS agent, use the **no cns config partial** {*ip-address* | *hostname*} global configuration command. To cancel a partial configuration, use the **cns config cancel** privileged EXEC command.

### EXAMPLE

The following example shows how to configure the CNS partial configuration agent to accept events from the event gateway at 172.28.129.22. The CNS partial configuration agent will connect to the CNS configuration server at 172.28.129.22, port number 80. The CNS partial configuration agent requests are redirected to a configuration server at 172.28.129.40, port number 80.

```
Switch(config)# cns event 172.28.129.22
Switch(config)# cns trusted-server config 172.28.129.40
Switch(config)# cns config partial 172.28.129.22
```

# Upgrading Devices with Cisco IOS Image Agent

Administrators maintaining large networks of Cisco IOS devices need an automated mechanism to load image files onto large numbers of remote devices. Existing network management applications are useful to determine which images to run and how to manage images received from the Cisco online software center. Other image distribution solutions do not scale to cover thousands of devices and cannot distribute images to devices behind a firewall. The CNS image agent enables the managed device to initiate a network connection and request an image download allowing devices behind firewalls to access the image server.

You can use image agent to download one or more devices. The switches must have the image agent running on them.

### BEFORE YOU BEGIN

Confirm these prerequisites before upgrading one or more devices with image agent:

- Determine where to store the Cisco IOS images on a file server to make the image available to the other networking devices. If the CNS Event Bus is to be used to store and distribute the images, the CNS event agent must be configured.
- Set up a file server to enable the networking devices to download the new images using the HTTPS protocol.
- Determine how to handle error messages generated by image agent operations. Error messages can be sent to the CNS Event Bus or an HTTP or HTTPS URL.

During automated image loading operations you must try to prevent the Cisco IOS device from losing connectivity with the file server that is providing the image. Image reloading is subject to memory issues and connection issues. Boot options must also be configured to allow the Cisco IOS device to boot another image if the first image reload fails.

### DETAILED STEPS

| | Command | Purpose |
|---|---|---|
| Step 1 | **configure terminal** | Enter global configuration mode |
| Step 2 | **ip host** {*ip-address*} {*hostname*} | Enter the IP address and the hostname of the event gateway. |
| Step 3 | **cns trusted-server all-agents** {*hostname*} | Specify a trusted server for CNS agent. |
| Step 4 | **no cns aaa enable cns event** {*ip-address*} {*port number*} | Disable AAA authentication on the event gateway. |
| Step 5 | **cns image retry** {*number*} | Specify the number of times to retry and download the image. |
| Step 6 | **cns image server** {*ip-address*} **status** {*ip-address*} | Download the image from the server to the switch. |
| Step 7 | **end** | Return to privileged EXEC mode. |

### EXAMPLE

This example shows how to upgrade a switch from a server with the address of **172.20.249.20**:

```
Switch(config)> configure terminal
Switch(config)# ip host cns-dsbu.cisco.com 172.20.249.20
Switch(config)# cns trusted-server all-agents cns-dsbu.cisco.com
Switch(config)# no cns aaa enable cns event 172.20.249.20 22022
Switch(config)# cns image retry 1
Switch(config)# cns image server http://172.20.249.20:80/cns/HttpMsgDispatcher status
http://172.20.249.20:80/cns/HttpMsgDispatcher
Switch(config)# end
```

# Verifying Configuration

| Command | Purpose |
|---|---|
| **show cns config connections** | Displays the status of the CNS Cisco IOS agent connections. |
| **show cns config outstanding** | Displays information about incremental (partial) CNS configurations that have started but are not yet completed. |
| **show cns config stats** | Displays statistics about the Cisco IOS agent. |
| **show cns event connections** | Displays the status of the CNS event agent connections. |
| **show cns event stats** | Displays statistics about the CNS event agent. |
| **show cns event subject** | Displays a list of event agent subjects that are subscribed to by applications. |
| **show cns image** | Displays the status of the image download. |

# Configuration Example

This example shows how to enable the CNS event agent, set the IP address gateway to 10.180.1.27, set 120 seconds as the keepalive interval, and set 10 as the retry count:

```
Switch(config)# cns event 10.180.1.27 keepalive 120 10
```

This example shows how to configure an initial configuration on a remote switch when the switch configuration is unknown (the CNS Zero Touch feature):

```
Switch(config)# cns template connect template-dhcp
Switch(config-tmpl-conn)# cli ip address dhcp
Switch(config-tmpl-conn)# exit
Switch(config)# cns template connect ip-route
Switch(config-tmpl-conn)# cli ip route 0.0.0.0 0.0.0.0 ${next-hop}
Switch(config-tmpl-conn)# exit
Switch(config)# cns connect dhcp
Switch(config-cns-conn)# discover interface gigabitethernet
Switch(config-cns-conn)# template template-dhcp
Switch(config-cns-conn)# template ip-route
Switch(config-cns-conn)# exit
Switch(config)# hostname RemoteSwitch
RemoteSwitch(config)# cns config initial 10.1.1.1 no-persist
```

This example shows how to configure an initial configuration on a remote switch when the switch IP address is known. The Configuration Engine IP address is 172.28.129.22.

```
Switch(config)# cns template connect template-dhcp
Switch(config-tmpl-conn)# cli ip address dhcp
Switch(config-tmpl-conn)# exit
Switch(config)# cns template connect ip-route
Switch(config-tmpl-conn)# cli ip route 0.0.0.0 0.0.0.0 ${next-hop}
Switch(config-tmpl-conn)# exit
Switch(config)# cns connect dhcp
Switch(config-cns-conn)# discover interface gigabitethernet
Switch(config-cns-conn)# template template-dhcp
Switch(config-cns-conn)# template ip-route
Switch(config-cns-conn)# exit
Switch(config)# hostname RemoteSwitch
RemoteSwitch(config)# ip route 172.28.129.22 255.255.255.255 11.11.11.1
RemoteSwitch(config)# cns id ethernet 0 ipaddress
RemoteSwitch(config)# cns config initial 172.28.129.22 no-persist
```

The following example shows how to configure the CNS partial configuration agent to accept events from the event gateway at 172.28.129.22. The CNS partial configuration agent will connect to the CNS configuration server at 172.28.129.22, port number 80. The CNS partial configuration agent requests are redirected to a configuration server at 172.28.129.40, port number 80.

```
Switch(config)# cns event 172.28.129.22
Switch(config)# cns trusted-server config 172.28.129.40
Switch(config)# cns config partial 172.28.129.22
```

This example shows how to upgrade a switch from a server with the address of **172.20.249.20**:

```
Switch(config)> configure terminal
Switch(config)# ip host cns-dsbu.cisco.com 172.20.249.20
Switch(config)# cns trusted-server all-agents cns-dsbu.cisco.com
Switch(config)# no cns aaa enable cns event 172.20.249.20 22022
Switch(config)# cns image retry 1
Switch(config)# cns image server http://172.20.249.20:80/cns/HttpMsgDispatcher status
http://172.20.249.20:80/cns/HttpMsgDispatcher
Switch(config)# end
```

# Related Documents

- Cisco IOS Master Command List, All Releases
- Cisco IOS Cisco Networking Services Command Reference
- Cisco Configuration Engine Installation and Configuration Guide
- Cisco Configuration Engine Administration Guide
- Configuration Fundamentals Configuration Guide, Cisco IOS Release 15M&T

# Working with the Cisco IOS File System, Configuration Files, and Software Images

This chapter describes how to manipulate the Cisco IE 2000U flash file system, how to copy configuration files, and how to archive (upload and download) software images to a switch.

**Note** For complete syntax and usage information for the commands used in this chapter, see the documents listed in the "Related Documents" section on page 4-40.


- Working with the Flash File System, page 4-1
- Working with Configuration Files, page 4-9
- Working with Software Images, page 4-25
- Related Documents, page 4-40


## Working with 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 image and configuration files. The default flash file system on the switch is named *flash:*.

The switch has a removable compact flash card that stores the Cisco IOS software image and configuration files. You can replace and upgrade the switch without reconfiguring it. Removing the compact flash card does not interrupt switch operation. When the compact flash card is removed, you do not have access to the flash file system, and any attempt to access it generates an error message. The switch ships with the compact flash memory card installed and supports any size compact flash card.

Use the **show flash:** privileged EXEC command to display the compact flash file settings. For information about how to remove or replace the compact flash memory card on the switch, see the *Cisco IE 2000U Connected Grid Switch Hardware Installation Guide*.


- Displaying Available File Systems, page 4-2
- Detecting an Unsupported SD Flash Memory Card, page 4-3
- Setting the Default File System, page 4-3
- Displaying Information about Files on a File System, page 4-4
- Creating and Removing Directories, page 4-5
- Copying Files, page 4-6

- Deleting Files, page 4-6
- Creating, Displaying, and Extracting tar Files, page 4-7
- Displaying the Contents of a File, page 4-9


# 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.

```
Switch# 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:
```

| 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.<br>**flash**—The file system is for a flash memory device.<br>**nvram**—The file system is for a NVRAM device.<br>**opaque**—The file system is a locally generated *pseudo* file system (for example, the *system*) or a download interface, such as brimux.<br>**unknown**—The file system is an unknown type. |
| Flags | Permission for file system.<br>**ro**—read-only.<br>**rw**—read/write.\<br>**wo**—write-only. |
| Prefixes | Alias for file system.<br>**flash:**—Flash file system.<br>**nvram:**—NVRAM.<br>**null:**—Null destination for copies. You can copy a remote file to null to find its size.<br>**rcp:**—Remote Copy Protocol (RCP) network server.<br>**system:**—Contains the system memory, including the running configuration.<br>**tftp:**—TFTP network server.<br>**xmodem:**—Obtain the file from a network machine by using the Xmodem protocol.<br>**ymodem:**—Obtain the file from a network machine by using the Ymodem protocol. |

# Detecting an Unsupported SD Flash Memory Card

When the switch starts and detects an unsupported Secure Digital (SD) flash memory card, or when you insert an unsupported SD flash memory card while the switch is running, the following warning message is displayed:

```
WARNING: Non-IT SD flash detected. Use of this card during normal
         operation can impact and severely degrade performance of the system.
          Please use supported SD flash cards only.
```

To display information about the SD flash memory card on the screen, use the **show platform sdflash** privileged EXEC command.

This example shows an unsupported SD flash memory card:

```
Switch# show platform sdflash
SD Flash Manufacturer      : SMART MODULAR (ID=27h) - Non IT
         Size              : 485MB
         Serial number     : B01000A5
         Revision          : 2.0
         Manufacturing date: 12/2009
```

This example shows a supported SD flash memory card:

```
Switch# show platform sdflash
SD Flash Manufacturer      : SMART MODULAR (ID=27h)
         Size                           : 972MB
         Serial number         : 07000019
         Revision                    : 2.0
         Manufacturing date: 3/2010
```

**Note** When you enter the **show platform sdflash** privileged EXEC command, the name, date, and other fields that are displayed depend on the manufacturer of the SD flash memory card. However, if the SD flash memory card is unsupported, “Non IT” is displayed after the manufacturer’s name.

**Note** The output of the **show platform sdflash** privileged EXEC command is also included in the **show tech-support** privileged EXEC command output.

# 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 following privileged EXEC commands:

| Command | Description |
|---|---|
| **dir** [**/all**] [*filesystem***:**][*filename*] | Display a list of files on a file system. |
| **show file systems** | Display more information about each of the files on a file system. |
| **show file information** *file-url* | Display information about a specific file. |
| **show file descriptors** | Display 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. |

# Changing Directories and Displaying the Working Directory

## BEFORE YOU BEGIN

Review the "Working with the Flash File System" section on page 4-1.

## DETAILED STEPS

| | Command | Purpose |
|---|---|---|
| **Step 1** | **dir** *filesystem***:** | Display the directories on the specified file system.<br>For *filesystem***:**, use **flash:** for the system board flash device. |
| **Step 2** | **cd new_configs** | Change to the directory of interest.<br>The command example shows how to change to the directory named *new_configs*. |
| **Step 3** | **pwd** | Display the working directory. |

## EXAMPLE

```
Switch# dir flash:
```

# Creating and Removing Directories

## BEFORE YOU BEGIN

Review the "Working with the Flash File System" section on page 4-1.

## DETAILED STEPS

| | Command | Purpose |
|---|---|---|
| **Step 1** | **dir** *filesystem***:** | Display the directories on the specified file system.<br>For *filesystem***:**, use **flash:** for the system board flash device. |
| **Step 2** | **mkdir old_configs** | Create a new directory.<br>The command example shows how to create the directory named *old_configs*.<br>Directory names are case sensitive.<br>Directory names are limited to 45 characters between the slashes (/); the name cannot contain control characters, spaces, deletes, slashes, quotes, semicolons, or colons. |
| **Step 3** | **dir** *filesystem***:** | Verify your entry. |

To delete 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. 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.

For *filesystem*, use **flash:** for the system board flash device. For *file-url*, enter the name of the directory to be deleted. All the files in the directory and the directory are removed.

**Caution** When files and directories are deleted, their contents cannot be recovered.

## EXAMPLE

The following example deletes the directory named old_image and all files and subdirectories in it.

```
Switch# delete /force /recursive flash:old_image

Delete flash:old_image? [confirm]
```

# 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*

In addition, the Secure Copy Protocol (SCP) provides a secure and authenticated method for copying switch configurations or switch image files. SCP relies on Secure Shell (SSH), an application and a protocol that provides a secure replacement for the Berkeley r-tools.

**Note** For more information on how to configure and verify SCP, see the "Secure Copy Protocol" chapter of the *Secure Shell Configuration Guide, Cisco IOS Release 15M&T*.

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)

For specific examples of using the **copy** command with configuration files, see the "Working with Configuration Files" section on page 4-9.

To copy software images either by downloading a new version or by uploading the existing one, use the **archive download-sw** or the **archive upload-sw** privileged EXEC command. For more information, see the "Working with Software Images" section on page 4-25.

# 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:

```
Switch# delete myconfig
```

# Creating, Displaying, and Extracting tar Files

You can create a tar file and write files into it, list the files in a tar file, and extract the files from a tar file as described in the next sections.

**Note** Instead of using the **copy** privileged EXEC command or the **archive tar** privileged EXEC command, we recommend using the **archive download-sw** and **archive upload-sw** privileged EXEC commands to download and upload software image files.

## Creating a tar File

To create a tar file and write files into it, use this privileged EXEC command:

**archive tar /create** *destination-url* **flash:/***file-url*

For *destination-url*, specify the destination URL alias for the local or network file system and the name of the tar file to create. These options are supported:

- For the local flash file system, the syntax is **flash:**
- For the FTP, the syntax is **ftp:**[[**//***username*[**:***password*]**@***location*]**/***directory***]/***tar-filename***.tar**
- For the RCP, the syntax is **rcp:**[[**//***username***@***location*]**/***directory*]**/***tar-filename***.tar**
- For the TFTP, the syntax is **tftp:**[[**//***location*]**/***directory*]**/***tar-filename***.tar**

The *tar-filename***.tar** is the tar file to be created.

For **flash:/***file-url*, specify the location on the local flash file system from which the new tar file is created. You can also specify an optional list of files or directories within the source directory to write to the new tar file. If none are specified, all files and directories at this level are written to the newly created tar file.

This example shows how to create a tar file. This command writes the contents of the *new-configs* directory on the local flash device to a file named *saved.tar* on the TFTP server at 172.20.10.30:

```
Switch# archive tar /create tftp:172.20.10.30/saved.tar flash:/new-configs
```

## Displaying the Contents of a tar File

To display the contents of a tar file on the screen, use this privileged EXEC command:

**archive tar /table** *source-url*

For *source-url*, specify the source URL alias for the local or network file system. These options are supported:

- For the local flash file system, the syntax is **flash:**
- For the FTP, the syntax is **ftp:**[[**//***username*[**:***password*]**@***location*]**/***directory*]**/***tar-filename***.tar**
- For the RCP, the syntax is **rcp:**[[**//***username***@***location*]**/***directory*]**/***tar-filename***.tar**
- For the TFTP, the syntax is **tftp:**[[**//***location*]**/***directory*]**/***tar-filename***.tar**

The *tar-filename***.tar** is the tar file to display.

This example shows how to display the contents of a switch tar file that is in flash memory:

```
Switch# archive tar /table flash:image-name.tar
info (219 bytes)
image-name/ (directory)
image-name/html/ (directory)
image-name/html/foo.html (0 bytes)
image-name/image-name.bin (4527884 bytes)
image-name/info (346 bytes)
info (110 bytes)
```

## Extracting a tar File

To extract a tar file into a directory on the flash file system, use this privileged EXEC command:

**archive tar /xtract** *source-url* **flash:/***file-url* [*dir/file...*]

For *source-url*, specify the source URL alias for the local file system. These options are supported:

- For the local flash file system, the syntax is **flash:**
- For the FTP, the syntax is **ftp:**[[**//***username*[**:***password*]**@***location*]**/***directory*]**/***tar-filename***.tar**
- For the RCP, the syntax is **rcp:**[[**//***username***@***location*]**/***directory*]**/***tar-filename***.tar**
- For the TFTP, the syntax is **tftp:**[[**//***location*]**/***directory*]**/***tar-filename***.tar**

The *tar-filename***.tar** is the tar file from which to extract files.

For **flash:/***file-url* [*dir/file...*], specify *t*he location on the local flash file system into which the tar file is extracted. Use the *dir/file...* option to specify an optional list of files or directories within the tar file to be extracted. If none are specified, all files and directories are extracted.

This example shows how to extract the contents of a tar file located on the TFTP server at 172.20.10.30. This command extracts just the *new-configs* directory into the root directory on the local flash file system. The remaining files in the *saved.tar* file are ignored.

```
Switch# archive tar /xtract tftp://172.20.10.30/saved.tar flash:/new-configs
```

## Displaying the Contents of a File

To display the contents of any readable file, including a file on a remote file system, use the **more** [**/ascii** | **/binary** | **/ebcdic**] *file-url* privileged EXEC command:.

This example shows how to display the contents of a configuration file on a TFTP server:

```
Switch# more tftp://serverA/hampton/savedconfig
!
! Saved configuration on server
!
version 11.3
service timestamps log datetime localtime
service linenumber
service udp-small-servers
service pt-vty-logging
!
<output truncated>
```

# Working with Configuration Files

This section describes how to create, load, and maintain configuration files.

Configuration files contain commands entered to customize the function of the Cisco IOS software. A way to create a basic configuration file is to use the **setup** program or to enter the **setup** privileged EXEC command. For more information, see the "Assigning the Switch IP Address and Default Gateway" chapter in the *Cisco Connected Grid Switches System Management Software Configuration Guide*.

You can copy (*download*) configuration files from a TFTP, FTP, or RCP server to the running configuration or startup configuration of the switch. You might want to perform this for one of these reasons:

- To restore a backed-up configuration file.
- To use the configuration file for another switch. For example, you might add another switch to your network and want it to have a configuration similar 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 all the switches in your network so that all the switches have similar configurations.

You can copy (*upload*) configuration files from the switch to a file server by using TFTP, FTP, or RCP. You might perform this task to back up a current configuration file to a server before changing its contents so that you can later restore the original configuration file from the server.

The protocol 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 FTP and RCP are built on and use the TCP/IP stack, which is connection-oriented.

This section includes the following topics:

- Guidelines for Creating and Using Configuration Files, page 4-10
- Configuration File Types and Location, page 4-10
- Creating a Configuration File By Using a Text Editor, page 4-11
- Copying Configuration Files By Using TFTP, page 4-11
- Copying Configuration Files By Using FTP, page 4-13

- Copying Configuration Files By Using RCP, page 4-16
- Clearing Configuration Information, page 4-20
- Replacing and Rolling Back Configurations, page 4-20

# Guidelines for Creating and Using Configuration Files

Creating configuration files can aid in your switch configuration. Configuration files can contain some or all of the commands needed to configure one or more switches. For example, you might want to download the same configuration file to several switches that have the same hardware configuration.

Use these guidelines when creating a configuration file:

- We recommend that you connect through the console port for the initial configuration of the switch. If you are accessing the switch through a network connection instead of through a direct connection to the console port, keep in mind that some configuration changes (such as changing the switch IP address or disabling ports) can cause a loss of connectivity to the switch.
- If no password has been set on the switch, we recommend that you set one by using the **enable secret** *secret-password* global configuration command.

**Note** The **copy** {**ftp: | rcp: | tftp:**} **system:running-config** privileged EXEC command loads the configuration files on the switch as if you were entering the commands at 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 might 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, copy the configuration file directly to the startup configuration (by using the **copy** {**ftp: | rcp: | tftp:**} **nvram:startup-config** privileged EXEC command), and reload the switch.

# Configuration File Types and Location

Startup configuration files are used during system startup to configure the software. Running configuration files contain the current configuration of the software. The two configuration files can be different. For example, you might want to change the configuration for a short time period rather than permanently. In this case, you would change the running configuration but not save the configuration by using the **copy running-config startup-config** privileged EXEC command.

The running configuration is saved in DRAM; the startup configuration is stored in the NVRAM section of flash memory.

# Creating a Configuration File By Using a Text Editor

When creating a configuration file, you must list commands logically so that the system can respond appropriately. This is one method of creating a configuration file:

**Step 1** Copy an existing configuration from a switch to a server.

For more information, see the "Downloading the Configuration File By Using TFTP" section on page 4-12, the "Downloading a Configuration File By Using FTP" section on page 4-14, or the "Downloading a Configuration File By Using RCP" section on page 4-18.

**Step 2** Open the configuration file in a text editor, such as vi or emacs on UNIX or Notepad on a PC.

**Step 3** Extract the portion of the configuration file with the desired commands, and save it in a new file.

**Step 4** Copy the configuration file to the appropriate server location. For example, copy the file to the TFTP directory on the workstation (usually /tftpboot on a UNIX workstation).

**Step 5** Make sure the permissions on the file are set to world-read.

# Copying Configuration Files By Using TFTP

You can configure the switch by using configuration files you create, download from another switch, or download from a TFTP server. You can copy (upload) configuration files to a TFTP server for storage.


- Preparing to Download or Upload a Configuration File By Using TFTP, page 4-11
- Downloading the Configuration File By Using TFTP, page 4-12
- Uploading the Configuration File By Using TFTP, page 4-12


## Preparing to Download or Upload a Configuration File By Using TFTP

Before you begin downloading or uploading a configuration file by using TFTP, do these tasks:

- Ensure that the workstation acting as the TFTP server is properly configured. On a Sun workstation, make sure that the /etc/inetd.conf file contains this line:

  ```
  tftp dgram udp wait root /usr/etc/in.tftpd in.tftpd -p -s /tftpboot
  ```

  Make sure that the /etc/services file contains this line:

  ```
  tftp 69/udp
  ```

  **Note** You must restart the inetd daemon after modifying the /etc/inetd.conf and /etc/services files. To restart the daemon, either stop the inetd process and restart it, or enter a **fastboot** command (on the SunOS 4.x) or a **reboot** command (on Solaris 2.x or SunOS 5.x). For more information on the TFTP daemon, see the documentation for your workstation.

- Ensure that the switch has a route to the TFTP server. The switch and the TFTP server must be in the same subnetwork if you do not have a router to route traffic between subnets. Check connectivity to the TFTP server by using the **ping** command.
- Ensure that the configuration file to be downloaded is in the correct directory on the TFTP server (usually /tftpboot on a UNIX workstation).

- For download operations, ensure that the permissions on the file are set correctly. The permission on the file should be world-read.
- Before uploading the configuration file, you might need to create an empty file on the TFTP server. To create an empty file, enter the **touch** *filename* command, where *filename* is the name of the file you will use when uploading it to the server.
- During upload operations, if you are overwriting an existing file (including an empty file, if you had to create one) on the server, ensure that the permissions on the file are set correctly. Permissions on the file should be world-write.

## Downloading the Configuration File By Using TFTP

Follow this procedure to configure the switch by using a configuration file downloaded from a TFTP server.

### BEFORE YOU BEGIN

Verify that the TFTP server is properly configured by referring to the "Preparing to Download or Upload a Configuration File By Using TFTP" section on page 4-11.

### DETAILED STEPS

**Step 1** Copy the configuration file to the appropriate TFTP directory on the workstation.

**Step 2** Log into the switch through the console port or a Telnet session.

**Step 3** Download the configuration file from the TFTP server to configure the switch.

Specify the IP address or hostname of the TFTP server and the name of the file to download.

Use one of these privileged EXEC commands:

- **copy tftp:**[[[*//location*]*/directory*]*/filename*] **system:running-config**
- **copy tftp:**[[[*//location*]*/directory*]*/filename*] **nvram:startup-config**

The configuration file downloads, and the commands are executed as the file is parsed line-by-line.

### EXAMPLE

This example shows how to configure the software from the file *tokyo-confg* at IP address 172.16.2.155:

```
Switch# 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]
```

## Uploading the Configuration File By Using TFTP

Follow this procedure to upload a configuration file from a switch to a TFTP server for storage.

### BEFORE YOU BEGIN

Verify that the TFTP server is properly configured by referring to the "Preparing to Download or Upload a Configuration File By Using TFTP" section on page 4-11.

### DETAILED STEPS

**Step 1** Log into the switch through the console port or a Telnet session.

**Step 2** Upload the switch configuration to the TFTP server. Specify the IP address or hostname of the TFTP server and the destination filename.

Use one of these privileged EXEC commands:

- **copy system:running-config tftp:**[[[**//***location*]**/***directory*]**/***filename*]
- **copy nvram:startup-config tftp:**[[[**//***location*]**/***directory*]**/***filename*]

The file is uploaded to the TFTP server.

### EXAMPLE

This example shows how to upload a configuration file from a switch to a TFTP server:

```
Switch# 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]
```

## Copying Configuration Files By Using FTP

You can copy configuration files to or from an FTP server.

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 by using FTP, the Cisco IOS software sends the first valid username in this list:

- The username specified in the **copy** command if a username is specified.
- The username set by the **ip ftp username** *username* global configuration command if the command is configured.
- Anonymous.

The switch sends the first valid password in this list:

- The password specified in the **copy** command if a password is specified.
- The password set by the **ip ftp password** *password* global configuration command if the command is configured.
- The switch forms a password named *username@switchname.domain*. The variable *username* is the username associated with the current session, *switchname* is the configured hostname, 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 your FTP write request.

Use the **ip ftp username** and **ip ftp password** commands to specify a username and password for all copies. Include the username in the **copy** command if you want to specify only a username for that copy operation.

If the server has a directory structure, the configuration file is written to or copied from the directory associated with the username on the server. For example, if the configuration file resides in the home directory of a user on the server, specify that user's name as the remote username.

For more information, see the documentation for your FTP server.

This section includes the following topics:


- Preparing to Download or Upload a Configuration File By Using FTP, page 4-14
- Downloading a Configuration File By Using FTP, page 4-14
- Uploading a Configuration File By Using FTP, page 4-15


## Preparing to Download or Upload a Configuration File By Using FTP

Before you begin downloading or uploading a configuration file by using FTP, do these tasks:

- Ensure that the switch has a route to the FTP server. The switch and the FTP server must be in the same subnetwork if you do not have a router to route traffic between subnets. Check connectivity to the FTP server by using the **ping** command.
- If you are accessing the switch through the console or a Telnet session and you do not have a valid username, make sure that the current FTP username is the one that you want to use for the FTP download. You can enter the **show users** privileged EXEC command to view the valid username. If you do not want to use this username, create a new FTP username by using the **ip ftp username** *username* global configuration command during all copy operations. The new username is stored in NVRAM. If you are accessing the switch through a Telnet session and you have a valid username, this username is used, and you do not need to set the FTP username. Include the username in the **copy** command if you want to specify a username for only that copy operation.
- When you upload a configuration file to the FTP server, it must be properly configured to accept the write request from the user on the switch.

For more information, see the documentation for your FTP server.

## Downloading a Configuration File By Using FTP

### BEFORE YOU BEGIN

Verify that the FTP server is properly configured by referring to the "Preparing to Download or Upload a Configuration File By Using FTP" section on page 4-14.

### DETAILED STEPS

| | Command | Purpose |
|---|---|---|
| **Step 1** | | Log into the switch through the console port or a Telnet session. |
| **Step 2** | **configure terminal** | Enter global configuration mode on the switch.<br>This step is required only if you override the default remote username or password (see Steps 4, 5, and 6). |
| **Step 3** | **ip ftp username** *username* | (Optional) Change the default remote username. |
| **Step 4** | **ip ftp password** *password* | (Optional) Change the default password. |

| | Command | Purpose |
|---|---|---|
| Step 5 | **end** | Return to privileged EXEC mode. |
| Step 6 | **copy ftp:**[[[**//**[*username*[**:***password*]**@**]*location*]**/***directory*]**/***filename*] **system:running-config**<br>or<br>**copy ftp:**[[[**//**[*username*[**:***password*]**@**]*location*]**/***directory*]**/***filename*] **nvram:startup-config** | Using FTP, copy the configuration file from a network server to the running configuration or to the startup configuration file. |

### EXAMPLE

This example shows how to copy a configuration file named *host1-confg* from the *netadmin1* directory on the remote server with an IP address of 172.16.101.101 and to load and run those commands on the switch:

```
Switch# 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]
Switch#
%SYS-5-CONFIG: Configured from host1-config by ftp from 172.16.101.101
```

This example shows how to specify a remote username of *netadmin1*. The software copies the configuration file *host2-confg* from the *netadmin1* directory on the remote server with an IP address of 172.16.101.101 to the switch startup configuration.

```
Switch# configure terminal
Switch(config)# ip ftp username netadmin1
Switch(config)# ip ftp password mypass
Switch(config)# end
Switch# copy ftp: 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]
Switch#
%SYS-5-CONFIG_NV:Non-volatile store configured from host2-config by ftp from
172.16.101.101
```

## Uploading a Configuration File By Using FTP

### BEFORE YOU BEGIN

Verify that the FTP server is properly configured by referring to the "Preparing to Download or Upload a Configuration File By Using FTP" section on page 4-14.

### DETAILED STEPS

| | Command | Purpose |
|---|---|---|
| **Step 1** | | Log into the switch through the console port or a Telnet session. |
| **Step 2** | **configure terminal** | Enter global configuration mode.<br>This step is required only if you override the default remote username or password (see Steps 4, 5, and 6). |
| **Step 3** | **ip ftp username** *username* | (Optional) Change the default remote username. |
| **Step 4** | **ip ftp password** *password* | (Optional) Change the default password. |
| **Step 5** | **end** | Return to privileged EXEC mode. |
| **Step 6** | **copy system:running-config ftp:**[[[//[*username*[**:***password*]@]*location*]*/directory*]*/filename*]<br>or<br>**copy nvram:startup-config ftp:**[[[//[*username*[**:***password*]@]*location*]*/directory*]*/filename*] | Using FTP, store the switch running or startup configuration file to the specified location. |

### EXAMPLE

This example shows how to copy the running configuration file named *switch2-confg* to the *netadmin1* directory on the remote host with an IP address of 172.16.101.101:

```
Switch# copy system:running-config ftp://netadmin1:mypass@172.16.101.101/switch2-confg
Write file switch2-confg on host 172.16.101.101?[confirm]
Building configuration...[OK]
Connected to 172.16.101.101
Switch#
```

This example shows how to store a startup configuration file on a server by using FTP to copy the file:

```
Switch# configure terminal
Switch(config)# ip ftp username netadmin2
Switch(config)# ip ftp password mypass
Switch(config)# end
Switch# copy nvram:startup-config ftp:
Remote host[]? 172.16.101.101
Name of configuration file to write [switch2-confg]?
Write file switch2-confg on host 172.16.101.101?[confirm]
![OK]
```

# Copying Configuration Files By Using RCP

The RCP provides another method of downloading, uploading, and copying configuration files between remote hosts and the switch. Unlike TFTP, which uses User Datagram Protocol (UDP), a connectionless protocol, RCP uses TCP, which is connection-oriented.

To use RCP to copy files, the server from or to which you will be copying files must support RCP. The RCP copy commands rely on the rsh server (or daemon) on the remote system. To copy files by using RCP, you do not need to create a server for file distribution as you do with TFTP. You only need 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.

The RCP requires a client to send a remote username with each RCP request to a server. When you copy a configuration file from the switch to a server, the Cisco IOS software sends the first valid username in this list:

- The username specified in the **copy** command if a username is specified.
- The username set by the **ip rcmd remote-username** *username* global configuration command if the command is configured.
- The remote username associated with the current TTY (terminal) process. For example, if the user is connected to the router through Telnet and was authenticated through the **username** command, the switch software sends the Telnet username as the remote username.
- The switch hostname.

For a successful RCP copy request, you must define an account on the network server for the remote username. If the server has a directory structure, the configuration file is written to or copied from the directory associated with the remote username on the server. For example, if the configuration file is in the home directory of a user on the server, specify that user's name as the remote username.

This section includes the following topics:

- Preparing to Download or Upload a Configuration File By Using RCP, page 4-17
- Downloading a Configuration File By Using RCP, page 4-18
- Uploading a Configuration File By Using RCP, page 4-19

## Preparing to Download or Upload a Configuration File By Using RCP

Before you begin downloading or uploading a configuration file by using RCP, do these tasks:

- Ensure that the workstation acting as the RCP server supports the remote shell (rsh).
- Ensure that the switch has a route to the RCP server. The switch and the server must be in the same subnetwork if you do not have a router to route traffic between subnets. Check connectivity to the RCP server by using the **ping** command.
- If you are accessing the switch through the console or a Telnet session and you do not have a valid username, make sure that the current RCP username is the one that you want to use for the RCP download. You can enter the **show users** privileged EXEC command to view the valid username. If you do not want to use this username, create a new RCP username by using the **ip rcmd remote-username** *username* global configuration command to be used during all copy operations. The new username is stored in NVRAM. If you are accessing the switch through a Telnet session and you have a valid username, this username is used, and you do not need to set the RCP username. Include the username in the **copy** command if you want to specify a username for only that copy operation.
- When you upload a file to the RCP server, it 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 that the switch contains these configuration lines:

```
hostname Switch1
ip rcmd remote-username User0
```

  If the switch IP address translates to *Switch1.company.com*, the .rhosts file for User0 on the RCP server should contain this line:

```
Switch1.company.com Switch1
```

For more information, see the documentation for your RCP server.

## Downloading a Configuration File By Using RCP

### BEFORE YOU BEGIN

Verify that the RCP server is properly configured by referring to the "Preparing to Download or Upload a Configuration File By Using RCP" section on page 4-17.

### DETAILED STEPS

| | Command | Purpose |
|---|---|---|
| **Step 1** | | Log into the switch through the console port or a Telnet session. |
| **Step 2** | **configure terminal** | Enter global configuration mode.<br>This step is required only if you override the default remote username (see Steps 4 and 5). |
| **Step 3** | **ip rcmd remote-username** *username* | (Optional) Specify the remote username. |
| **Step 4** | **end** | Return to privileged EXEC mode. |
| **Step 5** | **copy rcp:**[[[//[*username*@]*location*]/*directory*]/*filename*] **system:running-config**<br>or<br>**copy rcp:**[[[//[*username*@]*location*]/*directory*]/*filename*] **nvram:startup-config** | Using RCP, copy the configuration file from a network server to the running configuration or to the startup configuration file. |

### EXAMPLE

This example shows how to copy a configuration file named *host1-confg* from the *netadmin1* directory on the remote server with an IP address of 172.16.101.101 and load and run those commands on the switch:

```
Switch# 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]
Switch#
%SYS-5-CONFIG: Configured from host1-config by rcp from 172.16.101.101
```

This example shows how to specify a remote username of *netadmin1*. Then it copies the configuration file *host2-confg* from the *netadmin1* directory on the remote server with an IP address of 172.16.101.101 to the startup configuration:

```
Switch# configure terminal
Switch(config)# ip rcmd remote-username netadmin1
Switch(config)# end
Switch# 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]
Switch#
%SYS-5-CONFIG_NV:Non-volatile store configured from host2-config by rcp from
172.16.101.101
```

## Uploading a Configuration File By Using RCP

### BEFORE YOU BEGIN

Verify that the RCP server is properly configured by referring to the "Preparing to Download or Upload a Configuration File By Using RCP" section on page 4-17.

### DETAILED STEPS

| | Command | Purpose |
|---|---|---|
| **Step 1** | | Log into the switch through the console port or a Telnet session. |
| **Step 2** | **configure terminal** | Enter global configuration mode.<br>This step is required only if you override the default remote username (see Steps 4 and 5). |
| **Step 3** | **ip rcmd remote-username** *username* | (Optional) Specify the remote username. |
| **Step 4** | **end** | Return to privileged EXEC mode. |
| **Step 5** | **copy system:running-config rcp:**[[[//[*username*@]*location*]/*directory*]/*filename*]<br>or<br>**copy nvram:startup-config rcp:**[[[//[*username*@]*location*]/*directory*]/*filename*] | Using RCP, copy the configuration file from a switch running or startup configuration file to a network server. |

### EXAMPLE

This example shows how to copy the running configuration file named *switch2-confg* to the *netadmin1* directory on the remote host with an IP address of 172.16.101.101:

```
Switch# copy system:running-config rcp://netadmin1@172.16.101.101/switch2-confg
Write file switch-confg on host 172.16.101.101?[confirm]
Building configuration...[OK]
Connected to 172.16.101.101
Switch#
```

This example shows how to store a startup configuration file on a server:

```
Switch# configure terminal
Switch(config)# ip rcmd remote-username netadmin2
Switch(config)# end
Switch# copy nvram:startup-config rcp:
Remote host[]? 172.16.101.101
Name of configuration file to write [switch2-confg]?
```

```
Write file switch2-confg on host 172.16.101.101?[confirm]
![OK]
```

# Clearing Configuration Information

You can clear the configuration information from the startup configuration. If you reboot the switch with no startup configuration, the switch enters the setup program so that you can reconfigure the switch with all new settings.

## Clearing the Startup Configuration File

To clear the contents of your startup configuration, use the **erase nvram:** or the **erase startup-config** privileged EXEC command.

**Caution** You cannot restore the startup configuration file after it has been deleted.

## Deleting a Stored Configuration File

To delete a saved configuration from flash memory, use the **delete flash:***filename* privileged EXEC command. Depending on the setting of the **file prompt** global configuration command, you might be prompted for confirmation before you delete a file. By default, the switch prompts for confirmation on destructive file operations.

**Caution** You cannot restore a file after it has been deleted.

# Replacing and Rolling Back Configurations

The configuration replacement and rollback feature replaces the running configuration with any saved Cisco IOS configuration file. You can use the rollback function to roll back to a previous configuration.

This section includes the following topics:


- Information About Configuration Replacement and Rollback, page 4-20
- Configuration Replacement and Rollback Guidelines, page 4-22
- Configuring the Configuration Archive, page 4-22
- Performing a Configuration Replacement or Rollback Operation, page 4-23


## Information About Configuration Replacement and Rollback


- Archiving a Configuration, page 4-21
- Replacing a Configuration, page 4-21
- Rolling Back a Configuration, page 4-21

### Archiving a Configuration

The configuration archive provides a mechanism to store, organize, and manage an archive of configuration files. The **configure replace** privileged EXEC command increases the configuration rollback capability. As an alternative, you can save copies of the running configuration by using the **copy running-config** *destination-url* privileged EXEC command, storing the replacement file either locally or remotely. However, this method lacks any automated file management. The configuration replacement and rollback feature can automatically save copies of the running configuration to the configuration archive.

You use the **archive config** privileged EXEC command to save configurations in the configuration archive by 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. You can specify how many versions of the running configuration are kept in the archive. After the maximum number of files are saved, the oldest file is automatically deleted when the next, most recent file is saved. The **show archive** privileged EXEC command displays information for all the configuration files saved in the configuration archive.

The Cisco IOS configuration archive, in which the configuration files are stored and available for use with the **configure replace** command, is in any of these file systems: FTP, HTTP, RCP, TFTP.

### Replacing a Configuration

The **configure replace** privileged EXEC command replaces the running configuration with any saved configuration file. When you enter the **configure replace** command, the running configuration is compared with the specified replacement configuration, and a set of configuration differences is generated. The resulting differences are used to replace the configuration. The configuration replacement operation is usually completed in no more than three passes. To prevent looping behavior no more than five passes are performed.

You can use the **copy** *source-url* **running-config** privileged EXEC command to copy a stored configuration file to the running configuration. When using this command as an alternative to the **configure replace** *target-url* privileged EXEC command, note these major differences:

- The **copy** *source-url* **running-config** command is a merge operation and preserves all the commands from both the source file and the running configuration. This command does not remove commands from the running configuration that are not present in the source file. In contrast, the **configure replace** *target-url* command removes commands from the running configuration that are not present in the replacement file and adds commands to the running configuration that are not present.
- You can use a partial configuration file as the source file for the **copy** *source-url* **running-config** command. You must use a complete configuration file as the replacement file for the **configure replace** *target-url* command.

### Rolling Back a Configuration

You can also use the **configure replace** command to roll back changes that were made since the previous configuration was saved. Instead of basing the rollback operation on a specific set of changes that were applied, the configuration rollback capability reverts to a specific configuration based on a saved configuration file.

If you want the configuration rollback capability, you must first save the running configuration before making any configuration changes. Then, after entering configuration changes, you can use that saved configuration file to roll back the changes by using the **configure replace** *target-url* command.

You can specify any saved configuration file as the rollback configuration. You are not limited to a fixed number of rollbacks, as is the case in some rollback models.

## Configuration Replacement and Rollback Guidelines

- Make sure that the switch has free memory larger than the combined size of the two configuration files (the running configuration and the saved replacement configuration). Otherwise, the configuration replacement operation fails.
- Make sure that the switch also has sufficient free memory to execute the configuration replacement or rollback configuration commands.
- Certain 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.
  - A configuration replacement operation cannot remove the **interface** *interface-id* command line from the running configuration if that interface is physically present on the device.
  - The **interface** *interface-id* command line cannot be added to the running configuration if no such interface is physically present on the device.
- When using the **configure replace** command, you must specify a saved configuration as the replacement configuration file for the 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).

**Note** If you generate the replacement configuration file externally, it must comply with the format of files generated by Cisco IOS devices.

## Configuring the Configuration Archive

Using the **configure replace** command with the configuration archive and with the **archive config** command is optional but offers significant benefit for configuration rollback scenarios. Before using the **archive config command**, you must first configure the configuration archive.

### BEFORE YOU BEGIN

Review the "Replacing and Rolling Back Configurations" section on page 4-20.

### DETAILED STEPS

| | Command | Purpose |
|---|---|---|
| Step 1 | **configure terminal** | Enter global configuration mode. |
| Step 2 | **archive** | Enter archive configuration mode. |
| Step 3 | **path** *url* | Specify the location and filename prefix for the files in the configuration archive. |

| | Command | Purpose |
|---|---|---|
| Step 4 | **maximum** *number* | (Optional) Set the maximum number of archive files of the running configuration to be saved in the configuration archive.<br>*number*—Maximum files of the running configuration file in the configuration archive. Valid values are from 1 to 14. The default is 10.<br>**Note** Before using this command, you must first enter the **path** archive configuration command to specify the location and filename prefix for the files in the configuration archive. |
| Step 5 | **time-period** *minutes* | (Optional) Set the time increment for automatically saving an archive file of the running configuration in the configuration archive.<br>*minutes*—Specify how often, in minutes, to automatically save an archive file of the running configuration in the configuration archive. |
| Step 6 | **end** | Return to privileged EXEC mode. |
| Step 7 | **show running-config** | Verify the configuration. |
| Step 8 | **copy running-config startup-config** | (Optional) Save your entries in the configuration file. |

### EXAMPLE

The following example shows how to specify the hostname, date, and time as the filename prefix for which to save archive files of the running configuration. In this example, the time-period command is also configured to automatically save an archive file of the running configuration every 20 minutes.

```
Switch(config)# archive
Switch (config-archive)# path disk0:$h$t
Switch (config-archive)# time-period 20
Switch (config-archive)# end
```

## Performing a Configuration Replacement or Rollback Operation

### BEFORE YOU BEGIN

Before using the **archive config command**, you must first enter the **path** archive configuration command as described in "Configuring the Configuration Archive" procedure on page 4-22.

### DETAILED STEPS

| | Command | Purpose |
|---|---|---|
| Step 1 | **archive config** | (Optional) Save the running configuration file to the configuration archive.<br>**Note** Enter the **path** archive configuration command before using this command. |
| Step 2 | **configure terminal** | Enter global configuration mode. |
| Step 3 | | Make necessary changes to the running configuration. |
| Step 4 | **exit** | Return to privileged EXEC mode. |

| | Command | Purpose |
|---|---|---|
| Step 5 | **configure replace** *target-url* [**list**] [**force**] [**time** *seconds*] [**nolock**] | Replace the running configuration file with a saved configuration file.<br>*target-url*—URL (accessible by the file system) of the saved configuration file that is to replace the running configuration, such as the configuration file created in Step 2 by using the **archive config** privileged EXEC command.<br>**list**—Display a list of the command entries applied by the software parser during each pass of the configuration replacement operation. The total number of passes also appears.<br>**force**— Replace the running configuration file with the specified saved configuration file without prompting you for confirmation.<br>**time** *seconds*—Specify the time (in seconds) within which you must enter the **configure confirm** command to confirm replacement of the running configuration file. If you do not enter the **configure confirm** command within the specified time limit, the configuration replacement operation is automatically stopped. (In other words, the running configuration file is restored to the configuration that existed before you entered the **configure replace** command).<br>**Note** You must first enable the configuration archive before you can use the **time** *seconds* command line option.<br>**nolock**—Disable the locking of the running configuration file that prevents other users from changing the running configuration during a configuration replacement operation. |
| Step 6 | **configure confirm** | (Optional) Confirm replacement of the running configuration with a saved configuration file.<br>**Note** Use this command only if the **time** *seconds* keyword and argument of the **configure replace** command are specified. |
| Step 7 | **copy running-config startup-config** | (Optional) Save your entries in the configuration file. |

## EXAMPLE

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. Note that the generated output of the **configure replace** command indicates that only one pass was performed to complete the rollback operation.

**Note** The path command must be configured before using the **archive config** command.

You first save the current running configuration in the configuration archive as follows:

```
Switch# archive config
```

You then enter configuration changes as shown in the following example:

```
Switch# configure terminal
Switch(config)# user netops2 password rain
Switch(config)# user netops3 password snow
```

```
Switch(config)# exit
```

After making changes to the running configuration file, you might 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 target file. The **configure replace** command is then used to revert to the target configuration file as shown in the following example:

```
Switch# show archive
There are currently 1 archive configurations saved.
The next archive file will be named disk0:myconfig-2
 Archive #  Name
   0
   1       disk0:myconfig-1 <- Most Recent
   2
   3
   4
   5
   6
   7
   8
   9
   10
Device# configure replace disk0:myconfig-1
Total number of passes: 1
Rollback Done
```

# Working with Software Images

This section describes how to archive (download and upload) software image files, which contain the system software, the Cisco IOS code, and the embedded device manager software.

**Note** Instead of using the **copy** privileged EXEC command or the **archive tar** privileged EXEC command, we recommend using the **archive download-sw** and **archive upload-sw** privileged EXEC commands to download and upload software image files.

You can download a switch image file from a TFTP, FTP, or RCP server to upgrade the switch software. For information about upgrading your switch by using a TFTP server, see the release notes for this release.

You can replace the current image with the new one or keep the current image in flash memory after a download.

You upload a switch image file to a TFTP, FTP, or RCP server for backup purposes. You can use this uploaded image for future downloads to the same switch or to another of the same type.

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 FTP and RCP are built on and use the TCP/IP stack, which is connection-oriented.

This section includes the following topics:


- Image Location on the Switch, page 4-26
- tar File Format of Images on a Server or Cisco.com, page 4-26
- Copying Image Files By Using TFTP, page 4-27
- Copying Image Files By Using FTP, page 4-31

- Copying Image Files By Using RCP, page 4-35

**Note** For a list of software images and the supported upgrade paths, see the release notes for your switch.

# Image Location on the Switch

The Cisco IOS image is stored as a *.bin* file in a directory that shows the version number. A subdirectory contains the files needed for web management. The image is stored on the system board flash memory (flash:).

You can use the **show version** privileged EXEC command to see the software version that is currently running on your switch. In the display, check the line that begins with `System image file is...` . It shows the directory name in flash memory where the image is stored.

You can also use the **dir** *filesystem***:** privileged EXEC command to see the directory names of other software images that you might have stored in flash memory.

# tar File Format of Images on a Server or Cisco.com

Software images located on a server or downloaded from Cisco.com are provided in a tar file format, which contains these files:

- An *info* file, which serves as a table of contents for the tar file
- One or more subdirectories containing other images and files, such as Cisco IOS images

This example shows some of the information contained in the info file. The following table provides additional details about this information:

```
version_suffix: image-name
version_directory: image-name
image_system_type_id: 0x00000000
image_name: image-name .bin
ios_image_file_size: 4526592
total_image_file_size: 4526592
image_feature: LAYER_2|MIN_DRAM_MEG=64
image_family: family
stacking_number: 1.11
board_ids: 0x00000029
info_end:
```

**Note** Disregard the stacking_number field. It does not apply to the switch.

| Field | Description |
|---|---|
| version_suffix | Specifies the Cisco IOS image version string suffix |
| version_directory | Specifies the directory where the Cisco IOS image and the HTML subdirectory are installed |
| image_name | Specifies the name of the Cisco IOS image within the tar file |
| ios_image_file_size | Specifies the Cisco IOS image size in the tar file, which is an approximate measure of how much flash memory is required to hold just the Cisco IOS image |

| Field | Description |
|---|---|
| total_image_file_size | Specifies the size of all the images (the Cisco IOS image and the web management files) in the tar file, which is an approximate measure of how much flash memory is required to hold them |
| image_feature | Describes the core functionality of the image |
| image_min_dram | Specifies the minimum amount of DRAM needed to run this image |
| image_family | Describes the family of products on which the software can be installed |

# Copying Image Files By Using TFTP

You can download a switch image from a TFTP server or upload the image from the switch to a TFTP server.

You download a switch image file from a server to upgrade the switch software. You can overwrite the current image with the new one or keep the current image after a download.

You upload a switch image file to a server for backup purposes; this uploaded image can be used for future downloads to the same or another switch of the same type.

**Note** Instead of using the **copy** privileged EXEC command or the **archive tar** privileged EXEC command, we recommend using the **archive download-sw** and **archive upload-sw** privileged EXEC commands to download and upload software image files.

This section includes the following topics:


- Preparing to Download or Upload an Image File By Using TFTP, page 4-27
- Downloading an Image File By Using TFTP, page 4-28
- Uploading an Image File By Using TFTP, page 4-30


## Preparing to Download or Upload an Image File By Using TFTP

Before you begin downloading or uploading an image file by using TFTP, do these tasks:

- Ensure that the workstation acting as the TFTP server is properly configured. On a Sun workstation, make sure that the /etc/inetd.conf file contains this line:

  ```
  tftp dgram udp wait root /usr/etc/in.tftpd in.tftpd -p -s /tftpboot
  ```

  Make sure that the /etc/services file contains this line:

  ```
  tftp 69/udp
  ```

  **Note** You must restart the inetd daemon after modifying the /etc/inetd.conf and /etc/services files. To restart the daemon, either stop the inetd process and restart it, or enter a **fastboot** command (on the SunOS 4.x) or a **reboot** command (on Solaris 2.x or SunOS 5.x). For more information on the TFTP daemon, see the documentation for your workstation.

- Ensure that the switch has a route to the TFTP server. The switch and the TFTP server must be in the same subnetwork if you do not have a router to route traffic between subnets. Check connectivity to the TFTP server by using the **ping** command.

- Ensure that the image to be downloaded is in the correct directory on the TFTP server (usually /tftpboot on a UNIX workstation).
- For download operations, ensure that the permissions on the file are set correctly. The permission on the file should be world-read.
- Before uploading the image file, you might need to create an empty file on the TFTP server. To create an empty file, enter the **touch** *filename* command, where *filename* is the name of the file you will use when uploading the image to the server.
- During upload operations, if you are overwriting an existing file (including an empty file, if you had to create one) on the server, ensure that the permissions on the file are set correctly. Permissions on the file should be world-write.

## Downloading an Image File By Using TFTP

You can download a new image file and replace the current image or keep the current image.

Follow Steps 1 through 3 to download a new image from a TFTP server and overwrite the existing image. To keep the current image, go to Step 4.

### BEFORE YOU BEGIN

Make sure the TFTP server is properly configured; see the "Preparing to Download or Upload an Image File By Using TFTP" section on page 4-27.

### DETAILED STEPS

| | Command | Purpose |
|---|---|---|
| **Step 1** | | Copy the image to the appropriate TFTP directory on the workstation. |
| **Step 2** | | Log into the switch through the console port or a Telnet session. |

| | Command | Purpose |
|---|---|---|
| Step 3 | **archive download-sw /overwrite /reload tftp:**[[**//***location*]**/***directory*]**/***image-name***.tar** | Download the image file from the TFTP server to the switch, and overwrite the current image.<br>• The **/overwrite** option overwrites the software image in flash memory with the downloaded image.<br>• The **/reload** option reloads the system after downloading the image unless the configuration has been changed and not been saved.<br>• For **//***location*, specify the IP address of the TFTP server.<br>• For **/***directory***/***image-name***.tar**, specify the directory (optional) and the image to download. Directory and image names are case sensitive. |
| Step 4 | **archive download-sw /leave-old-sw /reload tftp:**[[**//***location*]**/***directory*]**/***image-name***.tar** | Download the image file from the TFTP server to the switch, and keep the current image.<br>• The **/leave-old-sw** option keeps the old software version after a download.<br>• The **/reload** option reloads the system after downloading the image unless the configuration has been changed and not been saved.<br>• For **//***location*, specify the IP address of the TFTP server.<br>• For **/***directory***/***image-name***.tar**, specify the directory (optional) and the image to download. Directory and image names are case sensitive. |

The download algorithm verifies that the image is appropriate for the switch model and that enough DRAM is present, or it aborts the process and reports an error. If you specify the **/overwrite** option, the download algorithm removes the existing image on the flash device whether or not it is the same as the new one, downloads the new image, and then reloads the software.

**Note** If the flash device has sufficient space to hold two images and you want to overwrite one of these images with the same version, you must specify the **/overwrite** option.

If you specify the **/leave-old-sw**, the existing files are not removed. If there is not enough space to install the new image and keep the current running image, the download process stops, and an error message is displayed.

The algorithm installs the downloaded image on the system board flash device (flash:). The image is placed into a new directory named with the software version string, and the BOOT environment variable is updated to point to the newly installed image.

If you kept the old image during the download process (you specified the **/leave-old-sw** keyword), you can remove it by entering the **delete /force /recursive** *filesystem***:/***file-url* privileged EXEC command. For *filesystem*, use **flash:** for the system board flash device. For *file-url*, enter the directory name of the old image. All the files in the directory and the directory are removed.

**Caution** For the download and upload algorithms to operate properly, do *not* rename image names.

### EXAMPLE

This example shows how to download a new image from a TFTP server at 172.20.129.10 and to overwrite the image on the switch:

```
Switch# archive download-sw /overwrite tftp://172.20.129.10/test-image.tar
```

## Uploading an Image File By Using TFTP

You can upload an image from the switch to a TFTP server. You can later download this image to the switch or to another switch of the same type.

Use the upload feature only if the web management pages associated with the embedded device manager have been installed with the existing image.

### BEFORE YOU BEGIN

Make sure the TFTP server is properly configured; see the "Preparing to Download or Upload an Image File By Using TFTP" section on page 4-27.

### DETAILED STEPS

| | Command | Purpose |
|---|---|---|
| Step 1 | | Log into the switch through the console port or a Telnet session. |
| Step 2 | **archive upload-sw tftp:**[[**//***location*]**/***directory*]**/***image-name***.tar** | Upload the currently running switch image to the TFTP server.<br>• For **//***location*, specify the IP address of the TFTP server.<br>• For */directory/image-name***.tar**, specify the directory (optional) and the name of the software image to be uploaded. Directory and image names are case sensitive. The *image-name***.tar** is the name of the software image to be stored on the server. |

The **archive upload-sw** privileged EXEC command builds an image file on the server by uploading these files in order: info, the Cisco IOS image, and the web management files. After these files are uploaded, the upload algorithm creates the tar file format.

**Caution** For the download and upload algorithms to operate properly, do *not* rename image names.

### EXAMPLE

This example shows how to upload the currently running image to a TFTP server at 172.20.140.2:

```
Switch# archive upload-sw tftp://172.20.140.2/test-image.tar
```

# Copying Image Files By Using FTP

You can download a switch image from an FTP server or upload the image from the switch to an FTP server.

You download a switch image file from a server to upgrade the switch software. You can overwrite the current image with the new one or keep the current image after a download.

You upload a switch image file to a server for backup purposes. You can use this uploaded image for future downloads to the switch or another switch of the same type.

**Note** Instead of using the **copy** privileged EXEC command or the **archive tar** privileged EXEC command, we recommend using the **archive download-sw** and **archive upload-sw** privileged EXEC commands to download and upload software image files.

This section includes the following topics:


- Preparing to Download or Upload an Image File By Using FTP, page 4-31
- Downloading an Image File By Using FTP, page 4-32
- Uploading an Image File By Using FTP, page 4-34


## Preparing to Download or Upload an Image File By Using FTP

You can copy images files to or from an FTP server.

The FTP protocol requires a client to send a remote username and password on each FTP request to a server. When you copy an image file from the switch to a server by using FTP, the Cisco IOS software sends the first valid username in this list:

- The username specified in the **archive download-sw** or **archive upload-sw** privileged EXEC command if a username is specified.
- The username set by the **ip ftp username** *username* global configuration command if the command is configured.
- Anonymous.

The switch sends the first valid password in this list:

- The password specified in the **archive download-sw** or **archive upload-sw** privileged EXEC command if a password is specified.
- The password set by the **ip ftp password** *password* global configuration command if the command is configured.
- The switch forms a password named *username@switchname.domain*. The variable *username* is the username associated with the current session, *switchname* is the configured hostname, 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 you.

Use the **ip ftp username** and **ip ftp password** commands to specify a username and password for all copies. Include the username in the **archive download-sw** or **archive upload-sw** privileged EXEC command if you want to specify a username only for that operation.

If the server has a directory structure, the image file is written to or copied from the directory associated with the username on the server. For example, if the image file resides in the home directory of a user on the server, specify that user's name as the remote username.

Before you begin downloading or uploading an image file by using FTP, do these tasks:

- Ensure that the switch has a route to the FTP server. The switch and the FTP server must be in the same subnetwork if you do not have a router to route traffic between subnets. Check connectivity to the FTP server by using the **ping** command.
- If you are accessing the switch through the console or a Telnet session and you do not have a valid username, make sure that the current FTP username is the one that you want to use for the FTP download. You can enter the **show users** privileged EXEC command to view the valid username. If you do not want to use this username, create a new FTP username by using the **ip ftp username** *username* global configuration command. This new name will be used during all archive operations. The new username is stored in NVRAM. If you are accessing the switch through a Telnet session and you have a valid username, this username is used, and you do not need to set the FTP username. Include the username in the **archive download-sw** or **archive upload-sw** privileged EXEC command if you want to specify a username for that operation only.
- When you upload an image file to the FTP server, it must be properly configured to accept the write request from the user on the switch.

For more information, see the documentation for your FTP server.

## Downloading an Image File By Using FTP

You can download a new image file and overwrite the current image or keep the current image.

Follow Steps 1 through 6 to download a new image from an FTP server and overwrite the existing image. To keep the current image, go to Step 7.

### BEFORE YOU BEGIN

Verify that the FTP server is properly configured by referring to the "Preparing to Download or Upload an Image File By Using FTP" section on page 4-31.

### DETAILED STEPS

| | Command | Purpose |
|---|---|---|
| **Step 1** | | Log into the switch through the console port or a Telnet session. |
| **Step 2** | **configure terminal** | Enter global configuration mode.<br>This step is required only if you override the default remote username or password (see Steps 4, 5, and 6). |
| **Step 3** | **ip ftp username** *username* | (Optional) Change the default remote username. |
| **Step 4** | **ip ftp password** *password* | (Optional) Change the default password. |
| **Step 5** | **end** | Return to privileged EXEC mode. |

| | Command | Purpose |
|---|---|---|
| Step 6 | **archive download-sw /overwrite /reload ftp:**[[*//username*[**:***password*]*@location*]*/directory*]*/image-name*.**tar** | Download the image file from the FTP server to the switch, and overwrite the current image.<br>• The **/overwrite** option overwrites the software image in flash memory with the downloaded image.<br>• The **/reload** option reloads the system after downloading the image unless the configuration has been changed and not been saved.<br>• For **//***username*[**:***password*], specify the username and password; these must be associated with an account on the FTP server. For more information, see the "Preparing to Download or Upload an Image File By Using FTP" section on page 4-31.<br>• For @*location*, specify the IP address of the FTP server.<br>• For *directory*/*image-name*.**tar**, specify the directory (optional) and the image to download. Directory and image names are case sensitive. |
| Step 7 | **archive download-sw /leave-old-sw /reload ftp:**[[*//username*[**:***password*]*@location*]*/directory*]*/image-name*.**tar** | Download the image file from the FTP server to the switch, and keep the current image.<br>• The **/leave-old-sw** option keeps the old software version after a download.<br>• The **/reload** option reloads the system after downloading the image unless the configuration has been changed and not been saved.<br>• For **//***username*[**:***password*], specify the username and password. These must be associated with an account on the FTP server. For more information, see the "Preparing to Download or Upload an Image File By Using FTP" section on page 4-31.<br>• For @*location*, specify the IP address of the FTP server.<br>• For *directory*/*image-name*.**tar**, specify the directory (optional) and the image to download. Directory and image names are case sensitive. |

The download algorithm verifies that the image is appropriate for the switch model and that enough DRAM is present, or it aborts the process and reports an error. If you specify the **/overwrite** option, the download algorithm removes the existing image on the flash device, whether or not it is the same as the new one, downloads the new image, and then reloads the software.

**Note** If the flash device has sufficient space to hold two images and you want to overwrite one of these images with the same version, you must specify the **/overwrite** option.

If you specify the **/leave-old-sw**, the existing files are not removed. If there is not enough space to install the new image and keep the running image, the download process stops, and an error message is displayed.

The algorithm installs the downloaded image onto the system board flash device (flash:). The image is placed into a new directory named with the software version string, and the BOOT environment variable is updated to point to the newly installed image.

If you kept the old image during the download process (you specified the **/leave-old-sw** keyword), you can remove it by entering the **delete /force /recursive** *filesystem***:/***file-url* privileged EXEC command. For *filesystem*, use **flash:** for the system board flash device. For *file-url*, enter the directory name of the old software image. All the files in the directory and the directory are removed.

**Caution** For the download and upload algorithms to operate properly, do *not* rename image names.

### EXAMPLE

This example shows how to download a new image from an FTP server at 172.20.140.2 and to keep the old image:

```
Switch(config)# ip ftp username user1
Switch(config)# ip ftp password password1
Switch(config)# end
Switch# archive download-sw /leave-old-sw /reload
ftp://user1:password1@172.20.140.2]/new-image.tar
```

## Uploading an Image File By Using FTP

You can upload an image from the switch to an FTP server. You can later download this image to the same switch or to another switch of the same type.

### BEFORE YOU BEGIN

Use the upload feature only if the web management pages associated with the embedded device manager have been installed with the existing image.

Verify that the FTP server is properly configured by referring to the "Preparing to Download or Upload a Configuration File By Using FTP" section on page 4-14.

### DETAILED STEPS

| | Command | Purpose |
|---|---|---|
| **Step 1** | | Log into the switch through the console port or a Telnet session. |
| **Step 2** | **configure terminal** | Enter global configuration mode.<br>This step is required only if you override the default remote username or password (see Steps 4, 5, and 6). |
| **Step 3** | **ip ftp username** *username* | (Optional) Change the default remote username. |
| **Step 4** | **ip ftp password** *password* | (Optional) Change the default password. |

| | Command | Purpose |
|---|---|---|
| Step 5 | **end** | Return to privileged EXEC mode. |
| Step 6 | **archive upload-sw** **ftp:**[[*//*[*username*[**:***password*]@]*location*]*/directory*]*/image-name*.**tar** | Upload the currently running switch image to the FTP server.<br>• For *//username**:**password*, specify the username and password. These must be associated with an account on the FTP server. For more information, see the "Preparing to Download or Upload an Image File By Using FTP" section on page 4-31.<br>• For @*location*, specify the IP address of the FTP server.<br>• For */directory/image-name*.**tar**, specify the directory (optional) and the name of the software image to be uploaded. Directory and image names are case sensitive. The *image-name*.**tar** is the name of the software image to be stored on the server. |

The **archive upload-sw** command builds an image file on the server by uploading these files in order: info, the Cisco IOS image, and the web management files. After these files are uploaded, the upload algorithm creates the tar file format.

**Caution** For the download and upload algorithms to operate properly, do *not* rename image names.

### EXAMPLE

This example shows how to upload an image from the switch to the FTP server at 172.20.140.2:

```
Switch(config)# ip ftp username user1
Switch(config)# ip ftp password password1
Switch(config)# end
Switch# archive upload-sw ftp://user1:password1@172.20.140.2]/new-image.tar
```

# Copying Image Files By Using RCP

You can download a switch image from an RCP server or upload the image from the switch to an RCP server.

You download a switch image file from a server to upgrade the switch software. You can overwrite the current image with the new one or keep the current image after a download.

You upload a switch image file to a server for backup purposes. You can use this uploaded image for future downloads to the same switch or another of the same type.

**Note** Instead of using the **copy** privileged EXEC command or the **archive tar** privileged EXEC command, we recommend using the **archive download-sw** and **archive upload-sw** privileged EXEC commands to download and upload software image files.

This section includes the following topics:

- Preparing to Download or Upload an Image File By Using RCP, page 4-36
- Downloading an Image File By Using RCP, page 4-37
- Uploading an Image File By Using RCP, page 4-39

## Preparing to Download or Upload an Image File By Using RCP

RCP provides another method of downloading and uploading image files between remote hosts and the switch. Unlike TFTP, which uses User Datagram Protocol (UDP), a connectionless protocol, RCP uses TCP, which is connection-oriented.

To use RCP to copy files, the server from or to which you will be copying files must support RCP. The RCP copy commands rely on the rsh server (or daemon) on the remote system. To copy files by using RCP, you do not need to create a server for file distribution as you do with TFTP. You only need 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.

RCP requires a client to send a remote username on each RCP request to a server. When you copy an image from the switch to a server by using RCP, the Cisco IOS software sends the first valid username in this list:

- The username specified in the **archive download-sw** or **archive upload-sw** privileged EXEC command if a username is specified.
- The username set by the **ip rcmd remote-username** *username* global configuration command if the command is entered.
- The remote username associated with the current TTY (terminal) process. For example, if the user is connected to the router through Telnet and was authenticated through the **username** command, the switch software sends the Telnet username as the remote username.
- The switch hostname.

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 image file is written to or copied from the directory associated with the remote username on the server. For example, if the image file resides in the home directory of a user on the server, specify that user's name as the remote username.

Before you begin downloading or uploading an image file by using RCP, do these tasks:

- Ensure that the workstation acting as the RCP server supports the remote shell (rsh).
- Ensure that the switch has a route to the RCP server. The switch and the server must be in the same subnetwork if you do not have a router to route traffic between subnets. Check connectivity to the RCP server by using the **ping** command.
- If you are accessing the switch through the console or a Telnet session and you do not have a valid username, make sure that the current RCP username is the one that you want to use for the RCP download. You can enter the **show users** privileged EXEC command to view the valid username. If you do not want to use this username, create a new RCP username by using the **ip rcmd remote-username** *username* global configuration command to be used during all archive operations. The new username is stored in NVRAM. If you are accessing the switch through a Telnet session and you have a valid username, this username is used, and there is no need to set the RCP username. Include the username in the **archive download-sw** or **archive upload-sw** privileged EXEC command if you want to specify a username only for that operation.

- When you upload an image to the RCP to the server, it 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 these configuration lines:

```
hostname Switch1
ip rcmd remote-username User0
```

  If the switch IP address translates to *Switch1.company.com*, the .rhosts file for User0 on the RCP server should contain this line:

```
Switch1.company.com Switch1
```

For more information, see the documentation for your RCP server.

## Downloading an Image File By Using RCP

You can download a new image file and replace or keep the current image.

Follow Steps 1 through 5 to download a new image from an RCP server and overwrite the existing image. To keep the current image, go to Step 6.

### BEFORE YOU BEGIN

Verify that the RCP server is properly configured by referring to the "Preparing to Download or Upload an Image File By Using RCP" section on page 4-36.

### DETAILED STEPS

| | Command | Purpose |
|---|---|---|
| **Step 1** | | Log into the switch through the console port or a Telnet session. |
| **Step 2** | **configure terminal** | Enter global configuration mode.<br>This step is required only if you override the default remote username (see Steps 4 and 5). |
| **Step 3** | **ip rcmd remote-username** *username* | (Optional) Specify the remote username. |
| **Step 4** | **end** | Return to privileged EXEC mode. |

| | Command | Purpose |
|---|---|---|
| Step 5 | **archive download-sw /overwrite /reload rcp:**[[[**//**[*username*@]*location*]**/***directory*]**/***image-name*.**tar**] | Download the image file from the RCP server to the switch, and overwrite the current image.<br>• The **/overwrite** option overwrites the software image in flash memory with the downloaded image.<br>• The **/reload** option reloads the system after downloading the image unless the configuration has been changed and not been saved.<br>• For **//***username,* specify the username. For the RCP copy request to execute successfully, an account must be defined on the network server for the remote username. For more information, see the "Preparing to Download or Upload an Image File By Using RCP" section on page 4-36.<br>• For @*location*, specify the IP address of the RCP server.<br>• For **/***directory***/***image-name*.**tar**, specify the directory (optional) and the image to download. Directory and image names are case sensitive. |
| Step 6 | **archive download-sw /leave-old-sw /reload rcp:**[[[**//**[*username*@]*location*]**/***directory*]**/***image-name*.**tar**] | Download the image file from the RCP server to the switch, and keep the current image.<br>• The **/leave-old-sw** option keeps the old software version after a download.<br>• The **/reload** option reloads the system after downloading the image unless the configuration has been changed and not been saved.<br>• For **//***username,* specify the username. For the RCP copy request to execute, an account must be defined on the network server for the remote username. For more information, see the "Preparing to Download or Upload an Image File By Using RCP" section on page 4-36.<br>• For @*location*, specify the IP address of the RCP server.<br>• **For /***directory***/***image-name*.**tar**, specify the directory (optional) and the image to download. Directory and image names are case sensitive. |

The download algorithm verifies that the image is appropriate for the switch model and that enough DRAM is present, or it aborts the process and reports an error. If you specify the **/overwrite** option, the download algorithm removes the existing image on the flash device whether or not it is the same as the new one, downloads the new image, and then reloads the software.

**Note** If the flash device has sufficient space to hold two images and you want to overwrite one of these images with the same version, you must specify the **/overwrite** option.

If you specify the **/leave-old-sw**, the existing files are not removed. If there is not enough room to install the new image an keep the running image, the download process stops, and an error message is displayed.

The algorithm installs the downloaded image onto the system board flash device (flash:). The image is placed into a new directory named with the software version string, and the BOOT environment variable is updated to point to the newly installed image.

If you kept the old software during the download process (you specified the **/leave-old-sw** keyword), you can remove it by entering the **delete /force /recursive** *filesystem***:/***file-url* privileged EXEC command. For *filesystem*, use **flash:** for the system board flash device. For *file-url*, enter the directory name of the old software image. All the files in the directory and the directory are removed.

**Caution** For the download and upload algorithms to operate properly, do *not* rename image names.

### EXAMPLE

This example shows how to download a new image from an RCP server at 172.20.140.2 and to overwrite the old image:

```
Switch(config)# ip rcmd remote-username user1
Switch(config)# end
Switch# archive download-sw /overwrite /reload rcp://user1@172.20.140.2/new-image.tar
```

## Uploading an Image File By Using RCP

You can upload an image from the switch to an RCP server. You can later download this image to the same switch or to another switch of the same type.

Verify that the RCP server is properly configured by referring to the "Preparing to Download or Upload an Image File By Using RCP" section on page 4-36.

### BEFORE YOU BEGIN

The upload feature should be used only if the web management pages associated with the embedded device manager have been installed with the existing image.

### DETAILED STEPS

| | Command | Purpose |
|---|---|---|
| **Step 1** | | Log into the switch through the console port or a Telnet session. |
| **Step 2** | **configure terminal** | Enter global configuration mode.<br>This step is required only if you override the default remote username (see Steps 4 and 5). |
| **Step 3** | **ip rcmd remote-username** *username* | (Optional) Specify the remote username. |

| | Command | Purpose |
|---|---|---|
| Step 4 | **end** | Return to privileged EXEC mode. |
| Step 5 | **archive upload-sw rcp:**[[[**//**[*username*@]*location*]*/directory*]*/image-name*.**tar**] | Upload the currently running switch image to the RCP server.<br>• For **//***username,* specify the username; for the RCP copy request to execute, an account must be defined on the network server for the remote username. For more information, see the "Preparing to Download or Upload an Image File By Using RCP" section on page 4-36.<br>• For @*location*, specify the IP address of the RCP server.<br>• For **/***directory*]*/image-name*.**tar**, specify the directory (optional) and the name of the software image to be uploaded. Directory and image names are case sensitive.<br>• The *image-name*.**tar** is the name of software image to be stored on the server. |

The **archive upload-sw** privileged EXEC command builds an image file on the server by uploading these files in order: info, the Cisco IOS image, and the web management files. After these files are uploaded, the upload algorithm creates the tar file format.

**Caution** For the download and upload algorithms to operate properly, do *not* rename image names.

### EXAMPLE

This example shows how to upload an image from the switch to the RCP server at 172.20.140.2:

```
Switch(config)# ip rcmd remote-username user1
Switch(config)# end
Switch# archive upload-sw rcp://user1@172.20.140.2]/new-image.tar
```

# Related Documents

- Cisco IOS Master Command List, All Releases
- Configuration Fundamentals Configuration Guide, Cisco IOS Release 15M&T
- Secure Shell Configuration Guide, Cisco IOS Release 15M&T
- Cisco Connected Grid Switches System Management Software Configuration Guide

CHAPTER 5

# Troubleshooting

This chapter describes how to identify and resolve software problems related to the Cisco IOS software on the Cisco Industrial Ethernet 2000U Series Switches, hereafter referred to as IE 2000U or switch.

You can use the command-line interface (CLI) to identify and solve problems.

Additional troubleshooting information related to hardware is provided in the hardware installation guide.

**Note** For complete syntax and usage information for the commands used in this chapter, see the documents listed in the "Related Documents" section on page 5-23.


- Recovering from a Software Failure, page 5-2
- Recovering from a Lost or Forgotten Password, page 5-4

**Note** Recovery procedures require that you have physical access to the switch.

- Preventing Autonegotiation Mismatches, page 5-5
- Troubleshooting Power over Ethernet Switch Ports, page 5-5
- SFP Module Security and Identification, page 5-6
- Monitoring SFP Module Status, page 5-7
- Monitoring Temperature and Power Supplies, page 5-7
- Using Ping, page 5-8
- Using Layer 2 Traceroute, page 5-11
- Using IP Traceroute, page 5-13
- Using TDR, page 5-14
- Using Debug Commands, page 5-15
- Using the show platform forward Command, page 5-17
- Using the crashinfo File, page 5-19
- Using On-Board Failure Logging, page 5-20
- Related Documents, page 5-23

# Recovering from a Software Failure

Switch software can be corrupted during an upgrade, by downloading the wrong 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.

## Recovery Procedure at 115200 Baud Line Speed

This procedure uses the Xmodem Protocol at 115200 baud line speed to recover from a corrupt or wrong image file. There are many software packages that support the Xmodem Protocol, and this procedure is largely dependent on the emulation software that you are using.

This recovery procedure requires that you have physical access to the switch.

**Step 1** From your PC, download the software image tar file (*image_filename.tar*) from Cisco.com.

The Cisco IOS image is stored as a bin file in a directory in the tar file. For information about locating the software image files on Cisco.com, see the release notes.

**Step 2** Extract the bin file from the tar file.

- If you are using Windows, use a zip program that can read a tar file. Use the zip program to navigate to and extract the bin file.
- If you are using UNIX, follow these steps:

  1. Display the contents of the tar file by using the **tar -tvf** <*image_filename.tar*> UNIX command.

     ```
     unix-1% tar -tvf image_filename.tar
     ```

  2. Locate the bin file, and extract it by using the **tar -xvf** <*image_filename.tar*> <*image_filename.bin*> UNIX command.

     ```
     unix-1% tar -xvf image_filename.tar image_filename.bin
     x ies-lanbase-mz.122-53.SX/ies-ipservices-mz.122-53.SX.bin, 2928176 bytes, 5720
     tape blocks
     ```

  3. Verify that the bin file was extracted by using the **ls -l** <*image_filename.bin*> UNIX command.

     ```
     unix-1% ls -l image_filename.bin
     -rwxr-xr-x   1 bschuett eng      6365325 May 19 13:03
     ies-lanbase-mz.122-53.SX/ies-ipservices-mz.122-53.SX.bin
     ```

**Step 3** Connect your PC with terminal-emulation software supporting the Xmodem Protocol to the switch console port through a connection at 9600 bps. (The remaining steps assume the use of a HyperTerminal.)

**Step 4** Ensure that the switch is in boot loader mode. If it is not, use *one* of these methods to the access boot loader mode:

- Use the **boot manual** global configuration command.
- Disconnect and then reconnect the switch power cord. After the switch performs POST, the switch begins the autoboot process. The boot loader prompts the user for a break key character during the boot-up sequence, as shown in this example:

  ```
  ***** The system will autoboot in 15 seconds *****

  Send a break key to prevent autobooting.
  ```

  On a PC, use Ctrl-Break. On a SUN work station running UNIX, use Ctrl-C.

**Step 5** Use the **set BAUD 115200** boot loader command to increase the baud rate of the switch console connection from 9600 bps to 115200 bps.

**Step 6** Change the baud rate on the HyperTerminal to 115200 bps.

**Step 7** On the switch, start the file transfer by using the Xmodem Protocol.

```
switch: copy xmodem: flash:image_filename.bin
```

**Step 8** After the Xmodem request appears, use the appropriate command on the terminal-emulation software to start the transfer and to copy the software image into flash memory.

**Step 9** Boot the newly downloaded Cisco IOS image.

```
switch:boot flash:image_filename.bin
```

**Step 10** Use the **archive download-sw** privileged EXEC command to download the software image to the switch.

**Step 11** Use the **reload** privileged EXEC command to restart the switch and to verify that the new software image is operating properly.

**Step 12** Delete the flash:*image_filename.bin* file from the switch.

# Recovery Procedure at 9600 Baud Line Speed Using Express Setup

This procedure uses the Xmodem Protocol at 9600 baud line speed and the Express Setup button to recover from a corrupt or wrong image file. There are many software packages that support the Xmodem Protocol, and this procedure is largely dependent on the emulation software that you are using.

This recovery procedure requires that you have physical access to the switch.

**Step 1** From your PC, download the software image tar file (*image_filename.tar*) from Cisco.com.

The Cisco IOS image is stored as a bin file in a directory in the tar file. For information about locating the software image files on Cisco.com, see the release notes.

**Step 2** Extract the bin file from the tar file.

- If you are using Windows, use a zip program that can read a tar file. Use the zip program to navigate to and extract the bin file.
- If you are using UNIX, follow these steps:

  1. Display the contents of the tar file by using the **tar -tvf** <*image_filename.tar*> UNIX command.

     ```
     unix-1% tar -tvf image_filename.tar
     ```

  2. Locate the bin file, and extract it by using the **tar -xvf** <*image_filename.tar*> <*image_filename.bin*> UNIX command.

     ```
     unix-1% tar -xvf image_filename.tar image_filename.bin
     x ies-lanbase-mz.122-53.SX/ies-ipservices-mz.122-53.SX.bin, 2928176 bytes, 5720
     tape blocks
     ```

  3. Verify that the bin file was extracted by using the **ls -l** <*image_filename.bin*> UNIX command.

     ```
     unix-1% ls -l image_filename.bin
     -rwxr-xr-x   1 bschuett eng      6365325 May 19 13:03
     ies-lanbase-mz.122-53.SX/ies-ipservices-mz.122-53.SX.bin
     ```

**Step 3** Connect your PC with terminal-emulation software supporting the Xmodem Protocol to the switch console port.

**Step 4** Set the line speed on the emulation software to 9600 baud.

**Step 5** Unplug the switch power cord.

**Step 6** Press the **Express Setup** button and at the same time, reconnect the power cord to the switch.

You can release the **Express Setup** button a second or two after the LED above port 1 goes off. Several lines of information about the software appear along with instructions:

```
The system has been interrupted prior to initializing the flash file system. The following
commands will initialize the flash file system, and finish loading the operating system
software#

flash_init
load_helper
boot
```

**Step 7** Initialize the flash file system:

```
switch: flash_init
```

**Step 8** If you had set the console port speed to anything other than 9600, it has been reset to that particular speed. Change the emulation software line speed to match that of the switch console port.

**Step 9** Load any helper files:

```
switch: load_helper
```

**Step 10** Start the file transfer by using the Xmodem Protocol.

```
switch: copy xmodem: flash:image_filename.bin
```

**Step 11** After the Xmodem request appears, use the appropriate command on the terminal-emulation software to start the transfer and to copy the software image into flash memory.

**Step 12** Boot the newly downloaded Cisco IOS image.

```
switch:boot flash:image_filename.bin
```

**Step 13** Use the **archive download-sw** privileged EXEC command to download the software image to the switch.

**Step 14** Use the **reload** privileged EXEC command to restart the switch and to verify that the new software image is operating properly.

**Step 15** Delete the flash:*image_filename.bin* file from the switch.

# Recovering from a Lost or Forgotten Password

If you lose or forget your password, you can delete the switch password and set a new one.

Before you begin, make sure that:

- You have physical access to the switch.
- At least one switch port is enabled and is not connected to a device.

To delete the switch password and set a new one, follow these steps:

**Step 1** Press the **Express Setup** button until the SETUP LED blinks green and the LED of an available downlink port blinks green.

If no switch downlink port is available for your PC or laptop connection, disconnect a device from one of the other downlink ports. Press the **Express Setup** button again until the SETUP LED and the port LED blink green.

**Step 2** Connect your PC or laptop to the port with the blinking green LED.

The SETUP LED and the switch downlink port LED stop blinking and stay solid green.

**Step 3** Press and hold the **Express Setup** button. Notice that the SETUP LED starts blinking green again. Continue holding the button until the SETUP LED turns solid green (approximately 5 seconds). Release the **Express Setup** button immediately.

This procedure deletes the password without affecting any other configuration settings. You can now access the switch without a password through the console port or by using the device manager.

**Step 4** Enter a new password through the device manager by using the Express Setup window or through the command line interface by using the **enable secret** global configuration command.

# Preventing Autonegotiation Mismatches

The IEEE 802.3ab autonegotiation protocol manages the switch settings for speed (10, 100, and 1000 Mbps, 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 Power over Ethernet Switch Ports

These sections describe how to troubleshoot Power over Ethernet (PoE) ports.

## Disabled Port Caused by Power Loss

If a powered device (such as a Cisco IP Phone) that is connected to a PoE switch port and is 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. 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.

Use these commands to monitor the PoE port status:

- **show controllers power inline** privileged EXEC command
- **show power inline** privileged EXEC command
- **debug ilpower** privileged EXEC command

## 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.

Do not connect a Cisco powered device to a port that has been configured with the **power inline never** command.

# 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. For more information about error messages, see *Cisco System Messages*.

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. For more information about the **errdisable recovery** command, see the *Cisco IOS Configuration Fundamentals Command Reference*.

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 re-insert 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. For more information, see the **show interfaces transceiver** command in the *Cisco IOS Interface and Hardware Component Command Reference*.

# Monitoring Temperature and Power Supplies

The switch monitors the temperature conditions to determine the health of the power supplies. The temperature value is the temperature in the switch (not the external temperature). Enter the **show env temperature** or **show env all** privileged EXEC command to see if the temperature is okay or exceeds a temperature threshold.

This is an example of the output from the **show env temperature** command:

```
Switch# show env temperature
TEMPERATURE is OK
POWER SUPPLY 1A TEMPERATURE is Failure-Thermal
POWER SUPPLY 1B TEMPERATURE is OK
```

This is an example of output from the **show env all** command:

```
Switch# show env all
TEMPERATURE is OK
Temperature Value: 39 Degree Celsius
POWER SUPPLY 1A TEMPERATURE is Failure-Thermal POWER SUPPLY 1B TEMPERATURE is OK POWER
SUPPLY 1A Temperature Value: 97 Degree Celsius POWER SUPPLY 1A Critical Temperature
Thresh: 110 Degree Celsius POWER SUPPLY 1A Over Temperature Thresh: 95 Degree Celsius
POWER SUPPLY 1B Temperature Value: 45 Degree Celsius POWER SUPPLY 1B Critical Temperature
Thresh: 110 Degree Celsius POWER SUPPLY 1B Over Temperature Thresh: 95 Degree Celsius

SW  PID                 Serial#     Status           Sys Pwr  PoE Pwr  Watts
--  ------------------  ----------  ---------------  -------  -------  -----
1A  PWR-150-HV          DTM1348000B Failure-Thermal  Good     Good     75/65
1B  PWR-150-HV          DTM1348000C OK               Good     Good     75/65

ALARM CONTACT 1 is not asserted
ALARM CONTACT 2 is not asserted
ALARM CONTACT 3 is not asserted
ALARM CONTACT 4 is not asserted
```

The power supply temperature is monitored every 30 seconds. There are two temperature thresholds for power supplies:

- Warning threshold: 95 degree Celsius
- Critical threshold: 110 degree Celsius

If the critical threshold is surpassed, a syslog message is displayed every 30 seconds. When the warning threshold is crossed, a syslog message is displayed first, and if the condition persists, the syslog message is displayed every 2 minutes. If the power supply temperature reaches below the warning threshold, a syslog message is also displayed.

These are examples of syslog message that could be displayed:

```
Mar  1 00:04:50.203: %HARDWARE-5-PSU_THERMAL_NORMAL: Power Supply 1A Temperature is
within the acceptable limit
```

```
Mar  1 00:04:53.207: %HARDWARE-2-PSU_THERMAL_WARNING: Power Supply 1B temperature has
reached warning threshold
Mar  1 00:04:56.210: %HARDWARE-5-PSU_THERMAL_NORMAL: Power Supply 1B Temperature is
within the acceptable limit
Mar  1 00:04:56.210: %HARDWARE-5-PSU_THERMAL_CRITICAL: Power Supply 1B temperature has
reached critical threshold
```

You can use the CISCO-ENVMON-MIB and IDENTITY-MIB to receive traps that display information about temperatures, temperature thresholds, temperature sensors, and other related information. You must configure SNMP on the switch to access CISCO-ENVMON-MIB and IDENTITY-MIB objects. For more information, see the "Configuring SNMP" chapter in the *Cisco Connected Grid Switches System Management Software Configuration Guide*.

# Using Ping


- Information About Ping, page 5-8
- Using Ping, page 5-8


## Information About 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.

The switch also provides the Control Plane Security feature, which by default drops ping response packets received on user network interfaces (UNIs) or enhanced network interfaces (ENIs). However, methods are available to ping successfully from the switch to a host connected to a UNI or ENI.

Control Plane Security does not drop ping response packets to or from network node interfaces (NNIs), and no special configuration is required to enable pings to or from hosts connected to NNIs.

## Using Ping

Beginning in privileged EXEC mode, use the **ping** command to ping another device on the network from the switch:

| Command | Purpose |
|---|---|
| **ping** [*host* \| *address*] | Ping a remote host by supplying the hostname or IP network address.<br>**Note** Though other protocol keywords are available with the **ping** command, they are not supported in this release. |

**Note** Ping is not supported on a UNI or ENI configured as an IEEE 802.1Q tunnel port.

Ping is supported on NNIs on all software images.

It is important to note that the software images available for the switch provide different options for pinging a host connected to a UNI or ENI:

- LAN base
- IP services

The next sections apply to both access ports and trunk ports.

## All Software Versions

For all software images for the switch, you can use a Layer 3 service policy to enable pings from the switch to a host connected to a UNI or ENI.

**Note** For a switch running the IP services image, IP routing is not enabled by default and does not have to be enabled to use a Layer 3 service policy.

This example is one possible configuration:

```
switch# configure terminal
switch(config)# access list 101 permit ip any any
switch(config)# class-map match-any ping-class
switch(config-cmap)# match access-group 101
switch(config-cmap)# exit
switch(config)# policy-map ping-policy
switch(config-pmap)# class ping-class
switch(config-pmap-c)# police 1000000
switch(config-pmap-c)# exit
switch(config-pmap)# exit
switch(config)# int fa0/1
switch(config-if)# service-policy input ping-policy
switch(config-if)# switchport access vlan 2
switch(config-if)# no shut
switch(config-if)# exit
switch(config)# int vlan 2
switch(config-if)# ip address 192.168.1.1 255.255.255.0
switch(config-if)# end
switch# ping 192.168.1.2
```

## IP Services Image

When your switch is running the IP services image, you can use any of these methods:

- Apply a Layer 3 service policy to a UNI or ENI.
- Enable IP routing globally and ping from a switch virtual interface (SVI).
- Enable IP routing and ping from a routed port.

For a sample configuration of how to add a Layer 3 service policy to a UNI or ENI, see the "All Software Versions" section.

For examples using IP routing and pinging from an SVI or a routed port, see the next sections.

### IP Routing and SVI

IP routing is only supported when the switch is running the IP services image.

You can use this configuration to enable IP routing and enable pings from an SVI to a host connected to a UNI or ENI.

```
Switch# configure terminal
Switch(config)# ip routing
Switch(config)# int fa0/1
Switch(config-if)# switchport access vlan 2
Switch(config-if)# no shutdown
Switch(config-if)# int vlan 2
Switch(config-if)# ip address 192.168.1.1 255.255.255.0
Switch(config-if)# end
Switch# ping 192.168.1.2
```

With this configuration, a host with an IP address of 192.168.1.2 can be pinged from the switch.

### IP Routing and Routed Port

You can use this configuration to enable IP routing, change a switchport to a routed port, and permit pings from the switch to a connected host:

```
switch# configure terminal
switch(config)# int fa0/1
switch(config-if)# no switchport
switch(config-if)# ip address 192.168.1.1 255.255.255.0
switch(config-if)# no shutdown
switch(config-if)# exit
switch(config)# ip routing
switch(config)# end
switch# ping 192.168.1.2
```

## Ping Responses

This response is typical of a successful ping to a host:

```
Switch# ping 72.20.52.3
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
Switch#
```

An unsuccessful ping results in this message:

```
Switch# ping 72.20.52.3
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echoes to 172.20.52.3, timeout is 2 seconds:
. . . . .

Success rate is 0 percent (0/5)
```

## Summary

Keep these guidelines in mind while pinging:

- IP routing is available only with the IP services image and is disabled by default.
- To ping a host in a different IP subnetwork from the switch, you must have IP routing configured to route between the subnets, and a static route to the destination might also be appropriate. If you need to enable or configure IP routing, see the *Cisco Connected Grid Switches Unicast Routing Software Configuration Guide*.

- All software versions can use a Layer 3 service policy to permit pings to and from a host connected to a UNI or ENI. For more information about policy maps, see the "Input and Output Policies" section in the *Cisco Connected Grid Switches QoS Software Configuration Guide*.

If your switch is running the IP services image, use one of these methods to ping a host connected to a UNI or ENI:

- Use a Layer 3 service policy to permit pings to and from a host connected to a UNI or ENI.
- Enable global IP routing and configure a port as a routed port by using the **no switchport** interface configuration command.
- Enable global IP routing, create an SVI, and assign an IP address to it. For more information about SVIs, see the "Switch Virtual Interfaces" section in the *Cisco Connected Grid Switches Interfaces Software Configuration Guide*.

To end a ping session, simultaneously press and release the **Ctrl**, **Shift**, and **6** keys, and then press the **X** key.

# Using Layer 2 Traceroute


- Information About Layer 2 Traceroute, page 5-11
- Layer 2 Traceroute Usage Guidelines, page 5-11
- Displaying the Physical Path, page 5-12


## Information About 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. It 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.

**Note** Layer 2 traceroute is available only on NNIs.

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 Usage 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.

**Note** CDP is enabled by default on NNIs. You can enable CDP on ENIs, but UNIs do not support CDP.

For a list of switches that support Layer 2 traceroute, see the "Layer 2 Traceroute Usage Guidelines" section on page 5-11. If any devices in the physical path are transparent to CDP, the switch cannot identify the path through these devices. For more information about enabling CDP, see the Configuring CDP" in the *Cisco Connected Grid Switches System Management Software Configuration Guide*.

- 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.

# Displaying the Physical Path

You can display the physical path that a packet takes from a source device to a destination device by using one of these privileged EXEC commands:

- **tracetroute mac** [**interface** *interface-id*] {*source-mac-address*} [**interface** *interface-id*] {*destination-mac-address*} [**vlan** *vlan-id*] [**detail**]
- **tracetroute mac ip** {*source-ip-address* | *source-hostname*}{*destination-ip-address* | *destination-hostname*} [**detail**]

**Note** Layer 2 traceroute is available only on NNIs.

For more information, see the *Cisco IOS Configuration Fundamentals Command Reference*.

# Using IP Traceroute


- Information About IP Traceroute, page 5-13
- Executing IP Traceroute, page 5-13


## Information About 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 output. Intermediate switches do not show up in the 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 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 this 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.

## Executing IP Traceroute

Beginning in privileged EXEC mode, follow this step to trace that the path packets take through the network:

| Command | Purpose |
|---|---|
| **traceroute ip** *host* | Trace the path that packets take through the network. |

**Note** Though other protocol keywords are available with the **traceroute** privileged EXEC command, they are not supported in this release.

This example shows how to perform a **traceroute** to an IP host:

```
Switch# traceroute ip 171.9.15.10

Type escape sequence to abort.
Tracing the route to 171.69.115.10

  1 172.2.52.1 0 msec 0 msec 4 msec
  2 172.2.1.203 12 msec 8 msec 0 msec
  3 171.9.16.6 4 msec 0 msec 0 msec
  4 171.9.4.5 0 msec 4 msec 0 msec
  5 171.9.121.34 0 msec 4 msec 4 msec
  6 171.9.15.9 120 msec 132 msec 128 msec
  7 171.9.15.10 132 msec 128 msec 128 msec
Switch#
```

The display shows the hop count, IP address of the router, and the round-trip time in milliseconds for each of the three probes that are sent. The following table describes the **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.

# Using TDR


- Information About TDR, page 5-15
- Running TDR and Displaying the Results, page 5-15

## Information About TDR

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.

On the switch, TDR is supported only on the copper Ethernet 10/100 ports or on dual-purpose ports configured as 10/100/100 ports by using the RJ-45 connector.

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.

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

## Running TDR and Displaying the Results

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. For a description of the fields in the display, see the *Cisco IOS Interface and Hardware Component Command Reference*.

**Note** TDR is supported only on the copper Ethernet 10/100 ports or on dual-purpose ports configured as 10/100/100 ports by using the RJ-45 connector.

# Using Debug Commands


- Enabling Debugging on a Specific Feature, page 5-16
- Enabling All-System Diagnostics, page 5-16
- Redirecting Debug and Error Message Output, page 5-17


**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.

**Note** For complete syntax and usage information for specific **debug** commands, see the *Cisco IOS Debug Command Reference*.

# Enabling Debugging on a Specific Feature

All **debug** commands are entered in privileged EXEC mode, and most **debug** commands take no arguments. For example, beginning in privileged EXEC mode, enter this command to enable the debugging for Switched Port Analyzer (SPAN):

```
Switch# debug span-session
```

The switch continues to generate output until you enter the **no** form of the command.

If you enable a **debug** command and no output appears, consider these possibilities:

- The switch might not be properly configured to generate the type of traffic that you want to monitor. Use the **show running-config** command to check its configuration.
- Even if the switch is properly configured, it might not generate the type of traffic that you want to monitor during the particular period that debugging is enabled. Depending on the feature you are debugging, you can use commands such as the TCP/IP **ping** command to generate network traffic.

To disable debugging of SPAN, enter this command in privileged EXEC mode:

```
Switch# no debug span-session
```

Alternately, in privileged EXEC mode, you can enter the **undebug** form of the command:

```
Switch# undebug span-session
```

To display the state of each debugging option, enter this command in privileged EXEC mode:

```
Switch# show debugging
```

# Enabling All-System Diagnostics

Beginning in privileged EXEC mode, enter this command to enable all-system diagnostics:

```
Switch# debug all
```

**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.

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.

## 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.

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. Logging messages to the console produces very high overhead, whereas logging messages to a virtual terminal produces less overhead. Logging messages to a syslog server produces even less, and logging to an internal buffer produces the least overhead of any method.

For more information about system message logging, see the "Configuring System Message Logging" chapter in the *Cisco Connected Grid Switches System Management Software Configuration Guide*.

# 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 ASICs. However, packet forwarding information can also be helpful in troubleshooting.

This is an example of the output from the **show platform forward** command on Gigabit Ethernet port 1 in VLAN 5 when the packet entering that port is addressed to unknown MAC addresses. The packet should be flooded to all other ports in VLAN 5.

```
Switch# show platform forward gigabitethernet0/1 vlan 5 1.1.1 2.2.2 ip 13.1.1.1 13.2.2.2
udp 10 20
Global Port Number:24, Asic Number:5
Src Real Vlan Id:5, Mapped Vlan Id:5

Ingress:
 Lookup                    Key-Used                     Index-Hit  A-Data
InptACL  40_0D020202_0D010101-00_40000014_000A0000     01FFA   03000000
L2Local  80_00050002_00020002-00_00000000_00000000     00C71   0000002B
Station Descriptor:02340000, DestIndex:0239, RewriteIndex:F005

=========================================
Egress:Asic 2, switch 1
Output Packets:

-----------------------------------------
Packet 1
 Lookup                    Key-Used                     Index-Hit  A-Data
OutptACL 50_0D020202_0D010101-00_40000014_000A0000     01FFE   03000000

Port       Vlan      SrcMac          DstMac    Cos  Dscpv
Gi0/1    0005 0001.0001.0001  0002.0002.0002
```

```
----------------------------------------
Packet 2
 Lookup                   Key-Used                    Index-Hit  A-Data
OutptACL 50_0D020202_0D010101-00_40000014_000A0000     01FFE   03000000

Port       Vlan      SrcMac          DstMac    Cos  Dscpv
Gi0/2    0005 0001.0001.0001  0002.0002.0002

----------------------------------------
<output truncated>
----------------------------------------
Packet 10
 Lookup                   Key-Used                    Index-Hit  A-Data
OutptACL 50_0D020202_0D010101-00_40000014_000A0000     01FFE   03000000
Packet dropped due to failed DEJA_VU Check on Gi0/2
```

This is an example of the output when the packet coming in on Gigabit Ethernet port 1 in VLAN 5 is sent to an address already learned on the VLAN on another port. It should be forwarded from the port on which the address was learned.

```
Switch# show platform forward gigabitethernet0/1 vlan 5 1.1.1 0009.43a8.0145 ip 13.1.1.1
13.2.2.2 udp 10 20
Global Port Number:24, Asic Number:5
Src Real Vlan Id:5, Mapped Vlan Id:5

Ingress:
 Lookup                   Key-Used                    Index-Hit  A-Data
InptACL  40_0D020202_0D010101-00_40000014_000A0000     01FFA   03000000
L2Local  80_00050009_43A80145-00_00000000_00000000     00086   02010197
Station Descriptor:F0050003, DestIndex:F005, RewriteIndex:0003

========================================
Egress:Asic 3, switch 1
Output Packets:


----------------------------------------
Packet 1
 Lookup                   Key-Used                    Index-Hit  A-Data
OutptACL 50_0D020202_0D010101-00_40000014_000A0000     01FFE   03000000

Port       Vlan      SrcMac          DstMac    Cos  Dscpv
Gi0/2    0005 0001.0001.0001  0009.43A8.0145
```

This is an example of the output when the packet coming in on Gigabit Ethernet port 1 in VLAN 5 has a destination MAC address set to the router MAC address in VLAN 5 and the destination IP address unknown. Because there is no default route set, the packet should be dropped.

```
Switch# show platform forward gigabitethernet0/1 vlan 5 1.1.1 03.e319.ee44 ip 13.1.1.1
13.2.2.2 udp 10 20
Global Port Number:24, Asic Number:5
Src Real Vlan Id:5, Mapped Vlan Id:5

Ingress:
 Lookup                   Key-Used                    Index-Hit  A-Data
InptACL  40_0D020202_0D010101-00_41000014_000A0000     01FFA   03000000
L3Local  00_00000000_00000000-90_00001400_0D020202     010F0   01880290
L3Scndr  12_0D020202_0D010101-00_40000014_000A0000     034E0   000C001D_00000000
Lookup Used:Secondary
Station Descriptor:02260000, DestIndex:0226, RewriteIndex:0000
```

This is an example of the output when the packet coming in on Gigabit Ethernet port 1 in VLAN 5 has a destination MAC address set to the router MAC address in VLAN 5 and the destination IP address set to an IP address that is in the IP routing table. It should be forwarded as specified in the routing table.

```
Switch# show platform forward gigabitethernet0/1 vlan 5 1.1.1 03.e319.ee44 ip 110.1.5.5
16.1.10.5
Global Port Number:24, Asic Number:5
Src Real Vlan Id:5, Mapped Vlan Id:5

Ingress:
 Lookup                    Key-Used                      Index-Hit  A-Data
InptACL  40_10010A05_0A010505-00_41000014_000A0000     01FFA   03000000
L3Local  00_00000000_00000000-90_00001400_10010A05     010F0   01880290
L3Scndr  12_10010A05_0A010505-00_40000014_000A0000     01D28   30090001_00000000
Lookup Used:Secondary
Station Descriptor:F0070007, DestIndex:F007, RewriteIndex:0007

========================================
Egress:Asic 3, switch 1
Output Packets:

----------------------------------------
Packet 1
 Lookup                    Key-Used                      Index-Hit  A-Data
OutptACL 50_10010A05_0A010505-00_40000014_000A0000     01FFE   03000000

Port       Vlan      SrcMac          DstMac    Cos  Dscpv
Gi0/2    0007 XXXX.XXXX.0246  0009.43A8.0147
```

# Using the crashinfo File

The crashinfo file saves information that helps Cisco technical support representatives to debug problems that caused the Cisco IOS image to fail (crash). The switch writes the crash information to the console at the time of the failure, and the file is created the next time you boot the Cisco IOS image after the failure (instead of while the system is failing).

The information in the 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.

All crashinfo files are kept in this directory on the flash file system:

flash:/crashinfo/crashinfo_*n* where *n* is a sequence number.

Each new crashinfo file that is created uses a sequence number that is larger than any previously existing sequence number, so the file with the largest sequence number describes the most recent failure. Version numbers are used instead of a timestamp because the switches do not include a real-time clock. You cannot change the name of the file that the system will use when it creates the file. However, after the file is created, you can use the **rename** privileged EXEC command to rename it, but the contents of the renamed file will not be displayed by the **show tech-support** privileged EXEC command. You can delete crashinfo files by using the **delete** privileged EXEC command.

You can display the most recent crashinfo file (that is, the file with the highest sequence number at the end of its filename) by entering the **show tech-support** privileged EXEC command. You also can access the file by using any command that can copy or display files, such as the **more** or the **copy** privileged EXEC command.

# Using On-Board Failure Logging

You can use the on-board-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.

This section has this information:


- Information About OBFL, page 5-20
- Configuring OBFL, page 5-20
- Displaying OBFL Information, page 5-21


## Information About OBFL

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 switch
- Environmental data—Unique device identifier (UDI) information for a switch and for all the connected devices: the product identification (PID), the version identification (VID), and the serial number
- Message—Record of the hardware-related system messages generated by a switch
- Temperature—Temperature of a switch
- Uptime data—Time when a switch 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 switch

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.

When an OBFL-enabled switch is restarted, there is a 10-minute delay before logging of new data begins.

## Configuring OBFL

To enable OBFL, use the **hw-module module logging onboard** [**message level** *level*] global configuration command. 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 logging onboard module 1** *destination* privileged EXEC command.

**Caution** We recommend that you keep OBFL enabled and that you do not remove the data stored in the flash memory.

Beginning in privileged EXEC mode, follow these steps to enable and configure OBFL. Note that OBLF is enabled by default; you need to enable it only if it has been disabled.

| | Command | Purpose |
|---|---|---|
| Step 1 | **configure terminal** | Enter global configuration mode. |
| Step 2 | **hw-module module** [*slot-number*] **logging onboard** [**message** *level*] | Enable OBFL on the switch.<br>You can specify these optional parameters:<br>• (Optional) *slot-number*—The slot number is always 1 and is not relevant for the switch.<br>• (Optional) **message** *level*—Specify the severity level of messages to be generated and stored. The range is from 1 to 7, with 1 being the most severe. |
| Step 3 | **end** | Return to privileged EXEC mode. |
| Step 4 | **copy logging onboard module** [*slot-number*] *destination* | (Optional) Copy the OBFL data to the local network or a specific file system.<br>• (Optional) *slot-number*—The slot number is always 1 and is not relevant for the switch.<br>• *destination*—See the **copy logging onboard module** command for destination options. |
| Step 5 | **show logging onboard** | Verify your entries. |
| Step 6 | **copy running-config startup-config** | (Optional) Save your entries in the configuration file. |

To disable OBFL, use the **no hw-module module 1 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 logging onboard** privileged EXEC command.

# Displaying OBFL Information

To display the OBFL information, use one or more of the privileged EXEC commands in the following table.

**Note** When an OBFL-enabled switch is restarted, there is a 10-minute delay before logging of new data begins.

| Command | Purpose |
|---|---|
| **show logging onboard clilog** | Display the OBFL CLI commands that were entered on a switch. |
| **show logging onboard environment** | Display the UDI information for a standalone switch and for all the connected FRU devices: the PID, the VID, and the serial number. |

| Command | Purpose |
|---|---|
| **show logging onboard message** | Display the hardware-related messages generated by a switch. |
| **show logging onboard temperature** | Display the temperature of a switch. |
| **show logging onboard uptime** | Display the time when a switch starts, the reason the switch restarts, and the length of time that the switch has been running since it last restarted. |
| **show logging onboard voltage** | Display the system voltages of a switch. |

These are examples of output from the show logging onboard commands:

```
Switch# show logging onboard clilog
--------------------------------------------------------------------------------
CLI LOGGING SUMMARY INFORMATION
--------------------------------------------------------------------------------
COUNT COMMAND
--------------------------------------------------------------------------------
    1 hw-module module logging onboard
    1 hw-module module logging onboard message level 7
    4 show logging onboard
    1 show logging onboard message
    1 show logging onboard summary
--------------------------------------------------------------------------------

Switch# show logging onboard temp
--------------------------------------------------------------------------------
TEMPERATURE SUMMARY INFORMATION
--------------------------------------------------------------------------------
Number of sensors          : 1
Sampling frequency         : 5 minutes
Maximum time of storage    : 720 minutes
--------------------------------------------------------------------------------
Sensor                             |   ID  | Maximum Temperature 0C
--------------------------------------------------------------------------------
System                               1     41
--------------------------------------
Temp                         Sensor ID
0C     1
--------------------------------------
No historical data to display
--------------------------------------

Switch# show logging onboard uptime
--------------------------------------------------------------------------------
UPTIME SUMMARY INFORMATION
--------------------------------------------------------------------------------
First customer power on : 03/01/1993 00:06:06
Total uptime            :   0 years  20 weeks   4 days   6 hours  20 minutes
Total downtime          :   0 years   0 weeks   0 days   0 hours   0 minutes
Number of resets        : 90
Number of slot changes  : 0
Current reset reason    : 0x0
Current reset timestamp : 03/01/1993 00:05:43
Current slot            : 1
Current uptime          :   0 years   0 weeks   2 days   6 hours   0 minutes
--------------------------------------------------------------------------------
Reset  |        |
Reason | Count  |
--------------------------------------------------------------------------------
```

```
No historical data to display
-------------------------------------------------------------------------------

Switch# show logging onboard voltage
-------------------------------------------------------------------------------------------------
VOLTAGE SUMMARY INFORMATION
-------------------------------------------------------------------------------------------------
Number of sensors          : 6
Sampling frequency         : 1 minutes
Maximum time of storage    : 720 minutes
-------------------------------------------------------------------------------------------------
Sensor                              |   ID  | Maximum Voltage
-------------------------------------------------------------------------------------------------
12.00V                               0      12.567
1.25V                                2       1.258
3.30V                                3       3.305
2.50V                                4       2.517
1.80V                                5       1.825
1.50V                                6       1.508
-------------------------------------------------------------------------------------------------
Nominal Range                          Sensor ID

-------------------------------------------------------------------------------------------------
No historical data to display
-------------------------------------------------------------------------------------------------
```

# Related Documents

- Cisco IOS Master Command List, All Releases
- Cisco System Messages
- Cisco IOS Interface and Hardware Component Command Reference
- Cisco IOS Configuration Fundamentals Command Reference
- Cisco IOS Debug Command Reference
- Cisco Connected Grid Switches System Management Software Configuration Guide
- Cisco Connected Grid Switches Unicast Routing Software Configuration Guide
- Cisco Connected Grid Switches QoS Software Configuration Guide
- Cisco Connected Grid Switches Interfaces Software Configuration Guide