



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

This chapter describes how to manipulate the flash file system, how to copy configuration files, and how to archive (upload and download) software images on the Cisco Industrial Ethernet 2000U Series (IE 2000U) and Connected Grid Switches, hereafter referred to as 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 4-41.

- [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 4-41](#)
- [Feature History, page 4-42](#)

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 *Hardware Installation Guide* for your switch.

- [Displaying Available File Systems, page 4-2](#)
- [Detecting an Unsupported SD Flash Memory Card, page 4-3](#)
- [Setting the Default File System, page 4-4](#)
- [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 4-7](#)
- [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. flash —The file system is for a flash memory device. nvram —The file system is for a NVRAM device. opaque —The file system is a locally generated <i>pseudo</i> file system (for example, the <i>system</i>) or a download interface, such as brimux. unknown —The file system is an unknown type.

Field	Value
Flags	Permission for file system. ro —read-only. rw —read/write. wo —write-only.
Prefixes	Alias for file system. flash: —Flash file system. nvr: —NVRAM. null: —Null destination for copies. You can copy a remote file to null to find its size. rcp: —Remote Copy Protocol (RCP) network server. system: —Contains the system memory, including the running configuration. tftp: —TFTP network server. xmodem: —Obtain the file from a network machine by using the Xmodem protocol. ymodem: —Obtain the file from a network machine by using the Ymodem protocol.

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 sdfs** privileged EXEC command.

This example shows an unsupported SD flash memory card:

```
Switch# show platform sdfs
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 sdfs
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 sdfsflash** 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 sdfsflash** 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 <i>file-url</i>	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. For <i>filesystem:</i> , use flash: for the system board flash device.
Step 2	cd new_configs	Change to the directory of interest. The command example shows how to change to the directory named <i>new_configs</i> .
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. For <i>filesystem:</i> , use flash: for the system board flash device.
Step 2	mkdir old_configs	Create a new directory. The command example shows how to create the directory named <i>old_configs</i> . Directory names are case sensitive. 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:**, **rnp:**, and **tftp:** and have these syntaxes:

- FTP—**ftp:**[[//username [:password]@location]/directory]/filename
- RCP—**rnp:**[[//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 the 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 linenumbers
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 *System Management Software Configuration Guide for Cisco IE 2000U and Connected Grid Switches*.

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 4-11](#)
- [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 4-17](#)
- [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 4-13](#)

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] **nvrnram: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-config* at IP address 172.16.2.155:

```
Switch# copy tftp://172.16.2.155/tokyo-config system:running-config
```

```
Configure using tokyo-config from 172.16.2.155? [confirm] y
Booting tokyo-config 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-config
Write file tokyo-config on host 172.16.2.155? [confirm] y
#
Writing tokyo-config!!! [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 4-16](#)

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. 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 <i>username</i>	(Optional) Change the default remote username.
Step 4	ip ftp password <i>password</i>	(Optional) Change the default password.
Step 5	end	Return to privileged EXEC mode.
Step 6	copy ftp:[[/[username[:password]@]location]/directory]/filename system:running-config or copy ftp:[[/[username[:password]@]location]/directory]/filename nvrnram: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-config* 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-config system:running-config
Configure using host1-config from 172.16.101.101? [confirm]
Connected to 172.16.101.101
Loading 1112 byte file host1-config:[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-config* 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: nvrnram:startup-config
Address of remote host [255.255.255.255]? 172.16.101.101
Name of configuration file[rtr2-config]? host2-config
Configure using host2-config from 172.16.101.101?[confirm]
Connected to 172.16.101.101
Loading 1112 byte file host2-config:[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. 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 <i>username</i>	(Optional) Change the default remote username.
Step 4	ip ftp password <i>password</i>	(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] or 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-config* 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-config
Write file switch2-config 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-config]?
Write file switch2-config 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. This step is required only if you override the default remote username (see Steps 4 and 5).
Step 3	ip rcmd remote-username <i>username</i>	(Optional) Specify the remote username.
Step 4	end	Return to privileged EXEC mode.
Step 5	copy rcp: [[[/[<i>username@</i>] <i>location</i>]/ <i>directory</i>]/ <i>filename</i>] system:running-config or copy rcp: [[[/[<i>username@</i>] <i>location</i>]/ <i>directory</i>]/ <i>filename</i>] 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. This step is required only if you override the default remote username (see Steps 4 and 5).
Step 3	ip rcmd remote-username <i>username</i>	(Optional) Specify the remote username.
Step 4	end	Return to privileged EXEC mode.
Step 5	copy system:running-config rcp:[[[[<i>username@</i>]<i>location</i>]<i>directory</i>]<i>filename</i>] or copy nvram:startup-config rcp:[[[[<i>username@</i>]<i>location</i>]<i>directory</i>]<i>filename</i>]	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-config]?
Write file switch2-config 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 4-21](#)
- [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 4-22](#)

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 <i>url</i>	Specify the location and filename prefix for the files in the configuration archive.
Step 4	maximum <i>number</i>	(Optional) Set the maximum number of archive files of the running configuration to be saved in the configuration archive. <i>number</i> —Maximum files of the running configuration file in the configuration archive. Valid values are from 1 to 14. The default is 10. 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 <i>minutes</i>	(Optional) Set the time increment for automatically saving an archive file of the running configuration in the configuration archive. <i>minutes</i> —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. 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.
Step 5	configure replace <i>target-url</i> [list] [force] [time <i>seconds</i>] [no lock]	Replace the running configuration file with a saved configuration file. <i>target-url</i> —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. 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. force — Replace the running configuration file with the specified saved configuration file without prompting you for confirmation. time <i>seconds</i> —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). Note You must first enable the configuration archive before you can use the time <i>seconds</i> command line option. no lock—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. Note Use this command only if the time <i>seconds</i> 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 4-36](#)


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
<code>version_suffix</code>	Specifies the Cisco IOS image version string suffix
<code>version_directory</code>	Specifies the directory where the Cisco IOS image and the HTML subdirectory are installed
<code>image_name</code>	Specifies the name of the Cisco IOS image within the tar file
<code>ios_image_file_size</code>	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
<code>total_image_file_size</code>	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
<code>image_feature</code>	Describes the core functionality of the image
<code>image_min_dram</code>	Specifies the minimum amount of DRAM needed to run this image
<code>image_family</code>	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 4-28](#)
- [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 4-28.

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.
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. <ul style="list-style-type: none"> • The /overwrite option overwrites the software image in flash memory with the downloaded image. • The /reload option reloads the system after downloading the image unless the configuration has been changed and not been saved. • For <i>//location</i>, specify the IP address of the TFTP server. • For <i>/directory/image-name.tar</i>, 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. <ul style="list-style-type: none"> • The /leave-old-sw option keeps the old software version after a download. • The /reload option reloads the system after downloading the image unless the configuration has been changed and not been saved. • For <i>//location</i>, specify the IP address of the TFTP server. • For <i>/directory/image-name.tar</i>, 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 4-28.

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. <ul style="list-style-type: none"> For <i>/location</i>, specify the IP address of the TFTP server. For <i>/directory/image-name.tar</i>, specify the directory (optional) and the name of the software image to be uploaded. Directory and image names are case sensitive. The <i>image-name.tar</i> 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 4-35](#)

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 subnet 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. 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 <i>username</i>	(Optional) Change the default remote username.
Step 4	ip ftp password <i>password</i>	(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	<p>Download the image file from the FTP server to the switch, and overwrite the current image.</p> <ul style="list-style-type: none"> • The /overwrite option overwrites the software image in flash memory with the downloaded image. • The /reload option reloads the system after downloading the image unless the configuration has been changed and not been saved. • For <i>//username[:password]</i>, 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. • For <i>@location</i>, specify the IP address of the FTP server. • For <i>directory/image-name.tar</i>, 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	<p>Download the image file from the FTP server to the switch, and keep the current image.</p> <ul style="list-style-type: none"> • The /leave-old-sw option keeps the old software version after a download. • The /reload option reloads the system after downloading the image unless the configuration has been changed and not been saved. • For <i>//username[:password]</i>, 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. • For <i>@location</i>, specify the IP address of the FTP server. • For <i>directory/image-name.tar</i>, 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. 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 <i>username</i>	(Optional) Change the default remote username.
Step 4	ip ftp password <i>password</i>	(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	<p>Upload the currently running switch image to the FTP server.</p> <ul style="list-style-type: none"> For <i>//username:password</i>, 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. For <i>@location</i>, specify the IP address of the FTP server. For <i>/directory/image-name.tar</i>, specify the directory (optional) and the name of the software image to be uploaded. Directory and image names are case sensitive. The <i>image-name.tar</i> 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 4-37](#)
- [Downloading an Image File By Using RCP, page 4-38](#)
- [Uploading an Image File By Using RCP, page 4-40](#)

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 4-37.

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. This step is required only if you override the default remote username (see Steps 4 and 5).
Step 3	ip rcmd remote-username <i>username</i>	(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]	<p>Download the image file from the RCP server to the switch, and overwrite the current image.</p> <ul style="list-style-type: none"> • The /overwrite option overwrites the software image in flash memory with the downloaded image. • The /reload option reloads the system after downloading the image unless the configuration has been changed and not been saved. • For <i>//username</i>, 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 4-37. • For <i>@location</i>, specify the IP address of the RCP server. • For <i>/directory/image-name.tar</i>, 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]	<p>Download the image file from the RCP server to the switch, and keep the current image.</p> <ul style="list-style-type: none"> • The /leave-old-sw option keeps the old software version after a download. • The /reload option reloads the system after downloading the image unless the configuration has been changed and not been saved. • For <i>//username</i>, 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 4-37. • For <i>@location</i>, specify the IP address of the RCP server. • For <i>/directory/image-name.tar</i>, 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 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 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 4-37.

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. This step is required only if you override the default remote username (see Steps 4 and 5).
Step 3	ip rcmd remote-username <i>username</i>	(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. <ul style="list-style-type: none"> For <i>//username</i>, 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 4-37. For <i>@location</i>, specify the IP address of the RCP server. For <i>/directory/image-name.tar</i>, specify the directory (optional) and the name of the software image to be uploaded. Directory and image names are case sensitive. The <i>image-name.tar</i> 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](#)
- [System Management Software Configuration Guide for Cisco IE 2000U and Connected Grid Switches](#)

Feature History

Platform	First Supported Release
IE 2000U	Cisco IOS Release 15.0(2)EH
CGS 2520	Cisco IOS Release 12.2(53)EX
Ethernet Switch Module (ESM) for CGR 2010	Cisco IOS Release 12.2(53)EX