



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

- [Working with the Flash File System, on page 1](#)
- [Working with Configuration Files, on page 8](#)
- [Replacing and Rolling Back Configurations, on page 19](#)
- [Working with Software Images , on page 23](#)
- [Copying Image Files Using TFTP, on page 25](#)
- [Copying Image Files Using FTP, on page 28](#)
- [Copying Image Files Using RCP, on page 31](#)

## Working with the Flash File System

### Information About the Flash File System

The flash file system is a single flash device on which you can store files. It also provides several commands to help you manage software bundles and configuration files. The default flash file system on the device is named flash:.

As viewed from the active switch, flash: refers to the local flash device, which is the device attached to the same switch on which the file system is being viewed.

Only one user at a time can manage the software bundles and configuration files.

### Displaying Available File Systems

To display the available file systems on your device, use the **show file systems** privileged EXEC command as shown in this example for a standalone device:

```
Device# 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:

```

Table 1: show file systems Field Descriptions

Field	Value
Size(b)	Amount of memory in the file system in bytes.
Free(b)	Amount of free memory in the file system in bytes.
Type	Type of file system. <b>disk</b> —The file system is for a flash memory device, USB flash, and crashinfo file. <b>network</b> —The file system for network devices; for example, an FTP server or and HTTP server. <b>nvr</b> am—The file system is for a NVRAM device. <b>opaque</b> —The file system is a locally generated pseudo file system (for example, the system) or a download interface, such as brimux. <b>unknown</b> —The file system is an unknown type.
Flags	Permission for file system. <b>ro</b> —read-only. <b>rw</b> —read/write. <b>wo</b> —write-only.

Field	Value
Prefixes	<p>Alias for file system.</p> <p><b>crashinfo:</b>—Crashinfo file.</p> <p><b>flash:</b>—Flash file system.</p> <p><b>ftp:</b>—FTP server.</p> <p><b>http:</b>—HTTP server.</p> <p><b>https:</b>—Secure HTTP server.</p> <p><b>nvr:</b>—NVRAM.</p> <p><b>null:</b>—Null destination for copies. You can copy a remote file to null to find its size.</p> <p><b>rcp:</b>—Remote Copy Protocol (RCP) server.</p> <p><b>scp:</b>—Session Control Protocol (SCP) server.</p> <p><b>system:</b>—Contains the system memory, including the running configuration.</p> <p><b>tftp:</b>—TFTP network server.</p> <p><b>usbflash0:</b>—USB flash memory.</p> <p><b>xmodem:</b>—Obtain the file from a network machine by using the Xmodem protocol.</p> <p><b>ymodem:</b>—Obtain the file from a network machine by using the Ymodem protocol.</p>

## Setting the Default File System

You can specify the file system or directory that the system uses as the default file system by using the **cd** *filesystem:* privileged EXEC command. You can set the default file system to omit the *filesystem:* argument from related commands. For example, for all privileged EXEC commands that have the optional *filesystem:* argument, the system uses the file system specified by the **cd** command.

By default, the default file system is *flash:*.

You can display the current default file system as specified by the **cd** command by using the **pwd** privileged EXEC command.

## Displaying Information About Files on a File System

You can view a list of the contents of a file system before manipulating its contents. For example, before copying a new configuration file to flash memory, you might want to verify that the file system does not already contain a configuration file with the same name. Similarly, before copying a flash configuration file to another location, you might want to verify its filename for use in another command. To display information about files on a file system, use one of the privileged EXEC commands listed in the following table.

Table 2: Commands for Displaying Information About Files

Command	Description
<b>dir</b> [/all] [filesystem:filename]	Displays a list of files on a file system.
<b>show file systems</b>	Displays more information about each of the files on a file system.
<b>show file information</b> file-url	Displays information about a specific file.
<b>show file descriptors</b>	Displays a list of open file descriptors. File descriptors are the internal representations of open files. You can use this command to see if another user has a file open.

## Changing Directories and Displaying the Working Directory

Follow these steps to change directories and to display the working directory:

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>enable</b>  <b>Example:</b> Device> <b>enable</b>	Enables privileged EXEC mode.  • Enter your password if prompted.
<b>Step 2</b>	<b>dir filesystem:</b>  <b>Example:</b> Device# <b>dir flash:</b>	Displays the directories on the specified file system.  For <i>filesystem:</i> , use <i>flash:</i> for the system board flash device.
<b>Step 3</b>	<b>cd directory_name</b>  <b>Example:</b> Device# <b>cd new_configs</b>	Navigates to the specified directory.  The command example shows how to navigate to the directory named <i>new_configs</i> .
<b>Step 4</b>	<b>pwd</b>  <b>Example:</b> Device# <b>pwd</b>	Displays the working directory.
<b>Step 5</b>	<b>cd</b>  <b>Example:</b> Device# <b>cd</b>	Navigates to the default directory.

## Creating Directories

Beginning in privileged EXEC mode, follow these steps to create a directory:

**Procedure**

	<b>Command or Action</b>	<b>Purpose</b>
<b>Step 1</b>	<b>dir</b> <i>filesystem:</i> <b>Example:</b> Device# <b>dir flash:</b>	Displays the directories on the specified file system.  For <i>filesystem:</i> , use <b>flash:</b> for the system board flash device.
<b>Step 2</b>	<b>mkdir</b> <i>directory_name</i> <b>Example:</b> Device# <b>mkdir new_configs</b>	Creates a new directory. Directory names are case sensitive and are limited to 45 characters between the slashes (/); the name cannot contain control characters, spaces, slashes, quotes, semicolons, or colons.
<b>Step 3</b>	<b>dir</b> <i>filesystem:</i> <b>Example:</b> Device# <b>dir flash:</b>	Verifies your entry.

## Removing Directories

To remove a directory with all its files and subdirectories, use the **delete /force /recursive** *filesystem:/file-url* privileged EXEC command.

Use the **/recursive** keyword to delete the named directory and all subdirectories and the files contained in it. Use the **/force** keyword to suppress the prompting that confirms a deletion of each file in the directory. You are prompted only once at the beginning of this deletion process.

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



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

## Copying Files

To copy a file from a source to a destination, use the **copy** *source-url destination-url* privileged EXEC command. For the source and destination URLs, you can use **running-config** and **startup-config** keyword shortcuts. For example, the **copy running-config startup-config** command saves the currently running configuration file to the NVRAM section of flash memory to be used as the configuration during system initialization.

You can also copy from special file systems (**xmodem:**, **ymodem:**) as the source for the file from a network machine that uses the Xmodem or Ymodem protocol.

Network file system URLs include ftp:, rcp:, tftp:, scp:, http:, and https: and have these syntaxes:

- FTP—ftp:[[/username [:password]@location]/directory]/filename
- RCP—rcp:[[/username@location]/directory]/filename
- TFTP—tftp:[[/location]/directory]/filename

- SCP—`scp:[[/username [:password]@location]/directory]/filename`
- HTTP—`http:[[/username [:password]@location]/directory]/filename`
- HTTPS—`https:[[/username [:password]@location]/directory]/filename`




---

**Note** The password must not contain the special character '@'. If the character '@' is used, the copy fails to parse the IP address of the server.

---

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)

## 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 device 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:

```
Device# delete myconfig
```

## Creating, Displaying and Extracting Files

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

Beginning in privileged EXEC mode, follow these steps to create a file, display the contents, and extract it:

## Procedure

	Command or Action	Purpose
<b>Step 1</b>	<p><b>archive tar /create <i>destination-url</i> flash: /<i>file-url</i></b></p> <p><b>Example:</b></p> <pre>Device# archive tar /create tftp:172.20.10.30/saved. flash:/new-configs</pre>	<p>Creates a file and adds files to it.</p> <p>For <i>destination-url</i>, specify the destination URL alias for the local or network file system and the name of the file to create:</p> <ul style="list-style-type: none"> <li>Local flash file system syntax: <p><b>flash:</b></p> </li> <li>FTP syntax: <p><b>ftp:[[/<i>username</i>[:<i>password</i>]]@<i>location</i>]/<i>directory</i>]/-<i>filename</i>.</b></p> </li> <li>RCP syntax: <p><b>rcp:[[/<i>username</i>@<i>location</i>]/<i>directory</i>]/-<i>filename</i>.</b></p> </li> <li>TFTP syntax: <p><b>tftp:[[/<i>location</i>]/<i>directory</i>]/-<i>filename</i>.</b></p> </li> </ul> <p>For <b>flash:/<i>file-url</i></b>, specify the location on the local flash file system in which the new file is created. You can also specify an optional list of files or directories within the source directory to add to the new file. If none are specified, all files and directories at this level are written to the newly created file.</p>
<b>Step 2</b>	<p><b>archive tar /table <i>source-url</i></b></p> <p><b>Example:</b></p> <pre>Device# archive tar /table flash: /new_configs</pre>	<p>Displays the contents of a file.</p> <p>For <i>source-url</i>, specify the source URL alias for the local or network file system. The <i>-filename</i>. is the file to display. These options are supported:</p> <ul style="list-style-type: none"> <li>Local flash file system syntax: <p><b>flash:</b></p> </li> <li>FTP syntax: <p><b>ftp:[[/<i>username</i>[:<i>password</i>]]@<i>location</i>]/<i>directory</i>]/-<i>filename</i>.</b></p> </li> <li>RCP syntax: <p><b>rcp:[[/<i>username</i>@<i>location</i>]/<i>directory</i>]/-<i>filename</i>.</b></p> </li> <li>TFTP syntax: <p><b>tftp:[[/<i>location</i>]/<i>directory</i>]/-<i>filename</i>.</b></p> </li> </ul> <p>You can also limit the file displays by specifying a list of files or directories after the file. Only those files appear. If none are specified, all files and directories appear.</p>
<b>Step 3</b>	<p><b>archive tar /xtract <i>source-url</i> flash:/<i>file-url</i> [<i>dir/file</i>...]</b></p>	<p>Extracts a file into a directory on the flash file system.</p>

	Command or Action	Purpose
	<p><b>Example:</b></p> <pre>Device# archive tar /xtract tftp://172.20.10.30/saved. flash:/new-configs</pre>	<p>For <i>source-url</i>, specify the source URL alias for the local file system. The <i>-filename</i> is the file from which to extract files. These options are supported:</p> <ul style="list-style-type: none"> <li>Local flash file system syntax: <p><b>flash:</b></p> </li> <li>FTP syntax: <p><b>ftp:</b><i>[[/username[password]@location]directory]-filename.</i></p> </li> <li>RCP syntax: <p><b>rcp:</b><i>[[/username@location]directory]-filename.</i></p> </li> <li>TFTP syntax: <p><b>tftp:</b><i>[[//location]directory]-filename.</i></p> </li> </ul> <p>For <b>flash:</b><i>/file-url [dir/file...]</i>, specify the location on the local flash file system from which the file is extracted. Use the <i>dir/file...</i> option to specify a list of files or directories within the file to be extracted. If none are specified, all files and directories are extracted.</p>
<b>Step 4</b>	<p><b>more</b> [ /ascii   /binary   /ebcdic ] /file-url</p> <p><b>Example:</b></p> <pre>Device# more flash:/new-configs</pre>	<p>Displays the contents of any readable file, including a file on a remote file system.</p>

## Working with Configuration Files

### Information on 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.

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.

## 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 or Ethernet management 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 or Ethernet management 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:

### Procedure

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

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

To configure the switch by using a configuration file downloaded from a TFTP server, follow these steps:

### Procedure

---

- Step 1** Copy the configuration file to the appropriate TFTP directory on the workstation.
- Step 2** Verify that the TFTP server is properly configured.
- Step 3** Log into the switch through the console port, the Ethernet management port, or a Telnet session.
- Step 4** Download the configuration file from the TFTP server to configure the switch.

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

Use one of these privileged EXEC commands:

```
copy tftp:[[/location]/directory]/filename system:running-config
copy tftp:[[/location]/directory]/filename nvram:startup-config
copy tftp:[[/location]/directory]/filename flash[n]:/directory/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:

```
Device# 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

To upload a configuration file from a switch to a TFTP server for storage, follow these steps:

### Procedure

---

- Step 1** Verify that the TFTP server is properly configured.
- Step 2** Log into the switch through the console port, the Ethernet management port, or a Telnet session
- Step 3** 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]
- **copy flash[n]:/directory/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:

```
Device# 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 a Configuration File from the Device to an FTP Server

You can copy a configuration file from the device to an FTP server.

### Understanding the FTP Username and Password




---

**Note** The password must not contain the special character '@'. If the character '@' is used, the copy fails to parse the IP address of the 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 device to a server using FTP, the Cisco IOS software sends the first valid username it encounters in the following sequence:

1. The username specified in the **copy** EXEC command, if a username is specified.
2. The username set by the **ip ftp username** global configuration command, if the command is configured.
3. Anonymous.

The device sends the first valid password it encounters in the following sequence:

1. The password specified in the **copy** command, if a password is specified.
2. The password set by the **ip ftp password** command, if the command is configured.
3. The device forms a password *username @devicename.domain*. The variable *username* is the username associated with the current session, *devicename* is the configured host name, and *domain* is the domain of the device.

The username and password must be associated with an account on the FTP server. If you are writing to the server, the FTP server must be properly configured to accept the FTP write request from the user on the device.

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

Refer to the documentation for your FTP server for more information.

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

## 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

Beginning in privileged EXEC mode, follow these steps to download a configuration file by using FTP:

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b>	Enter global configuration mode on the switch.  This step is required only if you override the default remote username or password (see Steps 2, 3, and 4).
<b>Step 2</b>	<b>ip ftp username <i>username</i></b>	(Optional) Change the default remote username.
<b>Step 3</b>	<b>ip ftp password <i>password</i></b>	(Optional) Change the default password.
<b>Step 4</b>	<b>end</b>	Return to privileged EXEC mode.
<b>Step 5</b>	Do one of the following:  • <b>copy system:running-config ftp:</b> [[[/ <i>username</i> [ <i>:password</i> ]@] <i>location</i> ]/ <i>directory</i> ]/ <i>filename</i> ]	Using FTP, copy the configuration file from a network server to the running configuration or to the startup configuration file.

	Command or Action	Purpose
	<ul style="list-style-type: none"> <li>• <b>copy nvram:startup-config ftp:</b> [[[/<i>username</i> [<i>:password</i> ]<i>@location</i>]/<i>directory</i> ]/<i>filename</i>]</li> </ul>	

### 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:

```
Device# 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]
Device#
%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.

```
Device# configure terminal
Device(config)# ip ftp username netadmin1
Device(config)# ip ftp password mypass
Device(config)# end
Device# copy ftp: nvram: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]
Device#
%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

Beginning in privileged EXEC mode, follow these steps to upload a configuration file by using FTP:

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b>	Enter global configuration mode on the switch.  This step is required only if you override the default remote username or password (see Steps 2, 3, and 4).
<b>Step 2</b>	<b>ip ftp username <i>username</i></b>	(Optional) Change the default remote username.
<b>Step 3</b>	<b>ip ftp password <i>password</i></b>	(Optional) Change the default password.
<b>Step 4</b>	<b>end</b>	Return to privileged EXEC mode.

	Command or Action	Purpose
<b>Step 5</b>	Do one of the following: <ul style="list-style-type: none"> <li>• <b>copy system:running-config ftp:</b> [[[//[username [:password ]@]location]/directory ]/filename ] or</li> <li>• <b>copy nvram:startup-config ftp:</b> [[[//[username [:password ]@]location]/directory ]/filename ]</li> </ul>	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:

```
Device# 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
Device#
```

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

```
Device# configure terminal
Device(config)# ip ftp username netadmin2
Device(config)# ip ftp password mypass
Device(config)# end
Device# 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.

## 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 RCPserver 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

Beginning in privileged EXEC mode, follow these steps to download a configuration file by using RCP:

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b>	Enter global configuration mode on the switch.



	Command or Action	Purpose
		This step is required only if you override the default remote username (see Steps 2 and 3).
<b>Step 2</b>	<code>ip rcmd remote-username <i>username</i></code>	(Optional) Change the default remote username.
<b>Step 3</b>	<code>end</code>	Return to privileged EXEC mode.
<b>Step 4</b>	Do one of the following: <ul style="list-style-type: none"> <li>• <code>copy rcp://<i>username@hostname</i>/dir/remote:running-config</code></li> <li>• <code>copy rcp://<i>username@hostname</i>/dir/remote:startup-config</code></li> </ul>	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-config` 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:

```
Device# copy rcp://netadmin1@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]
Device#
%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-config` from the `netadmin1` directory on the remote server with an IP address of 172.16.101.101 to the startup configuration:

```
Device# configure terminal
Device(config)# ip rcmd remote-username netadmin1
Device(config)# end
Device# copy rcp: nvram: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]
Device#
%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

Beginning in privileged EXEC mode, follow these steps to upload a configuration file by using RCP

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<code>configure terminal</code>	Enter global configuration mode on the switch.

	Command or Action	Purpose
		This step is required only if you override the default remote username (see Steps 2 and 3).
<b>Step 2</b>	<code>ip rcmd remote-username <i>username</i></code>	(Optional) Specify the remote username.
<b>Step 3</b>	<code>end</code>	Return to privileged EXEC mode.
<b>Step 4</b>	Do one of the following: <ul style="list-style-type: none"> <li>• <code>copy system:running-config</code>  <code>rcp:[[/username@]location]directory\filename]</code></li> <li>• <code>copy nvram:startup-config</code>  <code>rcp:[[/username@]location]directory\filename]</code></li> </ul>	Using RCP, copy the configuration file from a switch running configuration or startup configuration file to a network server.

### 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`:

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

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

```
Device# configure terminal
Device(config)# ip rcmd remote-username netadmin2
Device(config)# end
Device# 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.



**Note** 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. For more information about the file prompt command, see the Cisco IOS Command Reference for Release 12.4.



---

**Note** 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.

## Information on Configuration Replacement and Rollback

### Configuration Archive

The Cisco IOS configuration archive is intended to provide a mechanism to store, organize, and manage an archive of Cisco IOS configuration files to enhance the configuration rollback capability provided by the **configure replace** command. Before this feature was introduced, you could save copies of the running configuration using the **copy running-config destination-url** command, storing the replacement file either locally or remotely. However, this method lacked any automated file management. On the other hand, the Configuration Replace and Configuration Rollback feature provides the capability to automatically save copies of the running configuration to the Cisco IOS configuration archive. These archived files serve as checkpoint configuration references and can be used by the **configure replace** command to revert to previous configuration states.

The **archive config** command allows you to save Cisco IOS configurations in the configuration archive using a standard location and filename prefix that is automatically appended with an incremental version number (and optional timestamp) as each consecutive file is saved. This functionality provides a means for consistent identification of saved Cisco IOS configuration files. You can specify how many versions of the running configuration are kept in the archive. After the maximum number of files are saved in the archive, the oldest file is automatically deleted when the next, most recent file is saved. The **show archive** command displays information for all configuration files saved in the Cisco IOS configuration archive.

The Cisco IOS configuration archive, in which the configuration files are stored and available for use with the **configure replace** command, can be located on the following file systems: FTP, HTTP, RCP, TFTP.

### Configuration Replace

The **configure replace** privileged EXEC command 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.

## Configuration Rollback

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 Guidelines

Follow these guidelines when configuring and performing configuration replacement and rollback:

- 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 terminal** 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. Starting in privileged EXEC mode, follow these steps to configure the configuration archive:

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b>	Enter global configuration mode.
<b>Step 2</b>	<b>archive</b>	Enter archive configuration mode.
<b>Step 3</b>	<b>path</b> <i>url</i>	Specify the location and filename prefix for the files in the configuration archive
<b>Step 4</b>	<b>maximum</b> <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.  <b>Note</b> Before using this command, you must first enter the <b>path</b> archive configuration command to specify the location and filename prefix for the files in the configuration archive.
<b>Step 5</b>	<b>time-period</b> <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
<b>Step 6</b>	<b>end</b>	Return to privileged EXEC mode.
<b>Step 7</b>	<b>show running-config</b>	Verify the configuration.
<b>Step 8</b>	<b>copy running-config startup-config</b>	(Optional) Save your entries in the configuration file.

## Performing a Configuration Replacement or Rollback Operation

Starting in privileged EXEC mode, follow these steps to replace the running configuration file with a saved configuration file:

## Procedure

---

**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** *target-url* [**list**] [**force**] [**time seconds**] [**no-lock**]

Replace the running configuration file with a saved configuration file.

*target-url*—URL (accessible by the file system) of the saved configuration file that is to replace the running configuration, such as the configuration file created in Step 2 by using the **archive config** privileged EXEC command

**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.

**timeseconds**—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** seconds 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** seconds keyword and argument of the **configure replace** command are specified.

**Step 7** **copy running-config startup-config**

(Optional) Save your entries in the configuration file.

---

# Working with Software Images

## Information on 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. If you do not have access to a TFTP server, you can download a software image file directly to your PC or workstation by using a web browser (HTTP) and then by using the device manager or Cisco Network Assistant to upgrade your switch. For information about upgrading your switch by using a TFTP server or a web browser (HTTP), see the release notes.

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.



---

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

---

## 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 might be stored in flash memory.

## 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 and web management files

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

```
system_type:0x00000000:image-name
  image_family:xxxx
  info_end:

version_suffix:xxxx
  version_directory:image-name
  image_system_type_id:0x00000000
  image_name:image-nameB.bin
  ios_image_file_size:6398464
  total_image_file_size:8133632
  image_feature:IP|LAYER_3|PLUS|MIN_DRAM_MEG=128
  image_family:xxxx
  board_ids:0x401100c4 0x00000000 0x00000001 0x00000003 0x00000002 0x00008000 0x00008002

0x40110000
  info_end
```

**Table 3: info File Description**

Field	Description
version_suffix	Specifies the Cisco IOS image version string suffix
version_directory	Specifies the directory where the Cisco IOS image and the HTML subdirectory are installed
image_name	Specifies the name of the Cisco IOS image within the tar file
ios_image_file_size	Specifies the Cisco IOS image size in the tar file, which is an approximate measure of how much flash memory is required to hold just the Cisco IOS image
total_image_file_size	Specifies the size of all the images (the Cisco IOS image and the web management files) in the tar file, which is an approximate measure of how much flash memory is required to hold them
image_feature	Describes the core functionality of the image
image_min_dram	Specifies the minimum amount of DRAM needed to run this image
image_family	Describes the family of products on which the software can be installed



## Copying Image Files 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.

---

## 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.

Beginning in privileged EXEC mode, 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 3.

### Procedure

- 
- Step 1** Copy the image to the appropriate TFTP directory on the workstation. Make sure that the TFTP server is properly configured.
- 
- 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.
- 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 // *location* , specify the IP address of the TFTP server.
  - For *directory/image-name.tar* specify the directory (optional) and the image to download. Directory and image names are case sensitive.
- Step 4** **archive download-sw /leave-old-sw/reload tftp:** [ [ // *location* ] / *directory* ] / *image-name.tar*  
 Download the image file from the TFTP server to the switch, and keep the current image.
- 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 // *location* , specify the IP address of the TFTP server.
  - For *directory/image-name.tar* specify the directory (optional) and the image to download. Directory and image names are case sensitive.

The download algorithm verifies that the image is appropriate for the switch model and that enough DRAM is present, or it cancels 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 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 keep 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.

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

---

## Uploading an Image File 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.

Beginning in privileged EXEC mode, follow these steps to upload an image to a TFTP server:

### Procedure

---

- Step 1** Make sure the TFTP server is properly configured  
—
- Step 2** Log into the switch through the console port or a Telnet session.  
—
- Step 3** **archive upload-sw tftp:[// location /directory /image-name .tar**

Upload the currently running switch image to the TFTP server.

- For *// location* , specify the IP address of the TFTP server.
- For */directory/image-name.tar* specify the directory (optional) and the name of the software image to be uploaded. Directory and image names are case sensitive. The *image-name.tar* is the name of the software image to be stored on the server.

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

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

---

## Copying Image Files 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.

---

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

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

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

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

The switch sends the first valid password in this list:

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

The username and password must be associated with an account on the FTP server. If you are writing to the server, the FTP server must be properly configured to accept the FTP write request from you.

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

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

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

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

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

## Downloading an Image File By Using FTP

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

Beginning in privileged EXEC mode, follow Steps 1 through 7 to download a new image from an FTP server and overwrite the existing image. To keep the current image, go to Step 7.

### Procedure

- 
- |               |  |
|---------------|--|
| <b>Step 1</b> | Verify that the FTP server is properly configured.<br>—  |
| <b>Step 2</b> | Log into the switch through the console port or a Telnet session.<br>—   |
| <b>Step 3</b> | <b>configure terminal</b><br>Enter global configuration mode.<br>This step is required only if you override the default remote username or password (see Steps 4, 5, and 6). |
| <b>Step 4</b> | <b>ip ftp username</b> <i>username</i><br>(Optional) Change the default remote username.   |
| <b>Step 5</b> | <b>ip ftp password</b> <i>password</i><br>(Optional) Change the default password.  |
| <b>Step 6</b> | <b>end</b><br>Return to privileged EXEC mode.  |
| <b>Step 7</b> | <b>archive download-sw /overwrite/reload</b><br><b>ftp:</b> [ [ / / <i>username</i> [ : <i>password</i> ] @ <i>location</i> ] / <i>directory</i> ] / <i>image-name.tar</i>   |

Download the image file from the FTP server to the switch, and overwrite the current image.

- 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 `//username[:password]` specify the username and password; these must be associated with an account on the FTP server.
- For `@ location`, specify the IP address of the FTP server.
- For `directory/image-name.tar`, specify the directory (optional) and the image to download. Directory and image names are case sensitive.

#### Step 8 **archive download-sw /leave-old-sw /reload**

**ftp:** [ [ //username[:password] @location ] /directory ] /image-name.tar

Download the image file from the FTP server to the switch, and keep the current image.

- 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 `//username[:password]` specify the username and password; these must be associated with an account on the FTP server.
- For `@ location`, specify the IP address of the FTP server.
- For `directory/image-name.tar`, specify the directory (optional) and the image to download. Directory and image names are case sensitive.

The download algorithm verifies that the image is appropriate for the switch model and that enough DRAM is present, or it cancels 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.

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

## 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.

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

Beginning in privileged EXEC mode, follow these steps to upload an image to an FTP server:

### Procedure

---

**Step 1**     **configure terminal**

Enter global configuration mode.

This step is required only if you override the default remote username or password (see Steps 2, 3, and 4.)

**Step 2**     **ip ftp username***username*

(Optional) Change the default remote username.

**Step 3**     **ip ftp password***password*

(Optional) Change the default password.

**Step 4**     **end**

Return to privileged EXEC mode.

**Step 5**     **archive upload-sw ftp:** [ [ / / [ *username* [ : *password* ] @ ] *location* ] / *directory* ] / *image-name.tar*

Upload the currently running switch image to the FTP server.

- For *//username:password*, specify the username and password. These must be associated with an account on the FTP server.
- For *@location*, specify the IP address of the FTP server.
- For */directory/image-name.tar*, specify the directory (optional) and the name of the software image to be uploaded. Directory and image names are case sensitive. The *image-name .tar* is the name of the software image to be stored on the server.

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

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

---

## Copying Image Files 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.

---

## Preparing to Download or Upload an Image File 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 using RCP

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

Beginning in privileged EXEC mode, follow Steps 1 through 6 to download a new image from an RCP server and overwrite the existing image. To keep the current image, go to Step 6.

### Procedure

- 
- Step 1** Verify that the RCP server is properly configured.
- 
- Step 2** Log into the switch through the console port or a Telnet session.
- 
- Step 3** **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 4** **ip rcmd remote-username *username***
- (Optional) Specify the remote username.
- Step 5** **end**
- Return to privileged EXEC mode.
- Step 6** **archive download-sw /overwrite/reload rcp: [ [ [ //*username@* ] /*location* ] /*directory* ] /*image-name.tar***
- Download the image file from the RCP server to the switch, and overwrite the current image.
- 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 `//username@` specify the username. For the RCP copy request to execute successfully, an account must be defined on the network server for the remote username.
  - For `@location`, specify the IP address of the RCP server.

- For `/directory/image-name.tar`, specify the directory (optional) and the image to download. Directory and image names are case sensitive.

**Step 7** **archive download-sw /leave-old-sw /reload rcp:** [ [ [ / [ *username@* ] *location* ] / *directory* ] / *image-name.tar*  
Download the image file from the FTP server to the switch, and keep the current image.

- 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 `/username` specify the username. For the RCP copy request to execute, an account must be defined on the network server for the remote username.
- For `@ location`, specify the IP address of the RCP server.
- For `/directory/image-name.tar`, specify the directory (optional) and the image to download. Directory and image names are case sensitive.

The download algorithm verifies that the image is appropriate for the switch model and that enough DRAM is present, or it cancels 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.

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

## Uploading an Image File 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.

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.

Beginning in privileged EXEC mode, follow these steps to upload an image to an RCP server:

### Procedure

	Command or Action	Purpose
Step 1	configure terminal	Enter global configuration mode.

	Command or Action	Purpose
		This step is required only if you override the default remote username or password (see Steps 2 and 3.)
<b>Step 2</b>	<b>ip rcmd remote-username</b> <i>username</i>	Optional) Specify the remote username.
<b>Step 3</b>	<b>end</b>	Return to privileged EXEC mode.
<b>Step 4</b>	<b>archive upload-sw</b> <b>rpx:</b> [[ [// [ <i>username@</i> ] <i>location</i> ] / <i>directory</i> ] / <i>image-name.tar</i>	<p>Upload the currently running switch image to the RCP server.</p> <ul style="list-style-type: none"> <li>• 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.</li> <li>• For @<i>location</i>, specify the IP address of the RCP server.</li> <li>• 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.</li> <li>• The <i>image-name.tar</i> is the name of software image to be stored on the server.</li> </ul> <p>The <b>archive upload-sw</b> 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.</p> <p><b>Note</b> For the download and upload algorithms to operate properly, do not rename image names.</p>

