Managing Firmware and Configurations

This chapter describes how to manipulate the Flash file system, how to copy configuration files, and how to archive (upload and download) software images.

Note For complete syntax and usage information for the commands used in this chapter, refer to the *Cisco IOS Command Reference for Access Points and Bridges* for this release and the *Cisco IOS Configuration Fundamentals Command Reference for Release 12.4*.

Working with the Flash File System

The Flash file system on your access point provides several commands to help you manage software image and configuration files.

The Flash file system is a single Flash device on which you can store files. This Flash device is called *flash:*.

This section contains this information:

Displaying Available File Systems

To display the available file systems on your access point, use the **show file systems** privileged EXEC command as shown in this example:

```
ap# show file systems
File Systems:


       Size(b)       Free(b)      Type  Flags  Prefixes
             -             -    opaque     rw   arch:
*     31739904      16701952     flash     rw   flash:
      11999232       7754752     flash     rw   ram:
             -             -    opaque     rw   bs:
      31739904      16701952   unknown     rw   zflash:
             -             -    opaque     rw   archive:
             -             -    opaque     rw   system:
         32768         26572     nvram     rw   nvram:
             -             -    opaque     rw   tmpsys:
             -             -   network     rw   tftp:
             -             -    opaque     rw   null:
             -             -    opaque     ro   xmodem:
             -             -    opaque     ro   ymodem:
             -             -   network     rw   rcp:
             -             -   network     rw   ftp:
             -             -   network     rw   http:
             -             -   network     rw   scp:
             -             -    opaque     ro   tar:
             -             -   network     rw   https:
```

Table 20-1 lists field descriptions for the **show file systems** command.

Table 20-1 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. **flash**—The file system is for a Flash memory device. **network**—The file system is for a network device. **nvram**—The file system is for a nonvolatile RAM (NVRAM) device. **opaque**—The file system is a locally generated *pseudo* file system (for example, the *system*) or a download interface, such as brimux. **unknown**—The file system is an unknown type.

Table 20-1 show file systems Field Descriptions (continued)

Field	Value
Flags	Permission for file system. **ro**—read-only. **rw**—read/write. **wo**—write-only.
Prefixes	Alias for file system. **arch:** **ram:** **bs:** **archive:** **tmpsys:** **xmoem:** **ymodem:** **scp:** **tar:** **https:** **flash:**—Flash file system. **ftp:**—File Transfer Protocol network server. Used to transfer files to or from the network device. **nvram:**—Non-volatile RAM memory (NVRAM). **null:**—Null destination for copies. You can copy a remote file to null to determine its size. **rcp:**—Remote Copy Protocol (RCP) network server. **system:**—Contains the system memory, including the running configuration. **tftp:**—Trivial File Transfer Protocol (TFTP) network server. **zflash:**—Read-only file decompression file system, which mirrors the contents of the Flash file system.

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 in Table 20-2.

Table 20-2 Commands for Displaying Information About Files

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

Changing Directories and Displaying the Working Directory

Beginning in privileged EXEC mode, follow these steps to change directories and display the working directory.

	Command	Purpose
Step 1	**dir** *filesystem***:**	Display the directories on the specified file system. For *filesystem***:**, use **flash:** for the system board Flash device.
Step 2	**cd** *directory_name*	Change to the directory of interest.
Step 3	**pwd**	Display the working directory.

Creating and Removing Directories

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

	Command	Purpose
Step 1	**dir** *filesystem***:**	Display the directories on the specified file system. For *filesystem***:**, use **flash:** for the system board Flash device.
Step 2	**mkdir** *directory_name*	Create a new directory. 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.

Copying Files

To copy a file from a source to a destination, use the **copy** [**/erase**] *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.

Note When adding the optional argument **/erase** to the copy command, the destination is overwritten. If a file with the same name exists at the destination, it is replaced with the new file that is being copied.

Network file system URLs include **ftp:**, **rcp:**, and **tftp:** and have the following syntax:

- File Transfer Protocol (FTP)—**ftp:**[[**//***username* [**:***password*]**@***location*]**/***directory*]**/***filename*
- Remote Copy Protocol (RCP)—**rcp:**[[**//***username***@***location*]**/***directory*]**/***filename*
- Trivial File Transfer Protocol (TFTP)—**tftp:**[[**//***location*]**/***directory*]**/***filename*

Local writable file systems include flash:.

Some invalid combinations of source and destination exist. Specifically, you cannot copy these combinations:

- From a running configuration to a running configuration
- From a startup configuration to a startup configuration
- From a device to the same device (for example, the **copy flash: flash:** command is invalid)

For specific examples of using the **copy** command with configuration files, see the "Working with Configuration Files" section on page 20-9.

To copy software images either by downloading a new version or 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 20-20.

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.

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

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 access point 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.

This example shows how to delete the file *myconfig* from the default Flash memory device:

```
ap# 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.

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:/***file-url*
- For the File Transfer Protocol (FTP), the syntax is **ftp:**[[**//***username*[**:***password*]**@***location*]**/***directory*]**/***tar-filename***.tar**
- For the Remote Copy Protocol (RCP), the syntax is **rcp:**[[**//***username***@***location*]**/***directory*]**/***tar-filename***.tar**
- For the Trivial File Transfer Protocol (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:

```
ap# 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 File Transfer Protocol (FTP), the syntax is **ftp:**[[**//***username*[**:***password*]**@***location*]**/***directory*]**/***tar-filename***.tar**
- For the Remote Copy Protocol (RCP), the syntax is **rcp:**[[**//***username***@***location*]**/***directory*]**/***tar-filename***.tar**
- For the Trivial File Transfer Protocol (TFTP), the syntax is **tftp:**[[**//***location*]**/***directory*]**/***tar-filename***.tar**

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

You can also limit the display of the files by specifying an optional list of files or directories after the tar file; then only these files are displayed. If none are specified, all files and directories are displayed.

This example shows how to display the contents of a *ap3g2-k9w7-tar.152-4.JB5.tar* file that is in Flash memory:

```
ap# archive tar /table flash:c1200-k9w7-mx.122-8.JA.tar
ap# archive tar /table flash:ap3g2-k9w7-tar.152-4.JB5.tar
info (286 bytes)
ap3g2-k9w7-mx.152-4.JB5/ (directory)
ap3g2-k9w7-mx.152-4.JB5/ap3g2-k9w7-mx.152-4.JB5 (208427 bytes)
ap3g2-k9w7-mx.152-4.JB5/ap3g2-k9w7-tx.152-4.JB5 (73 bytes)
ap3g2-k9w7-mx.152-4.JB5/html/ (directory)
ap3g2-k9w7-mx.152-4.JB5/html/level/ (directory)
ap3g2-k9w7-mx.152-4.JB5/html/level/1/ (directory)
ap3g2-k9w7-mx.152-4.JB5/html/level/1/appsui.js (563 bytes)
ap3g2-k9w7-mx.152-4.JB5/html/level/1/back.shtml (512 bytes)
.../...
```

This example shows how to display a *ap3g2-k9w7-mx.152-4.JB5/html/* directory and its contents:

```
ap# archive tar /table flash:/ap3g2-k9w7-tar.152-4.JB5.tar ap3g2-k9w7-mx.152-4.JB5/html
ap3g2-k9w7-mx.152-4.JB5/html/ (directory)
ap3g2-k9w7-mx.152-4.JB5/html/level/ (directory)
ap3g2-k9w7-mx.152-4.JB5/html/level/1/ (directory)
ap3g2-k9w7-mx.152-4.JB5/html/level/1/appsui.js (563 bytes)
ap3g2-k9w7-mx.152-4.JB5/html/level/1/back.shtml (512 bytes)
ap3g2-k9w7-mx.152-4.JB5/html/level/1/cookies.js (5032 bytes)
ap3g2-k9w7-mx.152-4.JB5/html/level/1/forms.js (20125 bytes)
ap3g2-k9w7-mx.152-4.JB5/html/level/1/sitewide.js (17089 bytes)
ap3g2-k9w7-mx.152-4.JB5/html/level/1/stylesheet.css (3220 bytes)
ap3g2-k9w7-mx.152-4.JB5/html/level/1/config.js (26330 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*

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 File Transfer Protocol (FTP), the syntax is **ftp:**[[**//***username*[**:***password*]**@***location*]**/***directory*]**/***tar-filename***.tar**
- For the Remote Copy Protocol (RCP), the syntax is **rcp:**[[**//***username***@***location*]**/***directory*]**/***tar-filename***.tar**
- For the Trivial File Transfer Protocol (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*, specify the location on the local Flash file system into which the tar file is extracted. You can also specify an optional list of files or directories within the tar file for extraction. 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.

```
ap# 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:

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

<output truncated>
```

Working with Configuration Files

This section describes how to create, load, and maintain configuration files. Configuration files contain commands entered to customize the function of the Cisco IOS software. To better benefit from these instructions, your access point contains a minimal default running configuration for interacting with the system software.

You can copy (*download*) configuration files from a TFTP, FTP, or RCP server to the running configuration of the access point for various reasons:

- To restore a backed-up configuration file.
- To use the configuration file for another access point. For example, you might add another access point to your network and want it to have a configuration similar to the original access point. By copying the file to the new access point, you can change the relevant parts rather than recreating the whole file.
- To load the same configuration commands on all the access points in your network so that all the access points have similar configurations.

You can copy (*upload*) configuration files from the access point 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 Transmission Control Protocol/Internet Protocol (TCP/IP) stack, which is connection oriented.

This section includes this information:

Guidelines for Creating and Using Configuration Files

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

Use these guidelines when creating a configuration file:

- If no passwords have been set on the access point, you must set them on each access point by entering the **enable secret** *secret-password* global configuration command. Enter a blank line for this command. The password is saved in the configuration file as clear text.

- If passwords already exist, you cannot enter the **enable secret** *secret-password* global configuration command in the file because the password verification will fail. If you enter a password in the configuration file, the access point mistakenly attempts to execute the passwords as commands as it executes the file.
- The **copy** {**ftp:** | **rcp:** | **tftp:**} **system:running-config** privileged EXEC command loads the configuration files on the access point as if you were entering the commands at the command line. The access point 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 access point.

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 an access point to a server.

For more information, see the "Downloading the Configuration File by Using TFTP" section on page 20-11, the "Downloading a Configuration File by Using FTP" section on page 20-13, or the "Downloading a Configuration File by Using RCP" section on page 20-16.

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

This section includes this information:

Preparing to Download or Upload a Configuration File by Using TFTP

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

- Ensure that the workstation acting as the TFTP server is properly configured.
- Ensure that the access point has a route to the TFTP server. The access point 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.
- For download operations, ensure that the permissions on the file are set correctly. The permission on the file should be world-read.
- During upload operations, if you are overwriting an existing file 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 access point by using a configuration file downloaded from a TFTP server, follow these steps:

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

Step 2 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 20-11.

Step 3 Log into the access point through a Telnet session.

Step 4 Download the configuration file from the TFTP server to configure the access point.

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

Use one of these privileged EXEC commands:

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

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

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

```
ap# copy tftp://172.16.2.155/tokyo-confg system:running-config
Configure using tokyo-confg from 172.16.2.155? [confirm] y
```

```
Booting tokyo-confg from 172.16.2.155:!!! [OK - 874/16000 bytes]
```

Uploading the Configuration File by Using TFTP

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

Step 1 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 20-11.

Step 2 Log into the access point through a Telnet session.

Step 3 Upload the access point configuration to the TFTP server. Specify the IP address or host name 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.

This example shows how to upload a configuration file from an access point to a TFTP server:

```
ap# copy system:running-config tftp://172.16.2.155/tokyo-confg
Write file tokyo-confg on host 172.16.2.155? [confirm] y
#
Writing tokyo-confg!!! [OK]
```

Copying Configuration Files by Using FTP

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

The FTP protocol requires a client to send a remote username and password on each FTP request to a server. When you copy a configuration file from the access point 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 access point 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 access point forms a password named *username@apname.domain*. The variable *username* is the username associated with the current session, *apname* is the configured host name, and *domain* is the domain of the access point.

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, refer to the documentation for your FTP server.

This section includes this information:

Preparing to Download or Upload a Configuration File by Using FTP

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

- Ensure that the access point has a route to the FTP server. The access point 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 access point through 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 access point 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 access point.

For more information, refer to 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:

	Command	Purpose
Step 1		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 20-13.
Step 2		Log into the access point through a Telnet session.
Step 3	**configure terminal**	Enter global configuration mode on the access point. This step is required only if you override the default remote username or password (continue with Step 4 to Step 6).
Step 4	**ip ftp username** *username*	(Optional) Change the default remote username.
Step 5	**ip ftp password** *password*	(Optional) Change the default password.

	Command	Purpose
Step 6	**end**	Return to privileged EXEC mode.
Step 7	**copy ftp:**[[[//[*username*[**:***password*]@]*location*]*/directory*] */filename*] **system:running-config** or **copy ftp:**[[[//[*username*[**:***password*]@]*location*]*/directory*] */filename*] **nvram:startup-config**	Using FTP, copy the configuration file from a network server to the running configuration or to the startup configuration file.

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

```
ap# copy ftp://netadmin1:mypass@172.16.101.101/host1-confg system:running-config
Configure using host1-confg from 172.16.101.101? [confirm]
Connected to 172.16.101.101
Loading 1112 byte file host1-confg:![OK]
ap#
%SYS-5-CONFIG: Configured from host1-config by ftp from 172.16.101.101
```

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

```
ap# configure terminal
ap(config)# ip ftp username netadmin1
ap(config)# ip ftp password mypass
ap(config)# end
ap# copy ftp: nvram:startup-config
Address of remote host [255.255.255.255]? 172.16.101.101
Name of configuration file[rtr2-confg]? host2-confg
Configure using host2-confg from 172.16.101.101?[confirm]
Connected to 172.16.101.101
Loading 1112 byte file host2-confg:![OK]
[OK]
ap#
%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:

	Command	Purpose
Step 1		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 20-13.
Step 2		Log into the access point through 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 (continue with Step 4 to Step 6).

	Command	Purpose
Step 4	**ip ftp username** *username*	(Optional) Change the default remote username.
Step 5	**ip ftp password** *password*	(Optional) Change the default password.
Step 6	**end**	Return to privileged EXEC mode.
Step 7	**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 access point running or startup configuration file to the specified location.

This example shows how to copy the running configuration file named *ap2-confg* to the *netadmin1* directory on the remote host with an IP address of 172.16.101.101:

```
ap# copy system:running-config ftp://netadmin1:mypass@172.16.101.101/ap2-confg
Write file ap2-confg on host 172.16.101.101?[confirm]
Building configuration...[OK]
Connected to 172.16.101.101
ap#
```

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

```
ap# configure terminal
ap(config)# ip ftp username netadmin2
ap(config)# ip ftp password mypass
ap(config)# end
ap# copy nvram:startup-config ftp:
Remote host[]? 172.16.101.101
Name of configuration file to write [ap2-confg]?
Write file ap2-confg on host 172.16.101.101?[confirm]
![OK]
```

Copying Configuration Files by Using RCP

The Remote Copy Protocol (RCP) provides another method of downloading, uploading, and copying configuration files between remote hosts and the access point. 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 access point 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 access point software sends the Telnet username as the remote username.
- The access point host name.

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 this information:

- Preparing to Download or Upload a Configuration File by Using RCP, page 20-16
- Downloading a Configuration File by Using RCP, page 20-16
- Uploading a Configuration File by Using RCP, page 20-17

Preparing to Download or Upload a Configuration File by Using RCP

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

- Ensure that the workstation acting as the RCP server supports the remote shell (rsh).
- Ensure that the access point has a route to the RCP server. The access point 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 access point through 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 access point 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 access point. 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 access point contains these configuration lines:

```
hostname ap1
ip rcmd remote-username User0
```

  If the access point IP address translates to *ap1.company.com*, the .rhosts file for User0 on the RCP server should contain this line:

```
ap1.company.com ap1
```

For more information, refer to 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:

	Command	Purpose
Step 1		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 20-16.
Step 2		Log into the access point through a Telnet session.
Step 3	**configure terminal**	Enter global configuration mode. This step is required only if you override the default remote username (continue with Step 4 and Step 5).
Step 4	**ip rcmd remote-username** *username*	(Optional) Specify the remote username.
Step 5	**end**	Return to privileged EXEC mode.
Step 6	**copy rcp:**[[[**//**[*username*@]*location*]*/directory*]*/filename*] **system:running-config** or **copy rcp:**[[[**//**[*username*@]*location*]*/directory*]*/filename*] **nvram:startup-config**	Using RCP, copy the configuration file from a network server to the running configuration or to the startup configuration file.

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 access point:

```
ap# 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]
ap#
%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:

```
ap# configure terminal
ap(config)# ip rcmd remote-username netadmin1
ap(config)# end
ap# 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]
ap#
%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:

	Command	Purpose
Step 1		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 20-16.
Step 2		Log into the access point through a Telnet session.
Step 3	**configure terminal**	Enter global configuration mode. This step is required only if you override the default remote username (continue with Step 4 and Step 5).
Step 4	**ip rcmd remote-username** *username*	(Optional) Specify the remote username.
Step 5	**end**	Return to privileged EXEC mode.
Step 6	**copy system:running-config rcp:**[[[**//**[*username*@]*location*]**/***directory*]**/***filename*] or **copy nvram:startup-config rcp:**[[[**//**[*username*@]*location*]**/***directory*]**/***filename*]	Using RCP, copy the configuration file from an access point running or startup configuration file to a network server.

This example shows how to copy the running configuration file named *ap2-confg* to the *netadmin1* directory on the remote host with an IP address of 172.16.101.101:

```
ap# copy system:running-config rcp://netadmin1@172.16.101.101/ap2-confg
Write file ap-confg on host 172.16.101.101?[confirm]
Building configuration...[OK]
Connected to 172.16.101.101
ap#
```

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

```
ap# configure terminal
ap(config)# ip rcmd remote-username netadmin2
ap(config)# end
ap# copy nvram:startup-config rcp:
Remote host[]? 172.16.101.101
Name of configuration file to write [ap2-confg]?
Write file ap2-confg on host 172.16.101.101?[confirm]
![OK]
```

Clearing Configuration Information

This section describes how to clear configuration information.

Deleting a Stored Configuration File

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

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 access point prompts for confirmation on destructive file operations. For more information about the **file prompt** command, refer to the *Cisco IOS Command Reference* guide.

Downloading Configuration File Always from TFTP Server

You can set the AP to download the configuration file (config.txt) always from the TFTP server, even when the NVRAM (flash) has a configuration file stored on it.

Before making this setting you must have the **AutoInstall using DHCP server** feature set for the access points on the router or switch. Without this the following configurations will not work.

To set the AP to download the configuration file always from the TFTP server, in global configuration mode, use the command **boot config-skip**. To disable this setting use the command **no boot config-skip**. This setting is disabled by default.

```
ap(config)# boot config-skip
ap(config)# no boot config-skip
```

In boot mode, you can use the following commands to enable or disable this setting:

- **ap: set BOOT_CONFIG_SKIP yes**, to enable.
- **ap: set BOOT_CONFIG no**, to disable.
- **ap: unset BOOT_CONFIG_SKIP**, to disable.

For setting this via the GUI:

Step 1 Go to **Software > System Configuration**.

Step 2 Against the **Boot Config Skip** option, click **Enable** or **Disable**, as required.

Step 3 Click **Apply**.

Working with Software Images

This section describes how to archive (download and upload) software image files, which contain the system software, Cisco IOS software, radio firmware, and the web management HTML files.

You download an access point image file from a TFTP, FTP, or RCP server to upgrade the access point software. You upload an access point image file to a TFTP, FTP, or RCP server for backup purposes. You can use this uploaded image for future downloads to the same access point or another of the same type.

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 Transmission Control Protocol/Internet Protocol (TCP/IP) stack, which is connection-oriented.

This section includes this information:

Note For a list of software images and supported upgrade paths, refer to the release notes for your access point.

Image Location on the Access Point

The Cisco IOS image is stored in a directory that shows the version number. A subdirectory contains the HTML 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 access point. 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 you might have stored in Flash memory.

Note Starting with the Cisco IOS releases 15.2(4)JB and 12.4(25e)JAO, on Cisco Aironet 3600, 3700, and 2700 series APs, the backup IOS image is deleted from the system board's Flash memory when the new image is downloaded on to it. This is designed to be so because the system board's Flash memory, which has a total of 31 MB, does not have enough space to store the recovery image, the new image, and the backup image.

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:

- *info* file

  The info file is always at the beginning of the tar file and contains information about the files within it.

- Cisco IOS image
- Web management files needed by the HTTP server on the access point
- radio firmware 5000.img file
- *info.ver* file

  The info.ver file is always at the end of the tar file and contains the same information as the info file. Because it is the last file in the tar file, its existence means that all files in the image have been downloaded.

Note The tar file sometimes ends with an extension other than *.tar*.

Copying Image Files by Using TFTP

You can download an access point image from a TFTP server or upload the image from the access point to a TFTP server.

You download an access point image file from a server to upgrade the access point software. You can overwrite the current image with the new one.

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

This section includes this information:

- Preparing to Download or Upload an Image File by Using TFTP, page 20-21
- Downloading an Image File by Using TFTP, page 20-22
- Uploading an Image File by Using TFTP, page 20-23

Preparing to Download or Upload an Image File by Using TFTP

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

- Ensure that the workstation acting as the TFTP server is properly configured.
- Ensure that the access point has a route to the TFTP server. The access point 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.
- For download operations, ensure that the permissions on the file are set correctly. The permission on the file should be world-read.
- During upload operations, if you are overwriting an existing file 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.

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

Beginning in privileged EXEC mode, follow Steps 1 through 3 to download a new image from a TFTP server and overwrite the existing image.

	Command	Purpose
Step 1	.	Copy the image to the appropriate TFTP directory on the workstation. Make sure the TFTP server is properly configured; see the "Preparing to Download or Upload an Image File by Using TFTP" section on page 20-21
Step 2		Log into the access point through a Telnet session.
Step 3	**archive download-sw /overwrite /reload tftp:**[[*//location*]*/directory*]*/image-name*	Download the image file from the TFTP server to the access point, and overwrite the current image. • The **/overwrite** option overwrites the software image in Flash with the downloaded image. • The **/reload** option reloads the system after downloading the image unless the configuration has been changed and not saved. • For *//location*, specify the IP address of the TFTP server. • For */directory/image-name*, 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*	Download the image file from the TFTP server to the access point, 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 saved. • For *//location*, specify the IP address of the TFTP server. • For */directory/image-name*, specify the directory (optional) and the image to download. Directory and image names are case sensitive.

Note To avoid an unsuccessful download, use the **archive download-sw /safe** command, which downloads the image first and does not delete the current running version until the download succeeds.

The download algorithm verifies that the image is appropriate for the access point 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 The procedure to downgrade an access point IOS is the same procedure for performing an IOS upgrade. To downgrade an access point IOS, enter **archive download-sw /overwrite /reload tftp:**[[*//location*]**/***directory*]**/***image-name.* The */overwrite* parameter erases the current IOS image, and the new downgraded version of IOS is loaded onto the access point. The */reload* option reloads the system after downloading the image unless the configuration has been changed and not saved.

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 system boot path 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.

Uploading an Image File by Using TFTP

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

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

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

	Command	Purpose
Step 1		Make sure the TFTP server is properly configured; see the "Preparing to Download or Upload an Image File by Using TFTP" section on page 20-21.

	Command	Purpose
Step 1		Log into the access point through a Telnet session.
Step 2	**archive upload-sw tftp:**[[*//location*]*/directory*]*/image-name*.**tar**	Upload the currently running access point 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, the HTML files, and info.ver. After these files are uploaded, the upload algorithm creates the tar file format.

Copying Image Files by Using FTP

You can download an access point image from an FTP server or upload the image from the access point to an FTP server.

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

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

This section includes this information:

- Preparing to Download or Upload an Image File by Using FTP, page 20-24
- Downloading an Image File by Using FTP, page 20-25
- Uploading an Image File by Using FTP, page 20-27

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 access point 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 access point 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 access point forms a password named *username@apname.domain*. The variable *username* is the username associated with the current session, ap*name* is the configured host name, and *domain* is the domain of the access point.

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, perform these tasks:

- Ensure that the access point has a route to the FTP server. The access point and the FTP server must be in the same subnetwork if you do not have a router to route traffic between subnets. Verify connectivity to the FTP server by using the **ping** command.
- If you are accessing the access point through 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 access point 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 access point.

For more information, refer to 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.

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

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

	Command	Purpose
Step 1		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 20-24.
Step 2		Log into the access point through 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).

	Command	Purpose
Step 4	**ip ftp username** *username*	(Optional) Change the default remote username.
Step 5	**ip ftp password** *password*	(Optional) Change the default password.
Step 6	**end**	Return to privileged EXEC mode.
Step 7	**archive download-sw /overwrite /reload ftp:**[[*//username*[**:***password*]*@location*]*/directory*] */image-name***.tar**	Download the image file from the FTP server to the access point, and overwrite the current image. • The **/overwrite** option overwrites the software image in Flash with the downloaded image. • The **/reload** option reloads the system after downloading the image unless the configuration has been changed and not saved. • For *//username*[**:***password*], specify the username and password; these must be associated with an account on the FTP server. For more information, see the "Preparing to Download or Upload an Image File by Using FTP" section on page 20-24. • 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 access point, 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 saved. • For *//username*[**:***password*], specify the username and password. These must be associated with an account on the FTP server. For more information, see the "Preparing to Download or Upload an Image File by Using FTP" section on page 20-24. • 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.

Note To avoid an unsuccessful download, use the **archive download-sw /safe** command, which downloads the image first and does not delete the current running version until the download succeeds.

The download algorithm verifies that the image is appropriate for the access point 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 path-list is updated to point to the newly installed image. Use the privileged EXEC mode **show boot** command to display boot attributes, and use the global configuration **boot** command to change the boot attributes.

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.

Uploading an Image File by Using FTP

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

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

The upload feature is available only if the HTML pages associated with the Cluster Management Suite (CMS) have been installed with the existing image.

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

	Command	Purpose
Step 1		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 20-13.
Step 2		Log into the access point through 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 (continue with Step 4 to Step 6).
Step 4	**ip ftp username** *username*	(Optional) Change the default remote username.
Step 5	**ip ftp password** *password*	(Optional) Change the default password.

	Command	Purpose
Step 6	**end**	Return to privileged EXEC mode.
Step 7	**archive upload-sw ftp:**[[**//**[*username*[**:***password*]**@**]*location*]**/***directory*]**/***image-name***.tar**	Upload the currently running access point 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 more information, see the "Preparing to Download or Upload an Image File by Using FTP" section on page 20-24. • 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, the HTML files, and info.ver. After these files are uploaded, the upload algorithm creates the tar file format.

Copying Image Files by Using RCP

You can download an access point image from an RCP server or upload the image from the access point to an RCP server.

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

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

This section includes this information:

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 access point. 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 access point 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 access point software sends the Telnet username as the remote username.
- The access point host name.

For the RCP copy request to execute successfully, an account must be defined on the network server for the remote username. If the server has a directory structure, the 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 access point has a route to the RCP server. The access point 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 access point through 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 access point 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 access point. For UNIX systems, you must add an entry to the .rhosts file for the remote user on the RCP server. For example, suppose the access point contains these configuration lines:

  ```
  hostname ap1
  ip rcmd remote-username User0
  ```

  If the access point IP address translates to *ap1.company.com*, the .rhosts file for User0 on the RCP server should contain this line:

  ```
  ap1.company.com ap1
  ```

For more information, refer to 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.

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

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, skip Step 6.

	Command	Purpose
Step 1		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 20-28.
Step 2		Log into the access point through a Telnet session.
Step 3	**configure terminal**	Enter global configuration mode. This step is required only if you override the default remote username (continue with Step 4 and Step 5).
Step 4	**ip rcmd remote-username** *username*	(Optional) Specify the remote username.
Step 5	**end**	Return to privileged EXEC mode.

	Command	Purpose
Step 6	**archive download-sw /overwrite /reload rcp:**[[[**//**[*username*@]*location*]*/directory*]*/image-name*.**tar**]	Download the image file from the RCP server to the access point, and overwrite the current image. • The **/overwrite** option overwrites the software image in Flash with the downloaded image. • The **/reload** option reloads the system after downloading the image unless the configuration has been changed and not 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 more information, see the "Preparing to Download or Upload an Image File by Using RCP" section on page 20-28. • 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 RCP server to the access point, 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 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 more information, see the "Preparing to Download or Upload an Image File by Using RCP" section on page 20-28. • 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.

Note To avoid an unsuccessful download, use the **archive download-sw /safe** command, which downloads the image first and does not delete the current running version until the download succeeds.

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

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

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

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

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

Uploading an Image File by Using RCP

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

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

The upload feature is available only if the HTML pages associated with the Cluster Management Suite (CMS) have been installed with the existing image.

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

	Command	Purpose
Step 1		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 20-28.
Step 2		Log into the access point through a Telnet session.
Step 3	**configure terminal**	Enter global configuration mode. This step is required only if you override the default remote username (continue with Step 4 and Step 5).
Step 4	**ip rcmd remote-username** *username*	(Optional) Specify the remote username.

	Command	Purpose
Step 5	**end**	Return to privileged EXEC mode.
Step 6	**archive upload-sw rcp:**[[[**//**[*username*@]*location*]*/directory*]*/image-name*.**tar**]	Upload the currently running access point image to the RCP server. • For **//***username*, specify the username; for the RCP copy request to execute, an account must be defined on the network server for the remote username. For more information, see the "Preparing to Download or Upload an Image File by Using RCP" section on page 20-28. • For @*location*, specify the IP address of the RCP 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 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, the HTML files, and info.ver. After these files are uploaded, the upload algorithm creates the tar file format.

Reloading the Image Using the Web Browser Interface

You can also use the Web browser interface to reload the access point image file. The Web browser interface supports loading the image file using HTTP or TFTP interfaces.

Note Your access point configuration is not changed when using the browser to reload the image file.

Browser HTTP Interface

The HTTP interface allows you to browse to the access point image file on your PC and download the image to the access point. Follow the instructions below to use the HTTP interface:

Step 1 Open your Internet browser.

Step 2 Enter the access point's IP address in the browser address line and press **Enter**. An Enter Network Password screen appears.

Step 3 Enter your username in the Username field.

Step 4 Enter the access point password in the Password field and press **Enter**. The Summary Status page appears.

Step 5 Choose **Software** > **Software Upgrade**. The HTTP Upgrade screen appears.

Step 6 Click the **Browse** button to locate the image file on your PC.

Step 7 Click the **Upgrade** button.

For additional information, click the **Help** icon on the Software Upgrade screen.

Browser TFTP Interface

The TFTP interface allows you to use a TFTP server on a network device to load the access point image file. Follow the instructions below to use a TFTP server:

Step 1 Open your Internet browser.

Step 2 Enter the access point's IP address in the browser address line and press **Enter**. An Enter Network Password screen appears.

Step 3 Enter your username in the Username field.

Step 4 Enter the access point password in the Password field and press **Enter**. The Summary Status page appears.

Step 5 Choose **Software > Software Upgrade**. The HTTP Upgrade screen appears.

Step 6 Click the **TFTP Upgrade** tab.

Step 7 Enter the IP address for the TFTP server in the TFTP Server field.

Step 8 Enter the file name for the access point image file in the Upload New System Image Tar File field. If the file is located in a subdirectory of the TFTP server root directory, include the relative path of the TFTP server root directory with the filename. If the file is located in the TFTP root directory, enter only the filename.

Step 9 Click the **Upgrade** button.

For additional information click the Help icon on the Software Upgrade screen.

Downloading Software Image Always from TFTP Server

You can set the AP to download the software image file, always from the TFTP server, even when an image exists on the NVRAM (flash). Once this is set, whenever the AP is reloaded, the AP will always download the software image file from the TFTP server.

Before making this setting you must have the **AutoInstall using DHCP server** feature set for the access points on the router or switch. Without this, the following configurations will not work.

To set the AP to download the software image file always from the TFTP server, add the following command in the configuration file stored on a TFTP server:

Boot sytem ***imagename***

For example:

```
boot system ap3g1-k9w7-tar.wnbu_bt.0101011010
```

As the **AutoInstall using DHCP server** feature is enabled, when the AP reloads, it will get the TFTP IP address and configuration file name. The AP will then download the configuration file from the TFTP server and apply it. If the configuration file has the afore mentioned **Boot sytem** command, it will download the image from the TFTP server and reload with the new image.

Note The download of the software image from the TFTP server will happen only if the image on the server is not the same as the one currently running on the AP.

Example:Configuration file with Boot System Command

```
no aaa new-model
led display off
no ip source-route
no ip cef
ip domain name Sardinia
!
dot11 syslog
!
dot11 ssid myssid
!
dot11 ssid mysssid
   authentication open
!
boot system ap1g1-k9w7-tar.v153_80mr.201410081600

interface Dot11Radio0
 no ip address
 !
 ssid myssid
 !
 antenna gain 0
 packet retries 64 drop-packet
 station-role root
 bridge-group 1
 bridge-group 1 subscriber-loop-control
 bridge-group 1 spanning-disabled
 bridge-group 1 block-unknown-source
 no bridge-group 1 source-learning
 no bridge-group 1 unicast-flooding
!
end
```