



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.

This chapter consists of these sections:

- [Working with the Flash File System, page 16-1](#)
- [Working with Configuration Files, page 16-7](#)
- [Working with Software Images, page 16-18](#)

Working with the Flash File System

The flash file system on your WMIC 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 provides information on the following topics:

- [Displaying Available File Systems, page 16-1](#)
- [Setting the Default File System, page 16-3](#)
- [Displaying Information About Files on a File System, page 16-3](#)
- [Changing Directories and Displaying the Working Directory, page 16-3](#)
- [Creating and Removing Directories, page 16-4](#)
- [Copying Files, page 16-4](#)
- [Deleting Files, page 16-5](#)
- [Creating, Displaying, and Extracting tar Files, page 16-5](#)
- [Displaying the Contents of a File, page 16-7](#)

Displaying Available File Systems

To display the available file systems on your WMIC, use the **show file systems** command as shown in this example:

```
bridge# show file systems
File Systems:
```

	Size(b)	Free(b)	Type	Flags	Prefixes
*	16128000	11118592	flash	rw	flash:
	16128000	11118592	unknown	rw	zflash:
	32768	26363	nvrn	rw	nvrn:
	-	-	network	rw	tftp:
	-	-	opaque	rw	null:
	-	-	opaque	rw	system:
	-	-	opaque	ro	xmodem:
	-	-	opaque	ro	yndem:
	-	-	network	rw	rcp:
	-	-	network	rw	ftp:

Table 16-1 lists field descriptions for the **show file systems** command.

Table 16-1 *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. nvrn —The file system is for a nonvolatile RAM (NVRAM) device. opaque —The file system is a locally generated <i>pseudo</i> file system (for example, the <i>system</i>) or a download interface, such as brimux. unknown —The file system is an unknown type.
Flags	Permission for file system. ro —read-only. rw —read/write. wo —write-only.
Prefixes	Alias for file system. flash: —flash file system. ftp: —File Transfer Protocol (FTP) network server. Used to transfer files to or from the network device. nvrn: —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 16-2](#):

Table 16-2 Commands for Displaying Information About Files

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

Changing Directories and Displaying the Working Directory

To change directories and display the working directory, follow these steps, beginning in privileged EXEC mode:

	Command	Purpose
Step 1	dir <i>filesystem:</i>	Displays the directories on the specified file system. For <i>filesystem:</i> , use flash: for the system board flash device.
Step 2	cd <i>new_configs</i>	Changes to the directory of interest. The command example shows how to change to the directory named <i>new_configs</i> .
Step 3	pwd	Displays 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 <i>filesystem:</i>	Displays the directories on the specified file system. For <i>filesystem:</i> , use flash: for the system board flash device.
Step 2	mkdir <i>old_configs</i>	Creates a new directory. The command example shows how to create the directory named <i>old_configs</i> . Directory names are case sensitive. Directory names are limited to 45 characters between the slashes (/); the name cannot contain control characters, spaces, deletes, slashes, quotes, semicolons, or colons.
Step 3	dir <i>filesystem:</i>	Verifies 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.

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 16-7.

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 16-18.

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 WMIC 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:

```
bridge# 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 the following command in privileged EXEC mode:

```
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:

```
bridge# 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
rnp:[*[[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 the *c1200-k9w7-mx.122-8.JA.tar* file that is in flash memory:

```
bridge# archive tar /table flash:c1200-k9w7-mx.122-8.JA.tar
info (219 bytes)
c1400-k9w7-mx.122-11.JA/ (directory)
c1400-k9w7-mx.122-11.JA/html/ (directory)
c1400-k9w7-mx.122-11.JA/html/foo.html (0 bytes)
c1400-k9w7-mx.122-11.JA/c1200-k9w7-mx.122-8.JA.bin (610856 bytes)
c1400-k9w7-mx.122-11.JA/info (219 bytes)
info.ver (219 bytes)
```

This example shows how to display only the *c1200-k9w7-mx.122-8.JA/html* directory and its contents:

```
bridge# archive tar /table flash:c1200-k9w7-mx.122-8.JA/html
c1400-k9w7-mx.122-11.JA/html/ (directory)
c1400-k9w7-mx.122-11.JA/html/foo.html (0 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.

```
bridge# 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:

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

Working with Configuration Files

This section describes how to create, load, and maintain configuration files. Configuration files contain commands entered to customize the function of the Cisco IOS software. To better benefit from these instructions, your WMIC 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 WMIC for various reasons:

- To restore a backed-up configuration file.
- To use the configuration file for another bridge. For example, you might add another bridge to your network and want it to have a configuration similar to the original bridge. By copying the file to the new bridge, 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 WMIC 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, page 16-8](#)
- [Configuration File Types and Location, page 16-9](#)
- [Creating a Configuration File by Using a Text Editor, page 16-9](#)
- [Copying Configuration Files by Using TFTP, page 16-9](#)
- [Copying Configuration Files by Using FTP, page 16-11](#)
- [Copying Configuration Files by Using RCP, page 16-14](#)
- [Clearing Configuration Information, page 16-17](#)

Guidelines for Creating and Using Configuration Files

Creating configuration files can aid in your WMIC 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 WMIC, you must set them on each bridge 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 WMIC 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 WMIC as if you were entering the commands at the command line. The WMIC 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 WMIC.

Configuration File Types and Location

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

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

Creating a Configuration File by Using a Text Editor

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

-
- | | |
|---------------|---|
| Step 1 | Copy an existing configuration from a WMIC to a server.

For more information, see the “Downloading the Configuration File by Using TFTP” section on page 16-10, the “Downloading a Configuration File by Using FTP” section on page 16-12, or the “Downloading a Configuration File by Using RCP” section on page 16-15. |
| 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 WMIC by using configuration files you create, download from another device, 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](#), page 16-10
- [Downloading the Configuration File by Using TFTP](#), page 16-10
- [Uploading the Configuration File by Using TFTP](#), page 16-11

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. 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, refer to the documentation for your workstation.

- Ensure that the WMIC has a route to the TFTP server. The WMIC 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 WMIC 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 16-10.
 - Step 3** Log in to the WMIC through a Telnet session.
 - Step 4** Download the configuration file from the TFTP server to configure the WMIC.

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

Use one of these privileged EXEC commands:

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

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

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

```
bridge# 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 WMIC 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 16-10.
 - Step 2** Log in to the WMIC through a Telnet session.
 - Step 3** Upload the WMIC configuration to the TFTP server. Specify the IP address or hostname of the TFTP server and the destination filename.

Use one of these privileged EXEC commands:

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

The file is uploaded to the TFTP server.

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

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

Copying Configuration Files by Using FTP

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

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

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, page 16-12](#)
- [Downloading a Configuration File by Using FTP, page 16-12](#)
- [Uploading a Configuration File by Using FTP, page 16-13](#)

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 WMIC has a route to the FTP server. The WMIC 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 WMIC 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 WMIC 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 WMIC.

For more information, refer to the documentation for your FTP server.

Downloading a Configuration File by Using FTP

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

	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 16-15.
Step 2		Log in to the WMIC through a Telnet session.
Step 1	configure terminal	Enters global configuration mode on the WMIC. This step is required only if you override the default remote username or password (see Steps 4, 5, and 6).

	Command	Purpose
Step 2	ip ftp username <i>username</i>	(Optional) Changes the default remote username.
Step 3	ip ftp password <i>password</i>	(Optional) Changes the default password.
Step 4	end	Returns to privileged EXEC mode.
Step 5	copy ftp:[[[//[username[:password]@]location]/directory] <i>/filename</i> system:running-config or copy ftp:[[[//[username[:password]@]location]/directory] <i>/filename</i> nvrn:startup-config	Using FTP, copies 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-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 WMIC:

```
bridge# 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]
bridge#
%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 WMIC startup configuration.

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

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

	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 16-15.
Step 2		Log in to the WMIC through a Telnet session.

	Command	Purpose
Step 3	configure terminal	Enters 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 ftp username <i>username</i>	(Optional) Changes the default remote username.
Step 5	ip ftp password <i>password</i>	(Optional) Changes the default password.
Step 6	end	Returns 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, stores the WMIC running or startup configuration file to the specified location.

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

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

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

```
bridge# configure terminal
bridge(config)# ip ftp username netadmin2
bridge(config)# ip ftp password mypass
bridge(config)# end
bridge# copy nvram:startup-config ftp:
Remote host[?] 172.16.101.101
Name of configuration file to write [ap2-config]?
Write file ap2-config 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 WMIC. 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 WMIC 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 WMIC software sends the Telnet username as the remote username.
- The WMIC hostname.

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

This section includes this information:

- [Preparing to Download or Upload a Configuration File by Using RCP, page 16-15](#)
- [Downloading a Configuration File by Using RCP, page 16-15](#)
- [Uploading a Configuration File by Using RCP, page 16-16](#)

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 WMIC has a route to the RCP server. The WMIC 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 WMIC 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 WMIC 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 WMIC. 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 WMIC contains these configuration lines:

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

If the WMIC 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

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

	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 16-15.
Step 2		Log in to the WMIC through a Telnet session.
Step 3	configure terminal	Enters global configuration mode. This step is required only if you override the default remote username (see Steps 4 and 5).
Step 4	ip rcmd remote-username <i>username</i>	(Optional) Specifies the remote username.
Step 5	end	Returns to privileged EXEC mode.
Step 6	copy rcp:[[[//[<i>username@</i>]<i>location</i>]/<i>directory</i>]/<i>filename</i>] system:running-config or copy rcp:[[[//[<i>username@</i>]<i>location</i>]/<i>directory</i>]/<i>filename</i>] nvrn:startup-config	Using RCP, copies 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-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 WMIC:

```
bridge# 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]
bridge#
%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:

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

To upload a configuration file by using RCP, follow these steps, beginning in privileged EXEC mode:

	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 16-15.
Step 2		Log in to the WMIC through a Telnet session.
Step 3	configure terminal	Enters global configuration mode. This step is required only if you override the default remote username (see Steps 4 and 5).
Step 4	ip rcmd remote-username <i>username</i>	(Optional) Specifies the remote username.
Step 5	end	Returns to privileged EXEC mode.
Step 6	copy system:running-config rcp:[[//[<i>username@</i>]<i>location</i>]/<i>directory</i>]/<i>filename</i>] or copy nvram:startup-config rcp:[[//[<i>username@</i>]<i>location</i>]/<i>directory</i>]/<i>filename</i>]	Using RCP, copies the configuration file from an WMIC 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:

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

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

```
bridge# configure terminal
bridge(config)# ip rcmd remote-username netadmin2
bridge(config)# end
bridge# 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 WMIC prompts for confirmation on destructive file operations. For more information about the **file prompt** command, refer to the *Cisco IOS Command Reference for Release 12.1*.

Working with Software Images

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

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

- [Image Location on the WMIC, page 16-18](#)
- [tar File Format of Images on a Server or Cisco.com, page 16-19](#)
- [Copying Image Files by Using TFTP, page 16-19](#)
- [Copying Image Files by Using FTP, page 16-22](#)
- [Copying Image Files by Using RCP, page 16-27](#)



Note

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

Image Location on the WMIC

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 WMIC. 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.

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.)
- IOS image
- Web management files needed by the HTTP server on the WMIC
- radio firmware 6500.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 WMIC image from a TFTP server or upload the image from the WMIC to a TFTP server.

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

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

This section includes this information:

- [Preparing to Download or Upload an Image File by Using TFTP, page 16-19](#)
- [Downloading an Image File by Using TFTP, page 16-20](#)
- [Uploading an Image File by Using TFTP, page 16-22](#)

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. 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, refer to the documentation for your workstation.

- Ensure that the WMIC has a route to the TFTP server. The WMIC 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.



Caution

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

To download a new image from a TFTP server and overwrite the existing image, follow these steps, beginning in privileged EXEC mode:

	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 16-19
Step 2		Log in to the WMIC through a Telnet session.

	Command	Purpose
Step 3	archive download-sw /overwrite /reload ftp:[[/location]/directory]/image-name	Downloads the image file from the TFTP server to the WMIC, and overwrite the current image. <ul style="list-style-type: none"> • 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 <i>location</i>, specify the IP address of the TFTP server. • For <i>directory/image-name</i>, specify the directory (optional) and the image to download. Directory and image names are case sensitive.
Step 4	archive download-sw /leave-old-sw /reload ftp:[[/location]/directory]/image-name	Downloads the image file from the TFTP server to the WMIC, and keep the current image. <ul style="list-style-type: none"> • The /leave-old-sw option keeps the old software version after a download. • The /reload option reloads the system after downloading the image unless the configuration has been changed and not saved. • For <i>location</i>, specify the IP address of the TFTP server. • For <i>directory/image-name</i>, 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 WMIC model and that enough DRAM is present, or it aborts the process and reports an error. If you specify the **/overwrite** option, the download algorithm removes the existing image on the flash device whether or not it is the same as the new one, downloads the new image, and then reloads the software.

**Note**

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

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

The algorithm installs the downloaded image on the system board flash device (flash:). The image is placed into a new directory named with the software version string, and the 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 WMIC to a TFTP server. You can later download this image to the WMIC or to another WMIC 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 16-19.
Step 1		Log in to the WMIC through a Telnet session.
Step 2	archive upload-sw tftp:[[/location]/directory]/image-name.tar	Uploads the currently running WMIC image to the TFTP server. <ul style="list-style-type: none"> For <i>location</i>, specify the IP address of the TFTP server. For <i>directory/image-name.tar</i>, specify the directory (optional) and the name of the software image to be uploaded. Directory and image names are case sensitive. The <i>image-name.tar</i> is the name of the software image to be stored on the server.

The **archive upload-sw** privileged EXEC command builds an image file on the server by uploading these files in order: info, the 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 a WMIC image from an FTP server or upload the image from the WMIC to an FTP server.

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

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

This section includes this information:

- [Preparing to Download or Upload an Image File by Using FTP, page 16-22](#)
- [Downloading an Image File by Using FTP, page 16-23](#)
- [Uploading an Image File by Using FTP, page 16-26](#)

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 WMIC 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 WMIC 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 WMIC forms a password named *username@apname.domain*. The variable *username* is the username associated with the current session, *apname* is the configured hostname, and *domain* is the domain of the WMIC.

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 WMIC has a route to the FTP server. The WMIC 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 WMIC 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 WMIC 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 WMIC.

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 Steps 1 through 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 16-22.
Step 2		Log in to the WMIC through a Telnet session.
Step 3	configure terminal	Enters 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 ftp username <i>username</i>	(Optional) Changes the default remote username.
Step 5	ip ftp password <i>password</i>	(Optional) Changes the default password.
Step 6	end	Returns to privileged EXEC mode.

Command	Purpose
Step 7 archive download-sw /overwrite /reload ftp:[[/username[:password]@location]/directory] image-name.tar	Downloads the image file from the FTP server to the WMIC, and overwrite the current image. <ul style="list-style-type: none"> • 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 <i>//username[:password]</i>, specify the username and password; these must be associated with an account on the FTP server. For more information, see the “Preparing to Download or Upload an Image File by Using FTP” section on page 16-22. • For <i>@location</i>, specify the IP address of the FTP server. • For <i>directory/image-name.tar</i>, specify the directory (optional) and the image to download. Directory and image names are case sensitive.
Step 8 archive download-sw /leave-old-sw /reload ftp:[[/username[:password]@location]/directory] image-name.tar	Downloads the image file from the FTP server to the WMIC, and keep the current image. <ul style="list-style-type: none"> • The /leave-old-sw option keeps the old software version after a download. • The /reload option reloads the system after downloading the image unless the configuration has been changed and not saved. • For <i>//username[:password]</i>, specify the username and password. These must be associated with an account on the FTP server. For more information, see the “Preparing to Download or Upload an Image File by Using FTP” section on page 16-22. • For <i>@location</i>, specify the IP address of the FTP server. • For <i>directory/image-name.tar</i>, specify the directory (optional) and the image to download. Directory and image names are case sensitive.

**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 WMIC 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 WMIC to an FTP server. You can later download this image to the same WMIC or to another WMIC 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 16-12.
Step 2		Log in to the WMIC through a Telnet session.
Step 3	configure terminal	Enters 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 ftp username <i>username</i>	(Optional) Changes the default remote username.
Step 5	ip ftp password <i>password</i>	(Optional) Changes the default password.

	Command	Purpose
Step 6	end	Returns to privileged EXEC mode.
Step 7	archive upload-sw ftp:[/[username[:password]@]location]/directory]/ image-name.tar	<p>Uploads the currently running WMIC image to the FTP server.</p> <ul style="list-style-type: none"> For <i>//username:password</i>, specify the username and password. These must be associated with an account on the FTP server. For more information, see the “Preparing to Download or Upload an Image File by Using FTP” section on page 16-22. For <i>@location</i>, specify the IP address of the FTP server. For <i>/directory/image-name.tar</i>, specify the directory (optional) and the name of the software image to be uploaded. Directory and image names are case sensitive. The <i>image-name.tar</i> is the name of the software image to be stored on the server.

The **archive upload-sw** command builds an image file on the server by uploading these files in order: info, the 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 a WMIC image from an RCP server or upload the image from the WMIC to an RCP server.

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

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

This section includes this information:

- [Preparing to Download or Upload an Image File by Using RCP, page 16-27](#)
- [Downloading an Image File by Using RCP, page 16-29](#)
- [Uploading an Image File by Using RCP, page 16-31](#)

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 WMIC. 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 WMIC 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 WMIC software sends the Telnet username as the remote username.
- The WMIC 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 WMIC has a route to the RCP server. The WMIC 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 WMIC 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 WMIC 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 WMIC. For UNIX systems, you must add an entry to the .rhosts file for the remote user on the RCP server. For example, suppose the WMIC contains these configuration lines:

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

If the WMIC 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 16-27.
Step 2		Log in to the WMIC through a Telnet session.
Step 3	configure terminal	Enters global configuration mode. This step is required only if you override the default remote username (see Steps 4 and 5).
Step 4	ip rcmd remote-username <i>username</i>	(Optional) Specifies the remote username.
Step 5	end	Returns to privileged EXEC mode.
Step 6	archive download-sw /overwrite /reload rcp: [[[// <i>username@</i>] <i>location</i>]/ <i>directory</i>]/ <i>image-name.tar</i>]	Downloads the image file from the RCP server to the WMIC, and overwrite the current image. <ul style="list-style-type: none"> 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 <i>//username</i>, specify the username. For the RCP copy request to execute successfully, an account must be defined on the network server for the remote username. For more information, see the “Preparing to Download or Upload an Image File by Using RCP” section on page 16-27. For <i>@location</i>, specify the IP address of the RCP server. For <i>/directory/image-name.tar</i>, specify the directory (optional) and the image to download. Directory and image names are case sensitive.

Command	Purpose
Step 7 archive download-sw /leave-old-sw /reload rcp:[[//[username@]location]/directory]/image-name.tar]	Downloads the image file from the RCP server to the WMIC, and keep the current image. <ul style="list-style-type: none"> • The /leave-old-sw option keeps the old software version after a download. • The /reload option reloads the system after downloading the image unless the configuration has been changed and not saved. • For <i>//username</i>, specify the username. For the RCP copy request to execute, an account must be defined on the network server for the remote username. For more information, see the “Preparing to Download or Upload an Image File by Using RCP” section on page 16-27. • For <i>@location</i>, specify the IP address of the RCP server. • For <i>/directory]/image-name.tar</i>, specify the directory (optional) and the image to download. Directory and image names are case sensitive.

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

**Note**

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

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

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

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

Uploading an Image File by Using RCP

You can upload an image from the WMIC to an RCP server. You can later download this image to the same WMIC or to another WMIC 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 16-27.
Step 2		Log in to the WMIC through a Telnet session.
Step 3	configure terminal	Enters global configuration mode. This step is required only if you override the default remote username (see Steps 4 and 5).
Step 4	ip rcmd remote-username <i>username</i>	(Optional) Specifies the remote username.
Step 5	end	Returns to privileged EXEC mode.
Step 6	archive upload-sw rmp: [[[/ <i>username@location</i>]/ <i>directory</i>]/ <i>image-name.tar</i>]	Uploads the currently running WMIC image to the RCP server. <ul style="list-style-type: none"> For <i>//username</i>, specify the username; for the RCP copy request to execute, an account must be defined on the network server for the remote username. For more information, see the “Preparing to Download or Upload an Image File by Using RCP” section on page 16-27. For <i>@location</i>, specify the IP address of the RCP server. For <i>/directory/image-name.tar</i>, specify the directory (optional) and the name of the software image to be uploaded. Directory and image names are case sensitive. The <i>image-name.tar</i> is the name of software image to be stored on the server.

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

