



Cisco IOS File System, Configuration Files, and Bundle Files Appendix, Cisco IOS XE Release 3SE (Catalyst 3850 Switches)

January 29, 2013

Americas Headquarters

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
<http://www.cisco.com>
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Text Part Number: OL-28266-01

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

Cisco IOS File System, Configuration Files, and Bundle Files Appendix, Cisco IOS XE Release 3SE (Catalyst 3850 Switches)
© 2013 Cisco Systems, Inc. All rights reserved.



CONTENTS

Working with the Flash File System	A-1
Displaying Available File Systems	A-2
Setting the Default File System	A-3
Displaying Information about Files on a File System	A-4
Changing Directories and Displaying the Working Directory	A-4
Creating and Removing Directories	A-5
Copying Files	A-6
Deleting Files	A-6
Creating, Displaying, and Extracting Files	A-8
Working with Configuration Files	A-10
Guidelines for Creating and Using Configuration Files	A-11
Configuration File Types and Location	A-12
Creating a Configuration File By Using a Text Editor	A-12
Copying Configuration Files By Using TFTP	A-13
Preparing to Download or Upload a Configuration File By Using TFTP	A-13
Downloading the Configuration File By Using TFTP	A-13
Uploading the Configuration File By Using TFTP	A-14
Copying Configuration Files By Using FTP	A-14
Preparing to Download or Upload a Configuration File By Using FTP	A-15
Downloading a Configuration File By Using FTP	A-16
Uploading a Configuration File By Using FTP	A-17
Copying Configuration Files By Using RCP	A-18
Preparing to Download or Upload a Configuration File By Using RCP	A-18
Downloading a Configuration File By Using RCP	A-19
Uploading a Configuration File By Using RCP	A-21
Clearing Configuration Information	A-22
Clearing the Startup Configuration File	A-22
Deleting a Stored Configuration File	A-22
Replacing and Rolling Back Configurations	A-22
Understanding Configuration Replacement and Rollback	A-22
Configuration Guidelines	A-23
Configuring the Configuration Archive	A-24
Performing a Configuration Replacement or Rollback Operation	A-25
Working with Cisco IOS XE Software Bundles	A-26
About Cisco IOS XE Software Bundles and Packages	A-27

Bundle and Package File Location on the Switch	A-27
Downloading and Uploading Cisco IOS XE Bundle Files	A-27
Copying Cisco IOS XE Bundle Files By Using TFTP	A-28
Copying Cisco IOS XE Bundle Files By Using FTP	A-29
Copying Cisco IOS XE Bundle Files By Using RCP	A-31
Upgrading Cisco IOS XE Software	A-33
Upgrading Cisco IOS XE Software: Installed Mode	A-33
Upgrading Cisco IOS XE Software: Bundle Mode	A-34
Converting from the Bundle Running Mode to the Installed Running Mode	A-35
Copying IOS XE Package and Bundle Files From One Stack Member to Another	A-36
Upgrading a Switch Running Incompatible Software	A-38
Upgrading a Switch Running in Incompatible Running Mode	A-39



APPENDIX **A**

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

This appendix describes how to manipulate the Catalyst 3850 switch flash file system, how to copy configuration files, and how to install and copy bundle files on a Catalyst 3850 switch or a Catalyst 3850 switch stack.

Unless otherwise noted, the term *switch* refers to a standalone switch and to a switch stack.



Note

For complete syntax and usage information for the commands used in this chapter, see the switch command reference for this release.

- [Working with the Flash File System, page A-1](#)
- [Working with Configuration Files, page A-10](#)
- [Working with Cisco IOS XE Software Bundles, page A-26](#)

Working with the Flash File System

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

As viewed from the stack master, or any stack member, *flash:* refers to the local flash device, which is the device attached to the same switch on which the file system is being viewed. In a switch stack, each of the flash devices from the various stack members can be viewed from the stack master. The names of these flash file systems include the corresponding switch member numbers. For example, *flash-3:*, as viewed from the stack master, refers to the same file system as does *flash:* on stack member 3. Use the **show file systems** privileged EXEC command to list all file systems, including the flash file systems in the switch stack.

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

- [Displaying Available File Systems, page A-2](#)
- [Setting the Default File System, page A-3](#)
- [Displaying Information about Files on a File System, page A-4](#)
- [Changing Directories and Displaying the Working Directory, page A-4](#)
- [Creating and Removing Directories, page A-5](#)

- [Copying Files, page A-6](#)
- [Deleting Files, page A-6](#)
- [Creating, Displaying, and Extracting Files, page A-8](#)

Displaying Available File Systems

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

```
Switch# show file systems
File Systems:
      Size(b)      Free(b)      Type  Flags  Prefixes
*    15998976      5135872      flash rw    flash:
      -            -            opaque rw    bs:
      -            -            opaque rw    vb:
      524288       520138       nvram  rw    nvram:
      -            -            network rw    tftp:
      -            -            opaque rw    null:
      -            -            opaque rw    system:
      -            -            opaque ro    xmodem:
      -            -            opaque ro    ymodem:
```

This example shows a switch stack. In this example, the stack master is stack member 1; the file system on stack member 2 is displayed as flash-2, the file system on stack member 3 is displayed as flash-3 and so on. The example also shows the crashinfo directories and a USB flash drive plugged into the stack master.

```
Switch# show file systems
File Systems:
      Size(b)      Free(b)      Type  Flags  Prefixes
      145898496      68792320      disk  rw    crashinfo:
      146014208      99090432      disk  rw    crashinfo-2:
      248512512      87031808      disk  rw    crashinfo-3:
      146276352      108003328     disk  rw    crashinfo-4:
*    1749458944      1258868736     disk  rw    flash:
      729546752      282853376     disk  rw    flash-2:
      1622147072     1173880832     disk  rw    flash-3:
      1749549056     1301282816     disk  rw    flash-4:
      -            0            disk  rw    unix:
      -            -            disk  rw    usbflash0:
      1027342336     64749568      disk  rw    usbflash0-2:
      -            -            disk  rw    usbflash0-3:
      -            -            disk  rw    usbflash0-4:
      -            -            opaque rw    system:
      -            -            opaque rw    tmpsys:
      -            -            nvram  rw    stby-nvram:
      -            -            nvram  rw    stby-rcsf:
      -            -            opaque rw    null:
      -            -            opaque ro    tar:
      -            -            network rw    tftp:
      2097152        2071500       nvram  rw    nvram:
      -            -            opaque wo    syslog:
      -            -            network rw    rcp:
      -            -            network rw    http:
      -            -            network rw    ftp:
      -            -            network rw    scp:
      -            -            network rw    https:
      -            -            opaque ro    cns:
```

Table A-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. disk —The file system is for a flash memory device, USB flash, and crashinfo file. network —The file system for network devices; for example, an FTP server or and HTTP server. nvr am—The file system is for a NVRAM device. opaque —The file system is a locally generated <i>pseudo</i> file system (for example, the <i>system</i>) or a download interface, such as brimux. unknown —The file system is an unknown type.
Flags	Permission for file system. ro —read-only. rw —read/write. wo —write-only.
Prefixes	Alias for file system. crashinfo: —Crashinfo file. flash: —Flash file system. ftp: —FTP server. http: —HTTP server. https: —Secure HTTP server. nvr am:—NVRAM. null: —Null destination for copies. You can copy a remote file to null to find its size. rcp: —Remote Copy Protocol (RCP) server. scp: —Session Control Protocol (SCP) server. system: —Contains the system memory, including the running configuration. tftp: —TFTP network server. xmodem: —Obtain the file from a network machine by using the Xmodem protocol. ymodem: —Obtain the file from a network machine by using the Ymodem protocol.

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 A-2](#):

Table A-2 Commands for Displaying Information About Files

Command	Description
dir [/all] [filesystem:][filename]	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 file-url	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.

To display information about the driver text object in the CISCO-MEMORY-POOL-MIB, use the **show memory** privileged EXEC command:

```
Switch# show memory
System memory   : 1939252K total, 1317664K used, 621588K free, 118580K kernel reserved
Lowest (b)      : 54189544

                Total (K)    Used (K)    Free (K)
Process         1939252    1317664    621588
Config          0          0          0
```

Changing Directories and Displaying the Working Directory

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

Command	Purpose
Step 1 dir filesystem:	Displays the directories on the specified file system. For <i>filesystem:</i> , use flash: for the system board flash device.
Example: Switch# dir flash:	To access flash partitions of switch members in a stack, use flash-n where <i>n</i> is the stack member number. For example, flash-4 .

	Command	Purpose
Step 2	<code>cd directory_name</code> Example: Switch# cd new_configs	Changes to the directory of interest. The command example shows how to change to the directory named <i>new_configs</i> .
Step 3	<code>pwd</code> Example: Switch# pwd	Displays the working directory.

Creating and Removing Directories

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

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

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

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

For *filesystem*, use **flash:** for the system board flash device. For *file-url*, enter the name of the directory to be deleted. All 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** *source-url destination-url* privileged EXEC command. For the source and destination URLs, you can use **running-config** and **startup-config** keyword shortcuts. For example, the **copy running-config startup-config** command saves the currently running configuration file to the NVRAM section of flash memory to be used as the configuration during system initialization.

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

Network file system URLs include **ftp:**, **rtp:**, and **tftp:** and have these syntaxes:

- FTP—**ftp:**[[//username [:password]@location]/directory]/filename
- RCP—**rtp:**[[//username@location]/directory]/filename
- SCP—**scp:**[[//username@location]/directory]/filename
- 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 A-10.

Deleting Files

When you no longer need files on a flash memory device, you can permanently delete them.

- Use the **delete** command to remove any type of file.
- Use the **software clean** command to remove unused package files and provisioning files.



Caution

When files are deleted, their contents cannot be recovered.

Use the **delete /recursive** [*filesystem:*]/*file-url* privileged EXEC command when you want to delete files on the flash device including the current package and provisioning files. Use the **/recursive** keyword to delete a directory and all subdirectories and the files contained in it. Use the *filesystem:* option to specify the device from which to delete the files. If you omit the *filesystem:* option, the switch uses the default device specified by the **cd** command. Use the *file-url* option, to specify the path (directory) and the name of the file to be deleted.

When you attempt to delete files, the system prompts you to confirm the deletion of each file. Use the **/force** keyword to suppress system prompts to confirm the deletion of each file. You are prompted only once at the beginning of the deletion process.

We recommend that you use the **software clean** command instead of the **delete** command when you are removing package files and provisioning files. The **software clean** command leaves the running package files and the current provisioning (*packages.cnf*) file intact.

Beginning in privileged EXEC mode, follow these steps to delete unnecessary package files and provisioning files on the flash memory device:

	Command	Purpose
Step 1	software clean flash: <i>/file-url</i>	Deletes unused files from the local flash memory device.
	Example: Switch# software clean flash:	For flash: <i>/file-url</i> , specify the location of the files you wish to delete. If a path is not specified, the path is the boot path.
Step 2	yes	Specifies that the listed files be deleted.
	or	or
	no	Specifies that the deletion process be canceled.

This example shows how to use the command to delete unused files on each switch in a two-switch stack:

```
3850-Stack# software clean
Preparing clean operation ...
[1 2]: Cleaning up unnecessary package files
[1 2]: No path specified, will use booted path flash:packages.conf
[1 2]: Cleaning flash:
[1]: Preparing packages list to delete ...
  cat3850-base.SSA.03.08.79.EMP1.pkg
    File is in use, will not delete.
  cat3850-drivers.SSA.03.08.79.EMP1.pkg
    File is in use, will not delete.
  cat3850-infra.SSA.03.08.79.EMP1.pkg
    File is in use, will not delete.
  cat3850-iosd-universalk9.SSA.150-8.79.EMP1.pkg
    File is in use, will not delete.
  cat3850-platform.SSA.03.08.79.EMP1.pkg
    File is in use, will not delete.
  cat3850-wcm.SSA.03.08.79.EMP1.pkg
    File is in use, will not delete.
  packages.conf
    File is in use, will not delete.
[2]: Preparing packages list to delete ...
  cat3850-base.SSA.03.08.79.EMP1.pkg
    File is in use, will not delete.
  cat3850-drivers.SSA.03.08.79.EMP1.pkg
    File is in use, will not delete.
  cat3850-infra.SSA.03.08.79.EMP1.pkg
    File is in use, will not delete.
  cat3850-iosd-universalk9.SSA.150-8.79.EMP1.pkg
    File is in use, will not delete.
  cat3850-platform.SSA.03.08.79.EMP1.pkg
    File is in use, will not delete.
  cat3850-wcm.SSA.03.08.79.EMP1.pkg
    File is in use, will not delete.
  packages.conf
    File is in use, will not delete.
[1]: Files that will be deleted:
  cat3850-base.SSA.03.08.72.EMP2.pkg
  cat3850-drivers.SSA.03.08.72.EMP2.pkg
  cat3850-infra.SSA.03.08.72.EMP2.pkg
  cat3850-iosd-universalk9.SSA.150-8.72.EMP2.pkg
  cat3850-platform.SSA.03.08.72.EMP2.pkg
  cat3850-universalk9.03.08.79.EMP1.bin
  cat3850-wcm.SSA.03.08.72.EMP2.pkg
  packages.conf.01-
[2]: Files that will be deleted:
```

```

cat3850-base.SSA.03.08.72.EMP2.pkg
cat3850-drivers.SSA.03.08.72.EMP2.pkg
cat3850-infra.SSA.03.08.72.EMP2.pkg
cat3850-iosd-universalk9.SSA.150-8.72.EMP2.pkg
cat3850-platform.SSA.03.08.72.EMP2.pkg
cat3850-universalk9.03.08.79.EMP1.bin
cat3850-wcm.SSA.03.08.72.EMP2.pkg
packages.conf.00-

```

```

[1 2]: Do you want to proceed with the deletion? [yes/no]: yes
[1 2]: Clean up completed

```

When the switch is running in installed mode and you attempt to delete the current package files or provisioning file, the system displays additional caution messages. The following example shows the warning message and confirmation prompts displayed when you try to delete a package file that is in use:

```

Switch# delete flash:cat3k_caa-base.SSA.03.09.19.EMP.pkg
Delete filename [cat3k_caa-base.SSA.03.09.19.EMP.pkg]?
Delete flash:/cat3k_caa-base.SSA.03.09.19.EMP.pkg? [confirm]
This package file is currently in use and is part of the committed package set.
Deleting it may cause system instability and may prevent the system from booting on the
next reload.

Still want to delete flash:/cat3k_caa-base.SSA.03.09.19.EMP.pkg? [confirm]no
Delete of flash:/cat3k_caa-base.SSA.03.09.19.EMP.pkg aborted!
Switch#

```

**Note**

The warning message and confirmation prompt are not displayed when the specified package file is not in use; the specified file is not a package file; or the **delete** command's **/force** option is used.

Creating, Displaying, and Extracting Files

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

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

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

Command	Purpose
<p>Step 3</p> <p>archive tar /xtract <i>source-url</i> flash:/file-url [<i>dir/file...</i>]</p> <p>Example: Switch# archive tar /xtract tftp:/172.20.10.30/saved. flash:/new-configs</p>	<p>Extracts a file into a directory on the flash file system.</p> <p>For <i>source-url</i>, specify the source URL alias for the local file system. The <i>-filename.</i> is the file from which to extract files. These options are supported:</p> <ul style="list-style-type: none"> local flash file system syntax: flash: FTP syntax: ftp:[[//<i>username</i>[:<i>password</i>]<i>@location</i>]/<i>directory</i>]/-<i>filename.</i> RCP syntax: rcp:[[//<i>username</i><i>@location</i>]/<i>directory</i>]/-<i>filename.</i> TFTP syntax: tftp:[[//<i>location</i>]/<i>directory</i>]/-<i>filename.</i> <p>For flash:/file-url [<i>dir/file...</i>], specify the location on the local flash file system from which the file is extracted. Use the <i>dir/file...</i> option to specify a list of files or directories within the file to be extracted. If none are specified, all files and directories are extracted.</p>
<p>Step 4</p> <p>more [<i>/ascii</i> <i>/binary</i> <i>/ebdic</i>] <i>file-url</i></p> <p>Example: Switch# more flash: /new-configs</p>	<p>Displays the contents of any readable file, including a file on a remote file system.</p>

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

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

This example shows how to extract the contents of a file located on the TFTP server at 172.20.10.30:

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

Working with Configuration Files

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

Configuration files contain commands entered to customize the function of the Cisco IOS software. A way to create a basic configuration file is to use the **setup** program or to enter the **setup** privileged EXEC command.

You can copy (*download*) configuration files from a TFTP, FTP, or RCP server to the running configuration or startup configuration of the switch. You perform this task when you want to:

- Restore a backed-up configuration file.
- Use the configuration file for another switch. For example, you might add another switch to your network and want it to have a configuration similar to the original switch. By copying the file to the new switch, you can change the relevant parts rather than recreating the whole file.
- Load the same configuration commands on all the switches in your network so that all the switches have similar configurations.

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

The protocol you use depends on which type of server you are using. The FTP and RCP transport mechanisms provide faster performance and more reliable delivery of data than TFTP. These improvements are possible because FTP and RCP are built on and use the TCP/IP stack, which is connection-oriented.

- [Guidelines for Creating and Using Configuration Files, page A-11](#)
- [Configuration File Types and Location, page A-12](#)
- [Creating a Configuration File By Using a Text Editor, page A-12](#)
- [Copying Configuration Files By Using TFTP, page A-13](#)
- [Copying Configuration Files By Using FTP, page A-14](#)
- [Copying Configuration Files By Using RCP, page A-18](#)
- [Clearing Configuration Information, page A-22](#)
- [Replacing and Rolling Back Configurations, page A-22](#)

Guidelines for Creating and Using Configuration Files

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

Use these guidelines when creating a configuration file:

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

**Note**

The **copy {ftp: | rcp: | tftp:} system:running-config** privileged EXEC command loads the configuration files on the switch as if you were entering the commands at the command line. The switch does not erase the existing running configuration before adding the commands. If a command in the copied configuration file replaces a command in the existing configuration file, the existing command is erased. For example, if the copied configuration file contains a different IP address in a particular command than the existing configuration, the IP address in the copied configuration is used. However, some commands in the existing configuration might not be replaced or negated. In this case, the resulting configuration file is a mixture of the existing configuration file and the copied configuration file, with the copied configuration file having precedence.

To restore a configuration file to an exact copy of a file stored on a server, copy the configuration file directly to the startup configuration (by using the **copy {ftp: | rcp: | tftp:} nvram:startup-config** privileged EXEC command), and reload the switch.

Configuration File Types and Location

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

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

Creating a Configuration File By Using a Text Editor

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

-
- Step 1** Copy an existing configuration from a switch to a server.
For more information, see the [“Downloading the Configuration File By Using TFTP”](#) section on page A-13, the [“Downloading a Configuration File By Using FTP”](#) section on page A-16, or the [“Downloading a Configuration File By Using RCP”](#) section on page A-19.
 - Step 2** Open the configuration file in a text editor, such as vi or emacs on UNIX or Notepad on a PC.
 - Step 3** Extract the portion of the configuration file with the desired commands, and save it in a new file.
 - Step 4** Copy the configuration file to the appropriate server location. For example, copy the file to the TFTP directory on the workstation (usually /tftpboot on a UNIX workstation).
 - Step 5** Make sure the permissions on the file are set to world-read.
-

Copying Configuration Files By Using TFTP

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

- [Preparing to Download or Upload a Configuration File By Using TFTP, page A-13](#)
- [Downloading the Configuration File By Using TFTP, page A-13](#)
- [Uploading the Configuration File By Using TFTP, page A-14](#)

Preparing to Download or Upload a Configuration File By Using TFTP

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

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

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

```
tftp 69/udp
```



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

- Ensure that the switch has a route to the TFTP server. The switch and the TFTP server must be in the same subnetwork if you do not have a router to route traffic between subnets. Check connectivity to the TFTP server by using the **ping** command.
- Ensure that the configuration file to be downloaded is in the correct directory on the TFTP server (usually `/tftpboot` on a UNIX workstation).
- For download operations, ensure that the permissions on the file are set correctly. The permission on the file should be world-read.
- Before uploading the configuration file, you might need to create an empty file on the TFTP server. To create an empty file, enter the **touch filename** command, where *filename* is the name of the file you will use when uploading it to the server.
- During upload operations, if you are overwriting an existing file (including an empty file, if you had to create one) on the server, ensure that the permissions on the file are set correctly. Permissions on the file should be world-write.

Downloading the Configuration File By Using TFTP

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

- Step 1** Copy the configuration file to the appropriate TFTP directory on the TFTP server.
- 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 A-13.
- Step 3** Log into the switch through the console port, the Ethernet management port, or a Telnet session.
- Step 4** Download the configuration file from the TFTP server to configure the switch.

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

Use one of these privileged EXEC commands:

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

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

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

```
Switch# copy tftp://172.16.2.155/tokyo-config system:running-config
Configure using tokyo-config from 172.16.2.155? [confirm] y
Booting tokyo-config from 172.16.2.155:!!! [OK - 874/16000 bytes]
```

Uploading the Configuration File By Using TFTP

To upload a configuration file from a switch 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 A-13.
 - Step 2** Log into the switch through the console port, the Ethernet management port, or a Telnet session.
 - Step 3** Upload the switch configuration to the TFTP server. Specify the IP address or hostname of the TFTP server and the destination filename.

Use one of these privileged EXEC commands:

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

The file is uploaded to the TFTP server.

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

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

Copying Configuration Files By Using FTP

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

- [Preparing to Download or Upload a Configuration File By Using FTP](#), page A-15
- [Downloading a Configuration File By Using FTP](#), page A-16
- [Uploading a Configuration File By Using FTP](#), page A-17

Preparing to Download or Upload a Configuration File By Using FTP

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

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

The switch sends the first valid password in this list:

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

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

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

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

Before you begin downloading or uploading a configuration file, do the following:

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

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

Downloading a Configuration File By Using FTP

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

	Command	Purpose
Step 1	configure terminal Example: Switch# <code>configure terminal</code>	(Optional) Enters global configuration mode on the switch. This step is required only if you override the default remote username or password.
Step 2	ip ftp username <i>username</i> Example: Switch(config)# <code>ip ftp username NetAdmin1</code>	(Optional) Changes the default remote FTP username.
Step 3	ip ftp password <i>password</i> Example: Switch(config)# <code>ip ftp password adminpassword</code>	(Optional) Changes the default FTP password.
Step 4	end Example: Switch(config)# <code>end</code>	Returns to privileged EXEC mode.
Step 5	copy ftp:[[[/[[<i>username</i>[:<i>password</i>]]@][<i>location</i>]/<i>directory</i>]/<i>filename</i>] system:running-config or copy ftp:[[[/[[<i>username</i>[:<i>password</i>]]@][<i>location</i>]/<i>directory</i>]/<i>filename</i>] nvram:startup-config Example: Switch# <code>copy ftp system:running-config</code>	Copies the configuration file from the FTP 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 home directory for user *netadmin1* on the remote server with an IP address of 172.16.101.101 and to load and run those commands on the switch:

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

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

```
Switch# configure terminal
```

```

Switch(config)# ip ftp username netadmin1
Switch(config)# ip ftp password mypass
Switch(config)# end
Switch# copy ftp: nvram:startup-config
Address of remote host [255.255.255.255]? 172.16.101.101
Name of configuration file[rtr2-config]? host2-config
Configure using host2-config from 172.16.101.101?[confirm]
Connected to 172.16.101.101
Loading 1112 byte file host2-config:[OK]
[OK]
Switch#
%SYS-5-CONFIG_NV:Non-volatile store configured from host2-config by ftp from
172.16.101.101

```

Uploading a Configuration File By Using FTP

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

	Command	Purpose
Step 1	configure terminal Example: Switch# configure terminal	(Optional) Enters global configuration mode. This step is required only if you override the default remote username or password.
Step 2	ip ftp username <i>username</i> Example: Switch(config)# ip ftp username NetAdmin1	(Optional) Changes the default remote username.
Step 3	ip ftp password <i>password</i> Example: Switch(config)# ip ftp password adminpassword	(Optional) Changes the default password.
Step 4	end Example: Switch(config)# end	Returns to privileged EXEC mode.
Step 5	copy system:running-config ftp:[[//[<i>username</i>[:<i>password</i>]@]<i>location</i>]/<i>directory</i>]/<i>filename</i>] or copy nvram:startup-config ftp:[[//[<i>username</i>[:<i>password</i>]@]<i>location</i>]/<i>directory</i>]/<i>filename</i>] Example: Switch# copy system:running-config ftp:	Copies the specified configuration file to the specified location on the FTP server.

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

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

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

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

Copying Configuration Files By Using RCP

You can copy configuration files from and to an RCP server.

- [Preparing to Download or Upload a Configuration File By Using RCP, page A-18](#)
- [Downloading a Configuration File By Using RCP, page A-19](#)
- [Uploading a Configuration File By Using RCP, page A-21](#)

Preparing to Download or Upload a Configuration File By Using RCP

To copy configuration files using RCP you need 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 with each RCP request to a server. When you copy a configuration file from the switch to a server, the Cisco IOS software sends the first valid username in this list:

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

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

Before you begin downloading or uploading a configuration file by using RCP, do the following:

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

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

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

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

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

Downloading a Configuration File By Using RCP

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

	Command	Purpose
Step 1	configure terminal Example: Switch# configure terminal	(Optional) Enters global configuration mode. This step is required only if you override the default remote username.
Step 2	ip rcmd remote-username <i>username</i> Example: Switch(config)# ip rcmd remote-username netadmin1	(Optional) Specifies the remote username.

	Command	Purpose
Step 3	end Example: Switch(config)# end	Returns to privileged EXEC mode.
Step 4	copy rcp:[[//[username@]location]/directory]/filename] system:running-config or copy rcp:[[//[username@]location]/directory]/filename] nvrn:startup-config Example: Switch# copy rcp: system:running-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 switch:

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

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

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

Uploading a Configuration File By Using RCP

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

	Command	Purpose
Step 1	configure terminal Example: Switch# configure terminal	(Optional) Enters global configuration mode. This step is required only if you override the default remote username.
Step 2	ip rcmd remote-username <i>username</i> Example: Switch(config)# ip rcmd remote-username netadmin1	(Optional) Specifies the remote username.
Step 3	end Example: Switch(config)# end	Returns to privileged EXEC mode.
Step 4	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>] Example: Switch# copy system:running-config rcp:	Using RCP, copies the specified configuration file from the switch running to the specified network server.

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

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

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

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

Clearing Configuration Information

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

Clearing the Startup Configuration File

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

**Caution**

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

Deleting a Stored Configuration File

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

**Caution**

You cannot restore a file after it has been deleted.

Replacing and Rolling Back Configurations

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

- [Understanding Configuration Replacement and Rollback, page A-22](#)
- [Configuration Guidelines, page A-23](#)
- [Configuring the Configuration Archive, page A-24](#)
- [Performing a Configuration Replacement or Rollback Operation, page A-25](#)

Understanding Configuration Replacement and Rollback

- [Archiving a Configuration, page A-22](#)
- [Replacing a Configuration, page A-23](#)
- [Rolling Back a Configuration, page A-23](#)

Archiving a Configuration

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

or remotely. However, this method lacks any automated file management. The configuration replacement and rollback feature can automatically save copies of the running configuration to the configuration archive.

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

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

Replacing a Configuration

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

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

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

Rolling Back a Configuration

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

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

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

Configuration Guidelines

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

- Make sure that the switch has free memory larger than the combined size of the two configuration files (the running configuration and the saved replacement configuration). Otherwise, the configuration replacement operation fails.
- Make sure that the switch also has sufficient free memory to execute the configuration replacement or rollback configuration commands.
- Certain configuration commands, such as those pertaining to physical components of a networking device (for example, physical interfaces), cannot be added or removed from the running configuration.
 - A configuration replacement operation cannot remove the **interface** *interface-id* command line from the running configuration if that interface is physically present on the device.
 - The **interface** *interface-id* command line cannot be added to the running configuration if no such interface is physically present on the device.
- When using the **configure replace** command, you must specify a saved configuration as the replacement configuration file for the running configuration. The replacement file must be a complete configuration generated by a Cisco IOS device (for example, a configuration generated by the **copy running-config destination-url** command).

**Note**

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

Configuring the Configuration Archive

Using the **configure replace** command with the configuration archive and with the **archive config** command is optional but offers significant benefit for configuration rollback scenarios. Before using the **archive config** command, you must first configure the configuration archive. Starting in privileged EXEC mode, follow these steps to configure the configuration archive:

	Command	Purpose
Step 1	configure terminal Example: Switch# configure terminal	Enters global configuration mode.
Step 2	archive Example: Switch(config)# archive	Enters archive configuration mode.
Step 3	path url Example: Switch(config-archive)# path flash:myconfiguration	Specifies the location and filename prefix for the files in the configuration archive.

	Command	Purpose
Step 4	maximum <i>number</i> Example: Switch(config-archive)# maximum 14	(Optional) Sets the maximum number of archive files of the running configuration to be saved in the configuration archive. <i>number</i> —Maximum files of the running configuration file in the configuration archive. Valid values are from 1 to 14. The default is 10. Note Before using this command, you must first enter the path archive configuration command to specify the location and filename prefix for the files in the configuration archive.
Step 5	time-period <i>minutes</i> Example: Switch(config-archive)# time-period 1440	(Optional) Sets the time increment for automatically saving an archive file of the running configuration in the configuration archive. <i>minutes</i> —Specifies how often, in minutes, to automatically save an archive file of the running configuration in the configuration archive.
Step 6	end	Returns to privileged EXEC mode.
Step 7	show running-config Example: Switch# show running-config	(Optional) Displays the contents of the running configuration.
Step 8	copy running-config startup-config Example: Switch# copy running-config startup-config	(Optional) Saves the current configuration to NVRAM.

Performing a Configuration Replacement or Rollback Operation

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

	Command	Purpose
Step 1	archive config Example: Switch# archive config	(Optional) Saves the running configuration file to the configuration archive. Note Enter the path archive configuration command before using this command.
Step 2	configure replace target-url [list] [force] [time seconds] [nolock] Example: Switch# configure replace flash:startup-config time 120	Replaces the running configuration file with a saved configuration file. <i>target-url</i> —URL (accessible by the file system) of the saved configuration file that is to replace the running configuration, such as the configuration file created in Step 2 by using the archive config privileged EXEC command. list —Display a list of the command entries applied by the software parser during each pass of the configuration replacement operation. The total number of passes also appears. force — Replace the running configuration file with the specified saved configuration file without prompting you for confirmation. time seconds —Specify the time (in seconds) within which you must enter the configure confirm command to confirm replacement of the running configuration file. If you do not enter the configure confirm command within the specified time limit, the configuration replacement operation is automatically stopped. (In other words, the running configuration file is restored to the configuration that existed before you entered the configure replace command). Note You must first enable the configuration archive before you can use the time seconds command line option. nolock —Disable the locking of the running configuration file that prevents other users from changing the running configuration during a configuration replacement operation.
Step 3	configure confirm Example: Switch# configure confirm	(Optional) Confirms replacement of the running configuration with a saved configuration file. Note Use this command only if the time seconds keyword and argument of the configure replace command are specified.
Step 4	show running-config Example: Switch# show running-config	(Optional) Displays the contents of the running configuration.

Working with Cisco IOS XE Software Bundles

This section describes how to download, upload, and install Cisco IOS XE software bundle files, which contain the system software packages.

You can download a switch bundle file to local storage media from a TFTP, FTP, or RCP server to upgrade the switch software.

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

- [About Cisco IOS XE Software Bundles and Packages, page A-27](#)
- [Bundle and Package File Location on the Switch, page A-27](#)
- [Downloading and Uploading Cisco IOS XE Bundle Files, page A-27](#)
- [Upgrading Cisco IOS XE Software, page A-33](#)
- [Converting from the Bundle Running Mode to the Installed Running Mode, page A-35](#)
- [Copying IOS XE Package and Bundle Files From One Stack Member to Another, page A-36](#)
- [Upgrading a Switch Running Incompatible Software, page A-38](#)
- [Upgrading a Switch Running in Incompatible Running Mode, page A-39](#)

About Cisco IOS XE Software Bundles and Packages

Cisco IOS XE software bundles include a set of IOS XE package (.pkg) files. You can install the package files on the switch or you can boot the switch from the IOS XE bundle itself.

To display information about the contents of a Cisco IOS XE bundle (.bin file), use the **show software package** command in privileged EXEC mode. Use the command to display information about an individual IOS XE package (.pkg) file as well.

Bundle and Package File Location on the Switch

When the switch is running in installed mode, the Cisco IOS XE package (.pkg) files and provisioning file (packages.conf) are stored in the system board flash memory (flash:). When the switch is running in bundle mode, the booted Cisco IOS XE software bundle (.bin) file is stored in the system board flash memory (flash:) or USB flash memory (usbflash0:).

To display information about the provisioning software that is currently running on the switch, use the **show version** privileged EXEC command. In the display, check the line that begins with

```
System bundle file is...
```

When the switch is running in installed mode, this line displays the name and location of the booted Cisco IOS XE provisioning file, typically flash:packages.conf.

When the switch is running in bundle mode, this line displays the name and location of the booted Cisco IOS XE bundle file.

To display information about the Cisco IOS XE package files that are running on the switch, use the **show version running** privileged EXEC command.

When the switch is running in installed mode, this command displays information about the set of package files contained in the booted provisioning file.

When the switch is running in bundle mode, this command displays information about the set of package files contained in the booted Cisco IOS XE software bundle.

Downloading and Uploading Cisco IOS XE Bundle Files

You can download a Cisco IOS XE bundle file from a network server (TFTP, FTP or RCP) for purposes of upgrading the Cisco IOS XE software.

You can upload a Cisco IOS XE bundle file to a network server for backup purposes; the uploaded bundle can be used for future downloads to the same or another switch of the same type.

This section contains the following information:

- [Copying Cisco IOS XE Bundle Files By Using TFTP, page A-28](#)
- [Copying Cisco IOS XE Bundle Files By Using FTP, page A-29](#)
- [Copying Cisco IOS XE Bundle Files By Using RCP, page A-31](#)

Copying Cisco IOS XE Bundle Files By Using TFTP

This section contains the following information:

- [Preparing to Download or Upload a Cisco IOS XE Bundle File By Using TFTP, page A-28](#)
- [Downloading a Bundle File By Using TFTP, page A-28](#)
- [Uploading a Bundle File By Using TFTP, page A-28](#)

Preparing to Download or Upload a Cisco IOS XE Bundle File By Using TFTP

For information about how to prepare before you begin downloading or uploading a Cisco IOS XE bundle file with TFTP, see the “[Preparing to Download or Upload a Configuration File By Using TFTP](#)” section on page A-13.

Downloading a Bundle File By Using TFTP

Beginning in privileged EXEC mode, do the following to download a software bundle file from a TFTP server:

	Command	Purpose
Step 1	copy tftp:[[/location]/directory]/bundle-name flash: Example: Switch# copy tftp:/cat3k_caa-universalk9.SPA.03.02.00 .SE.150-1.EX.bin flash:	Upload the currently running bundle file 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/bundle-name</i> specify the directory (optional) and the name of the software bundle file to be uploaded. Directory and bundle names are case sensitive.

Uploading a Bundle File By Using TFTP

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

Beginning in privileged EXEC mode, do the following to upload a bundle to a TFTP server:

	Command	Purpose
Step 1	copy flash: tftp:[[/location]/directory]/bundle-name Example: Switch# copy flash: tftp:/cat3k_caa-universalk9.SPA.03.02.00 .SE.150-1.EX.bin	Upload the currently running bundle file 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/bundle-name</i> specify the directory (optional) and the name of the software bundle file to be uploaded. Directory and bundle names are case sensitive.

Copying Cisco IOS XE Bundle Files By Using FTP

This section contains the following information:

- [Preparing to Download or Upload Bundle Files By Using FTP, page A-29](#)
- [Downloading a Bundle File By Using FTP, page A-29](#)
- [Uploading a Cisco IOS XE Bundle File By Using FTP, page A-30](#)

Preparing to Download or Upload Bundle Files By Using FTP

For information about how to prepare before you begin downloading or uploading a Cisco IOS XE bundle file with TFTP, see the [“Preparing to Download or Upload a Configuration File By Using FTP” section on page A-15](#).

Downloading a Bundle File By Using FTP

You can download a new bundle file from an FTP server.

Beginning in privileged EXEC mode, follow these steps to download a new Cisco IOS XE bundle from an FTP server:

	Command	Purpose
Step 1	configure terminal Example: Switch# configure terminal	(Optional) Enters global configuration mode. This step is required only if you override the default remote username or password.
Step 2	ip ftp username <i>username</i> Example: Switch(config)# ip ftp username Admin01	(Optional) Changes the default remote username.
Step 3	ip ftp password <i>password</i> Example: Switch(config)# ip ftp password adminpassword	(Optional) Changes the default password.

	Command	Purpose
Step 4	end	Returns to privileged EXEC mode.
	Example: Switch(config)# end	
Step 5	copy ftp:[[/location]/directory]/bundle_name flash:	(Optional) Downloads the bundle files from the FTP server to the switch.
	Example: Switch# copy ftp:/cat3k_caa-universalk9.SPA.03.02.00. SE.150-1.EX.bin flash:	<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 Bundle Files By Using FTP” section on page A-29. For <i>@location</i>, specify the IP address of the FTP server. For <i>/directory/bundle_name</i>, specify the directory (optional) and the bundles to download. Directory and bundle file names are case sensitive.

Uploading a Cisco IOS XE Bundle File By Using FTP

You can upload an Cisco IOS XE bundle from the switch to an FTP server. You can later download this bundle to the same switch or to another switch of the same type.

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

	Command	Purpose
Step 1	configure terminal	(Optional) Enters global configuration mode.
	Example: Switch# configure terminal	This step is required only if you override the default remote username or password.
Step 2	ip ftp username <i>username</i>	(Optional) Changes the default remote username.
	Example: Switch(config)# ip ftp username Admin01	
Step 3	ip ftp password <i>password</i>	(Optional) Changes the default password.
	Example: Switch(config)# ip ftp password adminpassword	

	Command	Purpose
Step 4	end Example: Switch(config)# end	Returns to privileged EXEC mode.
Step 5	copy flash: ftp:[[/[username[:password]@]location]/directory]/bundle_name Example: Switch# copy flash: ftp:/cat3k_caa-universalk9.SPA.03.02.00. SE.150-1.EX.bin	Uploads the bundle file from the switch to the FTP server. <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 <i>@location</i>, specify the IP address of the FTP server. For <i>/directory/bundle_name</i>, specify the directory and the name of the software bundle to be uploaded. Directory and bundle names are case sensitive.

Copying Cisco IOS XE Bundle Files By Using RCP

You can download a Cisco IOS XE bundle from an RCP server or upload the bundle from the switch to an RCP server.

This section contains the following information:

- [Preparing to Download or Upload a Cisco IOS XE Bundle File By Using RCP, page A-31](#)
- [Downloading a Bundle File By Using RCP, page A-31](#)
- [Uploading a Bundle File By Using RCP, page A-32](#)

Preparing to Download or Upload a Cisco IOS XE Bundle File By Using RCP

For information about preparing to download or upload bundle files, see “[Preparing to Download or Upload a Configuration File By Using RCP](#)” section on page A-18.

Downloading a Bundle File By Using RCP

Beginning in privileged EXEC mode, follow these steps to download a new Cisco IOS XE bundle from an RCP server.

	Command	Purpose
Step 1	configure terminal Example: Switch# configure terminal	Enters global configuration mode. This step is required only if you override the default remote username.
Step 2	ip rcmd remote-username username Example: Switch(config)# ip rcmd remote-username Admin01	(Optional) Specifies the remote username.

	Command	Purpose
Step 3	end Example: Switch(config)# end	Returns to privileged EXEC mode.
Step 4	copy rcp: [[[//[username@]location]directory]/ bundle_name] flash: Example: Switch# copy rcp: //netadmin@172.16.101.101/bundle1 flash:	Downloads the bundle file from the RCP server to the switch. <ul style="list-style-type: none"> 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 a Cisco IOS XE Bundle File By Using RCP” section on page A-31. For <i>@location</i>, specify the IP address of the RCP server. For <i>/directory/bundle_name</i>, specify the directory (optional) and the software bundle to download. Directory and bundle file names are case sensitive.

Uploading a Bundle File By Using RCP

You can upload a software bundle file from the switch to an RCP server. You can later download this bundle to the same switch or to another switch of the same type.

Beginning in privileged EXEC mode, follow these steps to upload a software bundle file to an RCP server:

	Command	Purpose
Step 1	configure terminal Example: Switch# configure terminal	(Optional) Enters global configuration mode. This step is required only if you override the default remote username.
Step 2	ip rcmd remote-username username Example: Switch(config)# ip rcmd remote-username Admin01	(Optional) Specify the remote username.

	Command	Purpose
Step 3	end Example: Switch(config)# end	Return to privileged EXEC mode.
Step 4	copy flash: rcp: [[[//[username@]location]/directory]/bundle_name] Example: Switch# copy flash: rcp://netadmin@172.16.101.101/bundle1	Uploads the software bundle on the switch to the RCP server. <ul style="list-style-type: none"> For //username, specify the username; for the RCP copy request to execute, define an account on the network server for the remote username. For more information, see the “Preparing to Download or Upload a Cisco IOS XE Bundle File By Using RCP” section on page A-31. For @location, specify the IP address of the RCP server. For /directory]/bundle_name specify the directory (optional) and the name of the software bundle to be uploaded. Directory and bundle file names are case sensitive.

Upgrading Cisco IOS XE Software

The method that you use to upgrade Cisco IOS XE software depends on whether the switch is running in installed mode or in bundle mode.

This section contains the following information:

- [Upgrading Cisco IOS XE Software: Installed Mode, page A-33](#)
- [Upgrading Cisco IOS XE Software: Bundle Mode, page A-34](#)

Upgrading Cisco IOS XE Software: Installed Mode

To upgrade the Cisco IOS XE software when the switch is running in installed mode, use the **software install** privileged EXEC command to install the packages from a new software bundle file. The software bundle can be installed from the local storage media or it can be installed over the network using TFTP or FTP.

The **software install** command expands the package files from the specified source bundle file and copies them to the local flash: storage device. When the source bundle is specified as a tftp: or ftp: URL, the bundle file is first downloaded into the switch's memory (RAM); the bundle file is not copied to local storage media.

After the package files are expanded and copied to flash: the running provisioning file (flash:packages.conf) is updated to reflect the newly installed packages, and the switch displays a reload prompt.



Note

The **software install** command is not supported when the switch is running in bundle mode. Use the **software expand** privileged EXEC command to convert the switch from bundle mode to installed mode.

This example shows the **software install** command being used to expand and copy the packages from a Cisco IOS XE bundle located on a TFTP server:

```

3850-Stack# software install file tftp://172.19.211.47/cat3k_caa-universalk9.SPA.03.02.00.SE.150-1.EX.bin

Preparing install operation ...
[1]: Downloading file tftp://172.19.211.47/cat3k_caa-universalk9.SPA.03.02.00.SE.150-1.EX.bin to active
switch 1
[1]: Finished downloading file tftp://172.19.211.47/cat3k_caa-universalk9.SPA.03.02.00.SE.150-1.EX.bin to
active switch 1
[1]: Starting install operation
[1]: Expanding bundle cat3k_caa-universalk9.SPA.03.02.00.SE.150-1.EX.bin
[1]: Copying package files
[1]: Package files copied
[1]: Finished expanding bundle cat3k_caa-universalk9.SPA.03.02.00.SE.150-1.EX.bin
[1]: Verifying and copying expanded package files to flash:
[1]: Verified and copied expanded package files to flash:
[1]: Starting compatibility checks
[1]: Finished compatibility checks
[1]: Starting application pre-installation processing
[1]: Finished application pre-installation processing
[1]: Old files list:
Removed cat3k_caa-base.SSA.03.09.17.EMP.pkg
Removed cat3k_caa-drivers.SSA.03.09.17.EMP.pkg
Removed cat3k_caa-infra.SSA.03.09.17.EMP.pkg
Removed cat3k_caa-iosd-universalk9.SSA.150-9.17.EMP.pkg
Removed cat3k_caa-platform.SSA.03.09.17.EMP.pkg
Removed cat3k_caa-wcm.SSA.03.09.17.EMP.pkg
[1]: New files list:
Added cat3k_caa-base.SPA.03.02.00.SE.pkg
Added cat3k_caa-drivers.SPA.03.02.00.SE.pkg
Added cat3k_caa-infra.SPA.03.02.00SE.pkg
Added cat3k_caa-iosd-universalk9.SPA.150-1.EX.pkg
Added cat3k_caa-platform.SPA.03.02.00.SE.pkg
Added cat3k_caa-wcm.SPA.03.02.00.SE.pkg
[1]: Creating pending provisioning file
[1]: Finished installing software. New software will load on reboot.
[1]: Setting rollback timer to 45 minutes

[1]: Do you want to proceed with reload? [yes/no]:

```

Upgrading Cisco IOS XE Software: Bundle Mode

To upgrade the Cisco IOS XE software when the switch is running in bundle mode, follow these steps:

1. Download the bundle file to local storage media.
2. Configure the **boot system** global configuration command to point to the bundle file.
3. Reload the switch.

This example shows the steps to upgrade the Cisco IOS XE software on a switch that is running in bundle mode. It shows using the **copy** command to copy the bundle file to flash:, configuring the **boot system** variable to point to the bundle file, saving a copy of the running configuration, and finally, reloading the switch.

```

3850-Switch# copy tftp://172.19.211.47/cat3k_caa-universalk9.SPA.03.02.00.SE.150-1.EX.bin flash:

Destination filename [cat3k_caa-universalk9.SPA.03.02.00.SE.150-1.EX.bin]?
Accessing tftp://172.19.211.47/cat3k_caa-universalk9.SPA.03.02.00.SE.150-1.EX.bin...Loading
/tftpboot/cstohs/cat3k_caa-universalk9.SPA.03.02.00.SE.150-1.EX.bin from 172.19.211.47 (via
GigabitEthernet0/0): !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
[OK - 220766688 bytes]

220766688 bytes copied in 124.330 secs (1775651 bytes/sec)

```

```

3850-Switch#
3850-Switch# configure terminal

Enter configuration commands, one per line. End with CNTL/Z.
3850-Switch(config)# boot system switch all flash:cat3k_caa-universalk9.SPA.03.02.00.SE.150-1.EX.bin

3850-Switch(config)# end

3850-Switch#
*Nov 19 14:02:42.441: %SYS-5-CONFIG_I: Configured from console by console
3850-Switch#
3850-Switch# write memory

Building configuration...
Compressed configuration from 4941 bytes to 2236 bytes[OK]
3850-Switch# reload

Reload command is being issued on Active unit, this will reload the whole stack
Proceed with reload? [confirm]

```

Converting from the Bundle Running Mode to the Installed Running Mode

To convert the running mode of a switch from bundle mode to installed mode, use the **software expand running** privileged EXEC command. This command expands the packages from the booted IOS XE software bundle and copies them and the provisioning file to the specified **to** destination.

When you use the **software expand running** command to convert the switch from bundle mode to installed mode, specify the **to** destination as **flash:**. After you execute the command, configure the **boot system** command to point to the expanded provisioning file (flash:packages.conf), then reload the switch to boot in installed mode.



Note

The **software expand running** command is not supported when the switch is running in installed mode.

This example shows using the **software expand running** command to convert the active switch in a switch stack from the bundle running mode to the installed running mode:

```

3850-Stack# dir flash:
Directory of flash:/

 7386  -rwx      2097152  Jan 23 2013 14:06:49 +00:00  nvram_config
 7378  drwx         4096  Jan 23 2013 09:35:11 +00:00  mnt
 7385  -rw-      221775876  Jan 23 2013 14:15:13 +00:00  cat3k_caa-universalk9.SPA.03.02.00.SE.150-1.EX.bin
 7389  -rwx         556  Jan 21 2013 20:47:30 +00:00  vlan.dat

712413184 bytes total (445063168 bytes free)
3850-Stack#
3850-Stack# software expand running to flash:

Preparing expand operation ...
[2]: Expanding the running bundle
[2]: Copying package files
[2]: Package files copied
[2]: Finished expanding the running bundle
3850-Stack#
3850-Stack# dir flash:

Directory of flash:/

```

```

7386 -rwx      2097152 Jan 23 2013 14:06:49 +00:00 nvram_config
7378 drwx         4096 Jan 23 2013 09:35:11 +00:00 mnt
7385 -rw-    221775876 Jan 23 2013 14:15:13 +00:00
cat3k_caa-universalk9.SPA.03.02.00.SE.150-1.EX.bin
7391 -rw-    74410468 Jan 23 2013 14:16:57 +00:00 cat3k_caa-base.SPA.03.02.00SE.pkg
7392 -rw-    2773680 Jan 23 2013 14:16:57 +00:00 cat3k_caa-drivers.SPA.03.02.00.SE.pkg
7393 -rw-    32478044 Jan 23 2013 14:16:57 +00:00 cat3k_caa-infra.SPA.03.02.00SE.pkg
7394 -rw-    30393116 Jan 23 2013 14:16:57 +00:00 cat3k_caa-iosd-universalk9.SPA.150-1.EX.pkg
7389 -rwx         556 Jan 21 2013 20:47:30 +00:00 vlan.dat
7395 -rw-    18313952 Jan 23 2013 14:16:57 +00:00 cat3k_caa-platform.SPA.03.02.00.SE.pkg
7396 -rw-    63402700 Jan 23 2013 14:16:57 +00:00 cat3k_caa-wcm.SPA.10.0.100.0.pkg
7388 -rw-         1218 Jan 23 2013 14:17:43 +00:00 packages.conf

```

```
712413184 bytes total (223019008 bytes free)
```

```
3850-Stack#
```

```
3850-Stack# configure terminal
```

```
Enter configuration commands, one per line. End with CNTL/Z.
```

```
3850-Stack(config)# boot system switch all flash:packages.conf
```

```
3850-Stack(config)# end
```

```
3850-Stack#
```

```
*Jan 23 14:28:47.722: %SYS-5-CONFIG_I: Configured from console by console
```

```
3850-Stack# write memory
```

```
Building configuration...
```

```
Compressed configuration from 4851 bytes to 2187 bytes[OK]
```

```
3850-Stack#
```

```
3850-Stack# reload
```

```
Reload command is being issued on Active unit, this will reload the whole stack
```

```
Proceed with reload? [confirm]
```

Copying IOS XE Package and Bundle Files From One Stack Member to Another

For switch stacks running in installed mode, use the **software install source switch** privileged EXEC command to install the running software packages from an existing stack member to one or more other stack members that are running different (but compatible) software packages.

This example shows a 2-member stack where each switch is running a different (but compatible) software packages. The **software install source switch** command is used to install the packages that are currently running on the standby switch (switch 1) onto the active switch (switch 2).

```
3850-Stack# show version running
```

```
Package: Base, version: 03.02.00SE, status: active
```

```
File: cat3k_caa-base.SPA.03.02.00SE.pkg, on: Switch1
```

```
Built: Wed Jan 09 21:59:52 PST 2013, by: gereddy
```

```
Package: Drivers, version: 03.02.00.SE, status: active
```

```
File: cat3k_caa-drivers.SPA.03.02.00.SE.pkg, on: Switch1
```

```
Built: Wed Jan 09 22:03:41 PST 2013, by: gereddy
```

```
Package: Infra, version: 03.02.00SE, status: active
```

```
File: cat3k_caa-infra.SPA.03.02.00SE.pkg, on: Switch1
```

```
Built: Wed Jan 09 22:00:56 PST 2013, by: gereddy
```

```
Package: IOS, version: 150-1.EX, status: active
```

```
File: cat3k_caa-iosd-universalk9.SPA.150-1.EX.pkg, on: Switch1
```

```
Built: Wed Jan 09 22:02:23 PST 2013, by: gereddy
```

```
Package: Platform, version: 03.02.00.SE, status: active
```

```
File: cat3k_caa-platform.SPA.03.02.00.SE.pkg, on: Switch1
Built: Wed Jan 09 22:01:46 PST 2013, by: gereddy
```

```
Package: WCM, version: 10.0.100.0, status: active
File: cat3k_caa-wcm.SPA.10.0.100.0.pkg, on: Switch1
Built: Wed Jan 09 22:03:05 PST 2013, by: gereddy
```

```
3850-Stack#
3850-Stack# software install source switch 1
Preparing install operation ...
[2]: Copying software from source switch 1 to switch 2
[2]: Finished copying software to switch 2
[2]: Starting install operation
[2]: Starting compatibility checks
[2]: Finished compatibility checks
[2]: Starting application pre-installation processing
[2]: Finished application pre-installation processing
[2]: Old files list:
Removed cat3k_caa-base.SSA.03.09.17.EMP.pkg
Removed cat3k_caa-drivers.SSA.03.09.17.EMP.pkg
Removed cat3k_caa-infra.SSA.03.09.17.EMP.pkg
Removed cat3k_caa-iosd-universalk9.SSA.150-9.17.EMP.pkg
Removed cat3k_caa-platform.SSA.03.09.17.EMP.pkg
Removed cat3k_caa-wcm.SSA.03.09.17.EMP.pkg
[2]: New files list:
Added cat3k_caa-base.SPA.03.02.00.SE.pkg
Added cat3k_caa-drivers.SPA.03.02.00.SE.pkg
Added cat3k_caa-infra.SPA.03.02.00.SE.pkg
Added cat3k_caa-iosd-universalk9.SPA.150-1.EX.pkg
Added cat3k_caa-platform.SPA.03.02.00.SE.pkg
Added cat3k_caa-wcm.SPA.10.0.100.0.pkg
[2]: Creating pending provisioning file
[2]: Finished installing software. New software will load on reboot.
[2]: Committing provisioning file

[2]: Do you want to proceed with reload? [yes/no]:
```

For switch stacks running in bundle mode, follow these steps to copy the bundle file from one stack member to another:

1. Use the **copy** privileged EXEC command to copy the running bundle from one switch in the stack to the other.
2. Configure the **boot system** global configuration command to point to the bundle file.
3. Reload the switch.

This example shows a 2-member stack where each switch is running a different (but compatible) software packages.

```
3850-Stack# copy flash:cat3k_caa-universalk9.SPA.03.02.00.SE.150-1.EX.bin flash-1:
Destination filename [cat3k_caa-universalk9.SPA.03.02.00.SE.150-1.EX.bin]?
Copy in progress...
...
220766688 bytes copied in 181.700 secs (1215007 bytes/sec)
3850-Stack#
3850-Stack# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.

3850-Stack(config)# boot system switch 1 flash:cat3k_caa-universalk9.SPA.03.02.00.SE.150-1EX.bin
3850-Stack(config)# end
3850-Stack#
```

```
*Nov 19 16:08:14.857: %SYS-5-CONFIG_I: Configured from console by console
3850-Stack# reload slot 1
Stack is in Half ring setup; Reloading a switch might cause stack split
Proceed with reload? [confirm]
```

Upgrading a Switch Running Incompatible Software

To upgrade a switch that is running in installed mode with software packages that are incompatible with the switch stack (also running in installed mode), use the **software auto-upgrade** privileged EXEC command to install the software packages from an existing stack member to the stack member that is running incompatible software. Upon completion of the auto-upgrade installation, the incompatible switch automatically reloads and joins the stack as a fully functioning member.



Note

If you configure the global **software auto-upgrade enable** command, the auto-upgrade functionality is initiated automatically when a switch with incompatible software running in installed mode joins the stack that is running in installed mode. For more information, see *Cisco IOS Configuration Fundamentals Command Reference, Cisco IOS XE Release 3SE (Catalyst 3850 Switches)*.

This example shows a 2-member switch stack; switch 2 is the active switch and switch 1 is running incompatible software.

```
3850-Stack# show switch
Switch/Stack Mac Address : 6400.f125.1100 - Local Mac Address
Mac persistency wait time: Indefinite
H/W Current
Switch# Role Mac Address Priority Version State
-----
1 Member 6400.f125.1a00 1 0 V-Mismatch
*2 Active 6400.f125.1100 1 V01 Ready

3850-Stack#
3850-Stack# software auto-upgrade
% Auto upgrade has been initiated for the following incompatible switches: 1

INFO level system messages will be generated to provide status information during
the auto upgrade process

3850-Stack#
*Oct 19 06:59:14.521: %INSTALLER-6-AUTO_UPGRADE_SW_INITIATED: 2 installer: Auto upgrade initiated for switch 1
*Oct 19 06:59:14.522: %INSTALLER-6-AUTO_UPGRADE_SW: 2 installer: Searching stack for software to upgrade switch 1
*Oct 19 06:59:14.523: %INSTALLER-6-AUTO_UPGRADE_SW: 2 installer: Found donor switch 2 to auto upgrade switch 1
*Oct 19 06:59:14.523: %INSTALLER-6-AUTO_UPGRADE_SW: 2 installer: Upgrading switch 1 with software from switch 2
*Oct 19 07:00:47.829: %INSTALLER-6-AUTO_UPGRADE_SW: 2 installer: Finished installing software on switch 1
*Oct 19 07:00:47.829: %INSTALLER-6-AUTO_UPGRADE_SW: 2 installer: Reloading switch 1 to complete the auto upgrade
```

To upgrade a switch that is running in bundle mode with a software bundle that is incompatible with the switch stack (also running in bundle mode), follow these steps:

1. Use the **copy** privileged EXEC command to copy the running bundle from one switch in the stack to the other.
2. Configure the **boot system** global configuration command to point to the bundle file.

3. Reload the switch.

This example shows a 2-member switch stack running in bundle mode; switch 2 is the active switch and switch 1 is running an incompatible bundle.

```
3850-Stack# show switch
Switch/Stack Mac Address : 6400.f125.1100 - Local Mac Address
Mac persistency wait time: Indefinite
H/W Current
Switch# Role Mac Address Priority Version State
-----
1 Member 6400.f125.1a00 1 0 V-Mismatch
*2 Active 6400.f125.1100 1 V01 Ready

3850-Stack#
3850-Stack# copy flash:cat3k_caa-universalk9.SPA.03.02.00.SE.150-1.EX.bin flash-1:
Destination filename [cat3k_caa-universalk9.SPA.03.02.00.SE.150-1.EX.bin]?
Copy in progress...
...
220766688 bytes copied in 181.700 secs (1215007 bytes/sec)
3850-Stack#
3850-Stack# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
3850-Stack(config)# boot system switch 1 flash:cat3k_caa-universalk9.SPA.03.02.00.SE.150-1.EX.bin
3850-Stack(config)# end
3850-Stack#
*Nov 19 16:08:14.857: %SYS-5-CONFIG_I: Configured from console by console
3850-Stack# reload slot 1
Stack is in Half ring setup; Reloading a switch might cause stack split
Proceed with reload? [confirm]
```

Upgrading a Switch Running in Incompatible Running Mode

When a switch running in bundle mode tries to join a stack running in installed mode, use the **software auto-upgrade** privileged EXEC command to install the incompatible switch's running packages and convert the switch to installed mode. Upon completion of the auto-upgrade running mode conversion, the incompatible switch automatically reloads and attempts to join the stack in installed mode.



Note

If you configure the global **software auto-upgrade enable** command, the auto-upgrade functionality is initiated automatically when a switch with incompatible software running in installed mode joins the stack that is running in installed mode. For more information, see *Cisco IOS Configuration Fundamentals Command Reference, Cisco IOS XE Release 3SE (Catalyst 3850 Switches)*.

This example shows a 2-member switch stack running in installed mode. Switch 2 is the active switch and switch 1 is running in bundle mode.

```
3850-Stack# show switch
Switch/Stack Mac Address : 6400.f125.1100 - Local Mac Address
Mac persistency wait time: Indefinite
H/W Current
Switch# Role Mac Address Priority Version State
-----
1 Member 6400.f125.1a00 1 0 V-Mismatch
```

```
*2 Active 6400.f125.1100 1 V01 Ready
```

```
3850-Stack#
```

```
3850-Stack# software auto-upgrade
```

```
% Auto upgrade has been initiated for the following incompatible switches: 1
```

```
INFO level system messages will be generated to provide status information during
the auto upgrade process
```

```
3850-Stack#
```

```
*Oct 19 07:17:16.694: %INSTALLER-6-AUTO_UPGRADE_SW_INITIATED: 2 installer: Auto upgrade initiated for switch 1
```

```
*Oct 19 07:17:16.694: %INSTALLER-6-AUTO_UPGRADE_SW: 2 installer: Converting switch 1 to installed mode by
```

```
*Oct 19 07:17:16.694: %INSTALLER-6-AUTO_UPGRADE_SW: 2 installer: installing its running software
```

```
*Oct 19 07:18:50.488: %INSTALLER-6-AUTO_UPGRADE_SW: 2 installer: Setting the boot var on switch 1
```

```
*Oct 19 07:18:51.553: %INSTALLER-6-AUTO_UPGRADE_SW: 2 installer: Finished installing the running software on switch
1
```

```
*Oct 19 07:18:51.553: %INSTALLER-6-AUTO_UPGRADE_SW: 2 installer: Reloading switch 1 to boot in installed mode
```



Note

When you use the **software auto-upgrade** command to convert an incompatible switch to installed mode, the command installs the packages from the incompatible switch's running bundle. If, after you reload and boot the incompatible switch in installed mode, the switch's installed packages are found to be incompatible with the stack, you can use the **software auto-upgrade** command again. For more information, see *Cisco IOS Configuration Fundamentals Command Reference, Cisco IOS XE Release 3SE (Catalyst 3850 Switches)*.

To convert a switch that is running in installed mode and joining a stack that is running in bundle mode, follow these steps:

1. Use the **copy** privileged EXEC command to copy the running bundle from one switch in the stack to the other.
2. Configure the **boot system** global configuration command to point to the bundle file.
3. Reload the switch.

After reloading, the incompatible switch boots in bundle mode and joins the stack as a fully functioning member.

This example shows a 2-member switch stack running in bundle mode; switch 2 is the active switch and switch 1 is running in installed mode:

```
3850-Stack#
3850-Stack# copy flash:cat3k_caa-universalk9.SPA.03.02.00.SE.150-1.EX.bin flash-1:
Destination filename [cat3k_caa-universalk9.SPA.03.02.00.SE.150-1.EX.bin]?
Copy in progress...
....
220766688 bytes copied in 181.700 secs (1215007 bytes/sec)
3850-Stack#
3850-Stack# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
3850-Stack(config)# boot system switch 1 flash:cat3k_caa-universalk9.SPA.03.02.00.SE.150-1.EX.bin
3850-Stack(config)# end
3850-Stack#
*Nov 19 16:08:14.857: %SYS-5-CONFIG_I: Configured from console by console
3850-Stack# reload slot 1
Stack is in Half ring setup; Reloading a switch might cause stack split
Proceed with reload? [confirm]
```



INDEX

B

bundle files

- copying from one switch to another [A-36](#)
- displaying contents of [A-27](#)
- downloading [A-27](#)
- installing [A-33](#)
- location on the switch [A-27](#)
- uploading [A-27](#)

C

configuration files

- archiving [A-22](#)
- clearing the startup configuration [A-22](#)
- creating and using, guidelines for [A-11](#)
- creating using a text editor [A-12](#)
- deleting a stored configuration [A-22](#)
- described [A-10](#)
- downloading
 - reasons for [A-11](#)
 - using FTP [A-16](#)
 - using RCP [A-19](#)
 - using TFTP [A-13](#)
- invalid combinations when copying [A-6](#)
- replacing and rolling back, guidelines for [A-23](#)
- replacing a running configuration [A-22, A-23](#)
- rolling back a running configuration [A-22, A-23](#)
- types and location [A-12](#)
- uploading
 - reasons for [A-11](#)
 - using FTP [A-17](#)
 - using RCP [A-21](#)

- using TFTP [A-14](#)
- configuration replacement [A-22](#)
- configuration rollback [A-22](#)

D

directories

- changing [A-4](#)
- creating and removing [A-5](#)
- displaying the working [A-4](#)

downloading

bundle files

- using FTP [A-29](#)
- using RCP [A-31](#)
- using TFTP [A-28](#)

configuration files

- reasons for [A-11](#)
- using FTP [A-16](#)
- using RCP [A-19](#)
- using TFTP [A-13](#)

F

files

- copying [A-6](#)
- deleting [A-6, A-7](#)
- displaying the contents of [A-10](#)
- tar
 - creating [A-9](#)
 - displaying the contents of [A-9](#)
 - extracting [A-10](#)
- file system
 - displaying available file systems [A-2](#)

- displaying file information [A-4](#)
- local file system names [A-1](#)
- network file system names [A-6](#)
- setting the default [A-3](#)

flash device, number of [A-1](#)

FTP

- bundle files
 - downloading [A-29](#)
 - uploading [A-30](#)
- configuration files
 - downloading [A-16](#)
 - overview [A-14](#)
 - uploading [A-17](#)

R

RCP

- bundle files
 - downloading [A-31](#)
 - uploading [A-32](#)
- configuration files
 - downloading [A-19](#)
 - overview [A-18](#)
 - uploading [A-21](#)

running configuration

- replacing [A-22, A-23](#)
- rolling back [A-22, A-23](#)

S

- software clean command [A-6](#)
- software expand command [A-33](#)
- software install command [A-33](#)
- software clean command [A-7](#)
- stacks, switch
 - copying a bundle file from one member to another [A-36](#)
 - upgrading [A-36](#)
 - upgrading, incompatible running mode [A-39](#)

- upgrading, incompatible software [A-38](#)
- startup configuration
 - clearing [A-22](#)

T

tar files

- creating [A-9](#)
- displaying the contents of [A-9](#)
- extracting [A-10](#)

TFTP

- bundle files
 - downloading [A-28](#)
 - uploading [A-28](#)
- configuration files
 - downloading [A-13](#)
 - uploading [A-14](#)

U

uploading

- bundle files
 - preparing [A-28, A-29](#)
 - using FTP [A-30](#)
 - using RCP [A-32](#)
 - using TFTP [A-28](#)
- configuration files
 - reasons for [A-11](#)
 - using FTP [A-17](#)
 - using RCP [A-21](#)
 - using TFTP [A-14](#)