A

File Transfers

Contents

Overview

The switches covered in this guide support several methods for transferring files to and from a physically connected device, or via the network, including TFTP, Xmodem, and USB. This appendix explains how to download new switch software, upload or download switch configuration files and software images, and upload command files for configuring Access Control Lists (ACLs). It contains the following information:

- Downloading switch software (begins on this page)
- Copying software images (page A-23)
- Transferring switch configurations (begins on page A-24)
- Uploading ACL command files (begins on page A-29)
- Copying diagnostic data (begins on page A-32)
- Using USB Autorun (begins on page A-37)

Downloading Switch Software

ProCurve periodically provides switch software updates through the ProCurve Networking web site. For more information, refer to the support and warranty booklet shipped with the switch, or visit **www.procurve.com** and click on **software updates**. After you acquire a new software version, you can use one of the following methods for downloading software to the switch:

Software Download Feature	Default	Menu	CLI	Web
TFTP	n/a	page A-5	page A-7	—
Xmodem	n/a	page A-16	page A-17	—
USB	n/a	n/a	page A-18	—
Switch-to-Switch	n/a	page A-20	page A-21	—
Software Update Manager in PCM+	Refer to the documentation provided with PCM+.			

Note

This manual uses the terms *switch software* and *software image* to refer to the downloadable software files the switch uses to operate its networking features. Other terms sometimes include *Operating System*, or *OS*.

General Software Download Rules

- Switch software that you download via the menu interface always goes to primary flash.
- After a software download, you must reboot the switch to implement the new software. Until a reboot occurs, the switch continues to run on the software it was using before the download commenced.

Note

Downloading new switch software does not change the current switch configuration. The switch configuration is contained in separate files that can also be transferred. Refer to “Transferring Switch Configurations” on page A-23.

In most cases, if a power failure or other cause interrupts a flash image download, the switch reboots with the image previously stored in primary flash. In the unlikely event that the primary image is corrupted (which may occur if a download is interrupted by a power failure), the switch goes into boot ROM mode. In this case, use the boot ROM console to download a new image to primary flash. Refer to “Restoring a Flash Image” on page C-80.

Using TFTP To Download Switch Software from a Server

This procedure assumes that:

- A software version for the switch has been stored on a TFTP server accessible to the switch. (The software file is typically available from the ProCurve Networking web site at **www.procurve.com**.)
- The switch is properly connected to your network and has already been configured with a compatible IP address and subnet mask.
- The TFTP server is accessible to the switch via IP.

Before you use the procedure, do the following:

- Obtain the IP address of the TFTP server in which the software file has been stored.
- If VLANs are configured on the switch, determine the name of the VLAN in which the TFTP server is operating.
- Determine the name of the software file stored in the TFTP server for the switch (for example, E0820.swi).

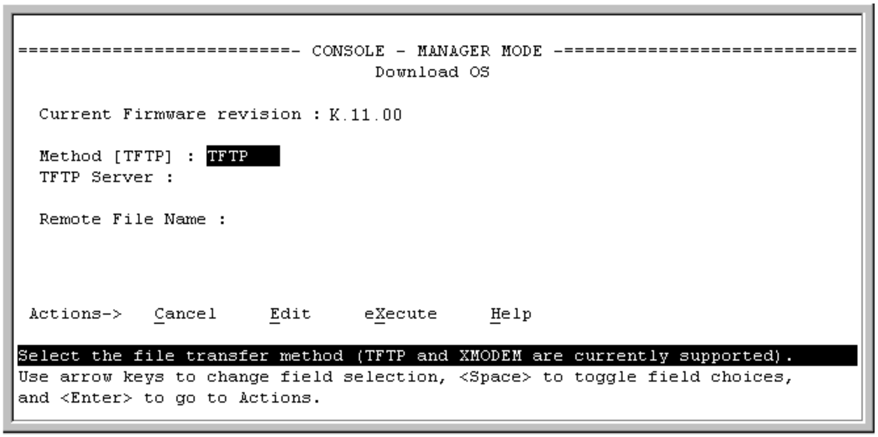
Note

If your TFTP server is a UNIX workstation, *ensure that the case (upper or lower) that you specify for the filename is the same case as the characters in the software filenames on the server.*

Menu: TFTP Download from a Server to Primary Flash

Note that the menu interface accesses only the primary flash.

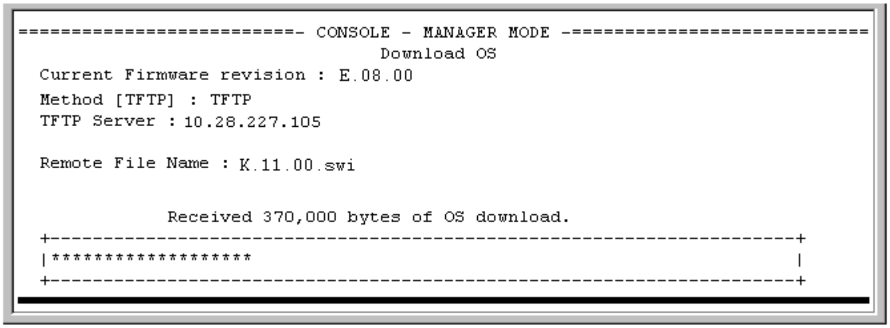
1. In the console Main Menu, select **Download OS** to display the screen in figure A-1. (The term “OS”, or “operating system” refers to the switch software):



```
==========================- CONSOLE - MANAGER MODE -============================
                              Download OS

  Current Firmware revision : K.11.00

  Method [TFTP]  : TFTP
  TFTP Server :

  Remote File Name :



 Actions->   Cancel     Edit     eXecute     Help

Select the file transfer method (TFTP and XMODEM are currently supported).
Use arrow keys to change field selection, <Space> to toggle field choices,
and <Enter> to go to Actions.
```

Figure A-1. Example of a Download OS (Software) Screen (Default Values)

2. Press **[E]** (for **Edit**).
3. Ensure that the **Method** field is set to **TFTP** (the default).
4. In the **TFTP Server** field, type in the IP address of the TFTP server in which the software file has been stored.
5. In the **Remote File Name** field, type the name of the software file. If you are using a UNIX system, remember that the filename is case-sensitive.
6. Press **[Enter]**, then **[X]** (for **eXecute**) to begin the software download. The following screen then appears:



```
==========================- CONSOLE - MANAGER MODE -============================
                              Download OS
  Current Firmware revision : E.08.00
  Method [TFTP]  : TFTP
  TFTP Server : 10.28.227.105

  Remote File Name : K.11.00.swi

              Received 370,000 bytes of OS download.
  +-----------------------------------------------------------------------+
  |*******************                                                    |
  +-----------------------------------------------------------------------+
```

Figure A-2. Example of the Download OS (Software) Screen During a Download

A "progress" bar indicates the progress of the download. When the entire software file has been received, all activity on the switch halts and you will see **Validating and writing system software to FLASH...**

7. After the primary flash memory has been updated with the new software, you must reboot the switch to implement the newly downloaded software. Return to the Main Menu and press **[6]** (for **Reboot Switch**). You will then see this prompt:

```
Continue reboot of system?  :  No
```

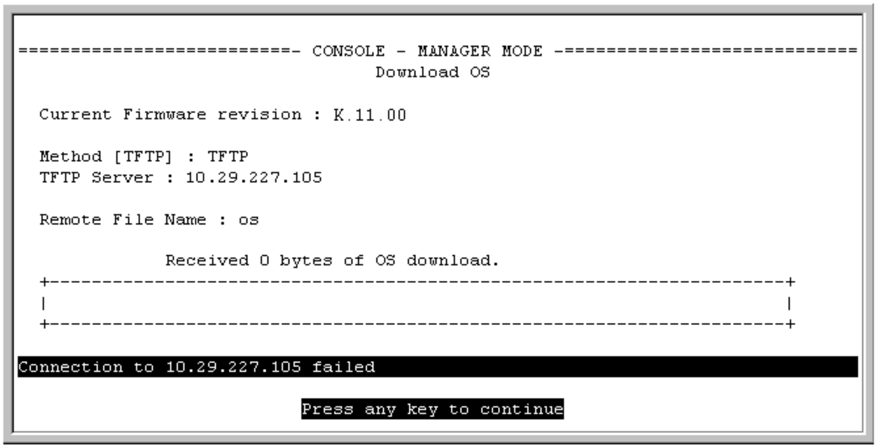
Press the space bar once to change `No` to `Yes`, then press **[Enter]** to begin the reboot.

Note

When you use the menu interface to download a switch software, the new image is always stored in primary flash. Also, using the Reboot Switch command in the Main Menu always reboots the switch from primary flash. Rebooting the switch from the CLI gives you more options. Refer to "Rebooting the Switch" on page 6-19.

8. After you reboot the switch, confirm that the software downloaded correctly:
   a. From the Main Menu, select **1. Status and Counters**, and from the Status and Counters menu, select **1. General System Information**
   b. Check the **Firmware revision** line.

Troubleshooting TFTP Download Failures. When using the menu interface, if a TFTP download fails, the Download OS (Operating System, or software) screen indicates the failure.



```
=========================- CONSOLE - MANAGER MODE -===========================
                                Download OS

  Current Firmware revision : K.11.00

  Method [TFTP] : TFTP
  TFTP Server : 10.29.227.105

  Remote File Name : os

              Received 0 bytes of OS download.
  +----------------------------------------------------------------------+
  |                                                                      |
  +----------------------------------------------------------------------+

Connection to 10.29.227.105 failed

                           Press any key to continue
```

Message Indicating cause of TFTP Download Failure

Figure A-3. Example of Message for Download Failure

To find more information on the cause of a download failure, examine the messages in the switch's Event Log by executing the **show log tftp** command from the CLI. (For more on the Event Log, see "Using the Event Log for Troubleshooting Switch Problems" on page C-27.)

Some of the causes of download failures include:

- Incorrect or unreachable address specified for the **TFTP Server** parameter. This may include network problems.
- Incorrect VLAN.
- Incorrect name specified for the **Remote File Name** parameter, or the specified file cannot be found on the TFTP server. This can also occur if the TFTP server is a UNIX machine and the case (upper or lower) for the filename on the server does not match the case for the filename entered for the **Remote File Name** parameter in the **Download OS** (Operating System, or software) screen.
- One or more of the switch's IP configuration parameters are incorrect.
- For a UNIX TFTP server, the file permissions for the software file do not allow the file to be copied.
- Another console session (through either a direct connection to a terminal device or through Telnet) was already running when you started the session in which the download was attempted.

Note

If an error occurs in which normal switch operation cannot be restored, the switch automatically reboots itself. In this case, an appropriate message is displayed after the switch reboots.

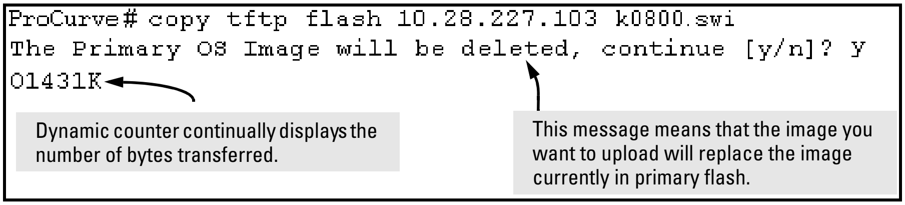
CLI: TFTP Download from a Server to Flash

Syntax: copy tftp flash <*ip-address*> <*remote-file*> [< primary | secondary >]

This command automatically downloads a switch software file to primary or secondary flash. Note that if you do not specify the flash destination, the TFTP download defaults to primary flash.

For example, to download a switch software file named k0800.swi from a TFTP server with the IP address of 10.28.227.103 to primary flash:

1. Execute **copy** as shown below:



```
ProCurve# copy tftp flash 10.28.227.103 k0800.swi
The Primary OS Image will be deleted, continue [y/n]? y
01431K
```

Dynamic counter continually displays the number of bytes transferred.

This message means that the image you want to upload will replace the image currently in primary flash.

Figure A-4. Example of the Command to Download an OS (Switch Software)

2. When the switch finishes downloading the software file from the server, it displays this progress message:

   Validating and Writing System Software to FLASH ...

3. When the download finishes, you must reboot the switch to implement the newly downloaded software image. To do so, use one of the following commands:

Syntax: boot system flash < primary | secondary >

Boots from the selected flash.

Syntax: reload

Boots from the flash image and startup-config file. A switch covered in this guide (with multiple configuration files), also uses the current startup-config file.

(For more on these commands, refer to "Rebooting the Switch" on page 6-19.)

4. To confirm that the software downloaded correctly, execute **show system** and check the Firmware revision line.

For information on primary/secondary flash memory and the boot commands, refer to "Using Primary and Secondary Flash Image Options" on page 6-14.

Note

If you use **auto-tftp** to download a new image in a redundant management system, the active management module downloads the new image to both the active and standby modules. Rebooting after the auto-tftp process completes reboots the entire system.

Using Secure Copy and SFTP

For some situations you may want to use a secure method to issue commands or copy files to the switch. By opening a secure, encrypted SSH session you can then use a third-party software application to take advantage of Secure Copy (SCP) and Secure ftp (SFTP). SCP and SFTP provide a secure alternative to TFTP for transferring information that may be sensitive (like switch configuration files) to and from the switch. Essentially you are creating a secure SSH tunnel as a way to transfer files with SFTP and SCP channels.

To use these commands you must install on the administrator workstation a third-party application software client that supports the SFTP and/or SCP functions. Some examples of software that supports SFTP and SCP are PuTTY, Open SSH, WinSCP, and SSH Secure Shell. Most of these are freeware and may be downloaded without cost or licensing from the internet. There are differences in the way these clients work, so be sure you also download the documentation.

As described earlier in this chapter you can use a TFTP client on the administrator workstation to update software images. This is a plain text mechanism and it connects to a standalone TFTP server or another ProCurve switch acting as a TFTP server to obtain the software image file(s). Using SCP and SFTP allows you to maintain your switches with greater security. You can also roll out new software images with automated scripts that make it easier to upgrade multiple switches simultaneously and securely.

SFTP (secure file transfer protocol) is unrelated to FTP, although there are some functional similarities. Once you set up an SFTP session through an SSH tunnel, some of the commands are the same as FTP commands. Certain commands are not allowed by the SFTP server on the switch, such as those that create files or folders. If you try to issue commands such as **create** or **remove** using SFTP the switch server returns an error message.

You can use SFTP just as you would TFTP to transfer files to and from the switch, but with SFTP your file transfers are encrypted and require authentication, so they are more secure than they would be using TFTP. SFTP works only with SSH version 2 (SSH v2).

Note

SFTP over SSH version 1 (SSH v1) is not supported. A request from either the client or the switch (or both) using SSH v1 generates an error message. The actual text of the error message differs, depending on the client software in use. Some examples are:

```
Protocol major versions differ: 2 vs. 1
Connection closed
```

```
Protocol major versions differ: 1 vs. 2
Connection closed

Received disconnect from <ip-addr>: /usr/local/
libexec/sftp-server: command not supported
Connection closed
```

SCP (secure copy) is an implementation of the BSD **rcp** (Berkeley UNIX remote copy) command tunneled through an SSH connection.

SCP is used to copy files to and from the switch when security is required. SCP works with both SSH v1 and SSH v2. Be aware that the most third-party software application clients that support SCP use SSHv1.

How It Works

The general process for using SCP and SFTP involves three steps:

1. Open an SSH tunnel between your computer and the switch if you haven't already done so. (This step assumes that you have already set up SSH on the switch.)
2. Execute **ip ssh filetransfer** to tell the switch that you want to enable secure file transfer.
3. Use a third-party client application for SCP and SFTP commands.

The SCP/SFTP Process

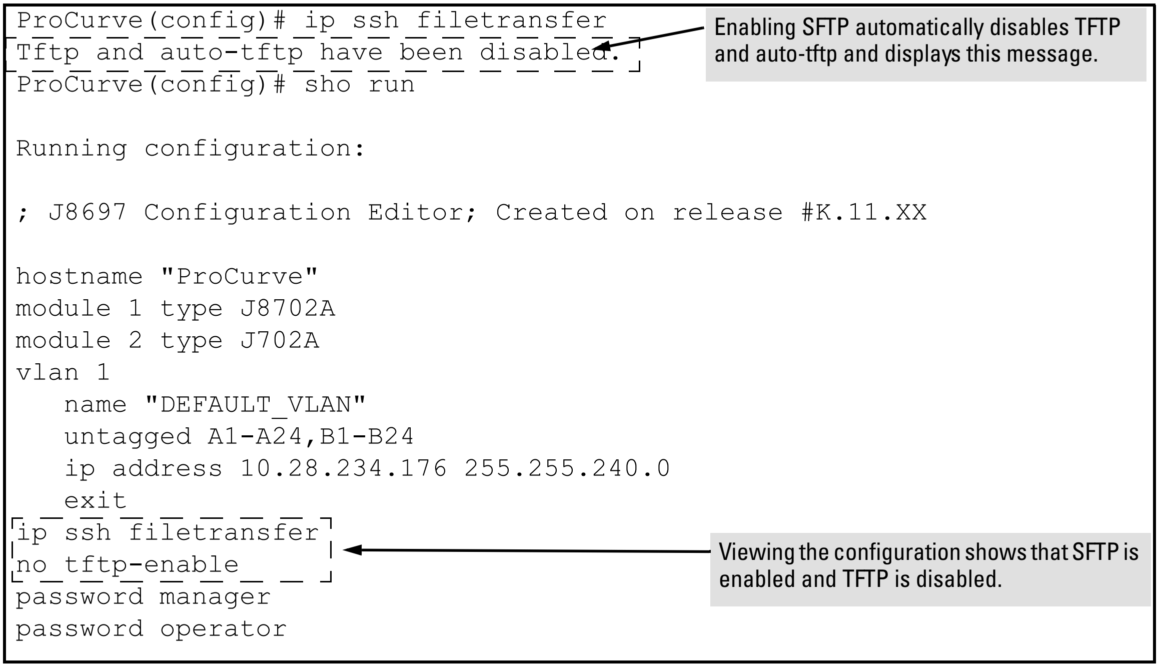
To use SCP and SFTP:

1. Open an SSH session as you normally would to establish a secure encrypted tunnel between your computer and the switch. For more detailed directions on how to open an SSH session refer to the chapter titled *"Configuring Secure Shell (SSH)"* in the *Access Security Guide* for your switch. Please note that this is a one-time procedure for new switches or connections. If you have already done it once you should not need to do it a second time.
2. To enable secure file transfer on the switch (once you have an SSH session established between the switch and your computer), open a terminal window and type in the following command:

   ```
   ProCurve(config)# ip ssh filetransfer
   ```

Disable TFTP and Auto-TFTP for Enhanced Security

Using the **ip ssh filetransfer** command to enable Secure FTP (SFTP) automatically disables TFTP and auto-TFTP (if either or both are enabled).



```
ProCurve(config)# ip ssh filetransfer
Tftp and auto-tftp have been disabled.
ProCurve(config)# sho run

Running configuration:

; J8697 Configuration Editor; Created on release #K.11.XX

hostname "ProCurve"
module 1 type J8702A
module 2 type J702A
vlan 1
   name "DEFAULT_VLAN"
   untagged A1-A24,B1-B24
   ip address 10.28.234.176 255.255.240.0
   exit
ip ssh filetransfer
no tftp-enable
password manager
password operator
```

Enabling SFTP automatically disables TFTP and auto-tftp and displays this message.

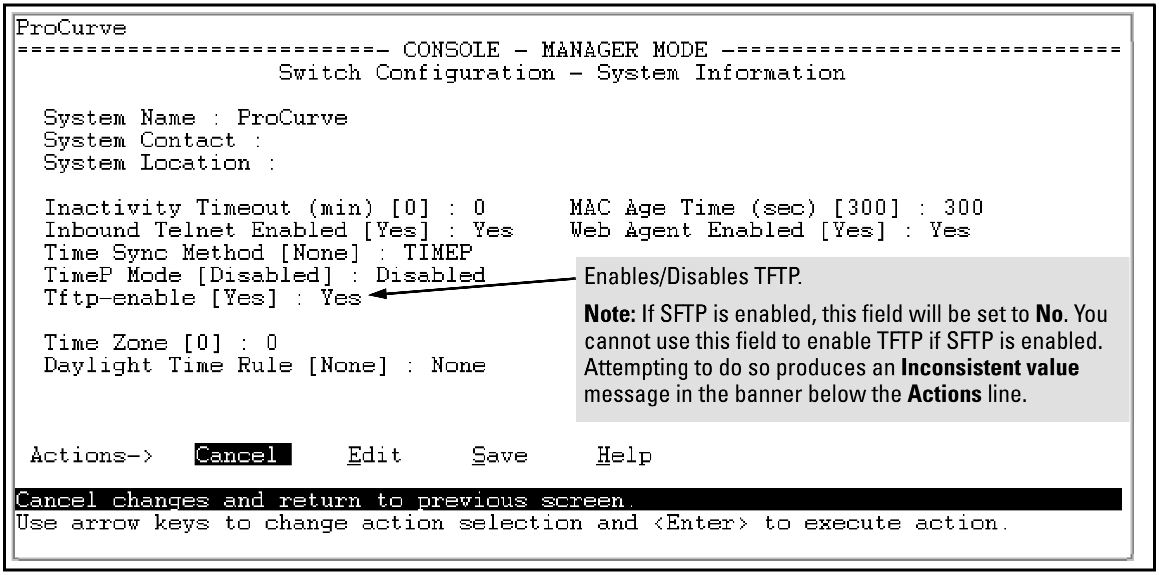
Viewing the configuration shows that SFTP is enabled and TFTP is disabled.

Figure A-5. Example of Switch Configuration with SFTP Enabled

If you enable SFTP, then later disable it, TFTP and auto-TFTP remain disabled unless they are explicitly re-enabled.

Operating rules are:

- The TFTP feature is enabled by default, and can be enabled or disabled through the CLI, the Menu interface, or an SNMP application. Auto-TFTP is disabled by default and must be configured through the CLI.



```
ProCurve
========================- CONSOLE - MANAGER MODE -============================
                  Switch Configuration - System Information

  System Name : ProCurve
  System Contact :
  System Location :

  Inactivity Timeout (min) [0] : 0      MAC Age Time (sec) [300] : 300
  Inbound Telnet Enabled [Yes] : Yes    Web Agent Enabled [Yes] : Yes
  Time Sync Method [None] : TIMEP
  TimeP Mode [Disabled] : Disabled
  Tftp-enable [Yes] : Yes

  Time Zone [0] : 0
  Daylight Time Rule [None] : None


 Actions->   Cancel     Edit     Save     Help

Cancel changes and return to previous screen.
Use arrow keys to change action selection and <Enter> to execute action.
```

Enables/Disables TFTP.

Note: If SFTP is enabled, this field will be set to **No**. You cannot use this field to enable TFTP if SFTP is enabled. Attempting to do so produces an **Inconsistent value** message in the banner below the **Actions** line.

Figure A-6. Using the Menu Interface To Disable TFTP

- While SFTP is enabled, TFTP and auto-TFTP cannot be enabled from the CLI. Attempting to enable either non-secure TFTP option while SFTP is enabled produces one of the following messages in the CLI:

```
SFTP must be disabled before enabling tftp.

SFTP must be disabled before enabling auto-tftp.
```

  Similarly, while SFTP is enabled, TFTP cannot be enabled using an SNMP management application. Attempting to do so generates an “inconsistent value” message. (An SNMP management application cannot be used to enable or disable auto-TFTP.)

- To enable SFTP by using an SNMP management application, you must first disable TFTP and, if configured, auto-TFTP on the switch. You can use either an SNMP application or the CLI to disable TFTP, but must use the CLI to disable auto-TFTP. The following two CLI commands disable TFTP and auto-TFTP on the switch.

Syntax: no tftp-enable

This command disables all TFTP operation on the switch except for the auto-TFTP feature. To re-enable TFTP operation, use the **tftp-enable** *command. When TFTP is disabled, the instances of* **tftp** *in the CLI copy command and the Menu interface "Download OS" screen become unavailable.*

Note: *This command does* ***not*** *disable auto-TFTP operation. To disable an auto-TFTP command configured on the switch, use the* **no auto-tftp** *command described below to remove the command entry from the switch's configuration.*

Syntax: no auto-tftp

If auto-TFTP is configured on the switch, this command deletes the **auto-tftp** *entry from the switch configuration, thus preventing auto-tftp operation if the switch reboots.*

Note: *This command does not affect the current TFTP-enable configuration on the switch.*

Command Options

If you need to enable SSH v2 (which is required for SFTP) enter this command:

```
ProCurve(config)# ip ssh version 2
```

Note

As a matter of policy, administrators should *not* enable the SSHv1-only or the SSHv1-or-v2 advertisement modes. SSHv1 is supported on only some legacy switches (such as the ProCurve Series 2500 switches).

To confirm that SSH is enabled type in the command

```
ProCurve(config)# show ip ssh
```

Once you have confirmed that you have enabled an SSH session (with the **show ip ssh** command) you can then open your third-party software client application to begin using the SCP or SFTP commands to safely transfer files or issue commands to the switch.

If you need to disable secure file transfer:

```
ProCurve(config)# no ip ssh filetransfer
```

Authentication

Switch memory allows up to ten public keys. This means the authentication and encryption keys you use for your third-party client SCP/SFTP software can differ from the keys you use for the SSH session, even though both SCP and SFTP use a secure SSH tunnel.

Note

SSH authentication is mutually exclusive with RADIUS servers.

Some clients such as PSCP (PuTTY SCP) automatically compare switch host keys for you. Other clients require you to manually copy and paste keys to the **$HOME/.ssh/known_hosts** file. Whatever SCP/SFTP software tool you use, after installing the client software you must verify that the switch host keys are available to the client.

Because the third-party software utilities you may use for SCP/SFTP vary, you should refer to the documentation provided with the utility you select before performing this process.

SCP/SFTP Operating Notes

- When an SFTP client connects, the switch provides a file system displaying all of its available files and folders. No file or directory creation is permitted by the user. Files may only be uploaded or downloaded, according to the permissions mask. All of the necessary files the switch will need are already in place on the switch. You do not need to (nor can you create) new files.
- The switch supports one SFTP session or one SCP session at a time.
- All files have read-write permission. Several SFTP commands, such as `create` or `remove`, are not allowed and return an error message. The switch displays the following files:

```
/
+---cfg
|   running-config
|   startup-config
+---log
|   crash-data
|   crash-data-a
|   crash-data-b
|   crash-data-c
|   crash-data-d         8212zl only
|   crash-data-e         “              “
|   crash-data-f         “              “
|   crash-data-g         8212zl only
|   crash-data-h         “         “
|   crash-data-I         “          “
|   crash-data-J         “          “
|   crash-data-K         “          “
|   crash-data-L         “          “
|   crash-log
|   crash-log-a
|   crash-log-b
|   crash-log-c
|   crash-log-d          8212zl only
|   crash-log-e          “              “
|   crash-log-f          “              “
|   crash-log-g          8212zl only
|   crash-log-h          “         “
|   crash-log-I          “         “
|   crash-log-J          “         “
|   crash-log-K          “         “
|   crash-log-L          “         “
|   event log
+---os
|   primary
|   secondary
\---ssh
    +---mgr_keys
    |   authorized_keys
    \---oper_keys
        authorized_keys
```

Once you have configured your switch for secure file transfers with SCP and SFTP, files can be copied to or from the switch in a secure (encrypted) environment and TFTP is no longer necessary.

Using Xmodem to Download Switch Software From a PC or UNIX Workstation

This procedure assumes that:

- The switch is connected via the Console RS-232 port to a PC operating as a terminal. (Refer to the *Installation and Getting Started Guide* you received with the switch for information on connecting a PC as a terminal and running the switch console interface.)
- The switch software is stored on a disk drive in the PC.
- The terminal emulator you are using includes the Xmodem binary transfer feature. (For example, in the HyperTerminal application included with Windows NT, you would use the **Send File** option in the **Transfer** dropdown menu.)

Menu: Xmodem Download to Primary Flash

Note that the menu interface accesses only the primary flash.

1. From the console Main Menu, select

   7. Download OS

2. Press **[E]** (for **Edit**).
3. Use the Space bar to select **XMODEM** in the **Method** field.
4. Press **[Enter]**, then **[X]** (for **eXecute**) to begin the software download. The following message then appears:

   Press enter and then initiate Xmodem transfer
   from the attached computer.....

5. Press **[Enter]** and then execute the terminal emulator command(s) to begin Xmodem binary transfer. For example, using HyperTerminal:
   a. Click on **Transfer**, then **Send File**.
   b. Type the file path and name in the Filename field.
   c. In the Protocol field, select **Xmodem**.
   d. Click on the **[Send]** button.

   The download will then commence. It can take several minutes, depending on the baud rate set in the switch and in your terminal emulator.

6. After the primary flash memory has been updated with the new software, you must reboot the switch to implement the newly downloaded software. Return to the Main Menu and press **[6]** (for **Reboot Switch**). You will then see the following prompt:

   Continue reboot of system? : No

   Press the space bar once to change `No` to `Yes`, then press **[Enter]** to begin the reboot.

7. To confirm that the software downloaded correctly:
   a. From the Main Menu, select

      1. Status and Counters

         1. General System Information

   b. Check the **Firmware revision** line.

CLI: Xmodem Download from a PC or UNIX Workstation to Primary or Secondary Flash

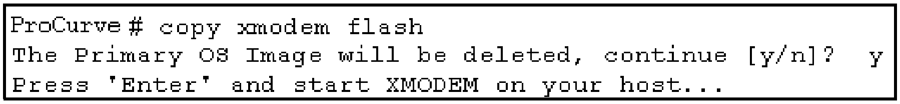
Using Xmodem and a terminal emulator, you can download a software file to either primary or secondary flash.

Syntax: copy xmodem flash [< primary | secondary >]

Downloads a software file to primary or secondary flash. If you do not specify the flash destination, the Xmodem download defaults to primary flash.

For example, to download a switch software file named E0822.swi from a PC (running a terminal emulator program such as HyperTerminal) to primary flash:

1. Execute the following command in the CLI:



```
ProCurve # copy xmodem flash
The Primary OS Image will be deleted, continue [y/n]?  y
Press 'Enter' and start XMODEM on your host...
```

2. Execute the terminal emulator commands to begin the Xmodem transfer. For example, using HyperTerminal:
   a. Click on **Transfer**, then **Send File**.
   b. Type the file path and name in the Filename field.
   c. In the Protocol field, select **Xmodem**.
   d. Click on the **[Send]** button.

   The download can take several minutes, depending on the baud rate used in the transfer.

3. When the download finishes, you must reboot the switch to implement the newly downloaded software. To do so, use one of the following commands:

   Syntax: boot system flash <primary | secondary>

   Reboots from the selected flash.

   Syntax: reload

   Reboots from the flash image currently in use.

   (For more on these commands, see "Rebooting the Switch" on page 6-19.)

4. To confirm that the software downloaded correctly:

```
ProCurve> show system
```

   Check the **Firmware revision** line. It should show the software version that you downloaded in the preceding steps.

If you need information on primary/secondary flash memory and the boot commands, refer to "Using Primary and Secondary Flash Image Options" on page 6-14.

Using USB to Transfer Files to and from the Switch

The switch's USB port (labeled as *Auxiliary Port*) allows the use of a USB flash drive for copying configuration files to and from the switch. Beginning with software release K_12_XX or later, **copy** commands that used either **tftp** or **xmodem**, now include an additional option for **usb** as a source or destination for file transfers.

Operating rules and restrictions on USB usage are:

- Unformatted USB flash drives must first be formatted on a PC (Windows FAT format). For devices with multiple partitions, only the first partition is supported. Devices with secure partitions are not supported.
- If they already exist on the device, sub-directories are supported. When specifying a <*filename*>, you must enter either the individual file name (if at the root) or the full path name (for example, /subdir/filename).
- To view the contents of a USB flash drive, use the **dir** command. This will list all files and directories at the root. To view the contents of a directory, you must specify the subdirectory name (that is, **dir** <s*ubdirectory*>).
- The USB port supports connection to a single USB device. USB hubs to add more ports are not supported.

Note

Some USB flash drives may not be supported on your switch. Consult the latest *Release Notes* for information on supported devices.

Using USB to Download Switch Software

This procedure assumes that:

- A software version for the switch has been stored on a USB flash drive. (The latest software file is typically available from the ProCurve Networking web site at **www.procurve.com**.)
- The USB device has been plugged into the switch's USB port.

Before you use the procedure:

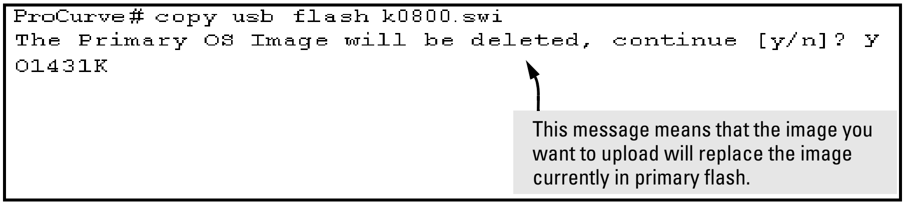
- Determine the name of the software file stored on the USB flash drive (for example, k0800.swi).
- Decide whether the image will be installed in the primary or secondary flash. (For more on primary/secondary flash memory and related boot commands, refer to "Using Primary and Secondary Flash Image Options" on page 6-14.)

Syntax: copy usb flash <*filename*> [< primary | secondary >]

This command automatically downloads a switch software file to primary or secondary flash. Note that if you do not specify the flash destination, the USB download defaults to primary flash.

For example, to copy a switch software file named k0800.swi from a USB device to primary flash:

1. Execute **copy** as shown below:



```
ProCurve# copy usb flash k0800.swi
The Primary OS Image will be deleted, continue [y/n]? y
01431K
```

This message means that the image you want to upload will replace the image currently in primary flash.

Figure A-7. Example of the Command to Copy Switch Software from USB

2. When the switch finishes copying the software file from the USB device, it displays this progress message:

   Validating and Writing System Software to the Filesystem....

3. When the copy finishes, you must reboot the switch to implement the newly loaded software. To do so, use one of the following commands:

Syntax: boot system flash < primary | secondary >

Boots from the selected flash.

Syntax: reload

Boots from the flash image and startup-config file. A switch covered in this guide (with multiple configuration files), also uses the current startup-config file.

(For more on these commands, refer to “Rebooting the Switch” on page 6-19.)

4. To confirm that the software downloaded correctly, execute **show system** and check the Firmware revision line.

Switch-to-Switch Download

You can use TFTP to transfer a software image between two switches of the same series. The menu interface enables you to transfer primary-to-primary or secondary-to-primary. The CLI enables all combinations of flash location options.

Menu: Switch-to-Switch Download to Primary Flash

Using the menu interface, you can download a switch software file from either the primary or secondary flash of one switch to the primary flash of another switch of the same series.

1. From the switch console Main Menu in the switch to receive the download, select **7. Download OS** screen.
2. Ensure that the **Method** parameter is set to **TFTP** (the default).
3. In the **TFTP Server** field, enter the IP address of the remote switch containing the software file you want to download.
4. For the **Remote File Name**, enter one of the following:
   - To download the software in the primary flash of the source switch, type “**flash**” in lowercase characters.
   - To download the software in the secondary flash of the source switch, type
     /os/secondary.
5. Press **[Enter]**, then **[X]** (for **eXecute**) to begin the software download.
6. A “progress” bar indicates the progress of the download. When the entire switch software download has been received, all activity on the switch halts and the following messages appear:

   Validating and writing system software to FLASH...

7. After the primary flash memory has been updated with the new software, you must reboot the switch to implement the newly downloaded software. Return to the Main Menu and press **[6]** (for **Reboot Switch**). You will then see this prompt:

   Continue reboot of system? : No

   Press the space bar once to change `No` to `Yes`, then press **[Enter]** to begin the reboot.

8. To confirm that the software downloaded correctly:

   a. From the Main Menu, select

      Status and Counters

         General System Information

   b. Check the **Firmware revision** line.

CLI: Switch-To-Switch Downloads

Where two switches in your network belong to the same series, you can download a software image between them by initiating a **copy tftp** command from the destination switch. The options for this CLI feature include:

■ Copy from primary flash in the source to either primary or secondary in the destination.

■ Copy from either primary or secondary flash in the source to either primary or secondary flash in the destination.

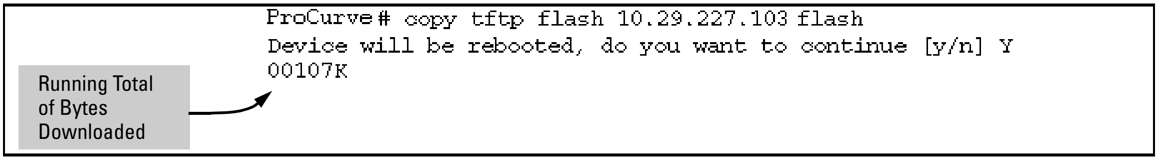
Downloading from Primary Only.

Syntax: copy tftp flash < *ip-addr* > flash [primary | secondary]

This command (executed in the destination switch) downloads the software flash in the source switch's primary flash to either the primary or secondary flash in the destination switch.

If you do not specify either a primary or secondary flash location for the destination, the download automatically goes to primary flash.

For example, to download a software file from primary flash in a switch with an IP address of 10.29.227.103 to the primary flash in the destination switch, you would execute the following command in the destination switch's CLI:



```
ProCurve# copy tftp flash 10.29.227.103 flash
Device will be rebooted, do you want to continue [y/n] Y
00107K
```

Running Total of Bytes Downloaded

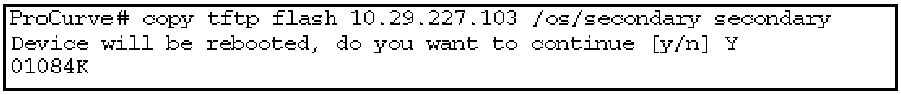
Figure A-8. Switch-To-Switch, from Primary in Source to Either Flash in Destination

Downloading from Either Flash in the Source Switch to Either Flash in the Destination Switch.

Syntax: copy tftp flash < *ip-addr* > < /os/primary > | < /os/secondary > [primary | secondary]

This command (executed in the destination switch) gives you the most options for downloading between switches. If you do not specify either a primary or secondary flash location for the destination, the download automatically goes to primary flash.

For example, to download a software file from secondary flash in a switch with an IP address of 10.28.227.103 to the secondary flash in a destination switch, you would execute the following command in the destination switch's CLI:



```
ProCurve# copy tftp flash 10.29.227.103 /os/secondary secondary
Device will be rebooted, do you want to continue [y/n] Y
01084K
```

Figure A-9. Switch-to-Switch, from Either Flash in Source to Either Flash in Destination

Using PCM+ to Update Switch Software

ProCurve Manager Plus includes a software update utility for updating on ProCurve switch products. For further information, refer to the *Getting Started Guide* and the *Administrator's Guide*, provided electronically with the application.

Copying Software Images

Using the CLI commands described in this section, you can copy software images from the switch to another device using tftp, xmodem, or usb.

Note

For details on how switch memory operates, including primary and secondary flash, refer to Chapter 6, "Switch Memory and Configuration".

TFTP: Copying a Software Image to a Remote Host

Syntax: copy flash tftp < *ip-addr* > < *filename* >

This command copies the primary flash image to a TFTP server.

For example, to copy the primary flash to a TFTP server having an IP address of 10.28.227.105:

```
ProCurve# copy flash tftp 10.28.227.105 k0800.swi
```

where `k0800.swi` is the filename given to the flash image being copied.

Xmodem: Copying a Software Image from the Switch to a Serially Connected PC or UNIX Workstation

To use this method, the switch must be connected via the serial port to a PC or UNIX workstation.

Syntax: copy flash xmodem < pc | unix >

Uses Xmodem to copy a designated configuration file from the switch to a PC or Unix workstation.

For example, to copy the primary flash image to a serially connected PC:

1. Execute the following command:

```
Procurve# copy xmodem flash
Press 'Enter' and start XMODEM on your host...
```

2. After you see the above prompt, press **[Enter]**.
3. Execute the terminal emulator commands to begin the file transfer.

USB: Copying a Software Image to a USB Device

To use this method, a USB flash memory device must be connected to the switch's USB port.

Syntax: copy flash usb < filename>

Uses the USB port to copy the primary flash image from the switch to a USB flash memory device.

For example, to copy the primary image to a USB flash drive:

1. Insert a USB device into the switch's USB port.
2. Execute the following command:

```
Procurve# copy flash usb k0800.swi
```

   where `k0800.swi` is the name given to the primary flash image that is copied from the switch to the USB device.

Transferring Switch Configurations

Transfer Features

Feature	Page
Use TFTP to copy from a remote host to a config file.	A-25
Use TFTP to copy a config file to a remote host.	A-26
Use Xmodem to copy a configuration from a serially connected host to a config file.	A-26
Use Xmodem to copy a config file to a serially connected host.	A-26
Use USB to copy a configuration from a USB device to a config file.	A-28
Use USB to copy a config file to a USB device.	A-28

Using the CLI commands described in this section, you can copy switch configurations to and from a switch, or copy a software image to configure or replace an ACL in the switch configuration.

Note

For greater security, you can perform all TFTP operations using SFTP as described in the section on *Using Secure Copy and SFTP* on page A-9.

The **include-credentials** command can also be used to save passwords, secret keys, and other security credentials in the running config file. For more information, see the section on “Saving Security Credentials in a Config File” in the *Access Security Guide* for your switch.

TFTP: Copying a Configuration File to a Remote Host

Syntax: copy < startup-config | running-config > tftp < *ip-addr* > < *remote-file* > [pc | unix]

copy config < *filename* > tftp < *ip-addr* > < *remote-file* > [pc | unix]

This command can copy a designated config file in the switch to a TFTP server. For more on multiple configuration files, refer to “Multiple Configuration Files” on page 6-26.

For example, to upload the current startup configuration to a file named **sw8200** in the configs directory on drive “**d**” in a TFTP server having an IP address of 10.28.227.105:

```
ProCurve# copy startup-config tftp 10.28.227.105
          d:\configs\sw8200
```

TFTP: Copying a Configuration File from a Remote Host

Syntax: copy tftp < startup-config | running-config > < *ip-address* > < *remote-file* > [pc | unix]

copy tftp config < *filename* > < *ip-address* > < *remote-file* > [pc | unix]

This command can copy a configuration from a remote host to a designated config file in the switch. For more on multiple configuration files, refer to “Multiple Configuration Files” on page 6-26.

(Refer to “Using Primary and Secondary Flash Image Options” on page 6-14 for more on flash image use.)

For example, to download a configuration file named **sw8200** in the **configs** directory on drive “**d**” in a remote host having an IP address of 10.28.227.105:

```
ProCurve# copy tftp startup-config 10.28.227.105
          d:\configs\sw8200
```

Xmodem: Copying a Configuration File to a Serially Connected PC or UNIX Workstation

To use this method, the switch must be connected via the serial port to a PC or UNIX workstation. You will need to:

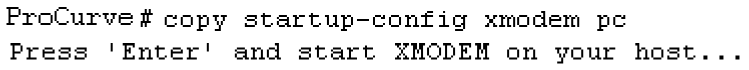
- Determine a filename to use.
- Know the directory path you will use to store the configuration file.

Syntax: copy < startup-config | running-config > xmodem < pc | unix >
copy config < *filename* > xmodem < pc | unix >

Uses Xmodem to copy a designated configuration file from the switch to a PC or Unix workstation. For more on multiple configuration files, refer to "Multiple Configuration Files" on page 6-26.

For example, to copy a configuration file to a PC serially connected to the switch:

1. Determine the file name and directory location on the PC.
2. Execute the following command:



```
ProCurve# copy startup-config xmodem pc
Press 'Enter' and start XMODEM on your host...
```

3. After you see the above prompt, press **[Enter]**.
4. Execute the terminal emulator commands to begin the file transfer.

Xmodem: Copying a Configuration File from a Serially Connected PC or UNIX Workstation

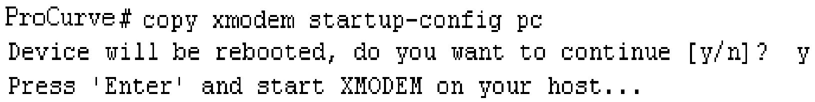
To use this method, the switch must be connected via the serial port to a PC or UNIX workstation on which is stored the configuration file you want to copy. To complete the copying, you will need to know the name of the file to copy and the drive and directory location of the file.

Syntax: copy xmodem startup-config < pc | unix >
copy xmodem config < *filename* > < pc | unix >

Copies a configuration file from a serially connected PC or UNIX workstation to a designated configuration file on the switch. For more on multiple configuration files, refer to "Multiple Configuration Files" on page 6-26.

For example, to copy a configuration file from a PC serially connected to the switch:

1. Execute the following command:



```
ProCurve# copy xmodem startup-config pc
Device will be rebooted, do you want to continue [y/n]?  y
Press 'Enter' and start XMODEM on your host...
```

2. After you see the above prompt, press **[Enter]**.
3. Execute the terminal emulator commands to begin the file transfer.
4. When the download finishes, you must reboot the switch to implement the newly downloaded software. To do so, use one of the following commands:

Syntax: boot system flash [primary | secondary]
boot system flash [config < *filename* >

Switches boot from the designated configuration file. For more on multiple configuration files, refer to "Multiple Configuration Files" on page 6-26.

Syntax: reload

Reboots from the flash image currently in use.

(For more on these commands, refer to "Rebooting the Switch" on page 6-19.)

USB: Copying a Configuration File to a USB Device

To use this method, a USB flash memory device must be connected to the switch's USB port.

Syntax: copy startup-config usb < filename>
copy running-config usb < filename >

Uses the USB port to copy a designated configuration file from the switch to a USB flash memory device. For more on multiple configuration files, refer to "Multiple Configuration Files" on page 6-26.

For example, to copy the startup configuration file to a USB flash drive:

1. Insert a USB device into the switch's USB port.
2. Execute the following command:

```
Procurve# copy startup-config usb procurve-config
```

   where `procurve-config` is the name given to the configuration file that is copied from the switch to the USB device.

USB: Copying a Configuration File from a USB Device

To use this method, the switch must be connected via the USB port to a USB flash drive on which is stored the configuration file you want to copy. To execute the command, you will need to know the name of the file to copy.

Syntax: copy usb startup-config < filename >

Copies a configuration file from a USB device to the startup configuration file on the switch.

For example, to copy a configuration file from a USB device to the switch:

1. Insert a USB device into the switch's USB port.
2. Execute the following command:

```
Procurve# copy usb startup-config procurve-config
```

   where `procurve-config` is the name of the file to copy.

3. At the prompt, press **[Enter]** to reboot the switch and implement the newly downloaded software.

Transferring ACL Command Files

This section describes how to upload and execute a command file to the switch for configuring or replacing an Access Control List (ACL) in the switch configuration. Such files should contain only ACE (Access Control Entry) commands. For more on this general topic, including an example of an ACL command file created offline, refer to the section titled "Editing ACLs and Creating an ACL Offline" in the "Access Control Lists (ACLs)" chapter of the latest *Access Security Guide* for your switch.

TFTP: Uploading an ACL Command File from a TFTP Server

Syntax: copy tftp command-file < *ip-addr* > < *filename*.txt > < unix | pc >

where:

< *ip-addr* > = *The IP address of a TFTP server available to the switch*

< *filename.txt* > = *A text file containing ACL commands and stored in the TFTP directory of the server identified by* < *ip-addr* >

< unix | pc > = *The type of workstation used for serial, Telnet, or SSH access to the switch CLI*

This command copies and executes the named text file from the specified TFTP server address and executes the ACL commands in the file. Depending on the ACL commands used, this action does one of the following in the running-config file:

- *Creates a new ACL.*
- *Replaces an existing ACL. (Refer to "Creating an ACL Offline" in the "Access Control Lists (ACLs)" chapter in the latest* Access Security Guide *for your switch.)*
- *Adds to an existing ACL.*

For example, suppose you:

1. Created an ACL command file named **vlan10_in.txt** to update an existing ACL.
2. Copied the file to a TFTP server at 18.38.124.16.

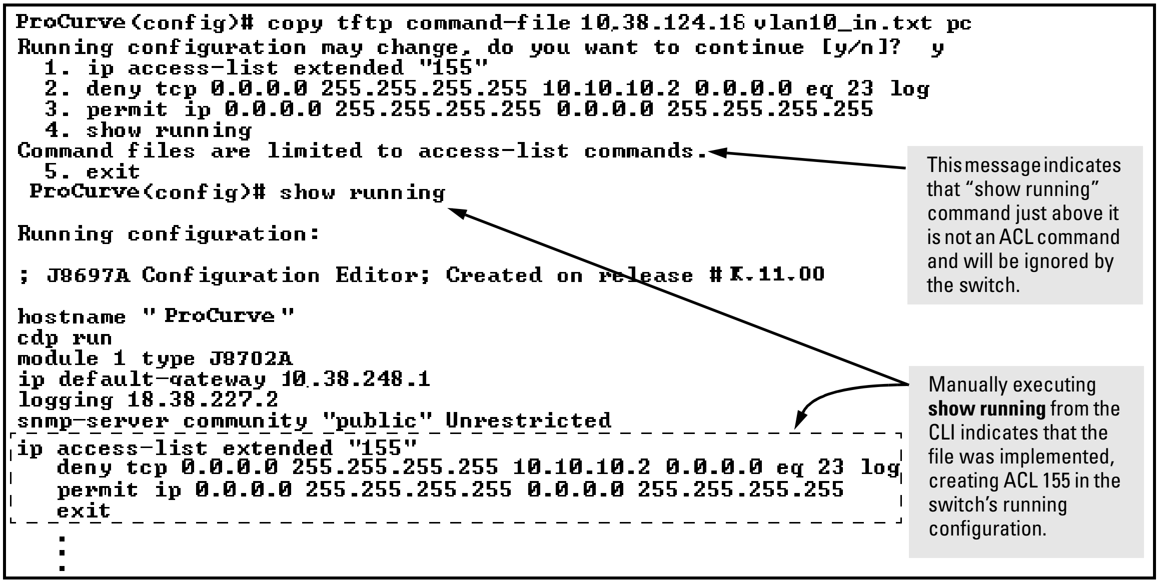
Using a PC workstation, you then execute the following from the CLI to upload the file to the switch and implement the ACL commands it contains:

```
ProCurve(config)# copy tftp command-file 18.38.124.16
vlan10_in.txt pc
```

The switch displays this message:

```
Running configuration may change, do you want to continue
[y/n]?
```

To continue with the upload, press the **[Y]** key. To abort the upload, press the **[N]** key. Note that if the switch detects an illegal (non-ACL) command in the file, it bypasses the illegal command, displays a notice as shown in figure A-10, and continues to implement the remaining ACL commands in the file.



```
ProCurve(config)# copy tftp command-file 10.38.124.16 vlan10_in.txt pc
Running configuration may change, do you want to continue [y/n]?  y
  1. ip access-list extended "155"
  2. deny tcp 0.0.0.0 255.255.255.255 10.10.10.2 0.0.0.0 eq 23 log
  3. permit ip 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255
  4. show running
Command files are limited to access-list commands.
  5. exit
 ProCurve(config)# show running

Running configuration:

; J8697A Configuration Editor; Created on release # K.11.00

hostname " ProCurve "
cdp run
module 1 type J8702A
ip default-gateway 10.38.248.1
logging 18.38.227.2
snmp-server community "public" Unrestricted
ip access-list extended "155"
   deny tcp 0.0.0.0 255.255.255.255 10.10.10.2 0.0.0.0 eq 23 log
   permit ip 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255
   exit
   :
   :
```

This message indicates that "show running" command just above it is not an ACL command and will be ignored by the switch.

Manually executing **show running** from the CLI indicates that the file was implemented, creating ACL 155 in the switch's running configuration.

Figure A-10. Example of Using the Copy Command to Download and Configure an ACL

Xmodem: Uploading an ACL Command File from a Serially Connected PC or UNIX Workstation

Syntax: copy xmodem command-file < unix | pc >

Uses Xmodem to copy and executes an ACL command from a PC or Unix workstation. Depending on the ACL commands used, this action does one of the following in the running-config file:

- *Creates a new ACL.*
- *Replaces an existing ACL. (Refer to "Creating an ACL Offline" in the "Access Control Lists (ACLs)" chapter in the latest* Access Security Guide *for your switch.)*
- *Adds to an existing ACL.*

USB: Uploading an ACL Command File from a USB Device

Syntax: copy usb command-file < *filename*.txt > < unix | pc >

where:

< *filename.txt* > = *A text file containing ACL commands and stored in the USB flash drive.*

< unix | pc > = *The type of workstation used to create the text file.*

This command copies and executes the named text file from a USB flash drive and executes the ACL commands in the file. Depending on the ACL commands used, this action does one of the following in the running-config file:

- *Creates a new ACL.*
- *Replaces an existing ACL. (Refer to "Creating an ACL Offline" in the "Access Control Lists (ACLs)" chapter in the latest* Access Security Guide *for your switch.)*
- *Adds to an existing ACL.*

For example, suppose you:

1. Created an ACL command file named **vlan10_in.txt** to update an existing ACL.
2. Copied the file to a USB flash drive.

Using a PC workstation, you then execute the following from the CLI to upload the file to the switch and implement the ACL commands it contains:

```
ProCurve(config)# copy usb command-file vlan10_in.txt pc
```

The switch displays this message:

```
Running configuration may change, do you want to continue
[y/n]?
```

To continue with the upload, press the **[Y]** key. To abort the upload, press the **[N]** key. Note that if the switch detects an illegal (non-ACL) command in the file, it bypasses the illegal command, displays a notice (as in the tftp example shown in Figure A-10 on page A-30), and continues to implement the remaining ACL commands in the file.

Copying Diagnostic Data to a Remote Host, USB Device, PC or UNIX Workstation

You can use the CLI to copy the following types of switch data to a text file in a destination device:

- Command Output: Sends the output of a switch CLI command as a file on the destination device.
- Event Log: Copies the switch's Event Log into a file on the destination device.
- Crash Data: software-specific data useful for determining the reason for a system crash.
- Crash Log: Processor-Specific operating data useful for determining the reason for a system crash.

The destination device and copy method options are as follows (CLI key word is in bold):

- Remote Host via **TFTP**.
- Physically connected USB flash drive via the switch's **USB** port.
- Serially connected PC or UNIX workstation via **Xmodem**.

Copying Command Output to a Destination Device

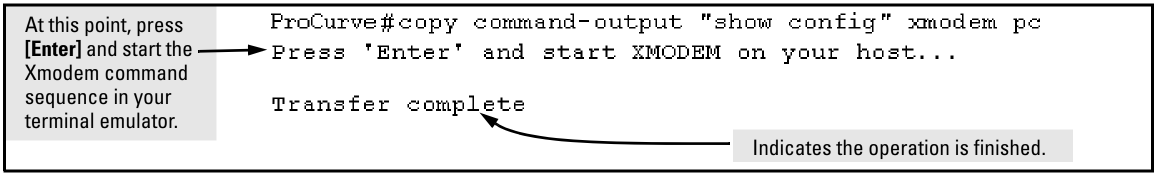
Syntax: copy command-output < “*cli-command*” > tftp < *ip-address* > < *filepath-filename* >

copy command-output < “*cli-command*” > usb < *filename* >

copy command-output <“*cli-command*”> xmodem

These commands direct the displayed output of a CLI command to a remote host, attached USB device, or to a serially connected PC or UNIX workstation.

For example, to use Xmodem to copy the output of **show config** to a serially connected PC:



```
ProCurve#copy command-output "show config" xmodem pc
Press 'Enter' and start XMODEM on your host...

Transfer complete
```

At this point, press **[Enter]** and start the Xmodem command sequence in your terminal emulator.

Indicates the operation is finished.

Figure A-11. Example of Sending Command Output to a File on an Attached PC

Note The command you specify must be enclosed in double-quote marks.

Copying Event Log Output to a Destination Device

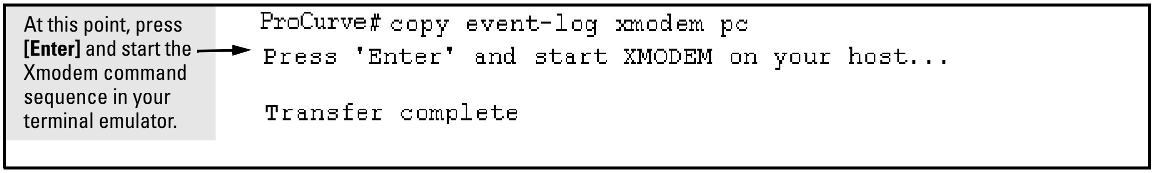
Syntax: copy event-log tftp < *ip-address* > < *filepath_filename* >

copy event-log usb < *filename* >

copy event-log xmodem <*filename*>

These commands copy the Event Log content to a remote host, attached USB device, or to a serially connected PC or UNIX workstation.

For example, to copy the event log to a PC connected to the switch:



At this point, press **[Enter]** and start the Xmodem command sequence in your terminal emulator.

```
ProCurve# copy event-log xmodem pc
Press 'Enter' and start XMODEM on your host...

Transfer complete
```

Figure A-12. Example of Sending Event Log Content to a File on an Attached PC

Copying Crash Data Content to a Destination Device

This command uses TFTP, USB, or Xmodem to copy the Crash Data content to a destination device. You can copy individual slot information or the master switch information. If you do not specify either, the command defaults to the master data.

Syntax: copy crash-data [<*slot-id* | master>] tftp <*ip-address*> <*filename*>

copy crash-data [<*slot-id* | master>] usb <*filename*>

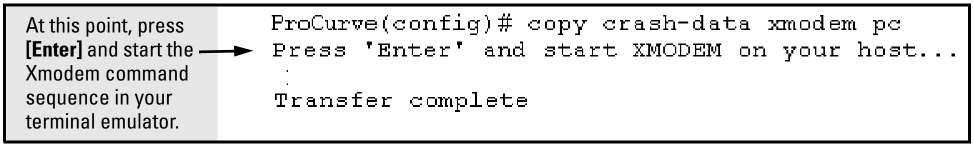
copy crash-data [<*slot-id* | master>] xmodem

where: *slot-id* = a - h, *and retrieves the crash log or crash data from the processor on the module in the specified slot.*

master *Retrieves crash log or crash data from the switch's chassis processor. When "master" is specified, crash files from both management modules are copied.*

These commands copy the crash data content to a remote host, attached USB device, or to a serially connected PC or UNIX workstation. You can copy individual slot information or the master switch information. If you do not specify either, the command defaults to the master data.

For example, to copy the switch's crash data to a file in a PC:



At this point, press **[Enter]** and start the Xmodem command sequence in your terminal emulator.

```
ProCurve(config)# copy crash-data xmodem pc
Press 'Enter' and start XMODEM on your host...
 :
Transfer complete
```

Figure A-13. Example of Copying Switch Crash Data Content to a PC

Copying Crash Data with Redundant Management. When you are using redundant management, the **copy crash-data** command operates somewhat differently.

Syntax: copy crash-data [<*slot-id*> | mm] tftp <*ip-address*> <*filename*>

Copies both the active and standby management modules' crash data to a user-specified file. If no parameter is specified, files from all modules (management and interface) are concatenated.

slot-id: *retrieves the crash data from the module in the specified slot.*

mm: *retrieves the crash data from both management modules and concatenates them.*

Copying Crash Log Data Content to a Destination Device

Syntax: copy crash-log [<*slot-id* | master>] tftp <*ip-address*> <*filepath and filename*>

copy crash-log [<*slot-id* | master>] usb <*filename*>

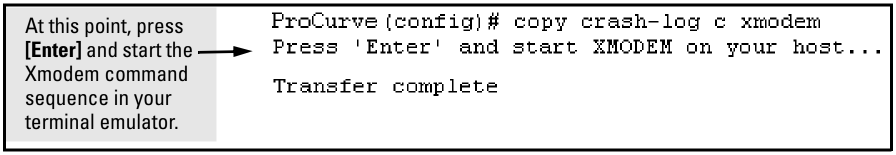
copy crash-log [<*slot-id* | master>] xmodem

where: *slot-id* = **a** - **h**, *and retrieves the crash log from the processor on the module in the specified slot.*

master *Retrieves the crash log from the switch's chassis processor. When master is specified, crash files from both management modules are copied.*

These commands copy the Crash Log content to a remote host, attached USB device, or to a serially connected PC or UNIX workstation. You can copy individual slot information or the master switch information. If you do not specify either, the command defaults to the master data.

For example, to copy the Crash Log for slot C to a file in a PC connected to the switch:



At this point, press **[Enter]** and start the Xmodem command sequence in your terminal emulator.

```
ProCurve(config)# copy crash-log c xmodem
Press 'Enter' and start XMODEM on your host...

Transfer complete
```

Figure A-14. Example of sending a Crash Log for Slot C to a File on an Attached PC

Copying Crash Logs with Redundant Management. When you are using redundant management, the **copy crash-log** command operates somewhat differently.

Syntax: copy crash-log [<*slot-id*> | mm] tftp <*ip-address*> <*filename*>

Copies both the active and standby management modules' crash logs to a user-specified file. If no parameter is specified, files from all modules (management and interface) are concatenated.

slot-id: *retrieves the crash log from the module in the specified slot.*

mm: *retrieves the crash logs from both management modules and concatenates them.*

Using USB Autorun

USB autorun helps ease the configuration of ProCurve switches by providing a way to auto-execute CLI commands from a USB flash drive. Using this solution, you can create a command file (also known as an AutoRun file), write it to a USB storage device, and then execute the file simply by inserting the USB device in to the switch's 'Auxiliary Port'. The AutoRun file gets executed automatically when autorun is enabled on the switch, and can be designed for various purposes: for example, to configure the switch, to update software, or to retrieve diagnostic logs for troubleshooting purposes.

The overall USB autorun solution requires the following components:

- A ProCurve switch which can securely use USB autorun to load authorized configurations and write reporting information. This requires software versions K.13.01, T.13.01 or greater.
- The network management application *ProCurve Manager Plus* (PCM+). PCM+ is required to create a valid AutoRun file and view the results after the file has been executed on the switch.
- A non-proprietary USB flash drive.

Note

The ability to create a valid AutoRun file will be incorporated into an upcoming ProCurve Manager update. Refer to the ProCurve Manager documentation for details. For guidelines on using the USB port for basic file copy capabilities, see "Using USB to Transfer Files to and from the Switch" on page A-18.

How It Works

The general process for using USB Autorun is as follows (*steps 1, 2, and 7 require an upcoming update to PCM+ as described above*):

1. Create an AutoRun file using PCM+. Refer to the ProCurve Manager documentation for details.

Note

Creating the AutoRun file in PCM+, includes the following steps:

a. specify the target device or devices.

b. create the CLI script to be executed on the target device(s).

c. determine if the file will be signed and/or encrypted.

d. determine if the file will be 'run once' (moved to a 'processed' directory on execution) or 'run many' (kept in the root directory of the flash drive from where it can be executed again).

2. Deploy the AutoRun file to a USB flash drive.
3. (If required) Enable the autorun feature on the switch (autorun is enabled by default unless an operator or manager password has been set—see "Autorun and Configuring Passwords" on page A-41).
4. (If the AutoRun file has been signed or encrypted) Enable secure-mode on the switch firstly by configuring an encryption key and a valid trusted certificate, and then by enabling secure-mode via the CLI. See "Enabling Secure Mode" on page A-40.
5. Insert the USB flash drive into the switch's USB auxiliary port.

   The switch processes the AutoRun file automatically and writes a result (.txt) file and report (.xml) file back to the USB flash drive, reporting on the command operations that were executed.
6. Remove the USB device from the USB port.

   The switch executes any post-commands, such as rebooting the switch to apply any configuration updates.
7. (Optional) Transfer the 'result file' and 'report file' to a PCM+-enabled computer for report checking. See "Troubleshooting Autorun Operations" on page A-39.

Security Considerations

By default, the switch is unsecured when shipped (that is, USB autorun is enabled by default). However, as soon as an operator or manager password is configured, autorun is disabled and must be re-enabled at the configuration level of the CLI before it can be used. The requirement to use PCM+ to create a valid AutoRun file helps prevent a non-authorized command file from being created and processed by the switch.

In terms of physical security, access to the switch's console port and USB port are equivalent. Keeping the switch in a locked wiring closet or other secure space helps to prevent unauthorized physical access. As additional precautions, you have the following configuration options via the CLI (see page A-40):

- Disable autorun by setting an operator or manager password.
- Disable or re-enable the USB autorun function via the CLI.
- Enable autorun in secure mode to verify signatures in autorun command files and to decrypt encrypted command files.

Troubleshooting Autorun Operations

You can verify autorun operations by checking the following items:

USB Auxiliary Port LEDs. The following table shows LED indications on the Auxiliary Port that allow you to identify the different USB operation states.

Color	State	Meaning
Green	Slow Blinking	Switch is processing USB AutoRun file.
Green	Solid	Switch has finished processing USB AutoRun file. This LED state indicates the AutoRun file was successfully executed, and the report files were generated. The report files may be reviewed on a USB-enabled computer for more details. Upon removal of the USB device, the LED will be turned OFF.
n/a	Off	Indicates that no USB device has been inserted, or that a USB device that cannot be recognized as a USB storage device has been inserted, or that no AutoRun file can be found on the inserted USB device. If the USB device has just been removed from the port, the switch will execute any post commands.
Amber	Fast Blinking	Processing Error. The AutoRun file will stop processing when an error is encountered (for example, no more disk space is available on the USB device to write the result and report files). Remove the USB device and inspect its contents on a USB-enabled computer for more information on the error.

AutoRun Status Files. The following files are generated during autorun operations and written to the USB flash drive:

- Report file(s) (.xml file)—shows which CLI commands have been run. The file name includes a serial number and datetime stamp to indicate when and on which device the AutoRun file was executed.
- Result file(s) (.txt file)—contains the CLI output for each command that was run on the switch, allowing you to verify whether a command was executed successfully or not.

Note

PCM+ provides a mechanism to read these status files and capture the results of the commands executed. It also allows you to verify the report files for their authenticity and reject files that have not been signed (refer to the ProCurve Manager documentation for details).

The status files will not include any records of post commands that may have been executed after the USB flash drive was removed from the switch.

Event Log or Syslog. For details on how to use the switch's event log or syslog for help in isolating autorun-related problems, see "Using the Event Log for Troubleshooting Switch Problems" on page C-27.

Configuring Autorun on the Switch

To enable/disable the autorun feature on the switch, the following commands can be executed from configuration mode in the CLI.

Syntax: [no] autorun [encryption-key <*key-string*> | secure-mode]

Enables/disables USB autorun on the switch.

Use the **encryption-key** *keyword to configure or remove an encryption-key (a base-64 encoded string). The encryption key is a pre-requisite for enabling autorun in secure-mode. Encryption is regarded only when the AutoRun file is also signed by an authentic source.*

Use the **secure-mode** *keyword to enable or disable secure mode for autorun.*

Default: Enabled (or Disabled if a password has been set).

Enabling Secure Mode

Autorun secure mode can be used to verify the authenticity of autorun command files. Secure-mode is configured using the **autorun secure-mode** command and can be enabled under the following conditions:

- an encryption-key has already been configured using the **autorun encryption key** command; and
- a trusted certificate for verifying autorun command files has been copied to the switch using the **copy** <tftp | usb> **autorun-cert-file** command.

There is an additional security option to install a valid key-pair for signing the result files that are generated during autorun operations. The key-pair can be generated on the switch using the **crypto key generate autorun** [*rsa*] command.

Note

The key-pair can also be installed from a tftp server or via the usb port using **copy** <tftp | usb> **autorun-key-file** <*ipaddr filename*> command. The filename must contain the private key and the matching public key in a X509 certificate structure. Both the private key and the X509 certificate must be in PEM format.

Operating Notes and Restrictions

- Autorun is enabled by default, until passwords are set on the device.
- Secure-mode and encryption-key are disabled by default.
- To enable secure mode both an encryption key and trusted certificate must be set.
- If secure-mode is enabled, the following conditions apply:
  - the encryption-key cannot be removed/un-configured;
  - the key-pair cannot be removed.
- If secure mode is disabled, the key-pair can be removed using the **crypto key zeorize autorun** command.
- When installing the autorun certificate file and/or the other key files, the files must be in PEM format.

Autorun and Configuring Passwords

When an operator or manager password is configured on a switch, autorun will be disabled automatically, and a message is displayed on the screen as shown in the following example:

```
ProCurve# password manager
New password for manager: *****
Please retype new password for manager: *****
Autorun is disabled as operator/manager is configured.
```

After passwords are set, autorun can be re-enabled as needed using the **autorun** command.

For more information on configuring passwords, refer to the chapter on “Username and Password Security” in the *Access Security Guide* for your switch.

Viewing Autorun Configuration Information

The **show autorun** command displays autorun configuration status information as shown in the following example.

```
ProCurve(config)# show autorun

 Autorun configuration status

  Enabled        : Yes
  Secure-mode    : Disabled
  Encryption-key :
```