

Overview

Contents

Using This Guide	1-3
Understanding Command Syntax Statements	1-4
CLI Prompt Convention	1-4
IP Address Convention	1-5
Interface Numbering Convention	1-5
Quick Start Sections	1-6
Obtaining Additional Information	1-6
Downloading Software Updates	1-7
Interface Management Options	1-9
CLI	1-9
Web Browser Interface	1-9
Accessing the Web Browser Interface	1-10
Using the ProCurve Web Browser Interface	1-11
CLI Tools	1-13
Help Tools	1-13
CLI Help Commands	1-13
Editing Commands	1-14
Basic Commands	1-15
no	1-15
do	1-15
exit	1-15
File Management Commands	1-16
copy	1-16
erase	1-19
write	1-19
autosynch	1-19

Troubleshooting Commands	1-20
reload in	1-20
show	1-21
show tech	1-21
safe-mode	1-22
Managing Configuration Files Using a Text Editor	1-25
Using Error Messages to Repair a Configuration	1-25
Quick Start	1-28
Accessing the Secure Router OS	1-28
Configuring the Enable Mode Password	1-29
Configuring the Ethernet Interface	1-29
Configuring Telnet Access	1-30
Configuring SSH Access	1-30
Configuring HTTP Access	1-31

Using This Guide

The *ProCurve Secure Router Advanced Management and Configuration Guide* describes how to use the ProCurve Secure Router 7000dl series in a network environment. Specifically, it focuses on two models:

- ProCurve Secure Router 7102dl
- ProCurve Secure Router 7203dl

Both this guide and the *ProCurve Secure Router Basic Management and Configuration Guide* describe how to use the command line interface (CLI) and the Web browser interface to configure, manage, monitor, and troubleshoot router operation.

The *Advanced Management and Configuration Guide* describes how to:

- increase bandwidth for particular WAN connections
- configure a backup WAN connection
- secure your network
- implement quality of service (QoS)
- configure multicast protocols
- select and implement a dynamic routing protocol

Refer to the *Basic Management and Configuration Guide* if you need information about configuring:

- Ethernet interfaces and virtual LAN (VLAN) support
- E1- or T1-carrier lines
- serial interfaces for E1- or T1-carrier lines
- Data Link Layer protocols
- Asymmetric Digital Subscriber Line (ADSL) connections
- Integrated Services Digital Network (ISDN) connections
- E1 + G.703 or T1 + DSX-1 interfaces
- bridging
- basic routing
- Domain Name System (DNS) server and client functions
- Dynamic Host Configuration Protocol (DHCP) server and client functions

Understanding Command Syntax Statements

This guide uses the following conventions for command syntax and information:

Syntax: show access-lists [*<listname>*]

Syntax: [permit | deny] [any | host *<A.B.C.D>* | *<A.B.C.D>* *<wildcard bits>*]

- Angle brackets (< >) enclose a description of a command element, a part of the command in which you enter information specific to your particular router or WAN. For example, in the first command shown above, you replace **<listname>** with the name of a particular access control list (ACL) configured on your router.
- Vertical bars (|) separate alternative, mutually exclusive elements.
- Square brackets ([]) are used in two ways:
 - They enclose a set of options. When entering the command, you select one option from the set. For example, in the second command shown above, you would enter **any** or **host <A.B.C.D>** or **<A.B.C.D> <wildcard bits>**.
 - They indicate an optional element. You can include the optional element in the command, but it is not required.
- Angle brackets within square brackets ([< >]) indicate that you may optionally add the information specific to your router or WAN to the command. For example, in the first command above, you can either replace **<listname>** with the name of a specific ACL or omit the name to view all ACLs.
- Braces ({ }) indicate an embedded option.
- Bold typeface is used for simulations of actual keys. For example, the “Y” key appears as **y**.
- Italics indicate an element that you must replace with information that is specific to your router or WAN.

When examples of commands are included in this guide, the guide notes the context required for the command and displays the context as it appears in the CLI.

CLI Prompt Convention

When you first boot up your ProCurve Secure Router, the CLI prompt indicates the router model:

```
ProCurveSR7102dl>
```

```
ProCurveSR7203dl>
```

For simplicity, throughout this manual the CLI prompt is shown as:

```
ProCurve>
```

You can change the name displayed at the prompt of your router by changing the router's hostname. For more instructions on changing the router's hostname and other basic router functions, see the *Basic Management and Configuration Guide, Chapter 1: Overview*.

IP Address Convention

You must sometimes enter an IP address or addresses as part of a command. For example, you might need to assign an IP address to a logical interface on the ProCurve Secure Router, or you might need to enter an IP address to be filtered by an ACL.

When you enter IP addresses, you must use one of the following formats:

- IP address with subnet mask:
Syntax: ip address 192.168.1.1 255.255.255.0
- IP address with Classless Inter-Domain Routing (CIDR) notation (or prefix length):
Syntax: ip address 192.168.1.1 /24

Interface Numbering Convention

When configuring a WAN connection, you will need to specify the slot and port of the interface that is providing the connection. The syntax for specifying an interface is **<interface> <slot>/<port>**.

Replace **<interface>** with the name of the interface. For example, for E1 interfaces, you would use **e1**, and for ADSL interfaces you would use **adsl**. For ISDN interfaces, use **bri**.

Replace **<slot>** with the slot number in which the module is inserted. The slots on the router are numbered from left to right. The left narrow slot is slot 1, and the slot to the right is slot 2. If you have a ProCurve Secure Router 7203dl, the wide module is installed in slot 3, the right most slot on the front of the router.

Finally, replace **<port>** with the number of the port on the module. Like the slots, the ports are numbered from left to right. The port number is printed below each port on the module.

For example, if you have a two-port T1 module in slot one, you would configure the left T1 port by entering:

```
ProCurve(config)# interface t1 1/1
```

To configure the other T1 port, you would enter:

```
ProCurve(config)# interface t1 1/2
```

As mentioned earlier, the Ethernet interfaces are also labeled in *<slot>/<port>* notation as **eth 0/2** and **eth 0/1**.

Quick Start Sections

Each chapter includes a Quick Start section that provides the instructions you need to quickly configure your ProCurve Secure Router. Designed for experienced network administrators, the Quick Start sections provide minimal explanation.

The first time you perform a task, ProCurve Networking strongly recommends that you read the entire chapter so you thoroughly understand how to manage the ProCurve Secure Router. If you begin to use the Quick Start instructions and find that you need additional information about a specific aspect of managing the OS, check the “Contents” for that chapter to locate the section that contains the explanation you need.

The Quick Start section is located at the end of each chapter. For the specific page number, consult the “Contents” page located at the beginning of each chapter.

Obtaining Additional Information

You can view, print, and save product documentation that is available on the Internet. To access this documentation, follow these steps:

1. Access the ProCurve Networking Web site at **<http://www.procurve.com>**.
2. Click *Technical support* in the bar on the left side of the screen, and then click *Product manuals*. (See Figure 1-1.)
3. Click the name of the product for which you want documentation.
4. On the resulting Web page, double-click the document that you want.
5. When the document file opens, click the disk icon in the Acrobat® toolbar and save a copy of the file.

You will need the Adobe Acrobat Reader to view documentation that you have saved.

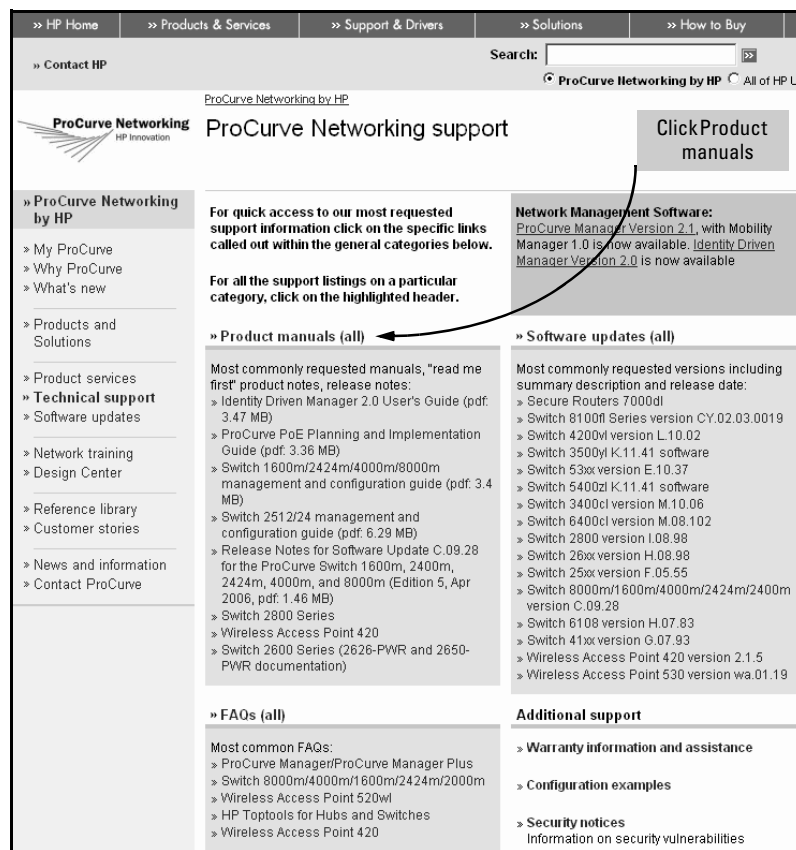


Figure 1-1. The ProCurve Technical Support Web Page

Downloading Software Updates

ProCurve Networking periodically updates the router software to include new features. You can download software updates and the corresponding release notes from ProCurve Networking's Web site as described below.

To download software, complete the following steps:

1. Access the ProCurve Networking Web site at <http://www.procurve.com>.
2. Click *Software updates* (in the sidebar). (See Figure 1-2.)
3. Under *Latest software*, click *Secure Router 7000dl Series*.

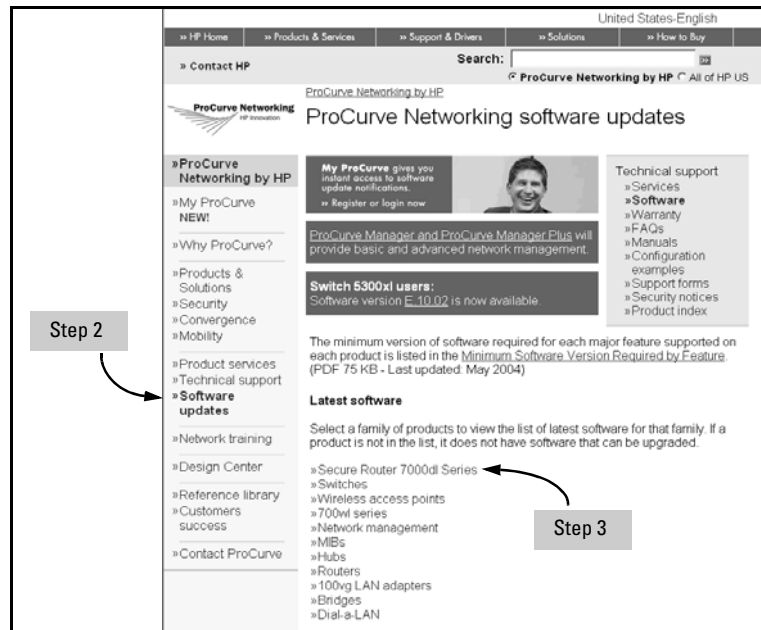


Figure 1-2. Downloading Software Updates

Release notes are included with the software updates and provide information about:

- new features and how to configure and use them
- software management, including downloading software to the router
- software fixes addressed in current and previous releases

For information on how to configure basic router functions, see the *Basic Management and Configuration Guide*.

Interface Management Options

The ProCurve Secure Router includes two management interfaces:

- the command line interface (CLI)
- the Web browser interface

The router also supports Simple Network Management Protocol (SNMP), which allows you to manage it through an SNMP management console. (For more information about SNMP support, see *Chapter 2: Controlling Management Access to the ProCurve Secure Router* in the *ProCurve Secure Router Basic Management and Configuration Guide*.)

CLI

To initially access the CLI, connect the COM port on your workstation to the console port on the front panel of the router. Use the serial cable (5184-1894) that was shipped with the ProCurve Secure Router. Then run terminal session software such as Tera Term or Hyper Terminal on your workstation, and set up the terminal session with the following parameters:

- Baud Rate = 9600
- Parity = None
- Data Bits = 8
- Stop Bits = 1
- Flow Control = None

This guide focuses primarily on configuring the router through the CLI.

Web Browser Interface

You can also manage the ProCurve Secure Router through the Web browser interface, which allows you to use a GUI to configure the router. Even if you are a dedicated CLI user, you should try this easy-to-use Web browser interface. You will find it especially helpful for more complicated tasks such as configuring access control policies (ACPs) and virtual private networks (VPNs). (See Figure 1-3.) In fact, the Web browser interface provides wizards to help you configure VPNs, the router's built-in firewall, and QoS for VoIP.

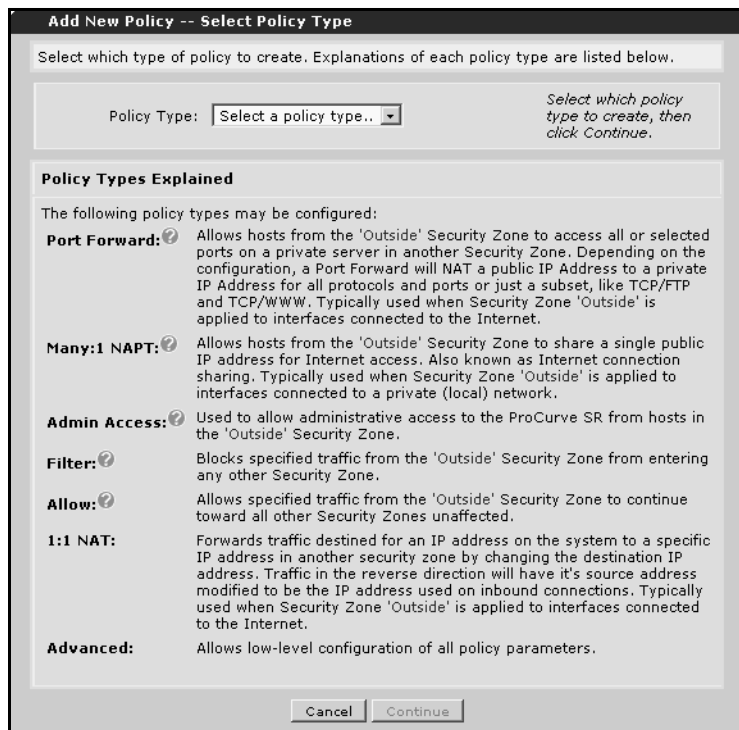


Figure 1-3. Configuring ACPs Using the Web Browser Interface

Accessing the Web Browser Interface

To access the Web browser interface, you must first establish a CLI session and configure at least one interface through which you can establish an HTTP session with the router. You must also enable the HTTP server or the HTTP over Secure Socket Layer (HTTPS) server and configure a password for HTTP access.

From the global configuration mode context, enter:

```
ProCurve(config)# ip http server
```

or

```
ProCurve(config)# ip https server
```

Configure a username and password for the HTTP server. This username and password also secure FTP and SSH access to the router. From the global configuration mode context, enter:

Syntax: `username <username> password <password>`

For more information on how to use the Web browser interface, see *Chapter 16: Using the Web Browser Interface for Advanced Configuration Tasks*.

Using the ProCurve Web Browser Interface

The ProCurve Web browser interface is organized into the following sections:

- *System*
- *Router/Bridge*
- *Network Monitor*
- *Firewall*
- *VPN*
- *Utilities*

The *System* section of the interface contains general router functions. In this section, you can:

- configure WAN and LAN connections
- configure IP services
- enable the Dynamic Host Configuration Protocol (DHCP) and Domain Name System (DNS) servers
- set the router's hostname and add entries to the DNS host table
- configure Link Layer Discovery Protocol (LLDP) settings

You can also click *Getting Started* to display a help menu, or select *System Summary* to display information about the router. Click *Physical Interfaces* for a list of interfaces (including status and type) on your router.

The *Router/Bridge* section allows you to configure the router's bridging and routing functions. You can set a default gateway, configure the IP interfaces, set up quality of service (QoS) maps and routing protocols, and add entries to the route table. You can also configure the router to act as a bridge and participate in a spanning tree.

In the *Network Monitor* section, you can configure the router to send probe packets and monitor connections to remote networks or servers. If a probe fails, a network monitoring track creates a log, removes a route (thereby allowing a backup route to take effect), or both. The Web browser interface

provides a Wizard to guide you through configuring network monitoring, or you can set up the feature manually by entering the necessary commands in the CLI.

The firewall wizard can be found in the *Firewall* section. Click *Firewall Wizard* to open the wizard in a new window. The wizard guides you through establishing policies for controlling access to your network. From the *Firewall* section, you can also enable specific application-level gateways (ALGs) and set protocol timeouts.

The *VPN* section includes a wizard that simplifies the process of configuring an IPSec-compliant VPN. The *VPN* section eliminates the difficulty of remembering the many commands necessary for configuring a VPN in the CLI. The *VPN* section only appears in the Web browser interface if you have installed an optional IPSec encryption module in the rear panel of your router.

You can perform most of your file maintenance in the *Utilities* section. Click *Configure* to complete tasks such as saving, downloading, uploading, and deleting files. You can also click *Firmware* to view information about your router's current OS and upload any necessary upgrades. You can click *Reboot* and restart the router, and you can also set up a Telnet session by clicking *Telnet to Unit*.

Note

In the CLI, boot and configuration files are referred to as software. In the Web browser interface, the boot and configuration files are called firmware.

For more information on how to configure basic router functioning on your ProCurve Secure Router using the Web browser interface, see the *Basic Management and Configuration Guide, Chapter 14: Using the Web Browser Interface for Basic Configuration Tasks*.

CLI Tools

This section gives a brief description of the CLI tools and commands that will help you to configure and troubleshoot your router. If you need more detailed information on the commands available in the CLI, it is highly recommended that you consult the *Basic Management and Configuration Guide*. The *Basic Management and Configuration Guide* lists and describes the router's **show** commands, file management commands, and interface configuration commands.

Help Tools

The Secure Router OS features help tools, editing functions, and global commands to help you navigate through the Secure Router OS and configure and maintain your WAN.

CLI Help Commands

You can enter the **?** character to help you enter commands in any mode context in the CLI. The **?** character displays information about the available commands and options available to those commands in your current router context. You will not need to press **Enter** to activate the **?** help tool; the character immediately triggers the display.

- **?**. Entering the **?** character displays a list of all the available commands in your current mode with a brief description of their functions.
- *letter?*. If you know the beginning of a command but need to be reminded of the entire word or if you want a more limited list of commands, enter a letter or set of letters followed immediately by the **?** command. *Do not put a space between the letters and the ?*. The router will then display only the specific commands that begin with those letters. For example,

```
ProCurve> e?
enable exception exit
```

- *command ?*. If you know the command but need to be reminded of the available options, type the command followed by a space and **?**. This will bring up a display of the available options for that command in the current mode and a brief description of each. For example,

```
ProCurve(config t1 1/1)#clock source ?
internal          -Use internal clock source
line              -Recover clock from line
```

Editing Commands

The router's CLI supports basic editing functions that can move the cursor through the command line and allow you to cycle through previous commands. Table 1-1 describes the ProCurve editing commands.

Table 1-1. Keystrokes for Moving Around the CLI

Editing Command	Action
Ctrl+p or up arrow	recall the most recent command
Ctrl+a	move to the beginning of the line
Ctrl+e	move to the end of the line
Ctrl+f or right arrow	move forward one character
Ctrl+b or left arrow	move backward one character
Tab	finish partially typed command

Command Recall. Recall the most recent command by entering **Ctrl+p** or pressing the **up arrow**. Pressing the **up arrow** again will cycle through the previous commands.

Moving within the Command Line. When typing a lengthy command, you may make an error and need to move the cursor within the command line. See Table 1-1 for a list of keystrokes that move the cursor within the command line.

Tab. The **Tab** key is a shortcut of sorts. Press **Tab** after typing the first few characters of a command. If you have typed enough characters to distinguish the command from all other available commands, the Secure Router OS will finish the word for you.

Truncation. The ProCurve Secure Router OS also recognizes truncated commands. You only need to enter enough characters in the CLI to distinguish the command you wish to execute. A good way to tell if you have typed enough characters is to press the **Tab** key. If, when you press **Tab**, the Secure Router OS is able to finish the command without having to list possible options, you have typed enough characters. For example, when entering the enable mode context, it is not necessary to type the whole word **enable**. At the basic mode context prompt there are three commands that begin with the letter “e” and only one command that begins with the letters “en.” To enter the enable mode context from basic mode you only need to enter **en** and press **Enter**. This can

be checked by pressing **Tab** after typing **en** at the basic mode context prompt. Because the Secure Router OS is able to finish the word **enable**, it completes the truncated command.

Basic Commands

This section gives some basic CLI commands that you will need to operate your router. Only basic commands are described here. For a more comprehensive list and description of router commands, see the *Basic Management and Configuration Guide, Chapter 1: Overview*; or the *SROS Command Line Interface Reference Guide*.

no

In the enable security mode context, typing the word **no** before a command turns off or resets a command option to its defaults. For example, if you want to stop events notices from displaying to the CLI screen, enter **no events**.

do

When in the configuration mode context, if you need to execute an enable mode command, type **do** before you enter the command. The **do** command allows you to stay in your current mode context while executing a command that is usually only available in the enable mode context. You will most often use this command with **show** commands. For example, to display the status of an interface while configuring a protocol interface, enter:

Syntax: do show interface <interface type> <slot>/<port>

```
ProCurve(config-ppp 1)# do show interface e1 1/1
```

exit

To leave a specific interface or configuration mode, type **exit**. The **exit** command moves you back one mode level. For example, if you were configuring an ATM interface in the ATM interface configuration mode context and entered **exit** when you were finished, you would return to the global configuration mode context.

When you enter the **exit** command in the global configuration mode context and return to the enable mode context, the CLI displays this message:

Appropriate commands must be issued to preserve configuration.

This message is a reminder to save the configuration you have completed. All configuration changes are initially saved only in the router's running-configuration file, which is stored in flash memory. If the router were powered down, the running config, and any changed that you have not saved, would be lost.

The next section describes the file management commands you need to save your configuration.

File Management Commands

This section describes the basic file management commands that allow you to save your configurations, copy files from the router to another medium, or erase files from your router's flash or compact flash memory.

The router has two configuration files that keep track of the router's settings: startup-config and running-config. The router uses the startup-config file as a map to setup the router's configuration during the boot process. This file contains saved configuration settings and is used to configure the router when it is powered on and boots.

As you make configuration changes, the router stores these configuration changes in the running-config file, which is stored in the routers RAM memory. Only the currently running and implemented configurations are stored in running-config. This file is lost when the router powers down. If you want to keep the configuration changes you have made to the router, you must save this file, as described in the following sections.

copy

This command has the following syntax:

Syntax: copy <source file location> <filename> <destination location> <destination filename>

This command is used to copy and save files in the router's internal flash and compact flash memories. Table 1-2 gives the available options for the **copy** command.

You can also use this command to save the changes you make in the running-config to the startup-config. If you do not save these changes, the next time the router reboots, any changes will be lost.

To save configuration changes while using the CLI, enter:

Syntax: copy running-config [<destination location> <destination filename> | <config-file>]

ProCurve# copy running-config startup-config

Table 1-2. Options for the copy Command

Source Location Options	Destination Location Options
cflash <filename> or flash <filename>	<ul style="list-style-type: none"> • boot • cflash [<filename>] • flash [<filename>] • interface (only from flash <filename>)
cflash or flash	<ul style="list-style-type: none"> • tftp • xmodem
console	<ul style="list-style-type: none"> • flash <filename>
running-config	<ul style="list-style-type: none"> • cflash <filename> • flash <filename> • startup-config • tftp • xmodem
startup-config	<ul style="list-style-type: none"> • cflash <filename> • flash <filename> • running-config • tftp • xmodem
tftp or xmodem	<ul style="list-style-type: none"> • flash • cflash • running-config • startup-config

Verify that the **Done. Success!** message is displayed, indicating that the copy process is complete.

To save a configuration as a file on compact flash, enter the following command from the enable mode context:

Syntax: copy flash <config-file> cflash <filename>

Replace <config-file> with either **running-config** or **startup-config** and replace <filename> with a name that you choose.

Verify that the **Percent Complete 100%** message is displayed, indicating that the download is complete. The current configuration is now saved in compact flash with the specified filename.

To save a configuration as a file on internal flash, enter the following command from the enable mode context:

```
ProCurve# copy <source file location> <source config-file> flash [<filename>]
```

Replace **<source file location>** with the location of the configuration file you are saving. Replace **<source config-file>** with **startup-config** or **running-config**. You must enter a destination filename unless the filename will be the same as that of the source. For example, if you need to save the startup-config file from the compact flash card to internal flash, enter:

```
ProCurve# copy cflash startup-config flash startup-config
```

Saving the Current or Start-up Configuration to a TFTP Server. To initiate an upload of a configuration file to an external TFTP server, enter one of the following commands from the enable mode context:

```
ProCurve# copy [flash | cflash] tftp  
ProCurve# copy [startup-config | running-config] tftp
```

For example, if you wanted to upload the startup-config on compact flash to your TFTP server, you would enter:

```
ProCurve# copy cflash tftp
```

When prompted for the **Address of remote host?**, enter the IP address of the TFTP server.

When prompted for the **Source filename?**, enter the name of the configuration file (**startup-config** or **running-config**) you would like to upload.

When you are prompted for the **Destination filename?**, enter the filename you'd like the uploaded configuration file to be named.

The **copy** command can be used for other file TFTP management tasks such as:

- loading a running-configuration file from the TFTP server—Enter **copy tftp running-config**.
- loading a startup-configuration from the TFTP server—Enter **copy tftp startup-config**.

erase

The **erase** command removes files from the specified file location.

Syntax: `erase <file location> <filename>`

For example, entering **erase flash <filename>** will delete the file you specify from internal flash:

```
ProCurve# erase flash oldconfig
```

This command also allows you to erase files from compact flash:

```
ProCurve# erase cflash config1.cfg
```

write

This command is similar to the **copy** and **erase** commands.

Entering **write memory** will save the running-configuration to the startup-configuration. In J03_01.biz and later, this file will automatically save to the compact flash card, if present. Otherwise the startup-config file will be saved on the router's internal flash.

Entering **write erase** deletes the startup-config file. If you have a compact flash card, the startup-config is erased from cflash. If you are running the AutoSynch™ function, this command erases startup-config from both flash and compact flash. If you do not have a compact flash card, the file is erased from flash.

The **write network** command saves the running config to a TFTP server. You can set the filename to something meaningful to you when you are prompted with **Destination filename?**.

The **write terminal** command is similar to the **show running-config** command; it displays the current running-configuration in the CLI.

autosynch

The **autosynch** command is used with a compact flash card. Enabling the AutoSynch™ function allows the router to automatically keep the startup-config and Secure Router OS files in internal flash synchronized with the startup-config and Secure Router OS files on the compact flash card.

The **autosynch** command is disabled in its default setting. To enable the AutoSynch™ technology, enter the global configuration mode and enter:

```
ProCurve (config)# autosynch-mode
```

```
AutoSynch: SROS.BIZ synched  
AutoSynch: startup-config synched
```

To disable AutoSynch™, use the **no** command:

```
ProCurve(config)# no autosynch-mode
```

```
AutoSynch: SROS.BIZ not synched  
AutoSynch: startup-config not synched
```

For more information on file management and router boot functioning, please see the *Basic Management and Configuration Guide, Chapter 1: Overview*.

Troubleshooting Commands

The following commands are some basic commands to help with troubleshooting router operation.

reload in

When you are configuring the ProCurve Secure Router through a Telnet, SSH, or Web session, you may want to enter a safeguard to ensure that you do not inadvertently block your access to the router. You can configure the ProCurve Secure Router to reload the startup-config at a specified future time, returning the router to its previous configurations.

To schedule a system reboot, enter the following command from the enable mode context:

```
ProCurve# reload in <mmm>
```

or

```
ProCurve# reload in <hhh:mm>
```

Replace **<mmm>** with the number of minutes. You can specify a three-digit number. Replace **<hhh:mm>** with a time such as 1:15 (1 hour and 15 minutes).

The CLI will prompt you to save the system configuration. If you have already made the configurations that you want to test, reply no. If you are getting ready to make the configurations to be tested and want to save previous configurations, reply yes. The CLI then displays:

```
You are about to reboot the system. Continue? [y/n]
```

Enter **y**. The system will not reboot immediately. It will wait the amount of time you have specified. Remember that you must not save the running-config to the startup-config (by entering either **write mem** or **copy run start**) while you are configuring the router. Otherwise, the ProCurve Secure Router will load these configurations when it reboots.

To cancel the reload, enter:

```
ProCurve# reload cancel
```

show

The **show** commands are only available in the enable mode context or by using the **do** command. These commands allow you to check the router's configured settings by displaying router functionality information in the CLI. This allows you to find miskeyed commands or problem configurations and repair them. Individual **show** commands are described throughout this book and the *Basic Management and Configuration Guide*. For a more detailed list and explanation of the available **show** commands, see the *Basic Management and Configuration Guide, Chapter 1: Overview*.

show tech

Unlike the other **show** commands, the **show tech** command does not display the information in the CLI. This command creates a file named showtech.txt in internal flash that contains a summary of the router's **show** command information.

To create this file enter **show tech** at the enable mode context prompt. This will prepare a showtech.txt file and save it in the router's internal flash.

After the showtech.txt file is created, you can save it to compact flash or upload it to a TFTP server. You can also save the contents of the showtech.txt file to your terminal's text editor. See "Managing Configuration Files Using a Text Editor" on page 1-25 for more information on how to manage files with a text editor.

Note

The showtech.txt file is saved to internal flash. If you intend to use a compact flash card to transport the file, you must save the showtech.txt file to a compact flash card.

The showtech.txt file contains a readout of many of the **show** commands. This readout allows a network administrator to pinpoint a router configuration problem without a connection to the router. To display the contents of the showtech.txt file, enter **show file flash showtech.txt** from the enable mode context.

To have the router display the show tech readout without creating or saving a showtech.txt file, use the **terminal** option:

Syntax: show tech terminal

ProCurve# show tech terminal

safe-mode

SafeMode is a CLI feature that allows you to perform configuration changes without the fear of being disconnected from a Telnet or SSH session. Some configuration changes can interrupt network connectivity. If you are managing a router remotely via SSH or Telnet, you can inadvertently lose your connection to the router.

For example, you may need to apply an ACL, but this ACL doesn't allow Telnet or SSH traffic. Once you applied the ACL, you would be locked out of the router. In order to fix the configuration that has locked you out, you would need physical access to the router so that you could establish a console session with it. SafeMode allows you to make configuration changes using Telnet or SSH without worrying about losing your connection and being unable to reestablish it.

SafeMode requires you to periodically reset a reload timer. If the reload timer runs out before you reset it, the Secure Router OS will assume that the current running configuration has disrupted your connection to the router. It will save the running-config to internal flash as "problem-config" and reboot the router. Once the router has reloaded, it will display a reboot cause message and load the currently saved startup-configuration file. The startup-config should allow you to regain access to the router. You will then be able to review the saved problem-config file and correct the setting that caused the disruption.

After you enable SafeMode and set the time limit, a reload timer is activated for the Telnet and SSH access lines and begins to count down. You also set a threshold timer, which is shorter than the reload timer. When the threshold timer expires, a warning message is displayed in the CLI that allows you to reset the timer. Unless you enter the reset keystroke before the reload timer finishes counting down, the router reboots. This prevents you from being locked out of the router if you lose the connection and are unable to reset the timer.

While SafeMode is enabled, it temporarily suspends the AutoSynch™ function. This prevents a disruptive configuration from being saved to both flash and compact flash. After the SafeMode configuration is complete and you have disabled the SafeMode counter, the **autosynch** command, if previously enabled, will automatically reenable and begin synchronization.

Enabling SafeMode. To enable SafeMode, access the global configuration mode context and enter:

Syntax: safe-mode [*<reload time>* *<threshold time>*]

For example:

```
ProCurve(config)# safe-mode 600 500
ProCurve(safe-config)#
```

Set the **<reload time>** to the number of seconds to countdown until the router reboots. Set the **<threshold time>** to the number of seconds to countdown until you receive a reminder to reset the timer. Both the reload time and threshold time must be between 30 and 3600 seconds. The default value for the reload time is 300 seconds, and the default value for the threshold time is 60 seconds. To enable SafeMode with the default settings, enter **safe-mode** at the global configuration prompt.

The reload time should be greater than the threshold time. If you enter a threshold value greater than the reload value, the CLI displays an error message.

When you are configuring in SafeMode from a Telnet or SSH session, the configuration mode context prompt is displayed as **safe-config**. For example:

```
ProCurve(safe-config)# interface ethernet 0/1
ProCurve(safe-config-eth 0/1)#
```

All configurations that you make during SafeMode are saved in RAM as part of the running-config.

After the countdown for the reload timer has begun, it continues until you either reset it by pressing **Ctrl+R**, you disable it by entering **no safe-mode**, or you exit out of the global configuration mode context.

Use the **no** form of the command to disable SafeMode and the countdown timer:

```
ProCurve(safe-config)# no safe-mode  
ProCurve(config)#
```

SafeMode Functioning. SafeMode events are displayed in the CLI. When the threshold timer reaches zero, a notice is displayed in the CLI reminding you to reset the timer:

```
SAFEMODE: SafeMode will reboot in <threshold> seconds.
```

When you activate SafeMode, or when you leave and re-enter the configuration mode context while SafeMode is enabled, the reload timer is activated and a message is displayed in the CLI:

```
SAFEMODE: SafeMode enabled. Reboot in <n> seconds!
```

Once SafeMode is enabled, any CLI user can reset the timer by entering **Ctrl+R**. You can reset the timer at any time, as often as you need to complete the configuration.

Caution

If you save your configuration to the startup-config while in SafeMode, you may essentially negate SafeMode's effect: the router may reboot with the saved disruptive configuration and you will still be locked out of the router. Be very careful about saving your in-process configurations when in SafeMode.

The problem-config file that is generated when the router reboots can be examined and edited in a text editor to repair the commands that caused the problems.

Note

The problem-config file is saved in the router's internal flash memory. If you want to transport the file or save a backup of the file using compact flash, you need to copy the file to compact flash by entering **copy flash problem-config cflash problem-config** from the enable mode context.

Managing Configuration Files Using a Text Editor

Configuration files can be adjusted to each router's needs using your computer's text editor. This allows you to set up a configuration on one router, save it to a file, and edit it for installation on another router.

Begin creating a configuration file by creating a base configuration on an originating router. Save the base configuration and import it—using a compact flash card, the router's console, or a TFTP server—to a terminal with a text editor. The readout of the configuration file will resemble the readout of the running-config for the router (displayed by entering **show run** at the enable mode context prompt). Once you have pasted this text into the text editor, you can adjust the IP address, hostname, ACLs and ACPs, and other configuration concerns to prepare the file for the target router. These adjustments are made by simply typing in the desired command or value using the format displayed in the file readout. Then move the file to the target router and save it as the startup-config. Reboot the router using the **reload** command and the router will boot with the new configuration.

Using Error Messages to Repair a Configuration

The ProCurve Secure router configuration files are robust. If you miskey a command or make a mistake in the text editor, the router will simply ignore the mistake and use the default settings. If any necessary command is missing, the router will simply substitute the default. Problem commands will trigger an error message during bootup.

If you do have a problem command that is running on its default setting, it is not necessary to re-edit the configuration in a text editor. To repair the problem, simply enter the pertinent command in the CLI. Use the error messages displayed during bootup to determine which command is faulty.

```
Persistence viewer: Restoring from CFLASH:/startup-config...
100%***** There were 99 errors. *****

Persistence viewer: ... done.
Copyright (c) 2004-2005, Hewlett-Packard, Co.
Platform: ProCurve Secure Router 7203dl
***** Error in line 42 of CFLASH:/startup-config *****
ProCurveSR7102dl(config-dhcp)#ip crypto
% Unrecognized command

***** Error in line 44 of CFLASH:/startup-config *****
ProCurveSR7102dl(config-dhcp)#crypto ike policy 100
% Unrecognized command

***** Error in line 45 of CFLASH:/startup-config *****
ProCurveSR7102dl(config-dhcp)# initiate main
% Unrecognized command

***** Error in line 46 of CFLASH:/startup-config *****
ProCurveSR7102dl(config-dhcp)# respond anymode
% Unrecognized command

***** Error in line 47 of CFLASH:/startup-config *****
ProCurveSR7102dl(config-dhcp)# local-id fqdn "Site A"
% Unrecognized command

***** Error in line 48 of CFLASH:/startup-config *****
ProCurveSR7102dl(config-dhcp)# peer 10.2.2.1
% Unrecognized command

***** Error in line 49 of CFLASH:/startup-config *****
ProCurveSR7102dl(config-dhcp)# attribute 1
% Unrecognized command
```

Figure 1-4. Boot Error Messages

The error messages in Figure 1-4 were displayed during bootup. In this particular case, the startup-config file has several VPNs configured, and the router that is booting does not have an IPSec VPN module to support it. The commands for the configuration of the VPNs are reported as errors.

Use error messages like these to locate and troubleshoot the problem in the router's configuration.

```
Persistence viewer: Restoring from NONVOL:/routing.cfg...
100%***** There was 1 error. *****
                                     Error location
Persistence viewer: ... done.
Copyright (c) 2004-2005, Hewlett-Packard, Co.
Platform: ProCurve Secure Router 7102d1
***** Error in line 58 of NONVOL:/routing.cfg
ProCurveSR7102d1(config-ike)# peer 10.2.2.1
%IP address 10.2.2.1 is assigned to IKE policy 100
                                     Resulting message
```

Figure 1-5. Using Boot Error Messages to Target a Configuration Problem

The line number given in the error message is the line number in the running-config. You can use this information to repair any configuration problems.

You will need to scroll up in your terminal session software window to read the error message. Make a note of the reported line number, the command, and the resulting error message, as shown in Figure 1-5. Then return to the command line and enter the enable mode context.

Enter **show running-config** to display the current configuration. When the running-config is displayed, begin with the first exclamation point and count down, line by line, until you reach the line that generated the error message. Check the resulting message from the error report. Repair the problem by re-entering the command on that line using the error report as a guide.

For example, in Figure 1-5, there is an error in line 58. The faulty command was

```
ProCurve(config-ike)# peer 10.2.2.1
```

The peer at 10.2.2.1 was already assigned to IKE policy 100 and cannot be assigned to more than one policy. In this example, the IKE policy configurations may need to be adjusted.

Quick Start

This section provides the instructions you need to quickly access the ProCurve Secure Router CLI and configure an enable mode password to protect the router from unauthorized access. This section also explains how to configure the Ethernet interface and the HTTP server so that you can access the Web browser interface. You will then be able to manage the ProCurve Secure Router through an Internet browser.

Only minimal explanation is provided. It is strongly recommended that you read the entire chapter so that you understand how the Secure Router operating system (OS) is organized and how to manage the OS. If you need information about a specific aspect of managing the OS, see the *Basic Management and Configuration Guide* to locate the section that contains the explanation you need.

Accessing the Secure Router OS

1. Use the serial cable (5184-1894) that shipped with the ProCurve Secure Router to connect the COM port on your laptop to the console port on the front panel of the router.
2. Open a terminal session with the ProCurve Secure Router, using the following settings:
 - Baud Rate = 9600
 - Parity = None
 - Data Bits = 8
 - Stop Bits = 1
 - Flow Control = None
3. Press **Enter** to access the basic mode context.
4. Access the enable mode context:
ProCurve> enable
5. Access the global configuration mode:
ProCurve# configure terminal

Configuring the Enable Mode Password

6. Configure an enable mode password.

Syntax: enable password [md5] <password>

Enter the **md5** option to encrypt the password. Replace <password> with an alphanumeric string of up to 16 characters.

For example, you might enter:

```
ProCurve(config)# enable password md5 ProCurve
```

Note

The word **ProCurve** is shown as the password only for simplicity. In a production environment, you should follow the standard guidelines for creating a password that cannot be easily guessed by unauthorized users. In addition, you should avoid writing the password down and posting it where others can read it.

Configuring the Ethernet Interface

1. Use a 10Base-T or 100Base-T cable to connect the Ethernet port on the ProCurve Secure Router to the appropriate device on your LAN. In most cases, you will connect the router to a core switch.
2. Access the configuration mode context for the Ethernet interface.

Syntax: interface ethernet 0/<port>

For example, if you want to configure the bottom Ethernet port, enter:

```
ProCurve(config)# interface ethernet 0/1
```

3. Assign the Ethernet interface an IP address.

Syntax: ip address <A.B.C.D> <subnet mask | /prefix length>

For example, if you want to assign the Ethernet interface an IP address of 192.168.115.1 /24, enter

```
ProCurve(config-eth 0/1)# ip address 192.168.115.1 /24
```

4. Activate the Ethernet interface.

```
ProCurve(config-eth 0/1)# no shutdown
```

A message should be displayed at the CLI, reporting that the interface is “administratively up.” In a few moments, another message should be displayed reporting that the interface is up. (If this message does not appear, you can find troubleshooting information in the *Basic Management and Configuration Guide, Chapter 3: Configuring Ethernet Interfaces.*)

Configuring Telnet Access

After you configure an Ethernet interface and establish a connection to the ProCurve Secure Router, you can configure Telnet access to the router. Complete the following steps:

1. Establish a console session to the ProCurve Secure Router and move to the global configuration mode context.

```
ProCurve# configure terminal
```

2. Enter the following command to access the Telnet line configuration mode context:

Syntax: line telnet [0-4]

The ProCurve Secure Router supports five lines. Enter the number of the line you want to configure. If you want to enable all five lines, enter:

```
ProCurve(configure)# line telnet 0 4
```

3. Create the Telnet password

Syntax: password [md5] <password>

Enter the **md5** option to encrypt the password. Replace <password> with an alphanumeric string of up to 16 characters.

For example, you might enter:

```
ProCurve(config-telnet0)# password md5 en$ter^tel
```

4. Exit to the global configuration mode context.

```
ProCurve(config-telnet0)# exit
```

5. Configure an enable mode password, if you have not done so already. The enable mode password is required for Telnet access.

Syntax: enable password [md5] <password>

Enter the **md5** option to encrypt the password. Replace <password> with an alphanumeric string of up to 30 characters.

Configuring SSH Access

After you configure an Ethernet interface and establish a connection to the ProCurve Secure Router, you can establish SSH access to the router. By default, SSH access to the ProCurve Secure Router is enabled. After you have set an enable mode password, you simply need to configure a username and password.

Complete the following steps:

1. Establish a console session to the ProCurve Secure Router and move to the global configuration mode context.

```
ProCurve> enable  
ProCurve# configure terminal
```

2. If you have not already done so, configure an enable mode password.
Enter:

Syntax: enable password <password>

3. Configure a username and password for SSH access. The username and password you enter can be used for FTP and HTTP access as well.

Syntax: username <username> password <password>

Replace <username> and <password> with an alphanumeric string of up to 30 characters.

Configuring HTTP Access

1. Enter the global configuration mode context.
2. Enable the HTTP or HTTPS server on the router.

```
ProCurve(config)# ip http server
```

or

```
ProCurve(config)# ip https server
```

3. If you have not already done so, configure a username and password for the HTTP server. The username and password also secure FTP and SSH access to the router.

Syntax: username <username> password <password>

4. Return to the enable mode context and save your configuration.

```
ProCurve(config)# exit
```

```
ProCurve# write memory
```

