# 1

# Overview

## Contents

# Using This Guide

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

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

This guide describes how to use the command line interface (CLI) and the Web browser interface to configure, manage, monitor, and troubleshoot basic router operation. In particular, this guide focuses on configuring the router's physical interfaces and basic Data Link Layer protocols to establish LAN and WAN connections.

This guide assumes that your router uses the J06_03 Secure Router operating system (OS) or above.

If you need information on how to configure advanced router functions such as virtual private networks (VPNs), multilink connections, backup connections, network address translation (NAT), quality of service (QoS), multicasting, or routing protocols, see the *ProCurve Secure Router Advanced Management and Configuration Guide*.

## 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

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. See "hostname Command" on page 1-61 for instructions.

### IP Address Notation 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

## Quick Start Sections

Each chapter includes a Quick Start section that provides the instructions you need to quickly configure the functions described in that chapter on 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 that you 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 the configuration, 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" pages 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 the documentation that you have saved.

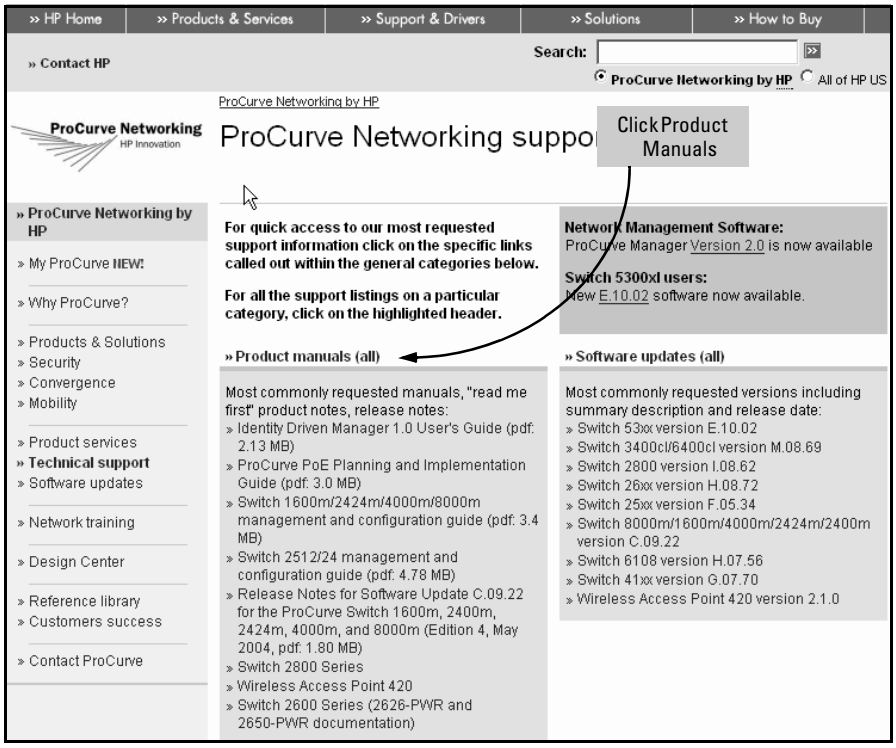


**Figure 1-1. The ProCurve Technical Support Web Page**

## 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*.

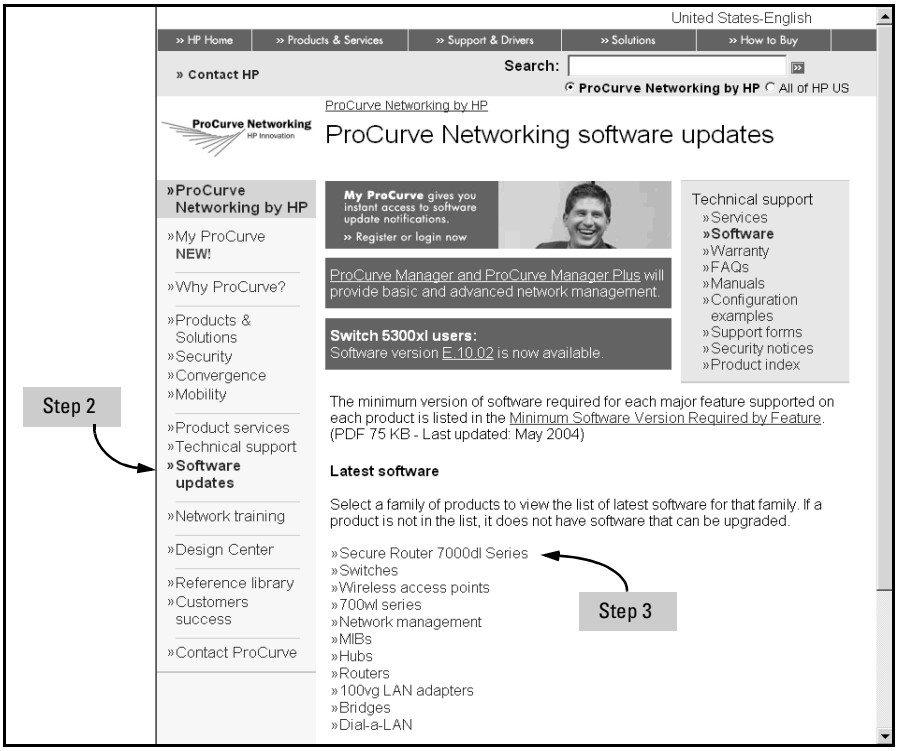


**Figure 1-2. Downloading Software Updates**

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 the new software to the router
- software fixes addressed in current and previous releases

# 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.)*

## 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 HyperTerminal on your workstation, setting the following parameters for the session:

- 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 navigate the router's OS in a GUI environment. 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 VPNs. (See Figure 1-3.) In fact, the Web browser interface provides wizards to help you configure VPNs, the router's built-in firewall, or QoS for VoIP.

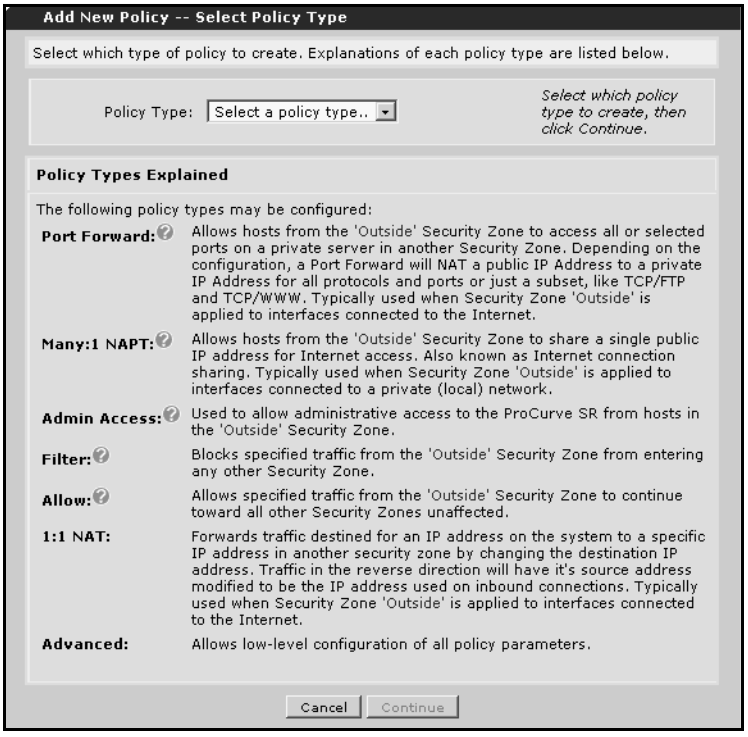


**Figure 1-3. Configuring ACPs Using the Web Browser Interface**

## 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 on the router and configure a password for HTTP access. (For information about enabling access to the Web browser interface, see “Enabling Access to the Web Browser Interface” on page 14-5.)

## 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 (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 the feature up 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 your ProCurve Secure Router using the Web browser interface, see *Chapter 14: Using the Web Browser Interface for Basic Configuration Tasks*.

# Hardware Overview

This section provides a brief overview of external features, slots, and modules on the ProCurve Secure Router 7000dl Series. The ProCurve Secure Router 7000dl Series includes two models: the ProCurve Secure Router 7102dl and the ProCurve Secure Router 7203dl. Both models include two narrow module slots. The ProCurve Secure Router 7203dl also includes one wide module slot.

## ProCurve Secure Router Front Panel

To make accessing the router and connecting it to other devices more convenient, the console interface and all physical link ports are located on the front panel of the router. The front panel of each router includes two Ethernet interfaces and two narrow dl option module slots that can house your two choices from among ten narrow modules. The ProCurve Secure Router 7203dl also provides a wide module slot to support up to eight additional T1 or E1 lines.

The following sections briefly introduce the features on the front of your ProCurve Secure Router.

## Console Port

The console port, which is a DB-9 DTE male connector, allows you to manage the ProCurve Secure Router locally. To access the CLI, use the serial cable (5184-1894) supplied with the router to connect the console port to the COM port on your laptop or PC. (See Figure 1-4.)

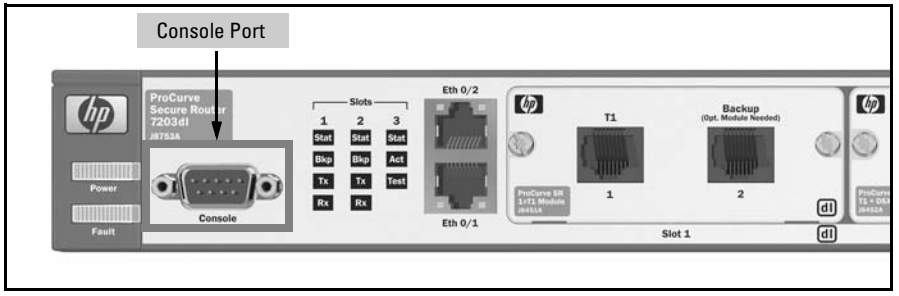


**Figure 1-4. Connecting to the Console Port**

## Ethernet Ports

Because the two Ethernet ports are not modular, they are assigned a fixed slot and port number. For interface notation purposes, these ports are labeled Eth 0/1 and Eth 0/2. (See Figure 1-5.)

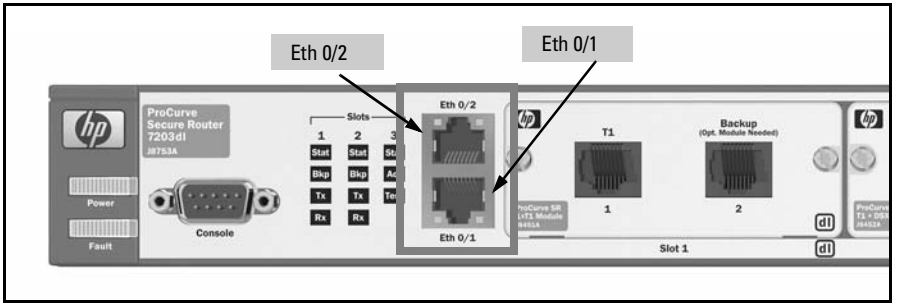


**Figure 1-5. Connecting to the Two Ethernet Ports**

The Ethernet ports support a 10 Mbps or a 100 Mbps connection. Connect these ports to your LAN using 10Base-T or 100Base-T cabling with an RJ-45 connector that meets the EIA/TIA-568-A and 568-B standards. For a 10 Mbps connection, use a Category 3 cable or better. For a 100 Mbps connection, use a Category 5 cable or better.

## Slots

The ProCurve Secure Router models 7102dl and 7203dl are both equipped with two narrow slots. (See Figure 1-6.)

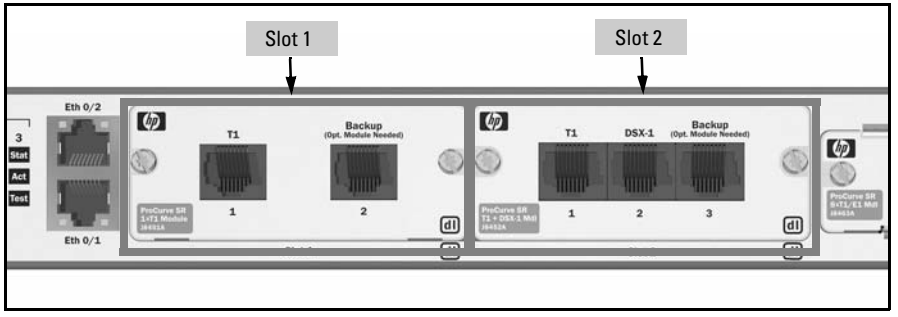


**Figure 1-6. Two Narrow Slots**

Each slot can house one of the ten narrow modules available for WAN connections. (See Table 1-1.)

**Table 1-1. Narrow Slot Modules**

| Module | Type of Module | Explanation |
|---|---|---|
| E1 modules:<br>• one-port module<br>• two-port module | E1 module with integrated DSU | supports E1-carrier lines when the service provider does not provide an external DSU |
| T1 modules:<br>• one-port module<br>• two-port module | T1 module with integrated CSU/DSU | supports T1-carrier lines when the service provider does not provide an external CSU/DSU |
| E1 + G.703 module | E1 for data and analog voice | allocates some channels of the E1-carrier line for data transmission and some channels for voice (through a PBX) |
| T1 + DSX-1 module | T1 for data and analog voice | allocates some channels of the T1-carrier line for data transmission and some channels for voice (through a PBX) |
| serial module | T1- or E1-carrier line that connects to an external CSU/DSU using a serial connector | supports E1- or T1-carrier lines when the service provider provides an external CSU/DSU |
| ADSL2+ Annex A module | ADSL2+ for most regions of North America | provides up to 25 Mbps downstream and 1.544 Mbps upstream; enables analog voice traffic to be transmitted at lower frequencies on the local loop |
| ADSL2+ Annex B module | ADSL2+ for Germany and other areas of the world | provides up to 25 Mbps downstream and 1.544 Mbps upstream; enables Integrated Services Digital Network (ISDN) voice and fax traffic to be transmitted at lower frequencies on the local loop |
| ISDN module (two ports) | ISDN BRI for voice and data | provides cost-efficient, dial-up WAN access |

**Note**

For information on these or additional modules, please check the ProCurve Web site at **www.procurve.com**. Click on *Products & Solutions* in the left bar, then click on *Secure Router 7000dl series* under *WAN*.

## E1 and T1 Modules

E-carrier lines are used in Europe, Asia, Australia, and South America. T-carrier lines are used in the United States, Canada, and, to some degree, in Japan.

**Note**

Japan uses J-carrier lines for voice and both T-carrier and E-carrier lines for data. J-carrier lines are not supported by the ProCurve Secure Router.

The type of module you purchase to support your E1 or T1 WAN connection depends on how your public carrier implements the Channel Service Unit/ Digital Service Unit (CSU/DSU) that is required for E1- and T1-carrier lines. The CSU/DSU has two main functions. The DSU accepts traffic from the router and translates it from the signaling format used on the LAN to the format necessary for transmission on the WAN. The CSU then generates the signal to be sent across the WAN.

The public carrier can provide:

- the CSU/DSU as one complete unit
- only the CSU
- neither the CSU nor the DSU

Common practice varies depending on the region in which the public carrier operates. In Europe, Asia, Australia, or South America, the public carrier will either provide the CSU/DSU or just the CSU. In North America, the public carrier will provide the CSU/DSU, or the public carrier will not provide either the CSU or DSU. (For more information about E1- and T1-carrier lines, see *Chapter 4: Configuring E1 and T1 Interfaces*.)

**E1 Modules.** If you are leasing an E1-carrier line and the public carrier provides only the CSU, you will need to purchase one of the E1 modules, which include a built-in DSU. (See Figure 1-7.) You can select:

- a one-port E1 module, which supports a full E1-carrier line (32 channels or 2.048 Mbps)
- a two-port E1 module, which provides 2.048 Mbps on each interface (4.096 Mbps total)
- an E1 + G.703 module, which enables you to use some channels for data and some channels for voice

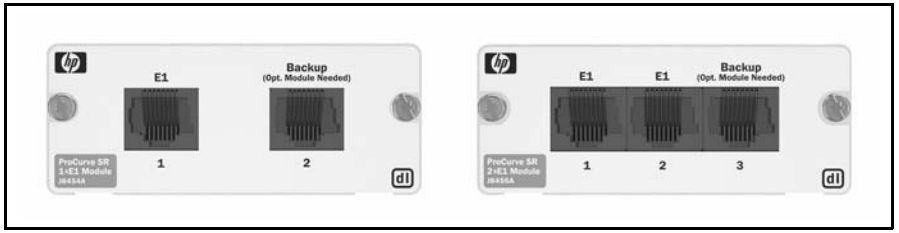


**Figure 1-7. E1 Modules**

**T1 Modules.** If you are leasing a T1-carrier line and the public carrier does not provide a CSU/DSU, you will need to purchase one of the three narrow slot T1 modules, which include a built-in CSU/DSU. (See Figure 1-8.) Select:

- a one-port T1 module, which supports a full T1-carrier line (24 channels or 1.544 Mbps)
- a two-port T1 module, which provides 1.544 Mbps on each interface (3.088 Mbps total)
- a T1 + DSX-1 module, which enables you to use some channels for data and some channels for voice


**Figure 1-8. T1 Modules**

**Serial Module.** If you lease an E1- or T1-carrier line and the public carrier provides an external CSU/DSU, you will need to purchase the serial module. (See Figure 1-9.)

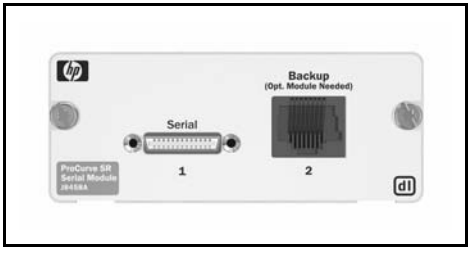


**Figure 1-9. Serial Module**

**ADSL2+ Annex A or Annex B Module.** The ADSL2+ modules provide bandwidth up to 25 Mbps downstream and 1.544 Mbps upstream. Because ADSL also supports analog voice on the local loop, existing telephone equipment and fax machines can continue to carry traffic on the same line. The ADSL2+ Annex A module supports analog voice over the Plain Old Telephone Service (POTS). The ADSL2+ Annex B module supports ISDN voice and fax traffic. (See Figure 1-10.)

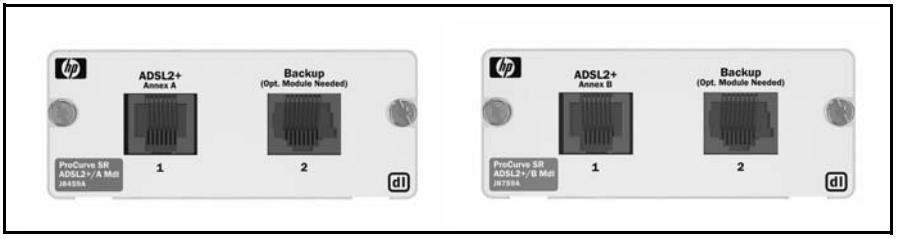


**Figure 1-10. ADSL Modules**

## ISDN Module

The two-port ISDN module provides two Basic Rate Interface (BRI) lines for dial-up connections. Each ISDN BRI line can deliver a maximum bandwidth of 128 Kbps. (See Figure 1-11.) The S/T interface module is most often used outside North America. The U interface module is used in WAN connections in the United States and Canada.

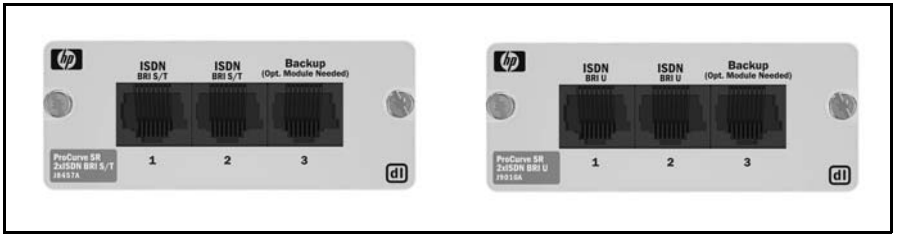


**Figure 1-11. ISDN BRI Modules**

## Backup Modules

A backup connection protects a company's WAN operations against system failure. Three types of backup modules are available for the ProCurve Secure Router:

- ISDN BRI S/T backup module for use outside of North America—supports a 64 Kbps backup call or a bonded 128 Kbps call
- ISDN BRI U backup module for use in the US and Canada—supports a 64 Kbps backup call or a bonded 128 Kbps call
- VTU V.90 compliant analog modem—provides a connection speed of up to 56 Kbps

**Note**

Backup ISDN call bonding is currently a ProCurve proprietary technology. If you bond your BRI backup call, your router can only place the call to another ProCurve Secure Router.

With the ProCurve Secure Router, it is not necessary to devote an entire module slot for a backup connection. Each module includes a backup interface port. To activate the backup interface, you must purchase a separate backup module and install it on top of the module, as shown in Figure 1-12.

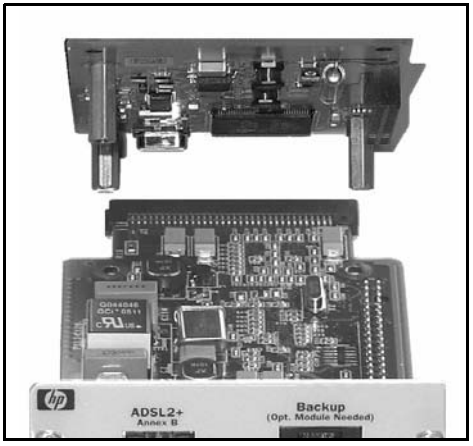


**Figure 1-12. Installing a Backup Module on Top of a Narrow Slot Module**

Each backup module can be used to back up any WAN connection on the router, no matter where the backup module is housed.

## Wide-Slot Option Modules

The ProCurve Secure Router 7203dl includes a third, wide-module slot. ProCurve offers an eight-port E1/T1 module and an eight-port serial module. (See Figure 1-14 and Figure 1-15.) The E1/T1 module supports both E1 and T1 formats and can be toggled between the two. The toggle switch is located on the top of the module. Set the switch to **ON** for E1 format; set the switch to **1** for T1 format. Figure 1-13 shows the location of the toggle switch on the module.

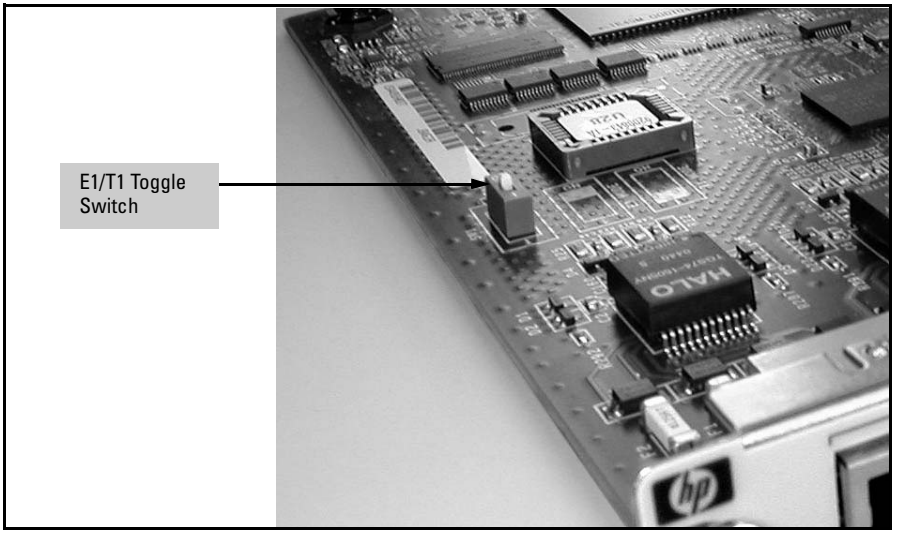


**Figure 1-13. E1/T1 Toggle Switch**

**Note**

Although the ProCurve Secure Router 7203dl can support up to 12 E1 or T1 lines, the router supports full throughput for up to 8 E1 or T1 lines.

You can configure each of the eight ports independently with separate clock sources, frame formats, and other specifications.

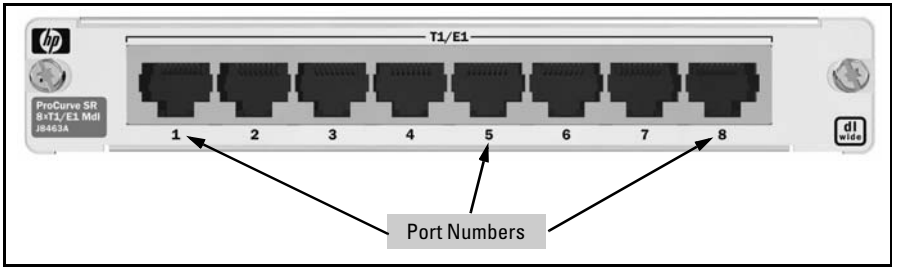


**Figure 1-14. The Eight-port T1/E1 Module**

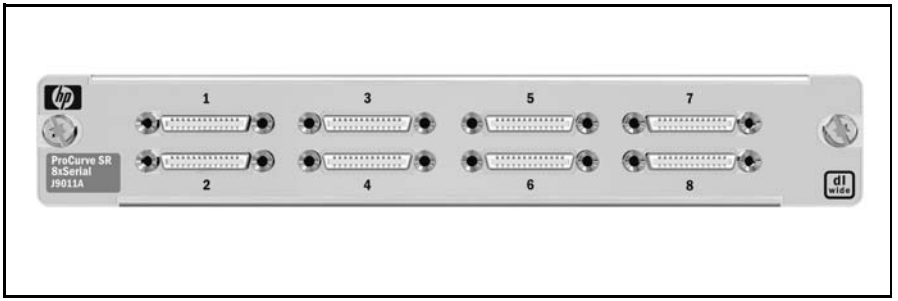


**Figure 1-15. The Eight-port T1/E1 Serial Module**

## Interface Numbering Conventions

When configuring a WAN connection, you will need to specify the slot and port of the physical interface that is providing the connection. The syntax for specifying a physical 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, you would 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 rightmost slot.

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. (See Figure 1-14.)

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 0/1** and **eth 0/2**.

# Status LEDs

ProCurve Secure Routers feature LEDs on the front panel to provide information about the condition of the router itself and of the modules you have installed. This section describes how to interpret these LEDs.

## Power LED

The power LED indicates the router's power status. (See Figure 1-16 for its location on the front panel.) It displays one of the following:

- **No light**—The AC power input is off.
- **Solid green**—The power is on.

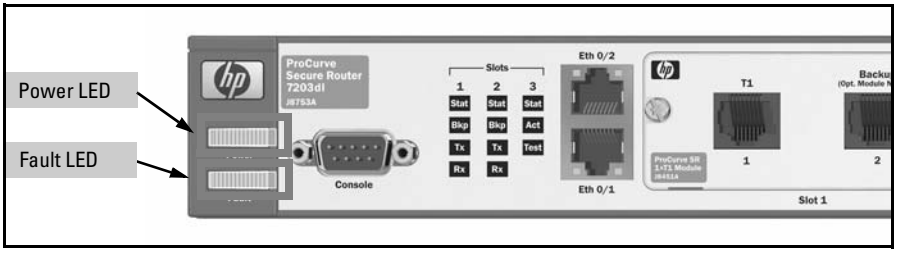


**Figure 1-16. Power and Fault LEDs**

## Fault LED

The fault LED is located directly below the power LED. (See Figure 1-16.) It flashes orange to indicate any fault condition, including:

- a cooling fan failure
- a failure in the option modules

If the power source in the ProCurve Secure Router 7102dl fails, the router turns off, as do its LEDs. However, the ProCurve Secure Router 7203dl features a redundant power source (RPS) outlet to provide greater network stability. When a problem occurs with the primary power source, the fault LED flashes orange, and the RPS begins to supply power to the ProCurve Secure Router. Problems with the primary power source include:

- AC power not being received
- primary AC/DC power converter failure

When the fault LED is flashing slowly on a ProCurve Secure Router 7203dl, the RPS is currently in use.

## LEDs for Slots 1 and 2

Both the ProCurve Secure Router 7102dl and 7203dl have two columns of LEDs that report information about the modules installed in the narrow slots. As you would expect, column 1 reports information about the module in slot 1, and column 2 reports information about the module in slot 2. Each column contains four LEDs; each LED monitors a different aspect of the module's Physical and Data Link Layer connections. (See Figure 1-17.)

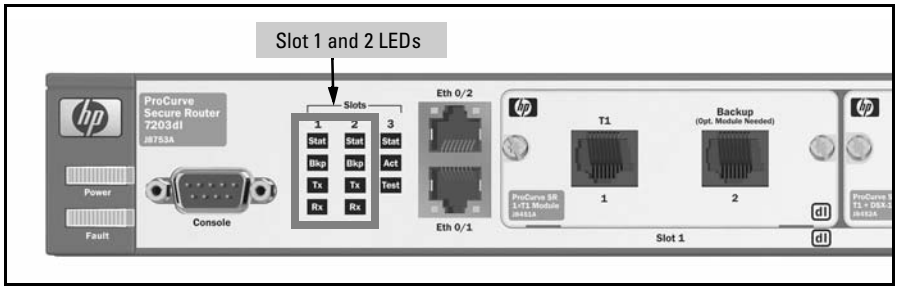


**Figure 1-17. Two Columns of LEDs Report Information about the Modules in Slots 1 and 2.**

### Status LEDs

The first LED in each column signals whether or not the module in the corresponding slot is functional and connected to the network. The status LED can display one of the following:

- **No light**—No module has been installed, or the interface is administratively down. An interface is administratively down until you activate it.
- **Red**—A module has been installed, and the corresponding interface has been activated, but no valid physical connection has been established. Red LEDs may also indicate other problems with the interface, such as:
  - a self-test failure
  - an active WAN alarm condition
- **Green**—A module has been installed and activated, and the physical connection is up and operational.
- **Yellow**—An interface on the module is being tested.

### Backup LEDs

The second LED in each column reports the status of the backup module, if a backup module is installed. The LED in the first column corresponds to the backup module in slot one, and the LED in the second column corresponds to the module in slot two. The status LEDs for backup modules can display one of the following:

- **No light**—A backup module has not been installed and activated.
- **Red**—The backup module has been activated and configured, but a valid physical connection has not been made. A red LED may also indicate that the backup interface has received a WAN alarm or has failed a self-test.
- **Solid green**—The module is ready to be used if a connection that it backs up should fail. For ISDN BRI backup modules, a solid green light further indicates that the module has completed negotiation with the switch.
- **Yellow**—A self-test is in process.
- **Flashing green**—The backup link is currently active.

### Tx and Rx LEDs

The Tx and Rx LEDs signal WAN activity across the corresponding interface's link. The third (Tx) LED in each column signals that the interface is transmitting data, and the fourth (Rx) LED indicates that the interface is receiving data. Tx and Rx LEDs signal the following:

- **Off**—The link is inactive.
- **Green**—Data is being transferred across the WAN or backup interface.

## Slot 3 LEDs

The ProCurve Secure Router 7203dl includes a third column of LEDs that represent the wide module. Unlike the other columns of LEDs, this column includes only three LEDs. (See Figure 1-18.)

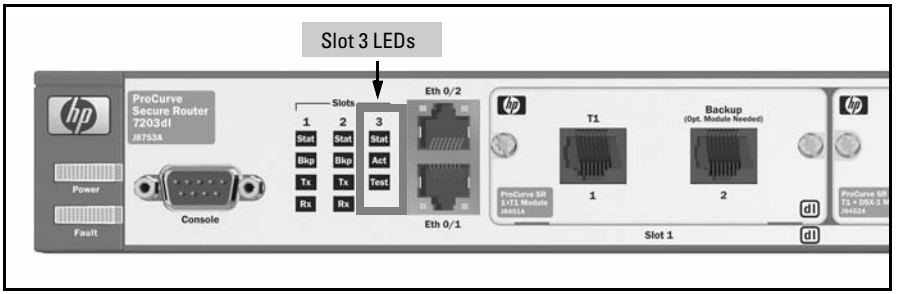


**Figure 1-18. On the ProCurve Secure Router 7203dl, the Third Column LEDs Report on the Wide Module.**

### Status LED

The first LED reports on the status of the wide module, indicating whether the wide module is installed and functional.

- **No light**—The module has not been installed, or none of the interface ports have been activated.
- **Green**—The module has been installed and recognized, and at least one interface is up.
- **Red**—There is an active alarm condition on one of the interfaces.

### Activity LED

The second LED reports activity across the WAN links established through the wide module. The LED flashes green to signal activity.

### Test LED

The third LED glows solid yellow if one of the interfaces on the module is in test mode.

## Ethernet and Activity LEDs

The Ethernet interfaces also have LEDs that report on their status and activity. (See Figure 1-19.)

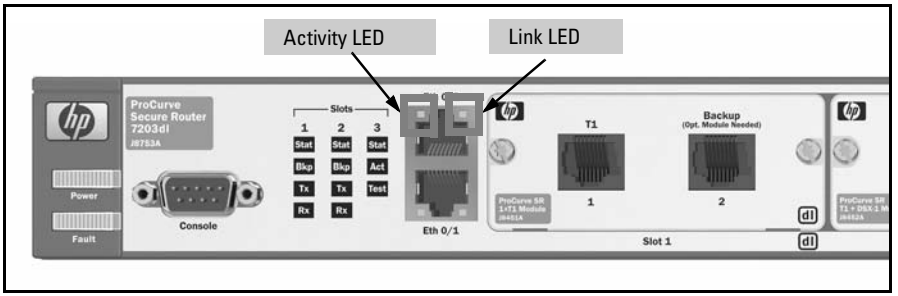


**Figure 1-19. LEDs for Ethernet Interfaces**

## Activity LEDs

Activity LEDs signal data transfer between the LAN and the router.

- **No light**—The Ethernet connection is inactive.
- **Flashing yellow—**The link is currently transmitting or receiving data.

## Link LEDs

Link LEDs signal whether or not the router recognizes a valid connection to a LAN.

- **No light**—The Ethernet interface is down.
- **Green—**The Ethernet interface is up.

# Rear Panel

The rear panel of the ProCurve Secure Router includes a slot for an optional IPSec VPN module and a slot for a compact flash card. The ProCurve Secure Router 7203dl also includes an additional feature: an outlet for a Redundant Power Source.

## Optional IPSec VPN Module

If your company wants to establish virtual private networks (VPNs) over the Internet, you can install the IPSec VPN module in the slot provided on the ProCurve Secure Router's rear panel. (See Figure 1-20.) The router can then establish a VPN with another router or with a VPN client that is installed on a user's workstation. Remote sites and individual users can then connect to your company's network through private Internet connections.

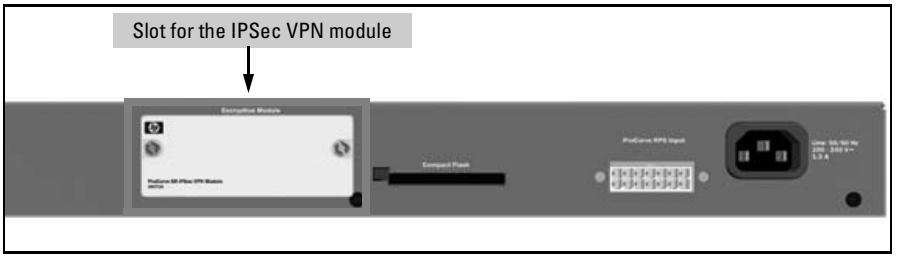


**Figure 1-20. IPSec VPN Module**

To protect your network from security breaches through the Internet, the ProCurve Secure Router establishes secure VPN tunnels using the industry-standard IP Security (IPSec) protocol. The IPSec VPN module enables the software that supports the IPSec protocols and relieves the CPU of the overhead associated with processing the encryption algorithms.

When the IPSec VPN module is installed, the ProCurve Secure Router 7102dl supports up to 500 VPN tunnels; the ProCurve Secure Router 7203dl supports up to 1,000 tunnels.

If your company operates on a smaller scale, you can install the IPSec Base Module instead. The IPSec Base Module enables either the ProCurve Secure Router 7102dl or 7203dl to support up to 10 VPN tunnels. Like the IPSec VPN Module, the IPSec Base Module is installed in the slot on the rear panel of the ProCurve Secure Router.

If VPN client connectivity is required, ProCurve Networking offers the ProCurve VPN Client. Your company can also use any pure IPSec client to allow users to establish a VPN with the router. However, VPN clients based on proprietary implementations will not work with the IPSec VPN Modules.

## Compact Flash Card

The compact flash slot on the ProCurve Secure Router's back panel supports most standard compact flash cards. (See Figure 1-21.) To protect your ProCurve Secure Router against system failure, you can store the Secure Router OS software and your configuration file on a compact flash card. In fact, the ProCurve Secure Router provides additional features that automatically use compact flash to safeguard the Secure Router OS and your configurations. These features are described in "Bootup Process" on page 1-30 and "AutoSynch™ Technology" on page 1-34.

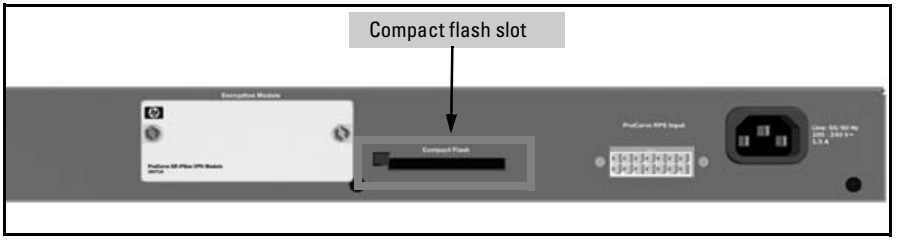


**Figure 1-21. Compact Flash Slot on Rear Panel of the ProCurve Secure Router**

## Redundant Power Source

The RPS outlet on the back panel of the ProCurve Secure Router 7203dl provides increased router reliability for mission-critical applications. (See Figure 1-22.) The RPS slot can be used with the ProCurve 600 Redundant External Power Supply.


**Figure 1-22. RPS Outlet on the ProCurve Secure Router 7203dl**

# Memory

Both the ProCurve Secure Router 7102dl and 7203dl have 32 MB of internal flash memory. The flash memory provides nonvolatile random access memory (NVRAM); in other words, the router retains what is stored in the internal flash even when the router is powered down.

Because internal flash memory is relatively limited, the Secure Router OS is stored in compressed form. The Secure Router OS file is approximately 6 MB. The number of configuration files that can be saved in internal flash is limited only by the amount of available memory. Because configuration files tend to be small, you will be able to save multiple configuration files in internal flash.

In addition to internal flash, the ProCurve Secure Router 7102dl has 128 MB of random access memory (RAM), which holds the running configuration. All information in RAM is lost when the router is powered off. The ProCurve Secure Router 7203dl has 256 MB of RAM.

# Software Overview

To manage your ProCurve Secure Router, you must understand basic router operations, including how the router uses:

- Secure Router OS boot code
- Secure Router OS
- the startup-config
- the running-config

Further, you must understand how the Secure Router OS is organized so that you can properly configure the router and enable safeguards to protect the router from unauthorized access.

This section describes software operations such as the boot process, the process of saving configurations, the OS hierarchy, and the bootstrap mode.

## Bootup Process

Concurrent with the release of J02_02A.biz software in July 2005, ProCurve Networking changed the boot process for the ProCurve Secure Router. By default, the ProCurve Secure Router now boots from compact flash. If a compact flash card is not inserted into the compact flash slot or if the card does not contain the required Secure Router OS file, the router will boot from internal flash. Previously, the ProCurve Secure Router booted only from internal flash.

This change has been made in routers that shipped after July 2005; these routers have the following serial numbers:

- ProCurve Secure Router 7102dl (J8752A) US525TRAP4 or later
- ProCurve Secure Router 7203dl (J8753A) US522TS252 or later

**Note**

If you purchased a ProCurve Secure Router before this change was made, you can enable the new boot process by upgrading to J02_02A.biz or later and making a small configuration change. For information about this configuration change, see *Appendix A: Configuring the Router to Boot from Compact Flash*.

The boot process begins when you power up the ProCurve Secure Router or manually reload it. It proceeds as follows:

1. The router first loads the Secure Router OS boot code.
2. The router then searches compact flash for the SROS.BIZ file, which contains the Secure Router OS.
   - If the router finds the SROS.BIZ file in compact flash, it will load the Secure Router OS and begin step 3.
   - If a compact flash card is not installed or the SROS.BIZ file on the card is missing or corrupted, the router searches for this file in internal flash. If the router finds the SROS.BIZ file in internal flash, it loads this SROS software and begins step 3.
   - If the router does not find a valid SROS.BIZ file in either compact flash or internal flash, the router boots up in bootstrap mode (as described in “Bootstrap Mode Context” on page 1-67).
3. After the router finds a valid SROS.BIZ file (either in compact flash or internal flash), it checks compact flash for the startup-config file, which contains the saved configurations for the router.
   - If the router finds the startup-config file in compact flash, it loads this file.
   - If the router does not find the startup-config in compact flash, it searches for the startup-config file in internal flash. If it finds the startup-config in flash, it loads this configuration.
   - If the router does not find the startup-config file in either compact flash or internal flash, the router boots in basic mode using the factory default configuration settings.

Figure 1-23 summarizes the boot process.

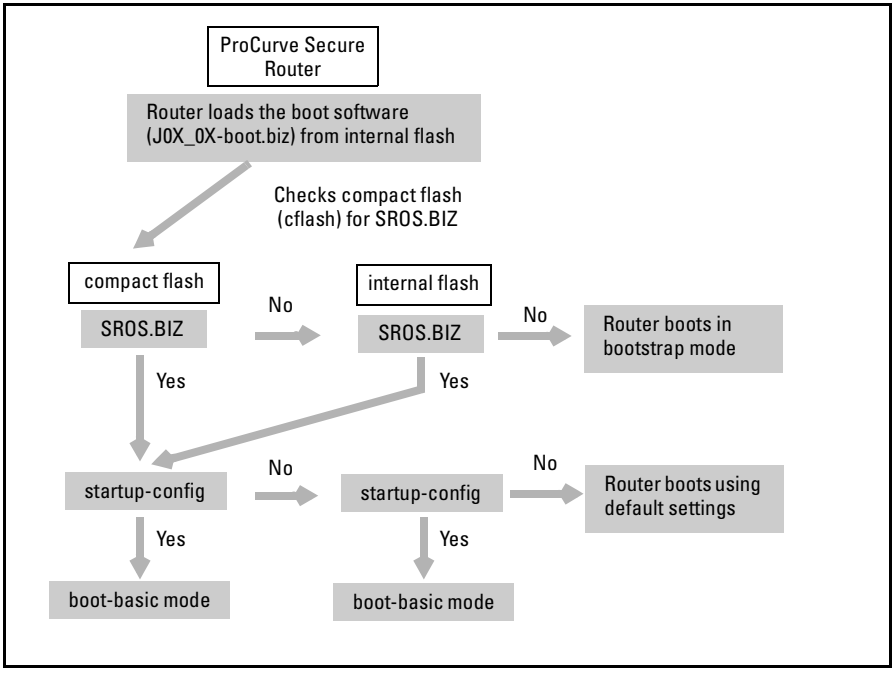


**Figure 1-23. Booting the ProCurve Secure Router**

## Advantages of Booting From Compact Flash

Booting from compact flash simplifies router setup. You can use a compact flash card to preconfigure a router and simply send the card to a remote site. Any person at the remote site can insert the compact flash card into the router, connect the cables that will enable the LAN and WAN connections, and power up the router. The ProCurve Secure Router will boot with the SROS.BIZ file and startup-config on compact flash, and the router will be immediately operational.

To check the configuration by remote, you can simply establish a Telnet or Secure Shell (SSH) session with the router or use the Web browser interface.

## Setting Up a Compact Flash Card from Which to Boot the Router

Newly shipped ProCurve Secure routers have an internal flash that contains two Secure Router OS files:

- J0X_0X.biz
- SROS.BIZ

The SROS.BIZ and J0X_0X.biz files are identical. The J0X_0X.biz file reflects the version number of the software, such as J06_03.biz. This file has then been resaved as SROS.BIZ.

Internal flash also contains the startup-config file. At this point, the startup-config file contains the default configuration for the router. After you have configured your router and saved the configurations, the new startup-config file will allow the router to boot up with the configurations you have made.

To set up a new compact flash card so that the router can boot from it, insert the card into the slot provided on the back panel of the router and copy the following files from flash memory to compact flash:

- J0X_0X.biz
- SROS.BIZ
- startup-config

After you copy the files to a compact flash card, take the card to any ProCurve Secure Router. Unless its boot process has been altered, the router will automatically boot from the software and startup-config file stored on the card.

When ProCurve Networking releases new software, part of the update process will include renaming the new file as SROS.BIZ and copying the new file to compact flash and to internal flash. When you need to know the version of software the router is using, the **show version** command will display the exact version. (This and other **show** commands are described later in this chapter.)

## Saving Configuration Changes

When the ProCurve Secure Router loads the startup-config, it executes it line by line as the running-config. As you make configuration changes, these changes are held in RAM. Because RAM is cleared every time the router is powered down, you must save any changes that you want to keep to the startup-config file.

When the command is entered, the ProCurve Secure Router first tries to save these changes to a startup-config file on compact flash. If no compact flash card is inserted into the slot on the back panel, the router saves the changes to the startup-config file that is stored in internal flash. If no startup-config file exists on either the compact flash or internal flash memories, the router creates the file and saves the configuration to it.

## AutoSynch™ Technology

The AutoSynch feature was first released as a free update in the J03_01.biz Secure Router OS. This feature ensures that the Secure Router OS (SROS.BIZ) and the startup-config file stored on compact flash are identical to those stored on internal flash. AutoSynch technology affects only the SROS.BIZ and startup-config files; any other files that you intend to keep on the compact flash drive will need to be manually copied from your router's internal flash to the compact flash card.

When you save your configurations, the ProCurve Secure Router saves the running-config to the startup-config stored on the compact flash. If the **autosynch** command is enabled, when you save your current configuration to the startup-config, the file is saved to both compact flash and internal flash at the same time.

AutoSynch technology ensures that you always have a backup copy of your configuration file and the version of the Secure Router OS you are using. If a hardware failure should occur, you simply contact ProCurve Networking to get a new part or even a new unit (if that is required). Then you replace the part, insert the compact flash card, and power up the router. The router automatically loads the Secure Router OS and the startup-config from the compact flash card.

Likewise, if the Secure Router OS or the configuration file becomes corrupted, you have up-to-date backup copies, so downtime is confined to the time it takes to load these copies. This is especially helpful if the Secure Router OS you are using is no longer available on the ProCurve Networking Web site (because subsequent versions have been released).

## Secure Router OS Hierarchy

The ProCurve Secure Router OS is organized into two security modes and then further organized into configuration modes. Each of these modes allows you to access and configure a separate aspect of your router's operation. This OS hierarchy creates levels of security by limiting certain functions to authorized users.

This section introduces the different mode contexts and describes the types of commands you can enter in each one. (See Figure 1-24.)

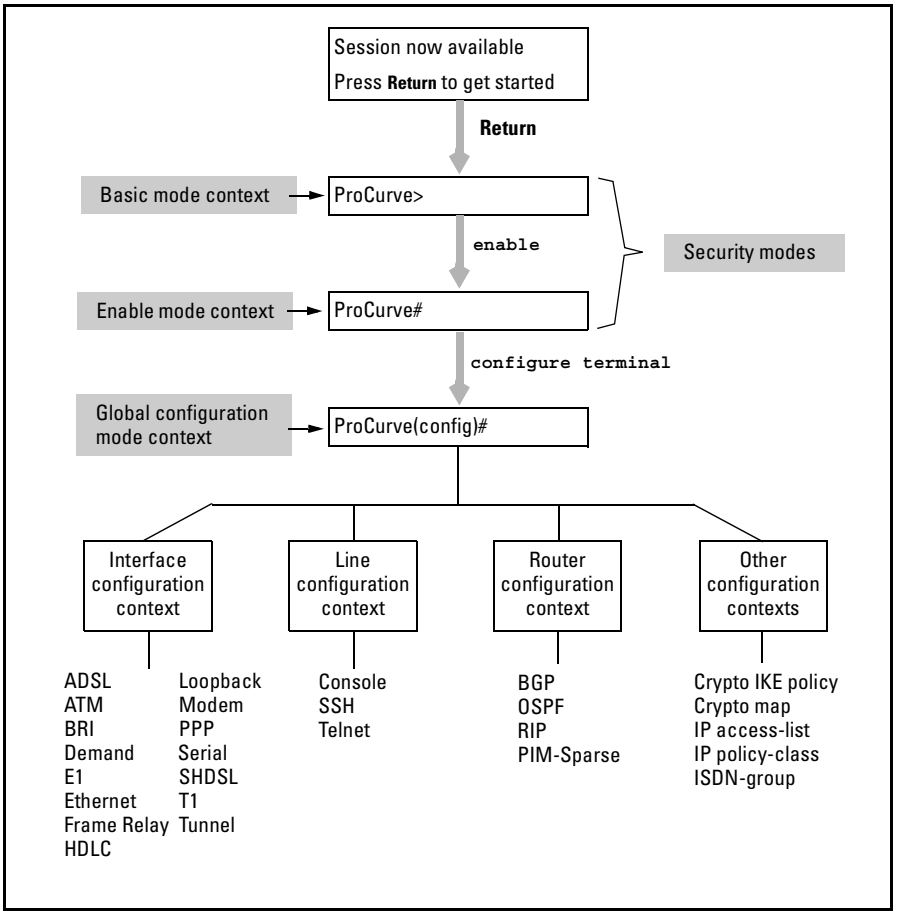


**Figure 1-24. Security and Configuration Modes in the Secure Router OS**

To protect your WAN against unauthorized access, the ProCurve Secure Router has two security modes:

- basic mode
- enable mode

## Basic Mode

The basic mode allows restricted access to the router, providing only a limited number of commands. From this mode, you can view basic system information, verify some processes, and enter **traceroute** and **ping** commands. You do not have access to any of the options that allow you to configure the router.

When you first access the Secure Router OS through the CLI and press **Enter**, the router is in the basic mode context. To verify your location in the CLI, check the prompt. In the basic mode context, the prompt is the > symbol, as shown below:

```
ProCurve>
```

From the basic mode context, you can access the enable mode by entering:

```
ProCurve> enable
```

## Enable Mode

The enable mode is sometimes called the privileged mode because it allows you to access all management and configuration commands. You can use this command to view detailed information about how your router is functioning, perform system management tasks, and gain access to all configuration modes on the router. From the enable mode, you can save, move, and delete the startup-config and running-config files and use the **show** and **debug** commands.

Although you cannot actually configure the ProCurve Secure Router from the enable mode, you can access the global configuration mode from this mode, and from there, you can access any configuration mode and configure any router feature. For additional security, you can—and should—password protect this more-secure OS level.

In the enable mode context, the prompt is followed by the # symbol, as shown below:

```
ProCurve#
```

From the enable mode context, you can access the global configuration mode context by entering:

```
ProCurve# configure terminal
```

## Global Configuration Mode

From the global configuration mode, you can make configuration changes that apply to the entire router and all interfaces. You can configure the system's global parameters, such as the hostname, passwords, and banners. You can also set parameters for IP services such as DHCP and DNS. You can enable the built-in firewall and configure global options for that firewall. You can also configure passwords to protect the enable mode and SSH, FTP, and HTTP access.

From the global configuration mode context, you can also access other configuration mode contexts to configure specific router interfaces and functions, such as routing protocols. There are four main types of contexts:

- interface
- router
- line
- other

**Interface.** The interface configuration mode contexts enable you to configure the LAN and the WAN connections to your router. To configure an interface, enter the following command from the global configuration mode context:

***Syntax:*** interface <*interface*> [<*slot*>/<*port*> | <*interface number*>]

Replace ***<interface>*** with the type of physical interface such as **e1**, **t1**, **serial**, **bri** (for ISDN interfaces), **adsl**, or **modem** (for analog backup interfaces). You can also replace ***<interface>*** with a logical interface such as **ppp**, **frame-relay**, **loopback**, or **tunnel**. For physical interfaces, replace ***<slot>/<port>*** with the slot and port location of the connection, and for logical interfaces, replace ***<interface number>*** with the interface number.

For example, if your router has a T1 module in slot one, you would type **interface t1 1/1** to configure this interface. The CLI prompt will change to show that you are in the T1 1/1 interface configuration mode context:

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

For another example, if you want to configure a PPP connection to an ISP, you would enter **interface ppp 1** to create and configure a PPP logical interface.

**Router.** You can configure dynamic routing protocols from the router configuration mode contexts. There are four router configuration modes: BGP, RIP, PIM-Sparse, and OSPF. To configure these protocols, move to the global configuration mode context and use this command:

***Syntax:*** router [bgp | ospf | pim-sparse | rip]

For example, to configure RIP, enter:

```
ProCurve(config)# router rip
ProCurve(config-rip)#
```

When configuring BGP, you must also designate an AS number, which can be between 1 and 65535, in the command line. (Your ISP will provide this number.)

***Syntax:*** router bgp <*AS number*>

For example, enter:

```
ProCurve(config)# router bgp 1
ProCurve(config-bgp)#
```

**Line.** Your router has three data lines that allow you to access the ProCurve Secure Router's OS: console, SSH, and Telnet. You can configure options for line sessions by accessing the line configuration mode context.

***Syntax:*** line [console 0 | ssh <*0-4*> | telnet <*0-4*>]

For example, you might enter:

```
ProCurve(config)# line ssh 2
```

For more information about configuring secure access to the router using these access lines, see *Chapter 2: Controlling Management Access to the ProCurve Secure Router*.

**Other.** You can access other configuration mode contexts from the global configuration mode context, such as those from which you configure ACLs, access control policies (ACPs), QoS maps, and crypto maps. You can enter these configuration contexts from the global configuration mode context or from individual interface configuration mode contexts.

## Commands Available in the Basic, Enable, or Global Configuration Mode Contexts

The ProCurve Secure Router OS permits you to use certain commands only in specific modes. When you are managing the ProCurve Secure Router and you try to use a command that is not supported from the current mode context, you will receive an error message.

To help you become familiar with the Secure Router OS, the following sections introduce the types of commands that are available in the three main modes: basic, enable, and global configuration.

# Basic Mode Commands

The basic mode commands include those discussed in the following sections.

## Clear

These commands reset router operations or statistical records. Table 1-2 shows the **clear** commands available in basic mode context.

**Table 1-2. Basic Mode Context clear Commands**

| Option | Result |
|---|---|
| **clear counters [<interface>]** | clears interface counters, such as the number of packets transmitted and received or errors detected |
| **clear event-history** | clears the event history log |
| **clear host [<hostname> \| *]** | deletes host table entries |
| **clear sip [location \| user-registration]** | clears local SIP information |
| **clear user [console \| ssh \| telnet]** | detaches a user from a particular line |

## Enable

To begin managing the router in the enable mode context, enter:

***Syntax:*** enable

## Logout

Exit the current CLI session and return to the login screen.

***Syntax:*** logout

## Ping

Send an ICMP echo to a specified destination. To send a default ping of 5 echoes, enter:

***Syntax:*** ping [<*A.B.C.D* > | <*domain name*>]

When you begin sending ICMP echoes, the router displays a legend to describe the types of responses the router receives. For example, Figure 1-25 shows a successful ping:

```
ProCurve> ping 1.1.1.1
Legend:     '!' = Success, '?' = Unknown host, '$' = Invalid host address
            '*' = Request timed out, '-' = Destination host unreachable
            'x' = TTL expired in transit
!!!!!
Success rate is 100 percent (5/5), round trip min/avg/max = 3/3.0/3 ms
```

**Figure 1-25. Sending a Ping**

Typing **ping** and pressing **Enter** without a destination address will allow you to set extended options for the ICMP echo. Extended options include the number of pings to be sent, the size of the datagram to be sent, and the timeout value. The CLI displays default settings in brackets; press **Enter** to accept the defaults. For example:

ProCurve> ping
Target IP address?
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands? [n]

Pressing **y** for the **Extended commands?** option allows you to set the source address and data pattern. You can also specify that the ping sweep a range of datagram sizes.

If you enter **y** for the **verbose** option in the extended commands, the output reports the result of each ping with a description of the datagram size and the echo's round-trip time. For example:

Reply from 1.1.1.1: bytes = 100 time = 4 ms

If you need to halt a ping operation, press **Ctrl+C**.

**Note** **Ping** commands are available in all areas of the Secure Router OS.

## Show

View information about, or the current status of, an interface or feature. Table 1-3 is a list of **show** commands available in the router's basic mode context. For a more comprehensive list of **show** commands, see "Show" on page 1-51.

**Table 1-3. Basic Mode Context show Commands**

| Option | Result |
|---|---|
| **show arp [realtime]** | shows the ARP table, which includes interfaces' IP and MAC addresses |
| **show autosynch-status** | reports whether the SROS.BIZ and startup-config in internal flash and compact flash are synchronized |
| **show clock** | displays clock information such as the time, date, and time source |
| **show demand** | shows demand routing parameters and statistics |
| **show dynamic-dns** | shows the dynamic DNS hostname and registered IP address |
| **show event-history** | displays the events log |
| **show frame-relay [fragment \| lmi \| multilink \| pvc]** | gives information on Frame Relay fragmentation, LMI status polls, permanent virtual connections (PVCs), and multilinks |
| **show interfaces [<interface ID> {performance-statistics \| realtime}]** | shows status reports for router interfaces; you can also specify a particular interface |
| **show ip access-list [<name>]** | displays configured ACLs and the number of packets the router has matched to each entry |
| **show ip interfaces [demand \| ethernet \| frame-relay \| hdlc \| loopback \| ppp \| tunnel]** | lists interfaces with their assigned IP addresses and network masks, the MTU for each interface, and whether fast caching is enabled on the interface |

| Option | Result |
|---|---|
| **show isdn-group [<interface number>]** | lists the ISDN group configurations and member interfaces |
| **show lldp [<cr> \| device <name> \| interface <interface ID> \| <neighbors>]** | displays LLDP settings and information, including information on specific neighbors |
| **show memory heap [realtime]** | displays statistics for the router memory, including how much has been used and how much is available |
| **show modules** | gives information on the router's modules, including the type of module in each slot and the number of ports in each module |
| **show processes cpu** | shows the process statistics, including the load percent for each process |
| **show snmp** | displays the SNMP information and packets received |
| **show sntp** | shows SNTP information |
| **show thresholds** | displays the thresholds that have been exceeded on each E1 or T1 interface |
| **show version** | displays the router system software and hardware versions |

## Telnet

Open a Telnet session. (You enable and set the parameters for Telnet sessions from the Telnet line configuration mode context.)

***Syntax:*** telnet <*A.B.C.D*>

For information on how to set up a Telnet session, see *Chapter 2: Controlling Management Access to the ProCurve Secure Router*.

## Traceroute

Ping an IP address and display the hops that the packet takes en route to the destination.

***Syntax:*** traceroute <*A.B.C.D*>

The router will display a route to a destination up to 30 hops away. You can end the traceroute process at any time by pressing **Ctrl+C**.

Similar to the **ping** command, you can set extended options for tracing a route by entering **traceroute** and pressing **Enter** without specifying the destination address. Options include the source address at which the trace begins and the maximum number of hops.

The **traceroute** command is also available from the enable mode context.

### Terminal

Set the maximum number of lines to display on the screen during a terminal session.

***Syntax:*** terminal length <0-480>

If a readout includes more lines than the configured terminal length amount, the display stops at the length limit and displays **--MORE--** at the bottom.

To continue the display after the **--MORE--**, press **Spacebar**. To only display the next line of the readout, press **Enter**. To return to the router prompt and end the display, press a key.

### Wall

Broadcast a message through the console port.

***Syntax:*** wall <*message*>

## Enable Mode Commands

To enter the enable mode context, enter **enable** from the basic mode context. The following sections briefly describe some of the enable mode commands and their functions.

**Important!**

ProCurve strongly recommends that you set an enable password to prevent unauthorized access to the router. If the enable mode context is not password protected, anyone with console access to the router will be able to change the configurations and compromise network security. See “Restricting Access to the Enable Mode Context” on page 2-4 for more information on how to configure an enable mode password.

## Clear

The enable mode context expands the options for the **clear** command. To view these options, enter:

***Syntax:*** clear ?

Table 1-4 lists the **clear** command options available in the enable mode context.

**Table 1-4. Enable Mode Context clear Commands**

| Option | Result |
|---|---|
| **clear access-list** | clears the statistics for packets matched to ACL entries |
| **clear arp-cache** | clears the ARP cache |
| **clear arp-entry** | clears a single ARP table entry |
| **clear bridge [<group number>]** | clears the bridge table |
| **clear buffers** | clears the buffer statistics |
| **clear counters [<interface>]** | clears interface counters |
| **clear crypto [ike \| ipsec] sa** | clears any existing crypto IKE or IPSec SAs |
| **clear dump-core** | clears core-dump debug information |
| **clear event-history** | clears the event-history log |
| **clear host** | deletes DNS host table entries |
| **clear ip [bgp \| cache \| dhcp-server \| igmp \| ospf \| policy-sessions\| policy-stats \| prefix-list \| route {* \| <A.B.C.D>}]** | clears IP routes or sessions established using an ACP |
| **clear lldp [counters \| neighbors]** | clears lldp information |
| **clear pppoe <ppp interface number>** | clears a single PPPoE session |
| **clear processes [cpu \| queue]** | clears router process statistics |
| **clear qos map** | clears the QoS map statistics |
| **clear route-map counters** | resets the statistics for packets selected by route maps |
| **clear sip [location \| proxy \| user-registration]** | clears local SIP-related information |
| **clear spanning-tree** | clears spanning tree statistics |
| **clear tacacs+ statistics** | clears TACACS+ server statistics |
| **clear user [console \| ssh \| telnet]** | detaches a user from a particular line |

Some examples of **clear** commands include the following:

***Syntax:*** clear ip policy-sessions

This command clears all sessions established using the ACPs applied to router interfaces.

***Syntax:*** clear ip route [** | <*A.B.C.D*>]

The ** option clears all routes learned through a routing protocol. Static routes are not affected. You can clear a single route by entering the destination IP address.

## Clock

The **clock** command in the enable mode context allows you to set the clock, adjust for the time zone, and manage the clock source. To view the options for the **clock** command, enter:

***Syntax:*** clock ?

For example, to set the clock and the time zone, enter:

***Syntax:*** clock set <*HH:MM:SS*>
***Syntax:*** clock timezone <*zone*>

Enter **clock timezone ?** for a complete list of keywords for the time zones of various locations.

**Daylight Saving Time Auto Correction.** The router is set to automatically correct the time for daylight saving time. If the router is operating in an area that does not observe daylight saving time, you should disable this option using the **clock no-auto-correct-dst** command. Enter:

```
ProCurve# clock no-auto-correct-dst
```

To re-enable daylight saving time correction, enter:

```
ProCurve# clock auto-correct-dst
```

## Configure

There are four options to this command: **memory**, **network**, **overwrite-network**, and **terminal**. The **configure memory**, **configure network**, and **configure overwrite-network** commands allow you to retrieve and apply a configuration file by saving the file as the router's running-config. Using this command causes your router to immediately begin using the specified configuration without rebooting the router.

The **configure memory** command pulls and activates the startup-config file from compact flash memory. If no compact flash card is mounted, this command pulls and activates the startup-config file from flash. The file you intend to use must be named startup-config.

The **configure network** command pulls and applies a file from a TFTP server as the running-config.

Enter **configure overwrite-network** to retrieve a file from a TFTP server and save it as startup-config and startup-config.bak on compact flash. This command only works if you have a compact flash card installed on the router. **Configure overwrite-network** overwrites any existing startup-config file on compact flash with the startup-config it retrieves from the TFTP server.

The last **configure** command, **configure terminal**, moves you to the CLI's global configuration mode context.

## Copy

This command is used for managing configuration files and other files on your router. It has the following syntax:

***Syntax:*** copy <*source file location*> <*source 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 1-5 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, all 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

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

**Table 1-5. Options for the copy Command**

| Source Location Options | Destination Location Options |
|---|---|
| **cflash <filename>** or **flash <filename>** | • **boot**<br>• **cflash [<filename>]**<br>• **flash [<filename>]**<br>• **interface** (only from **flash <filename>**) |
| **cflash** or **flash** | • **tftp**<br>• **xmodem** |
| **console** | • **flash <filename>** |
| **running-config** | • **cflash <filename>**<br>• **flash <filename>**<br>• **startup-config**<br>• **tftp**<br>• **xmodem** |
| **startup-config** | • **cflash <filename>**<br>• **flash <filename>**<br>• **running-config**<br>• **tftp**<br>• **xmodem** |
| **tftp** or **xmodem** | • **flash**<br>• **cflash**<br>• **running-config**<br>• **startup-config** |

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 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, either compact flash (**cflash**) or internal flash (**flash**) memory. Replace ***<source config-file>*** with **startup-config** or **running-config** (You can also enter a filename to copy a file to another location). 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 under which the uploaded configuration should be saved.

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**.

## Debug

Entering **debug** will display debug messages as packets arrive on the router. Debugging is useful when troubleshooting or testing your router's operation.

The Secure Router OS provides many **debug** commands, including options for most protocols and processes run on the router.

For a list of **debug** commands, go to the enable mode context and enter:

```
ProCurve# debug ?
```

For example, you could debug the establishment of a PPP connection:

```
ProCurve# debug ppp negotiation
```

You can find the exact command syntax for relevant **debug** commands in the troubleshooting section of each chapter.

**Caution**

This guide will describe how to use **debug** commands to troubleshoot your router. You should be aware that **debug** commands are processor-intensive and could seriously degrade network performance.

## Dir

This command shows the current files in internal flash or compact flash.

***Syntax:*** dir [flash | cflash] [*.<*file extension*>]

Use the **flash** option to list all files in the router's flash memory. Use the **cflash** option to display all the files on the router's compact flash card.

The * symbol is a wildcard that allows you to specify a file pattern to display. For example, if you want the router to list all the Secure Router OS files in internal flash memory, you would enter:

```
ProCurve# dir flash *.biz
```

Or if you wanted to display all the router configuration files stored on the compact flash card, you might enter:

```
ProCurve# dir cflash *.cfg
```

**Note**

If you do not specify an option for **flash** or **cflash**, the CLI displays only files in the internal flash.

## Disable

To leave the enable mode context, type **disable**. The Secure Router OS will return you to basic mode context.

## Erase

The **erase** command is a file management command. Table 1-6 shows the **erase** command options.

***Syntax:*** erase [{cflash | flash} <*filename*> | startup-config | file-system cflash]

**Table 1-6. File Locations for the erase Command**

| File location | Description |
|---|---|
| **cflash <filename>** | erases the specified file from compact flash |
| **file-system cflash** | formats compact flash |
| **flash <filename>** | erases the specified file from flash |
| **startup-config** | erases the startup-config file |

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

```
ProCurve# erase flash oldconfig
```

**Note**

When erasing files, be sure to enter the filename exactly as it appears in the directory.

Erasing the startup-config files will return the router to the factory default settings at the next reboot. Entering **erase startup** after executing the **autosynch** command will delete the startup-config files from both flash and compact flash. If you have a compact flash card, and are not running the **autosynch** command, this command erases the startup-config only from compact flash. If you do not have a compact flash card, this command erases the startup-config file from flash.

Use the **erase file-system cflash** command to format your compact flash card memory. Using this command will erase any existing files on your compact flash card.

## Events

The **events** command enables the Secure Router OS to display a notice to the CLI whenever an event occurs. This command is useful for troubleshooting, because it lets you immediately determine whether a connection is up and working properly. This command is active in the default router settings. To turn off the events reporting, enter **no events**.

## Reload

This command exits the current session and reboots the router. Before exiting the session, the Secure Router OS will ask whether you want to save the running-config. It will also ask you to confirm that you want to reboot the router.

## Show

The enable mode context includes the complete set of **show** commands for the Secure Router OS. Table 1-7 lists these **show** commands.

**Table 1-7. Enable Mode Context show Commands**

| Option | Result |
|---|---|
| **show access-lists [<name>]** | displays ACLs, including all entries and the number of packets the router has matched to each entry |
| **show arp [interfaces <interface ID>] [realtime]** | shows the ARP table, which includes interfaces' IP and MAC addresses |
| **show atm pvc [interfaces atm <number.subinterface>]** | shows information about ATM PVCs on an ADSL connection |
| **show atm traffic interface atm <number.subinterface>** | shows information about ATM traffic on a specific virtual channel |
| **show autosynch-status** | reports whether the SROS.BIZ and startup-config in internal flash and compact flash are synchronized |
| **show backup interfaces** | displays the backup configuration, including backup phone numbers |
| **show bridge [<interface ID> \| <bridge group>]** | displays the bridge table and, optionally, the table for a particular logical interface or bridge group |
| **show buffers [users] [realtime]** | lists the buffer pool statistics |
| **show cflash** | lists files in compact flash |
| **show clock [detail]** | displays clock information such as the time, date, and time source |

| Option | Result |
|---|---|
| **show configuration** | shows the startup configuration |
| **show connections** | lists all logical interface binds |
| **show crypto [ca \| ike \| ipsec \| map]** | shows certificates and VPN configurations, such as IKE policies, transform sets, and crypto maps |
| **show debugging** | displays the active debugging switches |
| **show demand** | shows the current statistics and settings for the demand interfaces |
| **show dialin interfaces** | displays interfaces that are configured to provide dial-in console sessions |
| **show dynamic-dns** | shows dynamic DNS status including hostname and registered IP address |
| **show event-history** | displays the events log |
| **show file [{cflash \| flash} <filename>]** | shows the contents of a file in internal flash or compact flash |
| **show flash** | lists the files in internal flash |
| **show frame-relay [fragment \| lmi \| multilink \| pvc]** | gives information on Frame Relay fragmentation, LMI status polls, permanent virtual connections (PVCs), and multilinks |
| **show hosts [verbose]** | displays IP domain name, style, name servers, and the IP host table |
| **show interfaces [<interface ID>]** | shows the interface table; input an interface ID to see information on a particular interface |
| **show interfaces <physical interface ID> performance-statistics** | shows the performance statistics for physical interface over the past 15 minutes |
| **show interfaces [<interface ID>] realtime** | displays interface statistics in realtime |
| **show ip <options>** | lists information on IP traffic, routes, ACLs, ACPs, and routing protocols |
| **show ip interfaces [demand \| ethernet \| frame-relay \| hdlc \| loopback \| ppp \| tunnel]** | lists interfaces with their assigned IP addresses and network masks, the MTU for each interface, and whether fast caching is enabled |
| **show isdn-group** | lists the ISDN group configurations and member interfaces |
| **show lldp [<cr> \| device <name> \| interface <interface ID> \| neighbors]** | shows LLDP settings and information, including information on specific neighbors |
| **show memory heap [realtime]** | displays statistics for the router memory, including how much has been used and how much is available |

| Option | Result |
|---|---|
| **show modules** | gives information on the router's modules, including the type of module in each slot and the number of ports in each module |
| **show output-startup** | lists the startup-config error log |
| **show port-auth supplicant [interface <interface ID> \| summary]** | displays port authentication information |
| **show pppoe** | displays the status of the PPPoE client |
| **show processes cpu [realtime]** | shows the process statistics, including the load percent for each process |
| **show qos map** | displays the QoS maps, including how many packets have been matched to the map |
| **show queue [<interface ID>]** | lists the statistics for queues on an interface or interfaces |
| **show queueing [fair]** | shows each interface queue's discard threshold and maximum number of subqueues |
| **show radius statistics** | displays RADIUS system statistics |
| **show route-map [<name>]** | displays the route-map |
| **show running-config** | shows the current operating configuration |
| **show sip [location \| resources \| statistics \| user-registration]** | displays information such as a local SIP location database, resources allocated to SIP sessions, and registered SIP users |
| **show snmp** | displays the SNMP information and packets received |
| **show sntp** | shows SNTP information |
| **show spanning-tree [<bridge group number>] [realtime]** | displays the spanning-tree topology |
| **show startup-config [checksum]** | displays the startup configuration |
| **show tacacs+ statistics** | lists TACACS+ packet and socket statistics |
| **show tcp info [<tcp index>] [realtime]** | lists information for TCP ports |
| **show tech [terminal]** | generates and displays the output of most **show** commands to the screen or to saves the output to showtech.txt |
| **show thresholds** | displays the thresholds that have been exceeded on each E1 or T1 interface |
| **show udp info [<session ID>] [realtime]** | lists information for UDP ports |
| **show users [realtime]** | displays the users currently connected to a session on the router |
| **show version** | displays the router system software and hardware versions |

The **show running-config** command can be particularly useful for troubleshooting problems. To help you troubleshoot more efficiently, the command includes options that allow you to view the settings for a particular router feature. For example, you can view the settings entered for a particular interface. Table 1-8 shows the **show running-config** options and the information displayed when you enter each one.

**Table 1-8. The Options for the show running-config Command**

| show running-config Options | Description |
|---|---|
| **access-lists** | Displays information about the access control lists (ACLs) that you have configured on the router. |
| **checksum** | Displays the MD5 digest for the running-config. |
| **interface <interface ID>** | Displays the settings for the interface you specify. Supported interfaces are listed below:<br>• adsl <slot>/<port><br>• atm <number><br>• bri <slot>/<port><br>• demand <number><br>• e1 <slot>/<port><br>• ethernet <slot>/<port><br>• frame-relay <number><br>• hdlc <number><br>• loopback <number><br>• modem <slot>/<port><br>• ppp <number><br>• serial <slot>/<port><br>• t1 <slot>/<port><br>• tunnel <number> |
| **ip crypto** | Displays settings for any IPSec VPNs configured on the router. |
| **ip rtp** | Displays all IP Real-time Transport Protocol (RTP) settings. |
| **ip sdp** | Displays all Session Description Protocol (SDP) settings. |
| **ip sip** | Displays all Session Initiation Protocol (SIP) settings. |
| **policy-class** | Displays the ACPs configured on the router. |
| **probe** | Displays information about the network monitoring probes you have configured. |
| **router [bgp{<AS number>}\| ospf \| pim-sparse \| rip]** | Displays information about the routing protocol you specify. |

| show running-config Options | Description |
|---|---|
| **track** | Displays settings for the network monitoring tracks you have configured on the router. |
| **verbose** | Displays the default settings and the settings you have configured. You can use this option with any other option listed for the show running-config command. |

The **verbose** option is available for many **show** commands, including the **show running-config** command. This option displays both the settings that you have entered and the default settings. For example, the **show running-config interface e1 1/1 verbose** command displays all the configurations currently running on your router for interface E1 1/1—including the settings you entered and the default settings that have not been altered.

The **show interfaces** command will display information on any of the router's physical or logical interfaces. When you enter this command without an option for a specific interface, the CLI will display information on all the router's interfaces. If you only need to see information on a particular interface, you can specify the physical interface by its slot and port numbers and the logical interfaces by the interface number.

You have the option to specify the types of information to be displayed by the **show interfaces <*interface*>** command. To see snapshots the errors detected on a physical interface's performance over a certain interval, enter:

***Syntax:*** show interface <*interface*> <*slot*>/<*port*> performance-statistics [Total-24-hour | <*range of intervals*>]

To view the performance statistics over the past 24-hours in 15-minute intervals, enter:

```
ProCurve# show interface t1 1/1 performance-statistics
```

You can also limit the display to a specific range of 15-minute intervals by replacing ***<range of intervals>*** with a range of values between 1 and 96. (Interval 1 is the interval which began 24 hours ago.) For example:

```
ProCurve# show interfaces e1 1/1 performance-statistics 74-76
```

A screen displays, showing statistics during the numbered intervals. Figure 1-26 shows the performance statistics for a T1 line.

```
Interval 74 Performance Statistics:
    0 Errored Seconds, 0 Bursty Errored Seconds
    0 Severely Errored Seconds, 0 Severely Errored Frame Seconds
    0 Unavailable Seconds, 0 Path Code Violations
    0 Line Code Violations, 0 Controlled Slip Seconds
    0 Line Errored Seconds, 0 Degraded Minutes
  Interval 75 Performance Statistics:
    0 Errored Seconds, 0 Bursty Errored Seconds
    0 Severely Errored Seconds, 0 Severely Errored Frame Seconds
    0 Unavailable Seconds, 0 Path Code Violations
    0 Line Code Violations, 0 Controlled Slip Seconds
    0 Line Errored Seconds, 0 Degraded Minutes
  Interval 76 Performance Statistics:
    0 Errored Seconds, 0 Bursty Errored Seconds
    0 Severely Errored Seconds, 0 Severely Errored Frame Seconds
    0 Unavailable Seconds, 0 Path Code Violations
    0 Line Code Violations, 0 Controlled Slip Seconds
    0 Line Errored Seconds, 0 Degraded Minutes
```

**Figure 1-26. show interfaces t1 performance-statistics Command**

Alternatively, you can specify the readout to only show a summary of the total statistics over the last 24 hours by entering the **Total-24-hour** option.

The **performance-statistics** command is available only for physical interfaces. To end the display, press **Ctrl+C**.

To see realtime information on a physical or logical interface, enter:

***Syntax:*** show interfaces <*interface*> <*slot*>/<*port*> realtime

or

***Syntax:*** show interfaces <*interface*> <*number*> realtime

For example, to display realtime information about the T1 interface that is installed in slot one, port one, enter:

ProCurve# show interface t1 1/1 realtime

This command displays a readout of the current statistics, which is updated once every second. Figure 1-27 shows the **realtime** command screen for a T1 interface.

To pause the update, press **f**. To resume the update, press **r**. To leave the realtime screen, press **Ctrl+C**.

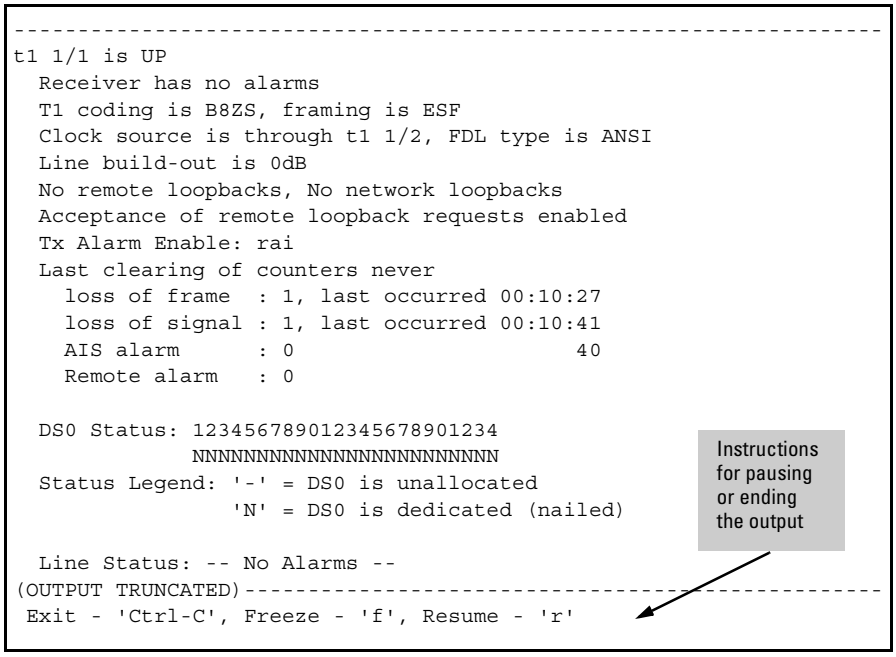


**Figure 1-27. show t1 1/1 realtime Command**

The **show event** command displays the event-history log. The event-history is a log of the dates, times, and description of events such as connections going up or down or attacks blocked by the Secure Router OS firewall.

Many **show** commands also have options that allow you to focus or specify the display. For a list of available options for a specific **show** command, enter the command at the CLI and press **?**.

## Undebug

This command disables a **debug** command. To turn off all currently active **debug** commands, enter **undebug all**.

## Write

This command is a file management command that manages the running-config file.

- **write memory**. This command is similar to the **copy** command. Entering **write memory** will save the running-configuration to the startup-configuration. In J03_01.biz and later, the running-config will automatically save

to the compact flash card, if present, as startup-config. Otherwise the running-config will be saved as startup-config on the router's internal flash.

- **write erase**. This command erases the startup-config. If you have a compact flash card, the startup-config is erased from cflash. If you are running the AutoSynch feature, 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.
- **write network**. This command saves the running-config to a TFTP server. Enter a filename meaningful to you when you are prompted with **Destination filename?**.
- **write terminal**. This command is similar to the **show running-config** command; it displays the current running-configuration in the CLI.

## 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** from the enable mode context. This will prepare the 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 1-75 for more information on performing these tasks. (When following the steps for copying a file, replace ***<filename>*** with showtech.txt.)

**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 compact flash.

The showtech.txt file contains a readout of many of the **show** commands:

- **show version**
- **show modules**
- **show cflash**
- **show run verbose**
- **show interfaces**
- **show atm pvc**

- **show dial-backup interfaces**
- **show dialin**
- **show frame-relay lmi**
- **show frame-relay pvc**
- **show ip bgp neighbors**
- **show ip bgp neighbor summary**
- **show ip ospf neighbor**
- **show ip ospf neighbor summary-add**
- **show ip route**
- **show bridge**
- **show spanning-tree**
- **show ip interfaces**
- **show connections**
- **show arp**
- **show ip traffic**
- **show tcp info**
- **show ip protocols**
- **show ip mroute**
- **show ip access-lists**
- **show event-history**
- **show output-startup**
- **show processes cpu**
- **show buffers**
- **show buffers users**
- **show memory heap**
- **show debugging**

To display the contents of a showtech.txt file, enter **show file [flash | cflash] showtech.txt** from the enable mode context.

This readout allows a network administrator to pinpoint a router configuration problem without a connection to the router.

You can also specify the **show tech** command readout be displayed to the CLI instead of generating and saving the showtech.txt file to flash memory. To display the readout to the screen, use the **terminal** option.

***Syntax:*** show tech [terminal]

## Updating the Boot Code

When applying a new boot configuration file, enter **boot** as the destination of a **copy** command. This command copies a file to the boot sector. For example, if you are upgrading from J05.biz to J06_03.biz, you might enter:

```
ProCurve# copy flash J06_03-boot.biz boot
```

The resulting text explains that other router tasks will be halted while the boot code is upgraded. See Figure 1-28.

```
Upgrading boot code is a critical process that cannot be interrupted.
If something were to happen and the process was not able to be completed,
it would render your unit inoperable. It is for this reason that during
a bootcode upgrade, all other system tasks will be halted. This means
packets will not be routed, and all console sessions will not respond
during the upgrade process. Once this process finishes, the system
will function as it did before. This process will take approximately
20 seconds.
Do you want to proceed? [yes/no] <-- Enter y
```

**Figure 1-28. Upgrading Boot Code**

Enter **y**. The router then begins to update the boot sector code with the file you specified. The output shown in Figure 1-29 is displayed.

```
WARNING!! A bootcode upgrade has been initiated. Your session will
become nonresponsive for the duration of the upgrade (approx. 20
seconds). A message will be sent when the upgrade is completed.
Reading 324883 bytes of code, stand by . . .
Image is compressed, inflating . . . . . .
. . . . . .
Verifying image
Erasing boot sector
Programming boot sector
Success!!!
Bootcode upgrade process done. Your session should function normally.
Success!!!!
ProCurve#
```

**Figure 1-29. Successfully Upgraded Boot Code**

# Global Configuration Mode Commands

From enable mode, access the global configuration mode context by entering **configure terminal**. It is from this mode context that you enter the commands to configure the router; most of the commands in the global configuration mode context are discussed in the various chapters included in this guide. This section explains how to create an enable mode password, activate the AutoSynch™ technology, and configure access to the Web browser interface. For information on how to configure a particular router interface or function, see the "Table of Contents" in either this *Guide* or the *Advanced Management and Configuration Guide*.

## hostname Command

It is often useful to give the router a name that helps to distinguish it from other routers in your network. To change the router's hostname, enter the following command from the global configuration mode context:

ProCurve(config)# hostname <*hostname*>

## autosynch Command

The AutoSynch™ feature is used with a compact flash card. Enabling AutoSynch technology 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, move to the global configuration mode context and enter:

ProCurve (config)# autosynch-mode

The CLI should display:

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

To disable the **autosynch** command, use the **no** command:

ProCurve(config)# no autosynch-mode

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

## SafeMode

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 AutoSynch functioning. 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 function, if previously enabled, will automatically re-enable 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!

After SafeMode is enabled, you or any other 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. For more information on using a text editor to edit router configurations, see "Configuration File Transfer Using the Console Port" on page 1-78, "Configuration File Transfer Using a TFTP Server" on page 1-80, or "Configuration File Transfer Using a Compact Flash Card" on page 1-83.

**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.

# 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 display the available command syntax for any command in the CLI.

The **?** character displays information about the available commands and options available to those commands in your current CLI 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 context 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. The following is an example:

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

## Editing Commands

The router's CLI supports basic editing functions that move the cursor through the command line and allow you to cycle through previous commands. Table 1-9 describes the Secure Router OS CLI editing commands.

**Table 1-9. 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 (**Home**) |
| **Ctrl**+**E** | move to the end of the line (**End**) |
| **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 by 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 1-9 for a list of keystrokes that move the cursor within the command line.

**Tab.** The **Tab** key is a shortcut key. 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 from other available commands. A good way to learn how many characters you must enter for a particular command 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**. The basic mode context includes 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 also recognizes the truncated command.

### no

In the enable and configuration mode contexts, typing the word **no** before a command negates that command. For example, if you want to stop event notices from displaying to the CLI screen, enter **no events**.

### do

If you need to execute an enable mode command from a configuration mode context, type **do** before you enter the command. The **do** command allows you to stay in your current mode context while executing other mode context commands. For example, to display the status of a physical interface while configuring its logical interface, enter:

***Syntax:*** do show interfaces <*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 in the ATM interface configuration mode context and entered **exit**, you would return to the global configuration mode context.

When you enter the **exit** command in the global configuration mode context, you return to the enable mode context and 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 in the router's running-configuration file. If the router were powered down, the running config, and any changes that you have not saved, would be lost.

Save your current configuration by entering either **write memory** or **copy run startup** from the enable mode context.

## Bootstrap Mode Context

The bootstrap mode context allows you access your router when a problem with the software, or a forgotten password, prevents you from accessing it through a console session. Bootstrap mode is a temporary measure to allow you enough access to the router to restore it to proper operation.

The ProCurve Secure Router automatically enters the bootstrap mode context if it cannot locate a valid Secure Router OS or if the Secure Router OS has been corrupted. You can also access the bootstrap mode by pressing **Esc** during the first five seconds of the startup process. During the startup process, the screen will display a countdown, alerting you to how much time you have left to access the bootstrap mode context.

You may want to access the bootstrap mode context if you need to replace corrupted software, cannot remember the system password, or have made configurations that have locked you out of the router. For security, the bootstrap mode context is available only through the console port and cannot be accessed through the Web browser interface.

When you enter the bootstrap mode context, this CLI prompt will display:

bootstrap#

The commands available in bootstrap mode are limited to those related to helping you to successfully boot the router. The following is a list of some of the bootstrap mode commands.

**Boot.** This command allows you to configure the software and configurations booted by the router.

***Syntax:*** boot [cflash <*filename*> | flash <*filename*> | config {flash | cflash} <*filename*> | system {flash | cflash} <*filename*> | <*filename*>] [<*backup boot file location*> <*backup filename*>]

To set the Secure Router OS software that you want the router to use to boot, enter:

***Syntax:*** boot system [flash | cflash] <*filename*> [<*backup location*> <*backup filename*>]

For example:

bootstrap# boot system cflash SROS.BIZ flash SROS.BIZ

To set the configuration file that you want the router to load, enter:

***Syntax:*** boot config [flash | cflash] <*filename*>

For example:

bootstrap# boot config cflash startup-config flash startup-config.bak

After you configure the boot software settings, enter **reload** or **boot** to reboot the server.

Use the **boot [cflash | flash] *<filename>*** option to immediately boot the router using the specified file. To set the backup boot code, replace ***<backup filename>*** with the name of the file you want the router to boot with in case the primary boot file you specified is unavailable or corrupted. Replace ***<backup boot file location>*** with **flash** or **cflash**.

**Bypass.** This command allows you to bypass passwords and configurations. If you are locked out because you have forgotten a console or enable password, you can reboot the system with the following commands:

```
bootstrap# bypass passwords
bootstrap# boot
```

This command will reboot the ProCurve Secure Router using the startup-config but with all passwords disabled.

If you inadvertently make configuration changes that lock you out of the router, you may need to bypass the startup-config to keep yourself from being locked out permanently. You can reboot the router using the default settings by entering the following commands:

```
bootstrap# bypass startup-config
bootstrap# boot
```

**Replacing Corrupted Software.** If the Secure Router OS software is invalid or corrupted, you need to load new software. However, the Secure Router OS may be corrupted to the point that you can no longer access the CLI or Web browser interface to upgrade it. You can upgrade the Secure Router OS software from the bootstrap mode by completing the following steps:

1. Configure an IP address for the Ethernet 0/1 interface by entering:

   bootstrap# ip address <*A.B.C.D*> <*subnet mask*>

   In this mode, the subnet mask must be in ***<A.B.C.D>*** format. The router will not accept a prefix length notation.

2. Copy the Secure Router OS software from a TFTP server by entering:

   bootstrap# copy tftp flash
   Address of remote host? <*A.B.C.D*>

   Source of filename? J06_03.biz
   Destination filename? J06_03.biz

   You can also copy the Secure Router OS software from a compact flash card.

   bootstrap# copy cflash <*filename*> flash [<*filename*>]

3. If your router uses the standard boot process, you should copy the new software as SROS.BIZ to both the compact flash memory (if your router uses a compact flash card) and the internal flash.

   bootstrap# copy flash J06_03.biz cflash SROS.BIZ
   bootstrap# copy flash J06_03.biz flash SROS.BIZ

4. Alternatively, you can enter the **boot system** command and specify the new Secure Router OS software by entering:

   ***Syntax:*** boot system [flash | cflash] <*filename*>

   bootstrap# boot system flash J06_03.biz

   This option, however, is not recommended because you must then enter a new **boot system** command whenever you upgrade the router's software.

5. Enter **reload** or **boot** to reboot the system.

**Note**

A quicker and easier way to replace corrupted software is to make sure that you have an uncorrupted backup copy of the Secure Router OS on compact flash. If you have a compact flash card with the good copy of the Secure Router OS, you only need to insert it into the router and boot it. Then copy the uncorrupted version to flash and erase the corrupt version.

# Troubleshooting

## Compact Flash

Compact flash performance can vary greatly between vendors. If there seems to be a delay when the ProCurve Secure Router saves changes to the compact flash card, the Secure Router OS is still functioning, though at times it may seem to be in a suspended state.

If your router does not have a dedicated compact flash card, you will need to copy needed files to the router's internal flash memory if you want to continue to use these files and configurations. To save a compact flash file to the router's internal flash, access the enable mode context and enter:

***Syntax:*** copy <*source*> <*filename*> <*destination*> <*filename*>

For example:

```
ProCurve# copy cflash SROS.BIZ flash SROS.BIZ
```

If you use the **show tech** command and intend to transport the file on your compact flash card, you will need to save the file to the compact flash card. From the enable mode context, enter:

```
ProCurve# copy flash showtech.txt cflash showtech.txt
```

## AutoSynch™ Error Messages

If the router is displaying AutoSynch error messages or messages that your files are not synchronized, you may need to do some file management tasks to get it up and running.

The **autosynch** command synchronizes files from compact flash to flash. It is very important to ensure that you have the current and proper SROS.BIZ and startup-config files on compact flash. Otherwise, once synchronization begins, the version of SROS.BIZ or startup-config on compact flash will be copied over the file on flash.

Table 1-10 is a short list of AutoSynch error messages.

**Table 1-10. AutoSynch™ Error Messages**

| Error Message | Action |
|---|---|
| compact flash removed | Make sure the compact flash card is firmly mounted in the compact flash slot |
| CFLASH startup-config does not exist | From the enable mode context, enter **write memory**. |
| CFLASH SROS.BIZ does not exist | From the enable mode context, enter **copy fl SROS.BIZ cfl SROS.BIZ**. |
| CFLASH startup-config not synched | Enter **autosynch** from the enable mode context. |

If the router is reporting that the compact flash card is removed, check the back panel to be sure that the compact flash card is firmly mounted in the slot.

Even if you have identical copies of SROS.BIZ on both flash and compact flash, the router will not be able to report that SROS.BIZ is synched until there are synchronized copies of startup-config on compact flash and flash. Both locations must have files with exactly the same filename.

Because the router always synchronizes files from compact flash to internal flash memory, it will report error messages if you do not have a copy of the SROS.BIZ or startup-config files on compact flash.

Copy the missing file from flash to cflash by entering the following commands from the enable mode context:

```
ProCurve# copy flash SROS.BIZ cflash SROS.BIZ
ProCurve# write memory
```

Then enter **autosynch** from the enable mode context to synchronize the files.

**Note**

During the AutoSynch synchronization process, do not remove the compact flash card. Wait for state completion.

If the router is reporting that the files are not synchronized after you have ensured that there are copies of SROS.BIZ and startup-config on the compact flash card, check the filenames.

**Note**

Filenames are case sensitive. SROS.biz is not the same file as SROS.BIZ. It is important that the filenames on the compact flash card are exactly correct.

**Caution**

Be very careful doing any kind of file management with the startup-config and SROS.BIZ files while the **autosynch** command is enabled. If you erase either the startup-config file or SROS.BIZ file from compact flash, the file will also be erased from the internal flash.

If you have managed to erase the SROS.BIZ file from both flash and compact flash, you can create the file by entering this command from the enable mode context:

```
ProCurve# copy flash J0X_0X.biz flash SROS.BIZ
```

Pay special attention to the filenames.

If you have erased the startup-config, entering **write memory** from the enable mode context will create a startup-config file and save it to compact flash.

## Using the reload in Command

When you are configuring the ProCurve Secure Router, 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 after a set time period has elapsed, 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 to countdown until the router reboots. You can specify a three-digit number. Replace ***<hhh:mm>*** with a countdown time such as 1:15 (1 hour and 15 minutes).

For example, if you wanted to set the router to reboot in 3 hours, you would enter:

```
ProCurve# reload in 3:00
```

or

```
ProCurve# reload in 180
```

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 while you are doing a delicate configuration and using the **reload in** command, you must not save the running-config to the startup-config (by entering either **write memory** or **copy run start**). Otherwise, the ProCurve Secure Router will load these configurations when it reboots.

To cancel the reload, enter:

```
ProCurve# reload cancel
```

**Note**

SafeMode automates this process if you are configuring the router using a Telnet or SSH session. (See “SafeMode” on page 1-62.)

# 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.

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 substitute the default. Problem commands will trigger an error message during bootup.

It is not necessary to re-edit the configuration in a text editor to repair a problem; simply enter the pertinent command in the CLI. View 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 1-30. Boot Error Messages**

The error messages in Figure 1-30 were displayed during bootup. In this particular case, the startup-config file has VPNs configured, and the router that is booting does not have the IPSec VPN module that enables these commands. The VPN commands are reported as errors.

You can use error messages like these to locate and troubleshoot a problem in the router's configuration.

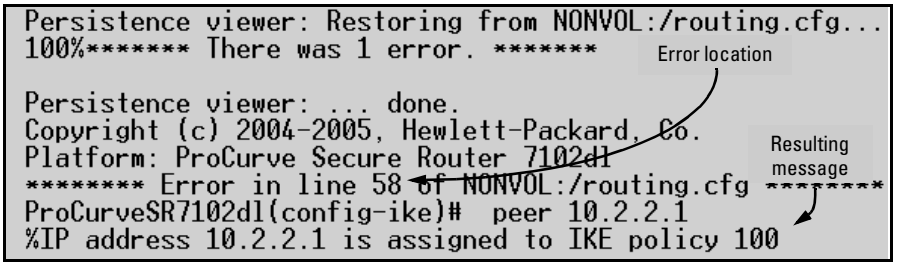


**Figure 1-31. Using Boot Error Messages to Target a Configuration Problem**

The line number given in the error message is the line number in the running-config. You can use this information to locate and 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 line, the command, and the resulting error message, as shown in Figure 1-31. 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 entering the appropriate configuration context and re-entering the command using the error report as a guide.

For example, in Figure 1-31 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, you should configure the IKE policy for a different peer.

## Creating and Transferring Configuration Files

To create a configuration file, begin by creating a base configuration on an originating router. Save the base configuration by entering **copy running-config *<destination location>* *<destination filename>*** or **write memory** from the enable mode context.

If you do not want the base router to use the base configuration, you should save the base configuration as a .cfg or .txt file. From the enable mode context, enter:

ProCurve# copy flash running-config <*destination location*> <*destination filename*>

If you entered **write memory** and are running the AutoSynch function, the configuration is saved as the startup-config file on the flash and compact flash memories. If you have a compact flash card but are not running the AutoSynch function, this command will save the configuration as startup-config on the compact flash card. If you do not have a compact flash card in your router, the file is saved in internal flash as the startup-config file.

## Configuration File Transfer Using the Console Port

In order to complete these steps, you must establish a console session with the ProCurve Secure Router.

1. Create a base configuration.

   Use either the router's factory defaults or another router's configuration as a base. This can be the contents of the startup-config file or the current running-configuration. Display this configuration from the enable mode context.

   ***Syntax:*** show file <*location*> <*filename*>

   ProCurve# show file cflash startup-config
   or
   ProCurve# show running-config verbose

2. Copy the text.

   Use your mouse to highlight the resulting display in the terminal session window. Copy this text either by pressing **Ctrl+C**, right-clicking the mouse and clicking *Copy*, or by clicking *Edit* > *Copy* in the window.

   Paste the copied text into a text editor program such as Notepad.

3. Edit the configuration.

   Change the configuration as needed. Adjust IP addresses, hostnames, and other settings.

4. Copy the edited text.

   Highlight the edited configuration in the text editor. Copy the highlighted text either by pressing **Ctrl+C**, right-clicking the mouse and clicking *Copy*, or clicking *Edit* > *Copy* in the window.

5. Save the edited configuration on the router.

   On the router you are configuring, enter the enable mode context. Then enter the following from the enable mode context:

   ***Syntax:*** copy console flash <*destination filename*>

   ```
   ProCurve# copy console flash configuration.txt
   Enter text to be saved to "configuration.txt"
       Type CTRL+D to finish
   ```

   Replace ***<destination filename>*** with the name you want to give this file.

   When the message **Enter text to be saved to "configuration.txt", Type CTRL+D to finish** appears, paste the text into the terminal session window. You may need to right-click the mouse and click *Paste to host*. Press **Ctrl+D** after the text has been entered.

   The text is saved as a file in the location you specified and with the filename you specified.

6. Erase files that may conflict with the new configuration.

   Enter **show flash** from the enable mode context. If there are files named startup-config or startup-config.bak, erase them:

   ```
   ProCurve# erase flash startup-config
   Deleted NONVOL:/startup-config
   ProCurve# erase flash startup-config.bak
   Deleted NONVOL:/startup-config.bak
   ```

   Do the same for compact flash by entering **show cflash** and erasing any startup-config files.

   ```
   ProCurve# erase cflash startup-config
   Deleted CFLASH:/startup-config
   ProCurve# erase cflash startup-config.bak
   Deleted CFLASH:/startup-config.bak
   ```

   Erasing the startup-config files will return the router configurations to the factory defaults.

7. Install the configuration.

   Copy the edited configuration file to startup-config.

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

   ProCurve# copy flash configuration.txt flash startup-config

   The router will create the startup-config file and save the edited configuration to the file.

8. Reboot the router.

   Enter **reload** from the enable mode context. When it prompts you to save the system configuration, press **n**.

**Note**

Be careful. If you press **y** when asked to save the system configuration, the new startup configuration you just entered will be erased and replaced by the current running configuration.

   Press **y** when asked whether you want to proceed.

   The router will boot up using the new configuration.

## Configuration File Transfer Using a TFTP Server

1. Create a base configuration. Then copy the base configuration to a file.

   ***Syntax:*** copy <*source*> <*base config filename*> <*destination*> <*destination filename.txt*>

   For example, you might enter:

   ProCurve# copy flash startup-config flash routerB.txt

   Replace ***<source>*** with the location of the base configuration file. If you have a compact flash card and the file is saved on compact flash, enter **cflash**. Otherwise, enter **flash**. Because you will be editing this file in a text editor, give the file a .txt extension.

2. Upload the file to the TFTP server.

   ***Syntax:*** copy <*source location*> tftp

   ```
   ProCurve# copy flash tftp
   Address of remote host? 192.168.100.2
   Source filename? routerB.txt
   Destination filename? [routerB.txt]
   ```

   After you enter **copy *<source location>* tftp** from the enable mode context, the router will prompt you for the information it needs to successfully complete the TFTP file transfer. When prompted, enter the IP address of the TFTP server that is to receive the file. Then enter the filename of the configuration file. When asked for the destination filename, you can either rename the file by entering the desired filename or keep the same name by pressing **Enter**.

**Note**

Filenames are case sensitive. When copying a file, be sure to enter the filename exactly.

3. Open the file in a text editor.

   Once the file has been successfully uploaded into a TFTP server, you can open the file using a text editor such as Notepad.

4. Enter the changes.

   Using the text editor, change the configurations that need to be customized. For example, you may need to change the IP addresses, hostname, and other configurations to suit the destination router. Save the edited configuration file back into the TFTP server.

5. Initiate a session with the router on which you want to install the customized configuration.

6. Erase files on the target router that may conflict with the new configuration.

   Make sure that the internal flash on the target router does not include a backup startup-config.

   ```
   ProCurve# show flash
   ProCurve# show cflash
   ```

   If there is a startup-config.bak, erase it.

```
ProCurve# erase flash startup-config.bak
Deleted NONVOL:/startup-config.bak
ProCurve# erase cflash startup-config.bak
Deleted CFLASH:/startup-config.bak
```

To be sure that old configurations do not interfere with the new configuration, erase any startup-config files. This will reset the router to its factory defaults.

```
ProCurve# erase flash startup-config
Deleted NONVOL:/startup-config
ProCurve# erase cflash startup-config
Deleted CFLASH:/startup-config
```

7. Upload and apply the edited configuration file to the destination router.

   Configure the destination router to upload TFTP files. In most cases, this will involve configuring a connection between the router and the TFTP server.

   After you have configured access to the TFTP server from the destination router, enter the enable mode context and enter:

   ***Syntax:*** configure network

   ```
   ProCurve# configure network
   Address of remote host? 192.168.100.2
   Source filename? routerB.txt
   Initiating TFTP transfer . . .
   Received 1044 bytes.
   Transfer complete.

   Opening and applying file . . .

   ProCurve2#
   ```

8. Save the new configuration.

   The **configure network** command saves the configuration to running-config. To preserve this configuration, you need to save the running-config as the startup-config.

   ***Syntax:*** write memory

   The router will now load and use the current configuration when it is booted.

## Configuration File Transfer Using a Compact Flash Card

1. Copy and rename the base configuration.

   ***Syntax:*** copy <*source*> <*base configuration name*> <*destination*> <*destination filename.txt*>

   For example, if your base configuration were the router's startup-config, you would enter:

   ProCurve# copy cflash startup-config cflash routerB.txt

   Replace ***<source>*** with the location of the base configuration file. Because you will be editing this file in a text editor, give the destination filename a .txt extension.

**Note**

Filenames are case sensitive. When copying a file, be sure to enter the filename exactly.

2. Move the file to a text editor.

   Remove the compact flash card from the router and put in into the compact flash card slot on your terminal. Open the configuration file in a text editor such as Notepad.

3. Enter the configuration changes.

   Using the text editor, change the configurations that need to be customized. For example, you may need to change the IP addresses, hostname, and other configurations to suit the destination router.

   Save the edited configuration to the compact flash card. Eject the card.

**Note**

If you are using a dedicated compact flash card on this router, you can simply name the edited configuration startup-config. As long as the destination router uses the standard boot process, the new configuration will load when you install it in the destination router and reboot it. Otherwise, you can follow the steps below.

4. Insert the compact flash card into the destination router's compact flash slot in the rear of the router.

5. Open a session with the destination router and erase files that may conflict with the new configuration.

   Make sure there are no startup-configuration files on the router's internal flash or compact flash. Backup files for the startup-config can also interfere with the installation of the new configuration.

   ```
   ProCurve# show cflash
   ```

   If you see files called startup-config.bak or startup-config, erase them.

   ```
   ProCurve# erase cflash startup-config.bak
   Deleted CFLASH:/ startup-config.bak
   ProCurve# erase flash startup-config.bak
   Deleted NONVOL:/ startup-config.bak
   ```

   Unless you saved the edited configuration as startup-config on the compact flash card, you will need to erase the existing startup-config files. These files can interfere with the installation of the edited configuration.

   ```
   ProCurve# erase cflash startup-config
   Deleted CFLASH:/ startup-config
   ProCurve# erase flash startup-config
   Deleted NONVOL:/ startup-config
   ```

   Erasing the startup files will reset the router to its factory defaults.

6. Install the edited configuration.

   From the enable mode context, load the edited configuration file and rename it "startup-config":

   ***Syntax:*** copy cflash <*filename*> cflash startup-config

   ```
   ProCurve# copy cflash routerB.txt cflash startup-config
   ```

7. Reboot the router.

   Enter **reload** from the enable mode context. When the Secure Router OS prompts you to save the system configuration, press **n**.

**Note**

Be careful. If you press **y** when asked to save the system configuration, the new startup configuration you just entered will be erased and replaced by the current running configuration.

Press **y** when asked whether you want to proceed. The router will boot up using the new configuration.

# Using the FTP Server on the ProCurve Secure Router

The J06_03 release of the Secure Router OS includes an FTP server, which you can use to store files and allow network administrators to download these files to other devices. The FTP server can use the router's internal flash or compact flash as its data store.

To enable the FTP server, enter the following command from the global configuration mode context:

***Syntax:*** ip ftp server [default-filesystem {flash | cflash}]

Enter **default-filesystem flash** to use the router's internal flash as the FTP server's data store. This is the default setting. Enter **default-file system cflash** to use compact flash as the FTP server's data store.

To allow network administrators to copy files to and from the FTP server, enter the following command from the global configuration mode context:

***Syntax:*** username <*username*> password <*password*>

If you have enabled the HTTP or HTTPS server, network administrators can enter this username and password to access the router's Web browser interface as well. For more information about this command, see *Chapter 2: Controlling Management Access to the ProCurve Secure Router*. For more information about enabling the HTTP or HTTPS server, see "Accessing the Web Browser Interface" on page 1-11.

## Troubleshooting the FTP Server

If users experience problems copying files to or from the FTP server, you can enable debug messages for the FTP server. From the enable mode context, enter:

***Syntax:*** debug ip ftp-server

Figure 1-32 shows debug messages that are displayed when a user enters the wrong password.

```
ProCurve# FTP: USER command - Password required for 'procurve'.
FTP: USER command - Login incorrect.
FTP: USER command - Password required for 'procurve'.
FTP: USER command - Login incorrect.
```

**Figure 1-32. Debug Messages for the FTP Server**

# Enabling the SNTP Server on the ProCurve Secure Router

The J06_03 release of the Secure Router OS also includes a Simple Network Time Protocol (SNTP) server. A simplified version of the Network Time Protocol (NTP), SNTP provides a client-server architecture for synchronizing the clocks on network devices. As an SNTP server, the ProCurve Secure Router can respond to clients' requests for the current time.

To enable the SNTP server on the ProCurve Secure Router, enter the following command from the global configuration mode context:

***Syntax:*** ip sntp server

The ProCurve Secure Router can then accept time requests from clients.

## Configuring the ProCurve Secure Router as an SNTP Client

The ProCurve Secure Router can also function as an SNTP client. You can configure:

- the host name of the SNTP server that the router should contact for the current time
- the version of SNTP to use—version 1, 2, or 3

To configure the host name or IP address of the SNTP server, enter:

***Syntax:*** sntp server [<*hostname*>| <*IP address*> | version <*version number*>]

Include the ***<hostname>*** *or* ***<IP address>*** option to specify the SNTP server.

Include **version 1, 2,** or **3** to specify the version of NTP that the ProCurve Secure Router should use. If you do not specify a version, the router uses version 1 by default.

For example, you might want to configure the ProCurve Secure Router to contact a National Institute of Standards and Technology (NIST) Internet time server to request the current time. (For more information about NIST Internet time servers, visit *http://tf.nist.gov/service/time-servers.html.)* To set the SNTP server to the Internet time server time.nist.gov, enter:

```
ProCurve(config)# sntp server time.nist.gov
```

The router will use NTP version 1, the default setting, because you did not enter a version number.

To specify the same SNTP server but use NTP version 2, you would enter:

```
ProCurve(config)# sntp server time.nist.gov version 2
```

Use the no form of this command to remove an SNTP server setting from the router's configuration.

***Syntax:*** no sntp server [<*hostname*>| <*ip address*> | version <*version number*>]

## Configuring a Source Address for the SNTP Server

You may want to configure a source address for the SNTP traffic that the ProCurve Secure Router sends. From the global configuration mode context, enter:

***Syntax:*** ip sntp source-interface <***interface***>

Replace the ***<interface>*** option with the interface that you want to provide the source address for SNTP traffic. Supported interfaces include:

- demand ***<number>***
- ethernet ***<slot>***/***<port>***
- frame-relay ***<number>***
- hdlc ***<number>***
- loopback ***<number>***
- tunnel ***<number>***

For example, if you wanted the Ethernet 0/2 interface to provide the IP address for SNTP traffic, you would enter:

```
ProCurve(config)# ip sntp source-interface ethernet 0/2
```

## Viewing SNTP Settings

To view the current SNTP settings and the status of the SNTP client or server, enter the following command from the enable mode context:

***Syntax:*** show sntp

## Troubleshooting SNTP

To troubleshoot SNTP, enter the following command from the enable mode context:

***Syntax:*** debug sntp [client | server]

If you want to enable debug messages for all SNTP activity on the ProCurve Secure Router, simply enter **debug sntp.** Include the **client** option if the router is acting as an SNTP client, and include the **server** option if you have enabled the SNTP server.

# Quick Start

This section provides the instructions you need to quickly access the ProCurve Secure Router CLI and establish a console session.

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 "Contents" on page 1-1 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 computer 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
   ```

For information about configuring Telnet, SSH, or HTTP access, see *Chapter 2: Controlling Management Access to the ProCurve Secure Router*. For information about configuring Web access to the router, see "Enabling Access to the Web Browser Interface" on page 14-5.

## Enabling the FTP Server

1. To enable the FTP server, enter the following command from the global configuration mode context:

   ***Syntax:*** ip ftp server [default-filesystem {flash | cflash}]

   Enter **default-filesystem flash** to use the router's internal flash as the FTP server's data store. This is the default setting. Enter **default-file system cflash** to use compact flash as the FTP server's data store.

2. To allow users to copy files to and from the FTP server, enter the following command from the global configuration mode context:

   ***Syntax:*** username <*username*> password <*password*>

   This command also enables access to the HTTP server, which is used to access the Web browser interface. For more information about this command, see *Chapter 2: Controlling Management Access to the ProCurve Secure Router*.

## Configuring SNTP on the ProCurve Secure Router

The ProCurve Secure Router can be an SNTP server or an SNTP client. To configure SNTP on the router, complete the following steps:

1. To enable the SNTP server on the ProCurve Secure Router, enter the following command from the global configuration mode context:

   ***Syntax:*** ip sntp server

   The ProCurve Secure Router can then accept time requests from clients.

2. To configure the ProCurve Secure Router as an SNTP client, enter the following command from the global configuration mode context:

   ***Syntax:*** sntp server [<*hostname*>| <*IP address*> | version <*version number*>]

   Include the ***<hostname>*** *or* ***<IP address>*** option to specify the SNTP server.

   Include **version 1, 2,** or **3** to specify the version of NTP that the ProCurve Secure Router should use. If you do not specify a version, the router uses version 1 by default.

3. To configure a source address for the SNTP traffic that the ProCurve Secure Router sends, enter the following command from the global configuration mode context:

   ***Syntax:*** ip sntp source-interface <***interface***>

Replace the ***<interface>*** option with the interface that you want to provide the source address for SNTP traffic. Supported interfaces include:

- demand ***<number>***
- ethernet ***<slot>/<port>***
- frame-relay ***<number>***
- hdlc ***<number>***
- loopback ***<number>***
- tunnel ***<number>***