1

Getting Started

Contents

Introduction

This *Access Security Guide* is intended for use with the following switches:

- ProCurve Switch 10G CX4 6400cl-6xg
- ProCurve Switch 10G X2 6400cl-6xg
- ProCurve Switch 5304xl
- ProCurve Switch 5348xl
- ProCurve Switch 5308xl
- ProCurve Switch 5372xl
- ProCurve Switch 4204vl
- ProCurve Switch 4208vl
- ProCurve Switch 4202vl-48G
- ProCurve Switch 4202vl-72
- ProCurve Switch 3400cl-24G
- ProCurve Switch 3400cl-48G

This guide describes how to use the command line interface (CLI), menu interface, and web browser to configure and use the switch security features covered in the following chapters.

For an overview of other product documentation for the above switches, refer to "Product Documentation" on page xvii.

The *Product Documentation CD-ROM* shipped with the switch includes a copy of this guide. You can also download a copy from the ProCurve Networking web site, **www.procurve.com**.

Conventions

This guide uses the following conventions for command syntax and displayed information.

Feature Descriptions by Model

In cases where a software feature is not available in all of the switch models covered by this guide, the section heading specifically indicates which product or product series offer the feature.

For example, (the switch is highlighted here in **bold italics**):

"QoS Pass-Through Mode on the **Series 5300xl and 4200vl Switches**".

Command Syntax Statements

Syntax: ip default-gateway < *ip-addr* >

Syntax: show interfaces [*port-list*]

■　Vertical bars (|) separate alternative, mutually exclusive elements.

■　Square brackets ([ ]) indicate optional elements.

■　Braces (< >) enclose required elements.

■　Braces within square brackets ([< >]) indicate a required element within an optional choice.

■　Boldface indicates use of a CLI command, part of a CLI command syntax, or other displayed element in general text. For example:

   "Use the **copy tftp** command to download the key from a TFTP server."

■　Italics indicate variables for which you must supply a value when executing the command. For example, in this command syntax, *<port-list>* indicates that you must provide one or more port numbers:

   Syntax: aaa port-access authenticator < *port-list* >

Command Prompts

In the default configuration, your switch displays one of the following CLI prompts:

```
ProCurve Switch 6400#
ProCurve Switch 5304#
ProCurve Switch 5308#
ProCurve Switch 4204vl#
ProCurve Switch 4208vl#
ProCurve Switch 3400-24#
ProCurve Switch 3400-48#
```

To simplify recognition, this guide uses ProCurve to represent command prompts for all models. That is:

```
ProCurve#
```

(You can use the **hostname** command to change the text in the CLI prompt.)

Screen Simulations

Figures containing simulated screen text and command output look like this:

```
ProCurve> show version
Image stamp:    /sw/code/build/info
                September 30 2004 13:43:13
                E.08.22
                139
ProCurve>
```

Figure 1-1.   Example of a Figure Showing a Simulated Screen

In some cases, brief command-output sequences appear without figure iden-
tification. For example:

```
ProCurve(config)# clear public-key
ProCurve(config)# show ip client-public-key
show_client_public_key: cannot stat keyfile
```

Port Identity Examples

This guide describes software applicable to both chassis-based and stackable
ProCurve switches. Where port identities are needed n an example, this guide
uses the chassis-based port identity system, such as "A1, "B3-B5", "C7", etc.
However, unless otherwise noted, such examples apply equally to the stack-
able switches, which typically use only numbers, such as "1", "3-5", "15", etc.
for port identities.

Keys

Simulations of actual keys use a bold, sans-serif typeface with square brackets.
For example, the Tab key appears as **[Tab]** and the "Y" key appears as **[Y]**.

Sources for More Information

For additional information about switch operation and features not covered
in this guide, consult the following sources:

■   For information on which product manual to consult on a given software
    feature, refer to "Product Documentation" on page xvii.

N o t e   For the latest version of all ProCurve switch documentation, including Release Notes covering recently added features, visit the ProCurve Networking web site at **www.procurve.com**, click on **Technical support**, and then click on **Product Manuals (all)**.

■ Software Release Notes—Release notes are posted on the ProCurve Networking web site and provide information on new software updates:

   • New features and how to configure and use them

   • Software management, including downloading software to the switch

   • Software fixes addressed in current and previous releases

   To view and download a copy of the latest release notes for your switch, refer to "Getting Documentation From the Web" on page 6.

■ Product Notes and Software Update Information—The printed *Read Me First* shipped with your switch provides software update information, product notes, and other information. A printed copy is shipped with your switch. For the latest version, refer to "Getting Documentation From the Web" on page 6.

■ Installation and Getting Started Guide—Use the *Installation and Getting Started Guide* shipped with your switch to prepare for and perform the physical installation. This guide also steps you through connecting the switch to your network and assigning IP addressing, as well as describing the LED indications for correct operation and trouble analysis. A PDF version of this guide is also provided on the *Product Documentation CD-ROM* shipped with the switch. And you can download a copy from the ProCurve Networking web site. (See "Getting Documentation From the Web" on page 6.)

■ Management and Configuration Guide—Use the *Management and Configuration Guide* for information on:

   • Using the command line interface (CLI), Menu interface, and web browser interface

   • Learning how memory operates in the switch

   • IP addressing

   • Time protocols

   • Port configuration options

   • Interaction with network management applications

   • File transfers, including operating systems, configuration files, ACL command files, and diagnostic data files

   • Monitoring and troubleshooting switch software operation

- MAC addressing
- Daylight time rules

■ Advanced Traffic Management Guide—Use the *Advanced Traffic Management Guide* for information on:

- VLANs: Static port-based and protocol VLANs, and dynamic GVRP VLANs
- Multicast traffic control (IGMP) and Protocol-Independent Multicast routing (PIM-DM)
- Spanning-Tree Operation: 802.1D (STP), 802.1w (RSTP), and 802.1s (MSTP)
- Meshing
- Quality-of-Service (QoS)
- Access Control Lists (ACLs)
- IP routing
- Static NAT for intranet applications
- XRRP (XL Router Redundancy Protocol)

Getting Documentation From the Web

1. Go to the ProCurve Networking web site at **www.procurve.com.**

2. Click on **Technical support**.

3. Click on **Product manuals**.

4. Click on the product for which you want to view or download a manual.

Figure 1-2.   Example of How To Locate Product Manuals on the ProCurve Networking Web Site

Figure 1-3.   Listing of ProCurve Manuals on the ProCurve Networking Web Site

Online Help

If you need information on specific parameters in the menu interface, refer to the online help provided in the interface.

```
===========================- CONSOLE - MANAGER MODE -========================
                    Switch Configuration - Internet (IP) Service


   Default Gateway : 10.35.204.1
   Default TTL     : 64
                                                          Online Help
   IP Config [DHCP/Bootp] : Manual                         for Menu
   IP Address   : 10.35.204.104
   Subnet Mask : 255.255.240.0


  Actions->   Cancel      Edit      Save      Help
 Display help information.
 Use arrow keys to change action selection and <Enter> to execute action.
```
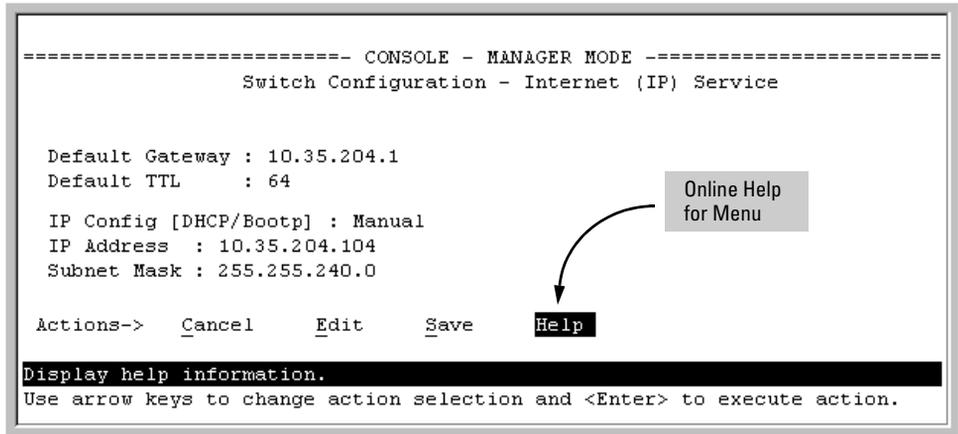
Figure 1-4.   Example of How To Display Online Help for the Menu Interface

■   If you need information on a specific command in the CLI, type the command name followed by "help". For example:

```
ProCurve# write help
Usage: write <memory|terminal>

Description: View or save the running configuration of the switch.

            write terminal - displays the running configuration of the
                             switch on the terminal
            write memory   - saves the running configuration of the
                             switch to flash. The saved configuration
                             becomes the boot-up configuration of the switch
                             the next time it is booted.
```

Figure 1-5.   Example of How To Display Help for a CLI Command

■   If you need information on specific features in the web browser interface use the online help available for the web browser interface. For more information on web browser Help options, refer to the *Management and Configuration Guide* for your switch.

■   If you need further information on Hewlett-Packard switch technology, visit the ProCurve Networking web site at:

   www.procurve.com

Need Only a Quick Start?

IP Addressing. If you just want to give the switch an IP address so that it can communicate on your network, or if you are not using VLANs, ProCurve recommends that you use the Switch Setup screen to quickly configure IP addressing. To do so, do one of the following:

■   Enter **setup** at the CLI Manager level prompt.

    ProCurve# setup

■   In the Main Menu of the Menu interface, select

    8. Run Setup

For more on using the Switch Setup screen, refer to the *Installation and Getting Started Guide* you received with the switch.

To Set Up and Install the Switch in Your Network

Use the ProCurve *Installation and Getting Started Guide* (shipped with your switch) for the following:

■   Notes, cautions, and warnings related to installing and using the switch and its related modules

■   Instructions for physically installing the switch in your network

■   Quickly assigning an IP address and subnet mask, set a Manager password, and (optionally) configure other basic features

■   Interpreting LED behavior

For the latest version of this guide, refer to "Getting Documentation From the Web" on page 6.

Overview of Access Security Features

- **Local Manager and Operator Passwords (page 2-1):** Control access and privileges for the CLI, menu, and web browser interfaces. Includes front-panel security information that allows you to disable or re-enable some of the functions of the Clear and the Reset buttons located on the switch's front panel.

- **Web and MAC Authentication (page 4-1):** Provides user or device authentication through a RADIUS server without requiring the client to use 802.1x supplicant software.

- **TACACS+ Authentication (page 5-1):** Uses an authentication application on a server to allow or deny access to the switch.

- **RADIUS Authentication and Accounting (page 6-1):** Uses RADIUS authentication on a central server to allow or deny access to the switch. RADIUS also provides accounting services for sending data about user activity and system events to a RADIUS server.

- **Secure Shell (SSH) Authentication (page 9-1):** Provides encrypted paths for remote access to switch management functions.

- **Secure Socket Layer (SSL) (page 8-1):** Provides remote web access to the switch via encrypted authentication paths between the switch and management station clients capable of SSL/TLS operation.

- **Port-Based Access Control (802.1X) (page 11-1):** On point-to-point connections, enables the switch to allow or deny traffic between a port and an 802.1x-aware device (supplicant) attempting to access the switch. Also enables the switch to operate as a supplicant for connections to other 802.1x-aware switches. Includes the option of allowing only the device having the first MAC address detected by a port.

- **Port Security (page 12-1):** Enables a switch port to maintain a unique list of MAC addresses defining which specific devices are allowed to access the network through that port. Also enables a port to detect, prevent, and log access attempts by unauthorized devices.

- **MAC Lockdown (page 12-22):** Permanently assigns a device MAC address to a specific port on the switch to restrict a client device to a specific port.

- **MAC Lockout (page 12-30):** Causes the switch to drop traffic carrying a specific MAC address as either a source or destination.

- **Authorized IP Managers (page 13-1):** Allows access to the switch by a networked device having an IP address previously configured in the switch as "authorized".

■ **Key Management System (page 14-1):** Centralizes the mechanisms used to configure and maintain security information for all routing protocols.

ProCurve recommends that you use local passwords together with the switch's other security features to provide a more comprehensive security fabric than if you use only local passwords.

General Switch Traffic Security Guideline

Where the switch is running multiple security options, it implements network traffic security based on the OSI (Open Systems Interconnection model) precedence of the individual options, from the lowest to the highest. The following list shows the order in which the switch implements configured security features on traffic moving through a given port.

1. Disabled/Enabled physical port

2. MAC lockout (Applies to all ports on the switch.)

3. MAC lockdown

4. Port security

5. Authorized IP Managers

6. Application features at higher levels in the OSI model, such as SSH.

(The above list does not address the mutually exclusive relationship that exists among some security features.)

Applications for Access Control Lists (ACLs)

Layer 3 IP filtering with Access Control Lists (ACLs) enables you to improve network performance and restrict network use by creating policies for:

■ **Switch Management Access:** Permits or denies in-band management access. This includes preventing the use of certain TCP or UDP applications (such as Telnet, SSH, web browser, and SNMP) for transactions between specific source and destination IP addresses.)

■ **Application Access Security:** Eliminating unwanted IP, TCP, or UDP traffic in a path by filtering packets where they enter or leave the switch on specific VLAN interfaces.

ACLs can filter traffic to or from a host, a group of hosts, or entire subnets.

Note on ACL Security Use

ACLs can enhance network security by blocking selected IP traffic, and can serve as one aspect of maintaining network security. *However, because ACLs do not provide user or device authentication, or protection from malicious manipulation of data carried in IP packet transmissions, they should not be relied upon for a complete security solution.*

For information on how to apply ACLs in a network populated with ProCurve switches that support the ACL feature, refer to the chapter titled "Access Control Lists (ACLs)" in the *Advanced Traffic Management Guide* for your switch.