

# Getting Started

---

## Contents

Introduction .....	1-2
Overview of Access Security Features .....	1-2
Management Access Security Protection .....	1-3
General Switch Traffic Security Guidelines .....	1-4
Conventions .....	1-5
Feature Descriptions by Model .....	1-5
Command Syntax Statements .....	1-5
Command Prompts .....	1-6
Screen Simulations .....	1-6
Port Identity Examples .....	1-6
Sources for More Information .....	1-7
Need Only a Quick Start? .....	1-8
IP Addressing .....	1-8
To Set Up and Install the Switch in Your Network .....	1-9

## Introduction

This *Access Security Guide* describes how to use ProCurve's switch security features to protect access to your switch. This guide is intended to support the following switches:

- ProCurve Series 2600
- ProCurve Series 2600-PWR
- ProCurve Series 2800
- ProCurve Series 4100gl
- ProCurve Switch 6108

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

The *Product Documentation CD-ROM* shipped with the switch includes a copy of this guide. You can also download a copy from the ProCurve website, <http://www.procurve.com>.

---

## Overview of Access Security Features

The access security features covered in this guide include:

- **Local Manager and Operator Passwords** (page 2-1): Control access and privileges for the CLI, menu, and web browser interfaces.
- **TACACS+ Authentication** (page 4-1): Uses an authentication application on a server to allow or deny access to a switch.
- **RADIUS Authentication and Accounting** (page 5-1): Like TACACS+, uses an authentication application 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 6-1): Provides encrypted paths for remote access to switch management functions.

- **Secure Socket Layer (SSL)** (page 7-1): 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 8-1): 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.
- **Port Security** (page 9-1): 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.
- **Traffic/Security Filters** (page 10-1): Source-Port filtering enhances in-band security by enabling outbound destination ports on the switch to forward or drop traffic from designated source ports (within the same VLAN).
- **Authorized IP Managers** (page 11-1): Allows access to the switch by a networked device having an IP address previously configured in the switch as "authorized".

## Management Access Security Protection

In considering management access security for your switch, there are two key areas to protect:

- Unauthorized client access to switch management features
- Unauthorized client access to the network.

Table 1-1 on page 1-4 provides an overview of the type of protection offered by each switch security feature.

---

**Note**

---

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

**Table 1-1. Management Access Security Protection**

Security Feature	Offers Protection Against Unauthorized Client Access to Switch Management Features					Offers Protection Against Unauthorized Client Access to the Network
	Connection	Telnet	SNMP (Net Mgmt)	Web Browser	SSH Client	
Local Manager and Operator Usernames and Passwords <sup>1</sup>	PtP:	<b>Yes</b>	<i>No</i>	<b>Yes</b>	<b>Yes</b>	<i>No</i>
	Remote:	<b>Yes</b>	<i>No</i>	<b>Yes</b>	<b>Yes</b>	<i>No</i>
TACACS+ <sup>1</sup>	PtP:	<b>Yes</b>	<i>No</i>	<i>No</i>	<b>Yes</b>	<i>No</i>
	Remote:	<b>Yes</b>	<i>No</i>	<i>No</i>	<b>Yes</b>	<i>No</i>
RADIUS <sup>1</sup>	PtP:	<b>Yes</b>	<i>No</i>	<i>No</i>	<b>Yes</b>	<i>No</i>
	Remote:	<b>Yes</b>	<i>No</i>	<i>No</i>	<b>Yes</b>	<i>No</i>
SSH	PtP:	<b>Yes</b>	<i>No</i>	<i>No</i>	<b>Yes</b>	<i>No</i>
	Remote:	<b>Yes</b>	<i>No</i>	<i>No</i>	<b>Yes</b>	<i>No</i>
SSL	PtP:	<i>No</i>	<i>No</i>	<b>Yes</b>	<i>No</i>	<i>No</i>
	Remote:	<i>No</i>	<i>No</i>	<b>Yes</b>	<i>No</i>	<i>No</i>
Port-Based Access Control (802.1X)	PtP:	<b>Yes</b>	<b>Yes</b>	<b>Yes</b>	<b>Yes</b>	<b>Yes</b>
	Remote:	<i>No</i>	<i>No</i>	<i>No</i>	<i>No</i>	<i>No</i>
Port Security (MAC address)	PtP:	<b>Yes</b>	<b>Yes</b>	<b>Yes</b>	<b>Yes</b>	<b>Yes</b>
	Remote:	<b>Yes</b>	<b>Yes</b>	<b>Yes</b>	<b>Yes</b>	<b>Yes</b>
Authorized IP Managers	PtP:	<b>Yes</b>	<b>Yes</b>	<b>Yes</b>	<b>Yes</b>	<i>No</i>
	Remote:	<b>Yes</b>	<b>Yes</b>	<b>Yes</b>	<b>Yes</b>	<i>No</i>

<sup>1</sup> The local Manager/Operator, TACACS+, and RADIUS options (direct connect or modem access) also offer protection for serial port access.

## General Switch Traffic Security Guidelines

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.)

# 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 model is highlighted here in ***bold italics***):

“Web and MAC Authentication for the ***Series 2600/2600-PWR and 2800 Switches***”.

## Command Syntax Statements

**Syntax:** `aaa port-access authenticator < port-list >`  
          [ control < authorized | auto | unauthorized > ]

- 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 4104#  
ProCurve Switch 4108#  
ProCurve Switch 2626#  
ProCurve Switch 2650#  
ProCurve Switch 6108#
```

To simplify recognition, this guide uses `ProCurve` to represent command prompts for all models. For example:

```
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  
              Apr  1 2005 13:43:13  
              G.07.7X  
              520  
ProCurve>
```

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

In some cases, brief command-output sequences appear outside of a numbered figure. For example:

```
ProCurve(config)# ip default-gateway 18.28.152.1/24  
ProCurve(config)# vlan 1 ip address 18.28.36.152/24  
ProCurve(config)# vlan 1 ip igmp
```

## Port Identity Examples

This guide describes software applicable to both chassis-based and stackable ProCurve switches. Where port identities are needed in 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 stackable switches, which for port identities typically use only numbers, such as “1”, “3-5”, “15”, etc.

---

## Sources for More Information

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

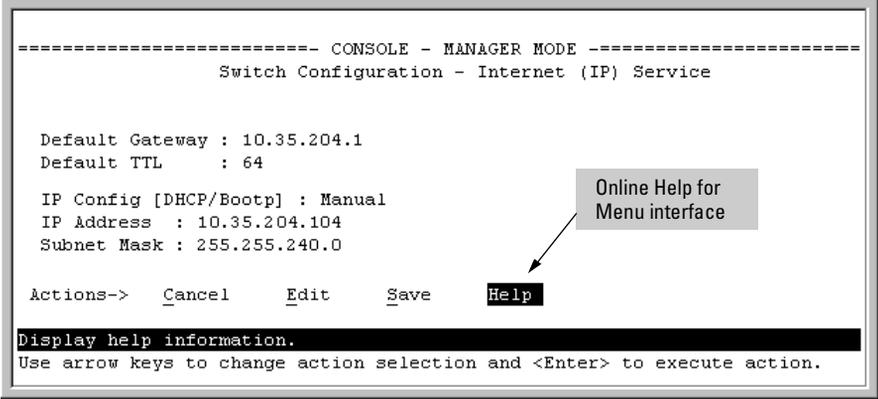
- For information on which product manual to consult on a given software feature, refer to “Product Documentation” on page xi.

---

### Note

For the latest version of all ProCurve switch documentation, including release notes covering recently added features, visit the ProCurve Networking website at <http://www.procurve.com>. Click on **Technical support**, and then click on **Product manuals**.

- For information on specific parameters in the menu interface, refer to the online help provided in the interface. For example:



```
----- CONSOLE - MANAGER MODE -----  
Switch Configuration - Internet (IP) Service  
  
Default Gateway : 10.35.204.1  
Default TTL      : 64  
  
IP Config [DHCP/Bootp] : Manual  
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 1-2. Getting Help in the Menu Interface**

- For 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 1-3. Getting Help in the CLI**

- For information on specific features in the Web browser interface, use the online help. For more information, refer to the *Management and Configuration Guide* for your switch.
- For further information on ProCurve Networking switch technology, visit the ProCurve website at:

<http://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 multiple 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, see the *Installation and Getting Started Guide* you received with the switch.

## To Set Up and Install the Switch in Your Network

---

**Important!**

---

Use the *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, setting a Manager password, and (optionally) configuring other basic features.
- Interpreting LED behavior.

For the latest version of the *Installation and Getting Started Guide* and other documentation for your switch, visit the ProCurve website. (Refer to “Product Documentation” on page xi of this guide for further details.)

— *This page is intentionally unused.* —