

Security Overview

Contents

Introduction	1-2
About This Guide	1-2
For More Information	1-2
Switch Access Security	1-2
Default Configuration Settings and Access Security	1-3
Local Manager Password	1-3
Inbound Telnet Access and Web Browser Access	1-3
SNMP Access (Simple Network Management Protocol)	1-4
Front-Panel Access and Physical Security	1-5
Secure File Transfers	1-5
Other Provisions for Management Access Security	1-6
Authorized IP Managers	1-6
Secure Management VLAN	1-6
TACACS+ Authentication	1-6
RADIUS Authentication	1-6
Network Security Features	1-7
802.1X Access Control	1-7
Web and MAC Authentication	1-7
Secure Shell (SSH)	1-8
Secure Socket Layer (SSLv3/TLSv1)	1-8
Traffic/Security Filters	1-8
Port Security, MAC Lockdown, and MAC Lockout	1-9
Key Management System (KMS)	1-10
Identity-Driven Manager (IDM)	1-10

Dynamic Configuration Arbiter	1-11
Network Immunity Manager	1-12
Arbitrating Client-Specific Attributes	1-13

Introduction

Before you connect your switch to a network, ProCurve strongly recommends that you review the Security Overview beginning on page 1-3. It outlines the potential threats for unauthorized switch and network access, and provides guidelines on how to use the various security features available on the switch to prevent such access. For more information on individual features, see the references provided.

About This Guide

This *Access Security Guide* describes how to configure security features on the switches covered in this guide.

Note

For an introduction to the standard conventions used in this guide, refer to the *Getting Started* chapter in the *Management and Configuration Guide* for your switch.

For More Information

For information on which product manual to consult for a specific software feature, refer to the “Feature Index” on page xiv of this guide.

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

Switch Access Security

This section outlines provisions for protecting access to the switch’s status information and configuration settings. ProCurve switches are designed as “plug and play” devices, allowing quick and easy installation in your network. However, when preparing the switch for network operation, ProCurve strongly recommends that you enforce a security policy to help ensure that the ease in getting started is not used by unauthorized persons as an opportu-

nity for access and possible malicious actions. Since security incidents can originate with sources inside as well as outside of an organization, your access security provisions must protect against internal and external threats while preserving the necessary network access for authorized clients and users.

Default Configuration Settings and Access Security

In its default configuration, the switch is open to unauthorized access of various types. In addition to applying local passwords, ProCurve recommends that you consider using the switch's other security features to provide a more complete security fabric.

Switch management access is available through the following methods:

- Inbound Telnet access and Web-browser access
- SNMP access
- Front-Panel access (serial port access to the console, plus resets and clearing the password(s) or current configuration)

It is important to evaluate the level of management access vulnerability existing in your network and take steps to ensure that all reasonable security precautions are in place. This includes both configurable security options and physical access to the switch hardware.

Local Manager Password

In the default configuration, there is no password protection. Configuring a local Manager password is a fundamental step in reducing the possibility of unauthorized access through the switch's Web browser and console (CLI and Menu) interfaces. The Manager password can easily be set using the CLI **password manager** command, the Menu interface **Console Passwords** option, or the password options under the **Security** tab in the Web browser interface.

Inbound Telnet Access and Web Browser Access

The default remote management protocols enabled on the switch are plain text protocols, which transfer passwords in open or plain text that is easily captured. To reduce the chances of unauthorized users capturing your passwords, secure and encrypted protocols such as SSH and SSL must be used for remote access. This enables you to employ increased access security while still retaining remote client access.

- SSHv2 provides Telnet-like connections through encrypted and authenticated transactions.

- SSLv3/TLSv1 provides remote Web browser access to the switch via encrypted paths between the switch and management station clients capable of SSL/TLS operation.

(For information on SSH, refer to Chapter 6 “Configuring Secure Shell (SSH)”; for details on SSL, refer to Chapter 7, “Configuring Secure Socket Layer (SSL)”.)

Also, access security on the switch is incomplete without disabling Telnet and the standard Web browser access. Among the methods for blocking unauthorized access attempts using Telnet or the Web browser are the following two CLI commands:

- **no telnet-server:** This command blocks inbound Telnet access.
- **no web-management:** This command prevents use of the Web browser interface through http (port 80) server access.

If you choose not to disable Telnet and Web browser access, you may want to consider using RADIUS accounting to maintain a record of password-protected access to the switch. Refer to Chapter 5, “RADIUS Authentication and Accounting” in this guide.

SNMP Access (Simple Network Management Protocol)

In the default configuration, the switch is open to access by management stations running SNMP management applications capable of viewing and changing the settings and status data in the switch’s MIB (Management Information Base). Thus, controlling SNMP access to the switch and preventing unauthorized SNMP access should be a key element of your network security strategy.

General SNMP Access to the Switch. The switch supports SNMP versions 1, 2c, and 3, including SNMP community and trap configuration. The default configuration supports versions 1 and 2c compatibility, which uses plain text and does not provide security options. ProCurve recommends that you enable SNMP version 3 for improved security. SNMPv3 includes the ability to configure restricted access and to block all non-version 3 messages (which blocks version 1 and 2c unprotected operation).

SNMPv3 security options include:

- configuring device communities as a means for excluding management access by unauthorized stations
- configuring for access authentication and privacy
- reporting events to the switch CLI and to SNMP trap receivers

- restricting non-SNMPv3 agents to either read-only access or no access
- co-existing with SNMPv1 and v2c if necessary

For information on SNMP, refer to “Using SNMP Tools To Manage the Switch” in the chapter titled “Configuring for Network Management Applications” in the *Management and Configuration Guide* for your switch.

Front-Panel Access and Physical Security

Physical access to the switch allows the following:

- use of the console serial port (CLI and Menu interface) for viewing and changing the current configuration and for reading status, statistics, and log messages.
- use of the switch’s Clear and Reset buttons for these actions:
 - clearing (removing) local password protection
 - rebooting the switch
 - restoring the switch to the factory default configuration (and erasing any non-default configuration settings)

Keeping the switch in a locked wiring closet or other secure space helps to prevent unauthorized physical access. As additional precautions, you can do the following:

- Disable or re-enable the password-clearing function of the Clear button.
- Configure the Clear button to reboot the switch after clearing any local usernames and passwords.
- Modify the operation of the Reset+Clear button combination so that the switch reboots, but does not restore the switch’s factory default settings.
- Disable or re-enable password recovery.

For the commands used to implement the above actions, refer to the section titled “Front-Panel Security” on page 2-23.

Secure File Transfers

Secure Copy and SFTP provide a secure alternative to TFTP and auto-TFTP for transferring sensitive information such as configuration files and log information between the switch and other devices. For more on these features, refer to the section on “Using Secure Copy and SFTP” in the “File Transfers” appendix of the *Management and Configuration Guide* for your switch.

Other Provisions for Management Access Security

The following features can help to prevent unauthorized management access to the switch.

Authorized IP Managers

This feature uses IP addresses and masks to determine whether to allow management access to the switch across the network through the following :

- Telnet and other terminal emulation applications
- The switch's Web browser interface
- SNMP (with a correct community name)

For more information, refer to Chapter 11, "Using Authorized IP Managers".

Secure Management VLAN

This feature creates an isolated network for managing the ProCurve switches that offer this feature. When a secure management VLAN is enabled, CLI, Menu interface, and Web browser interface access is restricted to ports configured as members of the VLAN. For more information, refer to the chapter titled "Static Virtual LANs (VLANs)" in the *Advanced Traffic Management Guide*.

TACACS+ Authentication

This application uses a central server to allow or deny access to TACACS-aware devices in your network. TACACS+ uses username/password sets with associated privilege levels to grant or deny access through either the switch's serial (console) port or remotely, with Telnet. If the switch fails to connect to a TACACS+ server for the necessary authentication service, it defaults to its own locally configured passwords for authentication control. TACACS+ allows both login (read-only) and enable (read/write) privilege level access. For more information, refer to Chapter 4, "TACACS+ Authentication".

RADIUS Authentication

For each authorized client, RADIUS can be used to authenticate operator or manager access privileges on the switch via the serial port (CLI and Menu interface), Telnet, SSH, and Secure FTP/Secure Copy (SFTP/SCP) access methods. Refer to Chapter 5, "RADIUS Authentication and Accounting".

Network Security Features

This section outlines features for protecting access through the switch to the network. For more detailed information, see the indicated chapters.

802.1X Access Control

This feature provides port-based or user-based authentication through a RADIUS server to protect the switch from unauthorized access and to enable the use of RADIUS-based user profiles to control client access to network services. Included in the general features are the following:

- user-based access control supporting up to 32 authenticated clients per port
- port-based access control allowing authentication by a single client to open the port
- switch operation as a supplicant for point-to-point connections to other 802.1X-compliant ProCurve switches

For more information, refer to Chapter 9 “Configuring Port-Based and User-Based Access Control (802.1X)”.

Web and MAC Authentication

These options are designed for application on the edge of a network to provide port-based security measures for protecting private networks and the switch itself from unauthorized access. Because neither method requires clients to run any special supplicant software, both are suitable for legacy systems and temporary access situations where introducing supplicant software is not an attractive option. Both methods rely on using a RADIUS server for authentication. This simplifies access security management by allowing you to control access from a master database in a single server. It also means the same credentials can be used for authentication, regardless of which switch or switch port is the current access point into the LAN. Web authentication uses a web page login to authenticate users for access to the network. MAC authentication grants access to a secure network by authenticating device MAC addresses for access to the network. For more information, refer to Chapter 3, “Web and MAC Authentication”.

Secure Shell (SSH)

SSH provides Telnet-like functions through encrypted, authenticated transactions of the following types:

- **client public-key authentication:** uses one or more public keys (from clients) that must be stored on the switch. Only a client with a private key that matches a stored public key can gain access to the switch.
- **switch SSH and user password authentication:** this option is a subset of the client public-key authentication, and is used if the switch has SSH enabled without a login access configured to authenticate the client's key. In this case, the switch authenticates itself to clients, and users on SSH clients then authenticate themselves to the switch by providing passwords stored on a RADIUS or TACACS+ server, or locally on the switch.
- **secure copy (SC) and secure FTP (SFTP):** By opening a secure, encrypted SSH session, you can take advantage of SC and SFTP to provide a secure alternative to TFTP for transferring sensitive switch information.

For more information on SSH, refer to Chapter 6, “Configuring Secure Shell (SSH)”. For more on SC and SFTP, refer to the section titled “Using Secure Copy and SFTP” in the “File Transfers” appendix of the *Management and Configuration Guide* for your switch.

Secure Socket Layer (SSLv3/TLSv1)

This feature includes use of Transport Layer Security (TLSv1) to provide remote web access to the switch via authenticated transactions and encrypted paths between the switch and management station clients capable of SSL/TLS operation. The authenticated type includes server certificate authentication with user password authentication. For more information, refer to Chapter 7, “Configuring Secure Socket Layer (SSL)”.

Traffic/Security Filters

These statically configured filters enhance in-band security (and improve control over access to network resources) by forwarding or dropping inbound network traffic according to the configured criteria. Filter options include:

- **source-port filters:** Inbound traffic from a designated, physical source-port will be forwarded or dropped on a per-port (destination) basis.
- **multicast filters:** Inbound traffic having a specified multicast MAC address will be forwarded to outbound ports or dropped on a per-port (destination) basis.

- **protocol filters:** Inbound traffic having the selected frame (protocol) type will be forwarded or dropped on a per-port (destination) basis.

For details, refer to Chapter 8, “Traffic/Security Filters and Monitors”.

Port Security, MAC Lockdown, and MAC Lockout

The features listed below provide device-based access security in the following ways:

- **Port security:** Enables configuration of each switch port with a unique list of the MAC addresses of devices that are authorized to access the network through that port. This enables individual ports to detect, prevent, and log attempts by unauthorized devices to communicate through the switch. Some switch models also include eavesdrop prevention in the port security feature.
- **MAC lockdown:** This “static addressing” feature is used as an alternative to port security to prevent station movement and MAC address “hijacking” by allowing a given MAC address to use only one assigned port on the switch. MAC lockdown also restricts the client device to a specific VLAN.
- **MAC lockout:** This feature enables blocking of a specific MAC address so that the switch drops all traffic to or from the specified address.

Precedence of Security Options. 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.)

For more information, refer to Chapter 10, “Configuring and Monitoring Port Security”.

Key Management System (KMS)

KMS is available in several ProCurve switch models and is designed to configure and maintain key chains for use with KMS-capable routing protocols that use time-dependent or time-independent keys. (A key chain is a set of keys with a timing mechanism for activating and deactivating individual keys.) KMS provides specific instances of routing protocols with one or more Send or Accept keys that must be active at the time of a request.

For more information, refer to Chapter 12, “Key Management System”.

Identity-Driven Manager (IDM)

IDM is a plug-in to ProCurve Manager Plus (PCM+) and uses RADIUS-based technologies to create a user-centric approach to network access management and network activity tracking and monitoring. IDM enables control of access security policy from a central management server, with policy enforcement to the network edge, and protection against both external and internal threats.

Using IDM, a system administrator can configure automatic and dynamic security to operate at the network edge when a user connects to the network. This operation enables the network to:

- approve or deny access at the edge of the network instead of in the core;
- distinguish among different users and what each is authorized to do;
- configure guest access without compromising internal security.

Criteria for enforcing RADIUS-based security for IDM applications includes classifiers such as:

- authorized user identity
- authorized device identity (MAC address)
- software running on the device
- physical location in the network
- time of day

Responses can be configured to support the networking requirements, user (SNMP) community, service needs, and access security level for a given client and device.

For more information on IDM, visit the ProCurve Web site at www.procurve.com, and click on **Products and Solutions**, then **Identity Driven Manager** (under **Network Management**).

Dynamic Configuration Arbiter

Starting in software release T.13.xx, the Dynamic Configuration Arbiter (DCA) is implemented to determine the client-specific parameters that are assigned in an authentication session.

A client-specific authentication configuration is bound to the MAC address of a client device and may include the following parameters:

- Untagged client VLAN ID
- Tagged VLAN IDs
- Per-port CoS (802.1p) priority

DCA allows client-specific parameters configured in any of the following ways to be applied and removed as needed in a specified hierarchy of precedence. When multiple values for an individual configuration parameter exist, the value applied to a client session is determined in the following order (from highest to lowest priority) in which a value configured with a higher priority overrides a value configured with a lower priority:

1. Attribute profiles applied through the Network Immunity network-management application using SNMP (see “Network Immunity Manager” on page 1-13)
2. 802.1X authentication parameters (RADIUS-assigned)
3. Web- or MAC-authentication parameters (RADIUS-assigned)
4. Local, statically-configured parameters

Although RADIUS-assigned settings are never applied to ports for non-authenticated clients, the Dynamic Configuration Arbiter allows you to configure and assign client-specific port configurations to non-authenticated clients, provided that a client’s MAC address is known in the switch in the forwarding database. DCA arbitrates the assignment of attributes on both authenticated and non-authenticated ports.

DCA does not support the arbitration and assignment of client-specific attributes on trunk ports.

Network Immunity Manager

Network Immunity Manager (NIM) is a plug-in to ProCurve Manager (PCM) and a key component of the ProCurve Network Immunity security solution that provides comprehensive detection and per-port-response to malicious traffic at the ProCurve network edge.

NIM allows you to apply policy-based actions to minimize the negative impact of a client's behavior on the network. For example, using NIM you can apply a client-specific profile that adds or modifies per-port VLAN ID assignments.

Note

NIM actions only support the configuration of per-port VLAN ID assignment; NIM does not support CoS (802.1p) priority assignment and ACL configuration.

NIM-applied parameters temporarily override RADIUS-configured and locally configured parameters in an authentication session. When the NIM-applied action is removed, the previously applied client-specific parameter (locally configured or RADIUS-assigned) is re-applied unless there have been other configuration changes to the parameter. In this way, NIM allows you to minimize network problems without manual intervention.

NIM also allows you to configure and apply client-specific profiles on ports that are not configured to authenticate clients (unauthorized clients), provided that a client's MAC address is known in the switch's forwarding database.

The profile of attributes applied for each client (MAC address) session is stored in the `hpicfUsrProfileMIB`, which serves as the configuration interface for Network Immunity Manager. A client profile consists of NIM-configured, RADIUS-assigned, and statically configured parameters. Using **show** commands for 802.1X, web or MAC authentication, you can verify which RADIUS-assigned and statically configured parameters are supported and if they are supported on a per-port or per-client basis.

A NIM policy accesses the `hpicfUsrProfileMIB` through SNMP to perform the following actions:

- Bind (or unbind) a profile of configured attributes to the MAC address of a client device on an authenticated or unauthenticated port.
- Configure or unconfigure an untagged VLAN for use in an authenticated or unauthenticated client session.

Note that the attribute profile assigned to a client is often a combination of NIM-configured, RADIUS-assigned, and statically configured settings. Precedence is always given to the temporarily applied NIM-configured parameters over RADIUS-assigned and locally configured parameters.

For more information on Network Immunity Manager, go to the ProCurve Web site at www.procurve.com, and click on **Products and Solutions**, then under **Network Management**, click on **ProCurve Network Immunity Manager 1.0**.

Arbitrating Client-Specific Attributes

In previous releases, client-specific authentication parameters for 802.1X Web, and MAC authentication are assigned to a port using different criteria. A RADIUS-assigned parameter is always given highest priority and overrides statically configured local passwords. 802.1X authentication parameters override Web or MAC authentication parameters.

Starting in release T.13.xx, DCA stores three levels of client-specific authentication parameters and prioritizes them according to the following hierarchy of precedence:

1. NIM access policy (applied through SNMP)
2. RADIUS-assigned
 - a. 802.1X authentication
 - b. Web or MAC authentication
3. Statically (local) configured

Client-specific configurations are applied on a per-parameter basis on a port. In a client-specific profile, if DCA detects that a parameter has configured values from two or more levels in the hierarchy of precedence described above, DCA decides which parameters to add or remove, or whether to fail the authentication attempt due to an inability to apply the parameters.

Also, you can assign NIM-configured parameters (for example, VLAN ID assignment) to be activated in a client session when a threat to network security is detected. When the NIM-configured parameters are later removed, the parameter values in the client session return to the RADIUS-configured or locally configured settings, depending on which are next in the hierarchy of precedence.

In addition, DCA supports conflict resolution for QoS (port-based CoS priority) by determining whether to configure either strict or non-strict resolution on a switch-wide basis.

For information about how to configure RADIUS-assigned and locally configured authentication settings, refer to:

- RADIUS-assigned 802.1X authentication:
“Configuring Port-Based and User-Based Access Control (802.1X)” chapter of the *Access Security Guide*
- RADIUS-assigned Web or MAC authentication:
“Web and MAC Authentication” chapter of the *Access Security Guide*
- RADIUS-assigned CoS
“Configuring RADIUS Server Support for Switch Services” chapter of the *Access Security Guide*
- Statically (local) configured:
“Configuring Username and Password Security” chapter of the *Access Security Guide*

