Configuring Secure Shell (SSH)

Contents

Overview

Feature	Default	Menu	CLI	Web
Generating a public/private key pair on the switch	No	n/a	page 6-10	n/a
Using the switch's public key	n/a	n/a	page 6-12	n/a
Enabling SSH	Disabled	n/a	page 6-15	n/a
Enabling client public-key authentication	Disabled	n/a	pages 6-19, 6-21	n/a
Enabling user authentication	Disabled	n/a	page 6-18	n/a

The ProCurve switches covered in this guide use Secure Shell version 1 or 2 (SSHv1 or SSHv2) to provide remote access to management functions on the switches via encrypted paths between the switch and management station clients capable of SSH operation.

SSH provides Telnet-like functions but, unlike Telnet, SSH provides encrypted, authenticated transactions. The authentication types include:

- Client public-key authentication
- Switch SSH and user password authentication

Client Public Key Authentication (Login/Operator Level) with User Password Authentication (Enable/Manager Level). This option 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. (The same private key can be stored on one or more clients.)

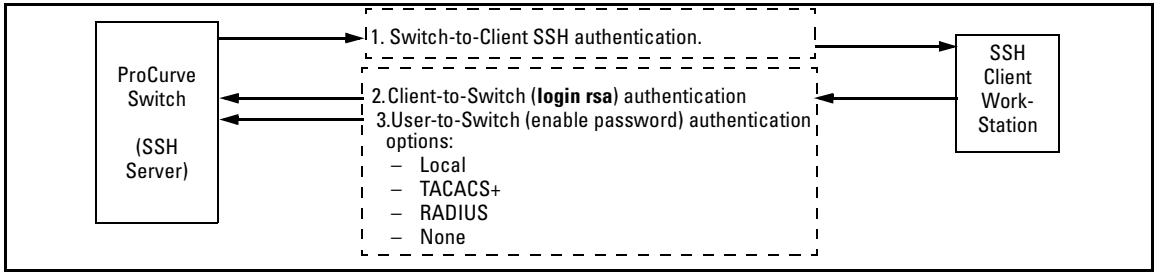

Figure 6-1. Client Public Key Authentication Model

Note

SSH in the ProCurve is based on the OpenSSH software toolkit. For more information on OpenSSH, visit **http://www.openssh.com**.

Switch SSH and User Password Authentication . This option is a subset of the client public-key authentication show in figure 6-1. It occurs if the switch has SSH enabled but does not have login access (**login public-key**) configured to authenticate the client's key. As in figure 6-1, the switch authenticates itself to SSH clients. Users on SSH clients then authenticate themselves to the switch (login and/or enable levels) by providing passwords stored locally on the switch or on a TACACS+ or RADIUS server. However, the client does not use a key to authenticate itself to the switch.

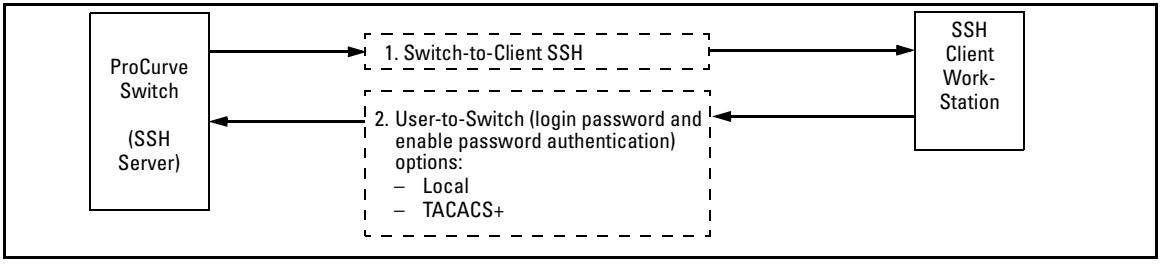

Figure 6-2. Switch/User Authentication

SSH on the ProCurve switches covered in this guide supports these data encryption methods:

- 3DES (168-bit)
- DES (56-bit)

Note

The ProCurve switches covered in this guide use the RSA algorithm for internally generated keys (v1/v2 shared host key & v1 server key). However, ProCurve switches support both RSA and DSA/DSS keys for client authentication. All references to either a public or private key mean keys generated using these algorithms unless otherwise noted

Terminology

- **SSH Server:** A ProCurve switch with SSH enabled.
- **Key Pair:** A pair of keys generated by the switch or an SSH client application. Each pair includes a public key, that can be read by anyone and a private key, that is held internally in the switch or by a client.
- **PEM (Privacy Enhanced Mode):** Refers to an ASCII-formatted client public-key that has been encoded for portability and efficiency. SSHv2 client public-keys are typically stored in the PEM format. See figures 6-3 and 6-4 for examples of PEM-encoded ASCII and non-encoded ASCII keys.
- **Private Key:** An internally generated key used in the authentication process. A private key generated by the switch is not accessible for viewing or copying. A private key generated by an SSH client application is typically stored in a file on the client device and, together with its public key counterpart, can be copied and stored on multiple devices.
- **Public Key:** An internally generated counterpart to a private key. A device's public key is used to authenticate the device to other devices.
- **Enable Level:** Manager privileges on the switch.
- **Login Level:** Operator privileges on the switch.
- **Local password or username:** A Manager-level or Operator-level password configured in the switch.
- **SSH Enabled:** (1) A public/private key pair has been generated on the switch (**crypto key generate ssh [rsa]**) and (2) SSH is enabled (**ip ssh**). (You can generate a key pair without enabling SSH, but you cannot enable SSH without first generating a key pair. See "2. Generate the Switch's Public and Private Key Pair" on page 6-10 and "4. Enable SSH on the Switch and Anticipate SSH Client Contact Behavior" on page 6-15.)

Prerequisite for Using SSH

Before using the switch as an SSH server, you must install a publicly or commercially available SSH client application on the computer(s) you use for management access to the switch. If you want client public-key authentication (page 6-2), then the client program must have the capability to generate or import keys.

Public Key Formats

Any client application you use for client public-key authentication with the switch must have the capability export public keys. The switch can accept keys in the PEM-Encoded ASCII Format or in the Non-Encoded ASCII format.

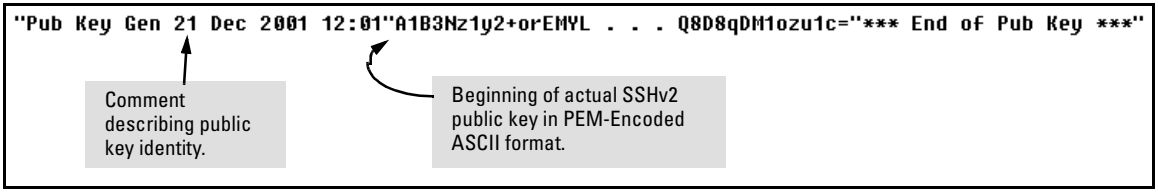

Figure 6-3. Example of Public Key in PEM-Encoded ASCII Format Common for SSHv2 Clients

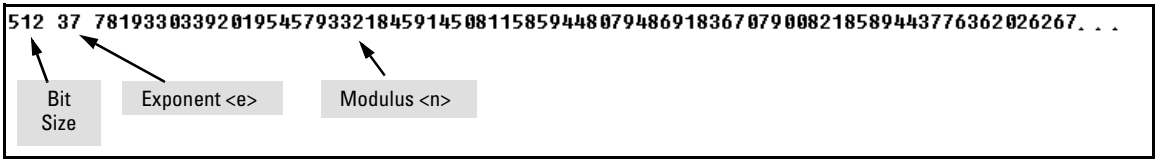

Figure 6-4. Example of Public Key in Non-Encoded ASCII Format (Common for SSHv1 Client Applications)