# 2

# Controlling Management Access to the ProCurve Secure Router

## Contents

# Securing Management Access to the ProCurve Secure Router

The ProCurve Secure Router supports both local and remote management. For local management, you can use a serial cable to attach your PC to the ProCurve Secure Router and establish a console terminal session. For remote management, you have the following options:

- Telnet session
- Secure Shell (SSH) session
- Web browser interface through HTTP or HTTP with Secure Sockets Layer (HTTPS)

You can also establish an FTP session with the router or use secure copy server to copy configuration files to internal or compact flash.

For tighter security, the ProCurve Secure Router allows you to restrict who can use these access methods to manage the router.

In addition to managing the ProCurve Secure Router through the command line interface (CLI) or Web browser interface, you can use a Simple Network Management Protocol (SNMP) application.

## Restricting Access to the Enable Mode Context

The first step you should take to protect your WAN is to configure a password for the enable mode context. If you do not configure this password, anyone who has physical access to your router can establish a console terminal session and view or change configurations on the router.

In addition, an enable mode password is required for remote management through a Telnet or SSH session. If you do not create an enable mode password, you may be able to establish a Telnet or SSH session (if the router is configured to permit this access), but you will not be able to move beyond the basic mode context.

To configure an enable mode password, move to the global configuration mode context and enter:

***Syntax:*** enable password [md5] <*password*>

Replace <*password*> with any combination of up to 30 characters. Include the Message Digest 5 (**md5**) option to encrypt the password.

For example, if you want to set the password as **procurve**, enter:

```
ProCurve(config)# enable password procurve
```

Because you did not include the **md5** option, the password you entered is stored as clear text and is displayed when you enter the **show running-config** command, as shown below.

```
hostname "ProCurve"
enable password procurve
```

To encrypt the password so that it is not stored as clear text, use the **md5** option. From the global configuration mode context, enter:

```
ProCurve(config)# enable password md5 procurve
```

The ProCurve Secure Router then uses the MD5 hashing algorithm to encrypt the password so that it is not readable when it is transmitted across the wire or when you display the running-config file. An encrypted password is displayed in the running-config as shown below:

```
hostname "ProCurveSR7203dl"
enable password md5 encrypted b46f9961af093fdfb9e177eda79
```

## Configuring a Password for Console Access

If possible, you should place the ProCurve Secure Router in a locked room so that unauthorized users do not have physical access to it. Restricting physical access to the router helps prevent malicious or curious users from damaging your WAN or LAN.

You can further protect the ProCurve Secure Router by configuring a password for console access. Then, if someone breaches the physical security you have set up to protect the router, the console password prevents that person from viewing information that is available at the basic mode context. Although the basic mode offers only a limited number of commands, you can still enter **show** commands and view some configuration information. For example, you can view information about:

- interfaces
- event-history

Configuring a password for the console access is a three-step process:

1. Access the console line configuration mode context.
2. Enter the **login** command, which requires users to provide a password before they can access the ProCurve Secure Router OS through a console session.
3. Enter the password that authorized users must supply when they start a console session.

From the global configuration mode context, enter:

```
ProCurve(config)# line console 0
```

The ProCurve Secure Router prompt will show that you are in the console line configuration mode context:

```
ProCurve(config-con0)#
```

Enter:

```
ProCurve(config-con0)#login
ProCurve(config-con0)#password <password>
```

Replace <*password*> with any combination of up to 30 characters.

The password you enter is stored as clear text and is displayed when you enter the **show running-config** command, as shown below.

```
line con 0
  login
  password procurve
```

To encrypt the password, use the **md5** option. From the global configuration mode context, enter:

```
ProCurve(config-con0)# password md5 <password>
```

The ProCurve Secure Router then uses the MD5 hashing algorithm to encrypt the password so that it is not readable when it is transmitted across the wire or when you display the running-config file.

# Enabling Remote Access to the ProCurve Secure Router

As mentioned earlier, you can access the ProCurve Secure Router through the Web browser interface, Telnet session, SSH session, or FTP session. To establish this access, you must configure at least one interface, such as an Ethernet interface.

## Configuring an Ethernet Interface

This section provides the minimum steps required to configure an Ethernet interface. (For more detailed information about configuring an Ethernet interface, see *Chapter 3: Configuring Ethernet Interfaces*.)

1. Use a 10Base-T or 100Base-T cable to connect the Ethernet port to a device (such as a switch) on your LAN.
2. Open your terminal session software and initiate a console session with the ProCurve Secure Router, using the following parameters:
   - Baud Rate = 9600
   - Parity = None
   - Data Bits = 8
   - Stop Bits = 1
   - Flow Control = None
3. Press **Enter** when you are prompted to start a session with the router. The router basic mode context prompt appears, as shown below:

   ```
   ProCurve>
   ```

4. Access the enable mode context:

   ```
   ProCurve> enable
   ```

5. Access the global configuration mode context:

   ```
   ProCurve# configure terminal
   ```

6. From the global configuration mode context, enter the Ethernet interface configuration mode context:

   ```
   ProCurve(config)# interface ethernet 0/<port>
   ```

7. Assign the Ethernet interface an IP address.

   ***Syntax:*** ip address <*A.B.C.D*> [<*subnet mask*> | /<*prefix-length*>]

   For example, if you want to assign the Ethernet interface an IP address of 192.168.1.1 with a subnet mask of 255.255.255.0, enter

   ```
   ProCurve(config-eth 0/1)# ip address 192.168.1.1 /24
   ```

8. Activate the Ethernet interface.

   ProCurve(config-eth 0/1)# no shutdown

9. Save your configuration.

   ProCurve(config-eth 0/1)# do write memory

## Configuring Telnet Access

By default, the ProCurve Secure Router requires a login password for Telnet sessions. Unless you configure a password for a Telnet line or disable the **login** option, no one can establish a Telnet session with the ProCurve Secure Router. This security helps protect your organization against unauthorized users who might try to access your ProCurve Secure Router and damage or get information about your WAN.

In addition to configuring a password for Telnet access, you must configure a password for the enable mode. If you do not configure a password for the enable mode, you can establish a Telnet session and enter the basic mode context. However, you cannot move beyond the basic mode context.

You can configure five Telnet lines, which are numbered 0 to 4. If you configure all five lines, a maximum of five people can establish a Telnet session with the ProCurve Secure Router at one time.

**Configuring the Telnet Lines.** Configuring Telnet access is a three-step process:

1. Access the Telnet line configuration mode context.
2. Enter the password that authorized users must supply when they start a Telnet session.
3. Configure a password for the enable mode context, if you have not done so already.

From the global configuration mode context, enter the following command:

***Syntax:*** line telnet <0–4>

For example, if you want to configure line 0, enter:

ProCurve(config)# line telnet 0

The ProCurve Secure Router prompt will show that you are in the Telnet line 0 configuration mode context:

ProCurve(config-telnet0)#

You can then enter the **password** command:

***Syntax:*** password [md5] <*password*>

The **md5** option encrypts the password as it is sent over the wire and when it is stored in the running-config.

For example, if you want to create the password as procurve, enter

```
ProCurve(config-telnet0)# password md5 procurve
```

**Note**

You can also configure an access control list (ACL) to block or limit Telnet access. For instructions on configuring this ACL, see the *Advanced Management and Configuration Guide*, *Chapter 5: Applying Access Control to Router Interfaces*.

**Configuring Multiple Telnet Lines at Once.** You can also create a password for all Telnet lines at once. Enter:

```
ProCurve(config) line telnet 0 4
```

Entering **0 4** indicates that you are configuring all four lines. The router context displays the lines you are configuring, as shown below:

```
ProCurve(config-telnet0–4)
```

You can then enter the **password** command.

**Note**

If you do not enter a space between **0** and **4**, you will configure only line **4**. The prompt will be displayed as:

```
ProCurve(config-telnet04)
```

**Configuring Multiple Passwords for Telnet Lines.** If you have a large IT staff, you may want to configure multiple Telnet lines. You may also want to configure a different password for one Telnet line and reserve that line for your access only.

You should always place the more restrictive password on the configured Telnet line with the highest number due to the way that the ProCurve Secure Router handles Telnet sessions. The router always assigns a remote user to the first available Telnet line, starting with line 0. That is, the first user to initiate a Telnet session connects over Telnet line 0, the second over Telnet line 1, and so forth.

If a user cannot enter the correct password, the router terminates the Telnet session. It does not allow the user to access the next Telnet line. If you place a password that only you know on Telnet line 0, no other user will be able to access the other Telnet lines for which they do know the password—except in the unlikely event that you have already established a Telnet session with the router.

**Configuring an Enable Mode Password.** To provide access to the enable mode context through a Telnet session, you must configure an enable mode password. If you do not configure an enable mode password, users will receive a message, telling them that no enable mode password is configured, and they will be denied access to the enable mode context.

To configure an enable mode password, move to the global configuration mode context and enter:

***Syntax:*** enable password [md5] <*password*>

**Configuring Timeout Setting for Telnet Access.** By default, the ProCurve Secure Router maintains your Telnet session until it has been inactive for 15 minutes. You can configure the number of minutes a line session can remain inactive before the Secure Router OS terminates the session. From the Telnet line configuration mode context, enter:

***Syntax:*** line-timeout <*minutes*>

Replace minutes with a number between 0 and 35791.

To return this setting to the default value, use the **no** command:

***Syntax:*** no line-timeout <*minutes*>

Entering 0 will disable the timeout.

**Disabling the Login Requirement.** If you do not want to require a password for users to establish a Telnet session, you can disable the **login** option. From the Telnet line configuration mode context, enter:

ProCurve(config-telnet0–4)# no login

Disabling this option is not recommended because it weakens your security and could compromise your entire network. However, if you do disable the **login** option, you are still required to create an enable mode password to allow users to configure the router through a Telnet session.

# Configuring Local User Lists

By default, access to HTTP, SSH, and FTP is controlled through the local user list. To add a username and password to the local user list, enter the following command from the global configuration mode:

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

Both the username and password can be an alphanumerical string up to 30 characters in length.

You can add multiple usernames and passwords to the local user list, and these usernames and passwords can be used for HTTP, HTTPS, SSH, and FTP access.

## Enabling Access to the Web Browser Interface

In addition to configuring a username and password, you must enable the HTTP or HTTPS server in order to access the Web browser interface. From the global configuration mode context, enter:

ProCurve(config)# ip http server [<*TCP port*>]

Include the <*TCP port*> option only if you want to change the port on which the server receives HTTP communications.

If you want to use SSL to protect the communications between your PC and the router, enter:

ProCurve(config)# ip http secure-server [<*TCP port*>]

Again, include the <*TCP port*> option only if you want to customize the port on which the HTTPS server receives and sends communications.

After you configure a username and password for the local user list and enable the HTTP or HTTPS server, you can access the Web browser interface. Make sure that your workstation is on a network segment that is connected to the ProCurve Secure Router. Then, open an Internet browser and enter the IP address assigned to the Ethernet interface. For example, if the IP address of the Ethernet interface is 192.168.1.1, enter:

http://192.168.1.1

If you have enabled the HTTP secure server, enter:

https://192.168.1.1

When prompted, enter a username and password that you configured in the local user list.

## Managing SSH Communications

With Telnet, communications between the server and your PC are sent over the wire in clear text. If you want to encrypt these communications, you can use SSH instead.

The SSH server on the ProCurve Secure Router is enabled by default. After you configure a username and password in the local user list, you can enter that username and password to access the router through SSH.

The ProCurve Secure Router supports up to five SSH lines, which are numbered 0 to 4. If you configure a username and password in the local user list, a maximum of five people can establish an SSH session with the ProCurve Secure Router at one time.

You can configure timeout settings for SSH lines just as you configure timeout settings for Telnet lines. First, move to the SSH line configuration mode context by entering the following command from the global configuration mode context:

***Syntax:*** line ssh <0–4>

To access all the SSH lines at once, enter:

```
ProCurve(config)# line ssh 0 4
```

By default, ProCurve Secure Router maintains your SSH session until it has been inactive for 15 minutes. To configure the number of minutes an SSH session can remain inactive before the Secure Router OS terminates the session, enter the following command from the SSH line configuration mode context:

***Syntax:*** line-timeout <*minutes*>

Replace minutes with a number between 0 and 35791.

To return this setting to the default value, use the **no** command:

***Syntax:*** no line-timeout <*minutes*>

Entering 0 will disable the timeout.

**Note**

If you want to use an ACL to restrict SSH access, you apply this ACL at the SSH line configuration mode context. For more information, see the *Advanced Management and Configuration Guide*, *Chapter 5: Applying Access Control to Router Interfaces*.

### Using FTP to Access the Router

After you add one username and password to the local user list, you can use FTP to access the router. You can then copy configuration files to and from the router's compact flash or internal flash. If you want to encrypt these files as they are copied to and from the router, see "Enabling Secure Copy Server" on page 2-14.

### Using the Local User List for Console or Telnet Access

You can configure the ProCurve Secure Router to use the usernames and passwords you configure from the global configuration mode context to control access to console terminal, SSH, or Telnet sessions. To use these passwords for console terminal sessions, move to the console configuration mode context and enter:

```
ProCurve(config-con0)# login local-userlist
```

By default, no login password is required for console terminal sessions.

To use these passwords for SSH or Telnet access, move to the appropriate line configuration mode context and enter the following command:

```
ProCurve(config-ssh0–4)# login local-userlist
ProCurve(config-telnet0–4)# login local-userlist
```

## Encrypting All the Passwords Configured on the Router

By default, the passwords that you enter in the local user list are not encrypted. You can enter one command to encrypt these passwords and *all* the other passwords configured on the ProCurve Secure Router, including the passwords configured for Telnet access, console access, and Point-to-Point Protocol (PPP) authentication. From the global configuration mode context, enter:

```
ProCurve(config)# service password-encryption
```

**Note**

The **service password-encryption** command is supported in the Secure Router OS version J.04 and above. If you upgrade to this version of the OS, enter this command but then need to revert back to a previous version (such as J.03.01), you must first disable this command and re-enter all the necessary passwords so that they are stored in clear text. If you do not disable this command and re-enter the passwords, you will not be able to log back in to the router after you revert to a previous version of the Secure Router OS that does not support global password encryption.

## Enabling Secure Copy Server

You can enable the secure copy (SCP) server, so that files are encrypted as they are copied to and from the ProCurve Secure Router. You use the SCP server in conjunction with SSH so that the user trying to access the server is authenticated and the data transmitted is encrypted.

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

***Syntax:*** ip scp server

To disable the SCP server, enter:

***Syntax:*** no ip scp server

## Viewing Information about Users

At any time, you can view information about the users who are accessing the ProCurve Secure Router through the console, Telnet, SSH, FTP, and Web browser interface. From the enable mode context, enter:

```
ProCurve# show users
```

Figure 2-1 shows the type of information that is displayed when you enter this command. You can view the username that the user entered to obtain access, the type of access (such as console or Telnet), and the time the connection has been idle. For Telnet, SSH, FTP, and Web access, you can also view the IP address of the device from which the user obtained access.

```
- CONSOLE 0 'password-only' logged in and enabled
 Idle for 00:00:00
- TELNET 0 (192.168.20.25:1029) 'geoff' logged in and enabled
 Idle for 00:00:09
```

**Figure 2-1. Viewing the Users Who Are Accessing the Router Through the Console, Telnet, SSH, FTP, and Web Browser Interface**

# Using the AAA Subsystem to Control Management Access

Authentication, authorization, and accounting (AAA) is an industry standard for controlling:

- which users can access a system (authentication)
- what they can do once they are granted access (authorization)
- what is recorded about their activities (accounting)

The AAA subsystem on the ProCurve Secure Router currently supports:

- authentication methods configured on the router itself
- authentication through Remote Authentication Dial-In User Service (RADIUS) servers
- authentication, authorization, and accounting through Terminal Access Controller Access-Control System Plus (TACACS+) servers

## Advantages of Using the AAA Subsystem

The AAA subsystem provides more flexibility than simple password-based authentication. If you enable the AAA subsystem, you can configure a list of authentication methods for the enable mode and for each access method. For example, you could configure a list of authentication methods for Telnet access or for SSH access. The authentication methods include:

- the Telnet password
- the enable mode password
- the local userlist
- a RADIUS server
- a TACACS+ server

You configure the list of authentication methods in the order in which you want them used. Then, if one method fails, the next method is used. (For information about what constitutes a failure, see "Criteria for Failure of Authentication Methods" on page 2-16.)

The AAA subsystem allows you to use a standard authentication method across your entire network. If you are using a RADIUS server or a TACACS+ server to authenticate network services and applications, you can use this same server to authenticate management access to the ProCurve Secure Router.

In addition to controlling management access, the AAA subsystem can be used to authenticate VPN users when Xauth is configured. (For more information about Xauth, see the ProCurve Secure Router *Advanced Management and Configuration Guide*, *Chapter 10: Virtual Private Networks*.)

The AAA subsystem also strengthens your WAN security by supporting authorization and accounting for management access to the ProCurve Secure Router. Enforced through a TACACS+ server, authorization and accounting go beyond password authentication to ensure that only authorized users perform management functions and to provide a record of the configuration commands entered.

## Criteria for Failure of Authentication Methods

The AAA subsystem skips an authentication method if the method itself fails. However, if a user fails to enter the correct password, that user is denied access to the router. The user failed in his or her attempt to authenticate; the authentication method did not fail.

The ProCurve Secure Router uses the following criteria to determine if an authentication method failed:

- Line and enable passwords fail if no line or enable passwords are configured.
- RADIUS or TACACS+ servers fail if the ProCurve Secure Router tries to communicate with them but they do not respond.
- The local user list fails if the given user is not listed in the database.

For example, if you configure the authentication methods with RADIUS as the first option and the RADIUS server goes down, that authentication method failed; the AAA subsystem will try the next authentication method you configured. If you listed the local user list after the RADIUS server, the AAA subsystem will use that authentication method next.

## Enabling the AAA Subsystem

By default, the AAA subsystem is disabled. To enable it, move to the global configuration mode context and enter:

```
ProCurve(config)# aaa on
```

After you enable the AAA subsystem, the complete set of AAA commands becomes available in the ProCurve Secure Router OS. For example, you can then configure AAA-based authentication, authorization, and accounting for SSH lines. The AAA authentication settings that you configure override any other authentication settings you have configured.

## Configuring AAA for Authentication

Configuring AAA for authentication involves the following steps:

1. Create a list that includes the authentication methods that you want to use to authenticate users who attempt to access and manage the ProCurve Secure Router. In this guide and in the *SROS Command Line Interface Reference Guide*, this list of authentication methods is called a "named list." You create this named list on the router.

   You can create a named list to authenticate users who try to access the enable mode context, and you can create multiple named lists to authenticate users who try to use the router's access lines (such as Telnet or SSH).

2. Assign the named list to the appropriate access line (such console line, Telnet lines, SSH lines, FTP server, or HTTP server). You do not have to complete this step to configure AAA authentication methods for the enable mode.

3. Configure the RADIUS or TACACS+ server if you want to use one of these servers to authenticate users who try to manage the ProCurve Secure Router. (To learn how to configure these servers, see "Define the RADIUS Server" on page 2-31 and "Define the TACACS+ Server" on page 2-35.)

## Creating a Named List for the Enable Mode Authentication

To create a named list for the enable mode, you must determine the authentication methods you want to use and the order in which you want the authentication methods applied. You then use the **aaa authentication** command to specify both the name of the list and its contents. When you create a named list for the enable mode, you always specify that you are creating the default named list; you cannot create a named list with a different name.

**Note**

If you enable the AAA subsystem but do not configure a named list for the enable mode, the Secure Router OS uses the enable mode password by default.

From the global configuration mode context, enter:

***Syntax:*** aaa authentication enable default [line | enable | none | {group <*groupname*> | radius | tacacs+}]

The options that you can use to authenticate users who attempt to access the enable mode are included in Table 2-1.

**Table 2-1. Authentication Options for the Enable Mode Named List**

| Option | Meaning |
|---|---|
| **line** | Requires users to enter the password configured for the Telnet or the console line. |
| **enable** | Requires users to enter the password configured for the enable mode context. |
| **none** | Does not require a password. If you enter multiple access methods (such as line or enable), you must enter the none option last. |
| **group [<groupname> \| radius \| tacacs+]** | Specifies that the ProCurve Secure Router should contact an access server to authenticate users:<br>• group of RADIUS or TACACS+ servers that you have configured<br>• all the RADIUS servers that you have defined (if you have not defined a group of RADIUS servers)<br>• all the TACACS+ servers that you have defined (if you have not defined a group of TACACS+ servers) |

When you configure a named list for authentication, you can include more than one option in a command. For example, you may decide that when a user attempts to access the enable mode context, you want the ProCurve Secure Router to use the following authentication methods, in the order they are listed:

- TACACS+
- enable

You would enter:

```
ProCurve(config)# aaa authentication enable default group tacacs+ enable
```

If you create this named list, the ProCurve Secure Router will first try to authenticate the user through the TACACS+ server. If the TACACS+ server does not respond, the ProCurve Secure Router will prompt the user to enter the enable mode password and will check the password that the user enters against the enable mode password that you configured.

After you create the default named list for the enable mode, it is automatically applied. If you are using a RADIUS or TACACS+ server as an authentication method, you must then configure the ProCurve Secure Router to locate and communicate with that server. For information about the configuration required for a RADIUS server, see "Configuring a RADIUS Server for Authentication" on page 2-31. For information about the configuration required for a TACACS+ server, see "Define the TACACS+ Server" on page 2-35.

## Creating a Named List for User Authentication

To create a named list for the router's access lines, you must determine the authentication methods that you want to use and the order in which you want the authentication methods applied. You can then use the **aaa authentication** command to specify both the name of the list and its contents. When you create a named list for the router's access lines, you can create the default named list, or you can create a named list with a specific name.

To create a named list for one of the router's access lines, enter the following command from the global configuration mode context:

***Syntax:*** aaa authentication login [default | <*listname*>] [enable | line | local | none | group [<*groupname*> | radius | tacacs+]

Specify **default** to create the default named list, or replace ***<listname>*** with the name that you want to give the named list that you create.

The options that you can select to authenticate users are listed in Table 2-2. When you configure a named list for authentication, you can include more than one option in a command.

**Table 2-2. Authentication Options for Named Lists**

| Option | Meaning |
|---|---|
| **enable** | Requires users to enter the password configured for the enable mode context. |
| **line** | Requires users to enter the password configured for the Telnet or the console line. |
| **local** | Requires users to enter a username and password from the local user database (which is defined on the router) for authentication. |
| **none** | No password is required. |
| **group [<groupname> \| radius \| tacacs+]** | Specifies that the ProCurve Secure Router should contact an access server to authenticate users:<br>• group of RADIUS or TACACS+ servers that you have configured<br>• all the RADIUS servers that you have defined (if you have not defined a group of RADIUS servers)<br>• all the TACACS+ servers that you have defined (if you have not defined a group of TACACS+ servers) |

**Note**

If you select the enable password as an authentication method for an access method that requires a username, the username is, by default, **$enab15$**. You can change this username for RADIUS servers when you enter the **radius-server** command, as explained in "Define the RADIUS Server" on page 2-31.

There is one difference between the list of options for the enable mode and the list of options for authenticating users: the local user database is *not* an option for the enable mode.

For example, when you configure a named list for user authentication, you may want to call this list UserLogin. You may also decide to use the following authentication methods:

- enable password
- line password
- local user database

In this case, you would enter:

```
ProCurve(config)# aaa authentication login UserLogin enable line local
```

If no enable password has been defined, the AAA subsystem moves to the line username and password. If no username and password have been defined for the line, the AAA subsystem moves to the local user database and tries to match the username and password that the user enters to a username and password in that database.

## Assign the Named List

After you create a named list for an access line, you must assign the list to the appropriate access line. To assign a named list to the console, Telnet, or SSH lines, move to the appropriate line configuration mode context and enter:

***Syntax:*** login authentication <*named list*>

For example, to assign ListA to the console line, enter:

```
ProCurve(config)# line console 0
ProCurve(config-con0)# login authentication ListA
```

To assign ListA to the Telnet 0 line, enter:

```
ProCurve(config)# line telnet 0
ProCurve(config-telnet0)# login authentication ListA
```

To assign ListA to all of the SSH lines, enter:

```
ProCurve(config)# line ssh 0 4
ProCurve(config-ssh0-4)# login authentication ListA
```

For FTP and HTTP access, you assign the list from the global configuration mode context. If you want to assign a named list to control FTP access, enter:

***Syntax:*** ftp authentication <*named list*>

If you want to assign a named list to control Web access, enter the following command from the global configuration mode context:

***Syntax:*** ip http authentication <*named list*>

**No Named List Assigned.** If you enable the AAA subsystem but do not configure a named list and assign it to an access method (console, Telnet, FTP, SSH, or HTTP), the ProCurve Secure Router handles authentication as outlined in Table 2-3.

**Table 2-3. Default Action if No Named List Is Configured**

| Access | Authentication Method |
|---|---|
| **console access** | no password required |
| **Telnet access** | Telnet password |
| **FTP access** | local user list |
| **HTTP access** | local user list |
| **SSH access** | local user list |

## Options for AAA Authentication: Configuring Banners, Messages, and Prompts

To help users log in to the ProCurve Secure Router successfully, you can customize the following:

- banner
- message that is displayed when a login attempt fails
- password prompt
- username prompt

To configure these displays, you use the following command syntax:

***Syntax:*** aaa authentication [banner <*banner*>| fail-message <*message*> | password-prompt <*prompt*> | username-prompt <*prompt*>]

**Configuring a Banner.** A banner is displayed before a user attempts to log in to the router. By default, the following banner is displayed:

```
User Access Verification
```

To configure a banner, move to the global configuration mode context and enter the **aaa authentication banner** command followed by any character that signals the beginning of the banner text. For example, you might enter the @ character, as shown below:

```
ProCurve(config)# aaa authentication banner @
```

You can then type the banner that you want to display. To end the banner, you must enter the same character that you used to signal the beginning of the banner. For example, you might enter:

```
Only authorized users allowed@
```

**Configuring a Fail Message.** A fail message is displayed if the user's attempts to log in to the router fails. By default, the fail message is:

```
Authentication Failed
```

To customize a fail message, move to the global configuration mode context and enter the **aaa authentication fail-message** command followed by a character that signals the beginning of the message that you want to display. For example, you might enter the @ character or even the ! character, as shown below:

```
ProCurve(config)# aaa authentication fail-message !
```

Then type the message that you want to be displayed if a login attempt fails. After entering the message, enter the same character you used to signal the beginning of the fail message.

For example, you might enter:

```
You entered the wrong username or password!
```

**Configuring a Username or Password Prompt.** By default, the ProCurve Secure Router displays the following prompts to help users log in to the router:

```
Username:
Password:
```

To customize the username prompt, move to the global configuration mode context and enter:

***Syntax:*** aaa authentication username-prompt <*prompt*>

Replace ***<prompt>*** with the prompt that you want to be displayed when users attempt to log in. If you want to create a prompt that includes spaces between words, you must enclose the prompt in quotation marks. For example, you might enter:

```
ProCurve(config)# aaa authentication username-prompt "Enter username now:"
```

To customize the password prompt, move to the global configuration mode context and enter:

***Syntax:*** aaa authentication password-prompt <*prompt*>

Replace ***<prompt>*** with the prompt that you want to be displayed when users attempt to log in. Again, if you want the prompt to include spaces, you must enclose it in quotation marks. For example, if you might enter:

```
ProCurve(config)# aaa authentication password-prompt "Enter your password:"
```

# Configuring Authorization

After you enable the AAA subsystem, you can use a TACACS+ server to control not only who can access the Secure Router OS but also who can actually enter unprivileged or privileged commands. That is, you can determine which users are authorized to configure the router from the basic or enable mode context.

Configuring authorization through the TACACS+ server involves the following steps:

1. Create a list to specify what an authorized user is allowed to access. In this guide and in the *SROS Command Line Interface Reference Guide*, this list is called a "named list." You can define a named list to authorize users to:
   - access the basic mode context or the enable mode context
   - immediately enter the enable mode context when they start a new CLI session
2. Assign the named list to a line configuration mode context.

If you want to enforce authorization for console sessions, you must also enable authorization for the console line.

Of course, the AAA subsystem must be enabled, and the TACACS+ server must be defined. (See "Define the TACACS+ Server" on page 2-35.)

## Creating a Named List to Allow Authorized Users to Access the Basic Mode Context or the Enable Mode Context

You must create a named list for authorization, just as you create a named list for authentication. In this named list, you specify if users are authorized to enter commands from the basic mode context or the enable mode context. You also define the TACACS+ servers that will answer the authorization request.

You use the **aaa authorization** command to both create the named list and specify its contents. From the global configuration mode context, enter:

***Syntax:*** aaa authorization commands [1 | 15] [default | <*named list*>] [group {tacacs+ | <*groupname*>}] [if-authenticated | none]

Include **1** or **15** to specify the level of commands for which you want to configure authorization: 1 is unprivileged access, which is the basic mode, and 15 is privileged access, which is the enable mode.

Specify **default** to create the default authorization list, or replace ***<named list>*** to create a named list with the name you specify.

Use the **group tacacs+** option to specify the default group of TACACS+ servers. Use the **group *<groupname>*** if you have created a group of TACACS+ servers.

Include the **if-authenticated** option to authorize authenticated users. Use the **none** option to grant access immediately. You may want to enter **none** as a second option. That way, if the ProCurve Secure Router cannot contact the TACACS+ server, you will still be able to configure the router.

For example, to create a named list that allows authorized users to configure the router from the enable mode context, enter:

```
ProCurve (config)# aaa authorization commands 15 default group tacacs+
if-authenticated
```

After you create a named list for authorization, you must assign it to an access method, such as a Telnet or SSH line.

## Create a Named List That Allows Authorized Users to Immediately Enter into the Enable Mode Context

You can create authorization lists for an exec shell, which allows an authorized user to enter directly into the enable mode context when that user starts a new CLI session. You use the **aaa authorization** command to both create this named list and specify its contents.

From the global configuration mode context, enter:

***Syntax:*** aaa authorization exec [default | <*named list*>] [none | if-authenticated] [group {tacacs+ | <*group name*>}]

Include **default** to create the default authorization list, or replace ***<named list>*** with the name of the list you want to create.

Include the **if-authenticated** option for authorization to succeed if the user authenticates. Include the **none** option to grant access automatically.

Include the **group tacacs+** option if you want the ProCurve Secure Router to use the TACACS+ server for authorization. Use **group *<groupname>*** to specify a group of remote servers that will verify if a user is authorized to enter the enable mode context. You can specify more than one group of TACACS+ servers. If the servers in one group are unavailable, the ProCurve Secure Router will contact another group. However, if the ProCurve Secure Router

contacts a TACACS+ server in the first group and that server does not authorize the user to enter the enable mode context, the ProCurve Secure Router will not attempt to authorize that user with any other TACACS+ groups listed.

For example, the following command creates the Admin named list and authorizes authenticated users to enter the enable mode context. That is, if a user authenticates successfully, that user will automatically enter the enable mode context when he or she starts a CLI session:

```
ProCurve (config)# aaa authorization exec Admin if-authenticated
```

## Assign the Named List

To assign the named list you created to a console, Telnet, or SSH line, you must move to the line configuration mode context. To completely enforce this security measure, you must ensure that you assign the named list to all of the Telnet or SSH lines that you have enabled. For example, if you have enabled all five Telnet lines, you must assign the named list to all five lines.

**Assign a Named List for the Basic or Enable Mode Context.** To assign a named list that grants access to the basic or enable mode context, enter the following command from the appropriate line configuration mode context:

***Syntax:*** authorization commands [1 | 15] [default | <*named list*>]

Enter **1** to grant access to the basic mode, or enter **15** to grant access to the enable mode.

Enter **default** to assign the default list, or replace ***<named list>*** with the list that you have created.

For example, you might use the **aaa authorization** command to create a named list called Authorize and then assign it to all of the Telnet lines. You might also include the **15** option because you want this named list to control who can enter commands from the enable mode context. From the global configuration mode context, enter:

```
ProCurve (config)# line telnet 0 4
ProCurve (config-telnet04)# authorization commands 15 Authorize
```

**Note**

If the AAA subsystem is not enabled (by entering **aaa on** at the global configuration mode context), the **authorization** command will not be available at the line configuration mode context.

**Assign a Named List That Allows Immediate Entry to the Enable Mode Context.** To assign a named list that allows authorized users to immediately enter the enable mode context when they start a new CLI session, enter the following command from the appropriate line configuration mode context:

***Syntax:*** authorization exec [default | <*named list*>]

Enter **default** if you configured a default named list or replace ***<named list>*** with the name of the list that you created.

### Enable Authorization Commands for Console Line

If you want to configure authorization commands for the console line, you must enable this capability. From the global configuration mode context, enter:

***Syntax:*** aaa authorization console

**Note**

Take care when you configure authorization for the console line. If you are not careful, you may prohibit yourself from entering commands from the console.

To disable authorization through the console line, enter:

***Syntax:*** no aaa authorization console

By default, authorization commands can be configured for the enable mode context. To disable authorization for the enable mode context, enter the following command from the global configuration mode context:

***Syntax:*** no aaa authorization config-command

To reinstate this capability, enter:

***Syntax:*** aaa authorization config-command

## Configuring AAA Accounting

If your network includes a TACACS+ server, you can use it to track which users access the ProCurve Secure Router and the configuration changes that those users make. When you configure AAA accounting on the ProCurve Secure Router, it will send configuration information to the TACACS+ server that you specify.

Configuring accounting involves the following steps:

1. Create a list to specify which events are tracked by the TACACS+ server. In this guide and in the *SROS Command Line Interface Reference Guide*, this list is called a "named list." You can create named lists to track the following events:
   - a user accesses the basic or enable mode context
   - a user logs in to the router
   - a user establishes an outbound Telnet session
2. Apply the named list.

Of course, the AAA subsystem must be enabled, and the TACACS+ server must be defined. (See "Define the TACACS+ Server" on page 2-35.)

## Creating a Named List to Track When Users Access the Basic or Enable Mode Context

You can create a named list to track which users access the basic or enable mode context. You can also configure:

- which TACACS+ server the information is sent to
- when the information is sent

You can use the **aaa accounting** command to create a named list and specify its contents. From the global configuration mode context, enter:

***Syntax:*** aaa accounting commands [1 |15] [default | <*named list*>] [none | stop-only] [group {tacacs+ | <*group name*>}]

Specify the level of commands for which you want to generate accounting: **1** is unprivileged access, which is the basic mode, and **15** is privileged access, which is the enable mode.

Create the default accounting list, or replace ***<named list>*** to create an accounting list with the name you specify.

Include the **stop-only** option if you want an accounting record to be generated when the user ends his or her session. Include the **none** option if you do not want an accounting record to be generated. If you specify the **none** option, you cannot include the **group** option (because a TACACS+ server is not required).

Include the **group tacacs+** option if you want the ProCurve Secure Router to send the accounting information to the default group of TACACS+ servers. Replace **group *<groupname>*** if you want to specify a TACACS+ group that you created. You can specify more than one group. (For information on creating a TACACS+ group, see "Creating a TACACS+ Group" on page 2-37.)

## Create a Named List to Track New Connections or Outbound Telnet Connections

You can configure the ProCurve Secure Router to send updates to the TACACS+ server for either of the following events:

- all new connections or logins
- outbound Telnet connections

**Note**

You can initiate an outbound Telnet session from both the basic and enable mode context. You simply enter **telnet <A.B.C.D>**, replacing ***<A.B.C.D>*** with the IP address of the device that you want to access.

You use the **aaa accounting** command to both create the named list and specify its contents. From the global configuration mode context, enter:

***Syntax:*** aaa accounting [exec | connection] [default | <*named list*>] [none | start-stop | stop-only] [group {tacacs+ | <*groupname*>}]

Specify the **exec** option to send records of all new connections, or specify the **connection** option to send records for outbound Telnet connections.

Include the **default** option to create the default accounting list, or replace ***<named list>*** to create an accounting list with the name you specify.

Include the **start-stop** option if you want an accounting record to be generated both when the user begins and ends his or her session. Include the **stop-only** option if you want an accounting record to be generated only when the user ends his or her session. Include the **none** option if you do not want an accounting record to be generated. If you specify the **none** option, you cannot include the **group** option (because a TACACS+ server is not required).

Include the **group tacacs+** option if you want the ProCurve Secure Router to send the accounting information to the default group of TACACS+ servers. Replace **group *<groupname>*** with a group of TACACS+ servers that you created. You can specify more than one group.

For example, the following command creates the Admin named list and sends the connection records to the TACACS+ server when the connection is terminated:

```
ProCurve (config)# aaa accounting exec Admin stop-only group tacacs+
```

As another example, the following command creates the Admin named list and sends the outbound Telnet connection information to the TACACS+ server when the connection is made and when it is terminated:

```
ProCurve (config)# aaa accounting connection Admin start-stop group tacacs+
```

## Assign the Named List

To assign the accounting named list that you created to a console, Telnet, or SSH line, you must move to the appropriate line configuration mode context. If you want to record configuration activities for all Telnet and SSH lines, you must ensure that you assign the named list to all of the Telnet or SSH lines that you have enabled. For example, if you have enabled all five Telnet lines, you must assign the named list to all five lines.

If you have created a named list to track the users who access the basic or enable mode context, you use the following command to assign the named list. From the appropriate line configuration mode context, enter:

***Syntax:*** accounting commands [1 | 15] [default | <*named list*>]

For example, you might create a named list called **Account** and then assign it to all of the Telnet lines. You might also include the **15** option because you want this named list to record information about the commands entered from the privileged mode. From the global configuration mode context, enter:

```
ProCurve (config)# line telnet 0 4
ProCurve (config-telnet04)# accounting commands 15 Account
```

If you have created a named list to track all connections, or logins, or if you have created a named list to track outbound Telnet connections, you use the following command to assign the named list. From the appropriate line configuration mode context (such as the Telnet 0-4 lines), enter:

***Syntax:*** accounting [connection | exec] [default | <*named list*>]

Include the **connection** option if you want to track all outbound Telnet connections made from this line. Include the **exec** option if you want to track all login connections made from this line.

### Configure Update Settings

You can configure when the ProCurve Secure Router sends updates to the TACACS+ server. To configure updates, enter the following command from the global configuration mode context:

***Syntax:*** aaa accounting update [newinfo | periodic <*minutes*>]

Include **newinfo** if you want all new records sent immediately, or include **periodic** if you want the records sent at specific intervals. If you specify **periodic**, replace ***<minutes>*** with a number from 1 to 2,147,483,647.

### Do Not Send Records for Null Users

By default, the ProCurve Secure Router does not send accounting information for the null usernames. Null usernames are any users that the TACACS+ system cannot identify. For example, if you do not control access to the console line through the TACACS+ servers, users who access and make changes through the console line will not be known to the TACACS+ server. The ProCurve Secure Router will not send information about such users to the TACACS+ server unless you change this default setting. To change the setting, enter:

***Syntax:*** no aaa accounting suppress null-username

## Configuring a RADIUS Server for Authentication

In order to use a RADIUS server in a named list, you must configure the Secure Router OS to locate and contact that RADIUS server. If your network includes multiple RADIUS servers, you can add these servers to the default group of RADIUS servers or define a group of RADIUS servers. In addition, you can configure specific settings for each RADIUS server, or you can configure global settings for all of the RADIUS servers you define.

### Define the RADIUS Server

The ProCurve Secure Router must be able to locate and communicate with the RADIUS server. (See Figure 2-2.)

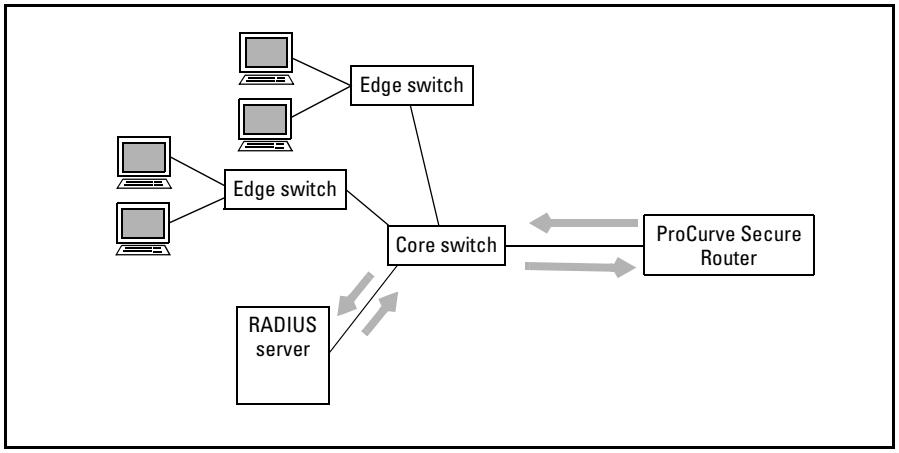


**Figure 2-2. Using a RADIUS Server for Authenticating Users Who Want to Manage the ProCurve Secure Router**

To set up this communication, you must specify the IP address of the RADIUS server. Enter the following command from the global configuration mode context:

***Syntax:*** radius-server host <*A.B.C.D* | *hostname*> [acct-port <*port number*> | auth-port <*port number*> | retransmit <*number*> | timeout <*seconds*> | key <*key*>]

To define the RADIUS server, you simply enter the first part of the command:

***Syntax:*** radius-server host <*A.B.C.D* | *hostname*>

Either replace <*A.B.C.D*> with an IP address or replace <*hostname*> with the RADIUS server's host name. For example, if your RADIUS server has the IP address of 192.168.115.5, enter:

```
ProCurve(config)# radius-server host 192.168.115.5
```

You can also configure other settings—such as the authentication port and the shared key—for the RADIUS server. Table 2-4 lists the available options.

**Table 2-4. Customizing Settings for Individual RADIUS Servers**

| Option | Meaning | Default Value |
|---|---|---|
| **acct-port <port number>** | Configures the router to send accounting requests to the port you specify. You can specify a number between 0 and 65535. | acct-port 1813 |
| **auth-port <port number>** | Configures the router to send authentication requests to the port you specify. You can specify a number between 0 and 65535. | auth-port 1812 |
| **retransmit <attempts>** | Specifies the number of times the router tries to contact the RADIUS server after the timeout expires. You can specify a number between 1 and 100. | global RADIUS setting |
| **timeout <seconds>** | Specifies the number of seconds the router waits if it does not receive a response from the RADIUS server. You can specify a number between 1 and 1000. | global RADIUS setting |
| **key <key>** | Defines the shared key the router uses to authenticate to the RADIUS server. | none |

For example, you might enter:

```
ProCurve(config)# radius-server host 192.168.115.5 acct-port 1646 key secret
```

After you define a RADIUS server, that server is added to the router's default RADIUS group. If you define a second RADIUS server, it is added to the default group, and the Secure Router OS contacts the servers in the order in which you entered them. Once you define the RADIUS servers in the default group, this order cannot be changed.

If you want to change the order in which the Secure Router OS contacts the RADIUS servers, you should create a RADIUS server group, as described in the next section.

## Define a Group of RADIUS Servers

To define a group of RADIUS servers, enter the following command from the global configuration mode context:

***Syntax:*** aaa group server radius <*groupname*>

Replace ***<groupname>*** with a name that is meaningful to you.

For example, the following command creates a group called myServers and enters the RADIUS group configuration mode context:

```
ProCurve(config)# aaa group server radius myServers
ProCurve(config-sg-radius)#
```

From this context, use the following command to add RADIUS servers to the group:

***Syntax:*** server <*hostname* | *A.B.C.D*> [acct-port <*port*> | auth-port <*port*> ]

Either replace <*hostname*> with the RADIUS server's hostname or replace <*A.B.C.D*> with the RADIUS server's IP address.

Include the **acct-port** or the **auth-port** option if you want to change the default ports that the ProCurve Secure Router uses to send information to the RADUIS server. By default, the router uses port 1813 for accounting updates and port 1812 for authorization updates.

The following examples add servers to the myServers group:

```
ProCurve(config)# aaa group server radius myServers
ProCurve(config-sg-radius)# server 1.2.3.4
ProCurve(config-sg-radius)# server 4.3.2.1
ProCurve(config-sg-radius)# exit
```

or

```
ProCurve(config)# aaa group server radius myServers
ProCurve(config-sg-radius)# server 2.2.2.2
ProCurve(config-sg-radius)# exit
```

You must use the **radius-server** command to define RADIUS servers before you can add them to a group. If a server is added to a named group but is not defined by a **radius-server** command, the router simply bypasses that server in the list.

Empty RADIUS groups are not saved. When the last server is removed from a group, the Secure Router OS automatically deletes the group.

## Configure Global Settings for RADIUS Servers

You can configure global settings that will be applied to all RADIUS servers defined on the router. However, if you configure specific settings for a RADIUS server, these settings will override the global settings.

To configure global settings, you use the **radius-server** command, but you do not specify a particular server. Instead, you use the following command syntax:

***Syntax:*** radius-server [challenge-noecho | deadtime <*minutes*> | enable-username <*name*> | key <*key*> | retry <*attempts*> | timeout <*seconds*>]

You must enter this command from the global configuration mode context. Table 2-5 lists all the options and what they do.

**Table 2-5. Global Settings for RADIUS Servers**

| Option | Meaning | Default Value |
|---|---|---|
| **challenge-noecho** | disables echoing of user challenge-entry; users will see the text of the challenge as they type responses (enabling this option hides the text as it is being entered) | on |
| **deadtime <minutes>** | specifies how long a RADIUS server is considered "dead" if a timeout occurs; the router will not contact the server again until after the deadtime expires | 1 minute |
| **enable-username <name>** | specifies a username to be used for enable authentication | enable-username $enab15$ |
| **key <key>** | specifies the shared key to use with RADIUS servers | none |
| **retry <attempts>** | specifies how many times the ProCurve Secure Router should try to contact a RADIUS server before marking it as "dead" | 3 |
| **timeout <seconds>** | specifies how long to wait for a RADIUS server to respond to a request | 5 seconds |

The following is an example configuration for global RADIUS settings:

```
ProCurve(config)# radius-server challenge-noecho
ProCurve(config)# radius-server deadtime 10
ProCurve(config)# radius-server timeout 2
ProCurve(config)# radius-server retry 4
ProCurve(config)# radius-server key my secret key
```

## Configuring the TACACS+ Server

In addition to supporting authentication, the ProCurve Secure Router supports authorization and accounting with TACACS+ servers. If you want to use a TACACS+ server to authenticate, authorize, or keep track of users who want to manage the ProCurve Secure Router, you must first define the TACACS+ server.

### Define the TACACS+ Server

In order to authenticate, authorize, and track users who try to access the ProCurve Secure Router, the TACACS+ server must be able to communicate with the router. (See Figure 2-3.)

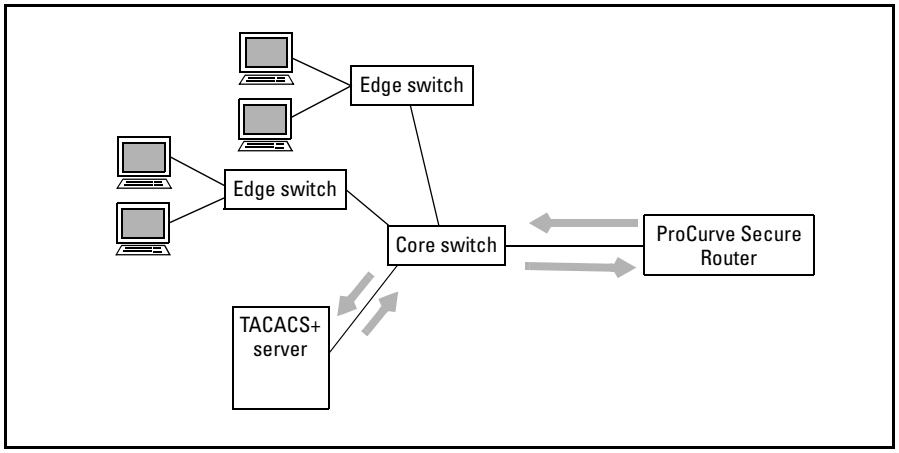


**Figure 2-3. Using a TACACS+ Server for Authenticating Users Who Want to Manage the ProCurve Secure Router**

To enable this communication, you must configure the IP address or host name of the TACACS+ server. From the global configuration mode context, enter:

***Syntax:*** tacacs-server host <*A.B.C.D* | *hostname*>

Either replace <*A.B.C.D*> with an IP address or replace <*hostname*> with the TACACS+ server's host name. For example, if the TACACS+ server has the IP address 192.168.7.1, enter:

```
ProCurve(config)# tacacs-server host 192.168.7.1
```

After you define a TACACS+ server, that server is added to the router's default TACACS+ group. If you define a second TACACS+ server, it is added to the default group, and the Secure Router OS contacts the servers in the order in which you entered them. After you define TACACS+ servers, you cannot change the order in which TACACS+ servers are listed in the default group. (Instead, you would have to delete servers by entering the **no tacacs-server host** command and then redefine them in the order you want them used.)

If you want to change the order in which the Secure Router OS contacts the TACACS+ servers, you can create a TACACS+ server group, as described in "Creating a TACACS+ Group" on page 2-37.

You can use the complete **tacacs-server** command to configure other settings for a TACACS+ server, as shown below:

***Syntax:*** tacacs-server host <*A.B.C.D* | *hostname*> [port <*number*> | timeout <*seconds*> | key <*key*>]

You can enter all of the options with one command if you include them in the order shown above. Table 2-6 lists these options and provides a brief explanation for each one.

**Table 2-6. Customizing Settings for TACACS+ Servers**

| Option | Meaning | Default Value |
|---|---|---|
| **port <number>** | Specifies the TCP port number to be used when connecting to the TACACS+ server. You can enter a number between 1 and 65535. | 49 |
| **timeout <seconds>** | Specifies the period of time (in seconds) that the router will wait for a response before it declares an error. You can specify a number between **1** and **1000**.<br>This command overrides any time you set with the **tacacs-server timeout** command. For more information about this command, see "Configure Global Settings for TACACS+ Servers" on page 2-38. | 5 |
| **key <key>** | Specifies the shared secret for the TACACS+ server. This command overrides any key specified with the **tacacs-server key** command. For more information about this command, see "Configure Global Settings for TACACS+ Servers" on page 2-38. | none |

For example, you might enter:

```
ProCurve(config)# tacacs-server host 192.168.7.1 timeout 10 key cool
```

After you entered this command, the ProCurve Secure Router would time out the connection if the TACACS+ server did not respond after 10 seconds, and the router would use cool as the shared secret with the TACACS+ server.

## Creating a TACACS+ Group

To define a group of TACACS+ servers, enter the following command from the global configuration mode context:

***Syntax:*** aaa group server tacacs+ <*groupname*>

Replace ***<groupname>*** with a name that is meaningful to you.

For example, the following command creates a group called tacacs and enters the TACACS+ group configuration mode context:

```
ProCurve(config)# aaa group server tacacs+ tacacs
ProCurve(config-sg-tacacs+)#
```

Use the following command to add TACACS+ servers to the group:

***Syntax:*** server <*hostname* | *A.B.C.D*>

Either replace <*hostname*> with the TACACS+ server's hostname or replace <*A.B.C.D*> with the server's IP address.

The following example adds two servers to the tacacs group:

```
ProCurve(config-sg-tacacs+)# server 192.168.1.1
ProCurve(config-sg-tacacs+)# server 192.168.7.101
ProCurve(config-sg-tacacs+)# exit
```

You must use the **tacacs-server** command to define TACACS+ servers before you can add them to a group. If you add a server to a group but the server is not defined by a **tacacs-server** command, the router simply bypasses that server in the group.

The Secure Router OS does not save empty TACACS+ groups. When the last server is removed from a group, the Secure Router OS automatically deletes the group.

## Configure Global Settings for TACACS+ Servers

You can configure global settings that will be applied to all TACACS+ servers defined on the router. However, if you configure specific settings for a TACACS+ server, those settings override the global settings.

To configure global settings, you use the **tacacs-server** command, but you do not specify a particular server. Instead, you use the following commands:

***Syntax:*** tacacs-server key <*key*>

***Syntax:*** tacacs-server packet maxsize <*size*>

***Syntax:*** tacacs-server timeout <*seconds*>

**Table 2-7. Global Settings for TACACS+ Servers**

| Option | Meaning | Default Value |
|---|---|---|
| **tacacs-server key <key>** | Specifies the shared key to use with TACACS+ servers. Any keys you configure for a particular TACACS+ server supersede the global key. | none |
| **packet maxsize <size>** | Defines the packet size to send to the TACACS+ server. You can specify a number between 10240 and 65535. | 10240 |
| **tacacs-server timeout <seconds>** | Specifies how long to wait for the TACACS+ server to respond to a request. You can specify a number between 1 and 1000. | 5 seconds |

# Troubleshooting AAA

The ProCurve Secure Router provides several commands to help you troubleshoot the AAA subsystem.

## debug aaa Command

You can view detailed messages about the AAA subsystem in real time. From the enable mode context, enter:

***Syntax:*** debug aaa

The Secure Router OS will then display AAA events such as connection notices, login attempts, and session tracking. Figure 2-4 shows the debug aaa messages when a user attempts to establish a Telnet session but does not enter a valid username and password. The AAA subsystem has been enabled on the router, but no named list has been defined for Telnet access, so the ProCurve Secure Router uses the default named list.

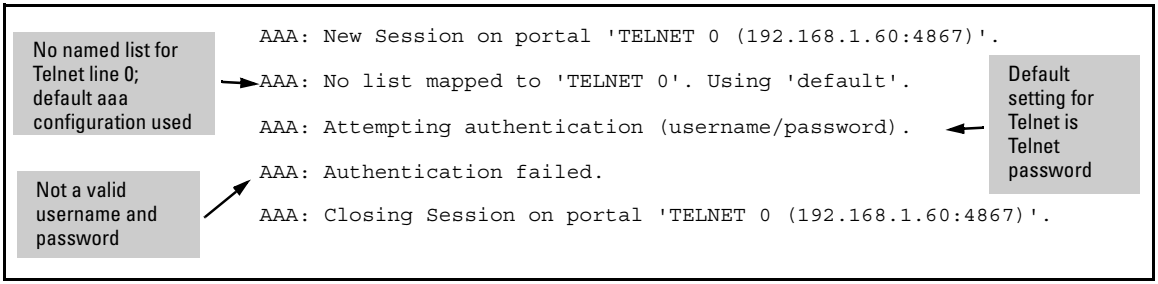


**Figure 2-4. debug aaa**

To end the debug messages, enter:

***Syntax:*** no debug aaa

## Troubleshooting the RADIUS Server

To view information about RADIUS servers, enter the following command from the enable mode context:

ProCurve# show radius statistics

This command displays information such as:

- number of packets sent
- number of invalid responses
- number of timeouts
- average packet delay
- maximum packet delay

Statistics are shown for both authentication and accounting packets. (See Figure 2-5.)

```
                                          Auth.       Acct.
Number of packets sent:                   10          0
Number of invalid responses:              2           0
Number of timeouts:                       0           0
Average delay:                            2 ms        0 ms
Maximum delay:                            3 ms        0 ms
```

**Figure 2-5. show radius statistics**

### debug radius Command

You can view debug messages about RADIUS servers in real time. From the enable mode context, enter:

***Syntax:*** debug radius

The RADIUS debug messages show the communication process with the remote RADIUS servers, as shown below.

RADIUS AUTHENTICATION: Sending packet to 172.22.48.1 (1645).
RADIUS AUTHENTICATION: Received response from 172.22.48.1.

To end the debug messages, enter one of the following commands:

***Syntax:*** no debug radius

## Troubleshooting the TACACS+ Server

You can display information about the authentication, authorization, and accounting packets that the ProCurve Secure Router exchanges with the TACACS+ server. From the enable mode context, enter:

***Syntax:*** show tacacs+ statistics

Figure 2-6 shows the type of information displayed with this command.

```
                  Authentication      Authorization      Accounting
Packets sent:                 25                  0               0
Invalid responses:             0                  0               0
Timeouts:                      0                  0               0
Average delay:               0ms                0ms             0ms
Maximum delay:               0ms                0ms             0ms


Socket Opens:                          10
Socket Closes:                         10
Socket Aborts:                          0
Socket Errors:                          0
Socket Timeouts:                        0
Socket Failed Connections:              0
Socket Packets Sent:                   25
Socket Packets Received:               25
```

**Figure 2-6. Viewing Information about Authentication, Authorization, and Accounting Through the TACACS+ Server**

To clear the statistics associated with TACACS+ protocol, enter the following command from the enable mode context:

***Syntax:*** clear tacacs+ statistics

To debug the authentication, authorization, or accounting with the TACACS+ server, enter the following command at the enable mode context:

***Syntax:*** debug tacacs+ [packets | events]

Figure 2-7 shows the output if you enter this command to monitor authentication through the TACACS+ server.

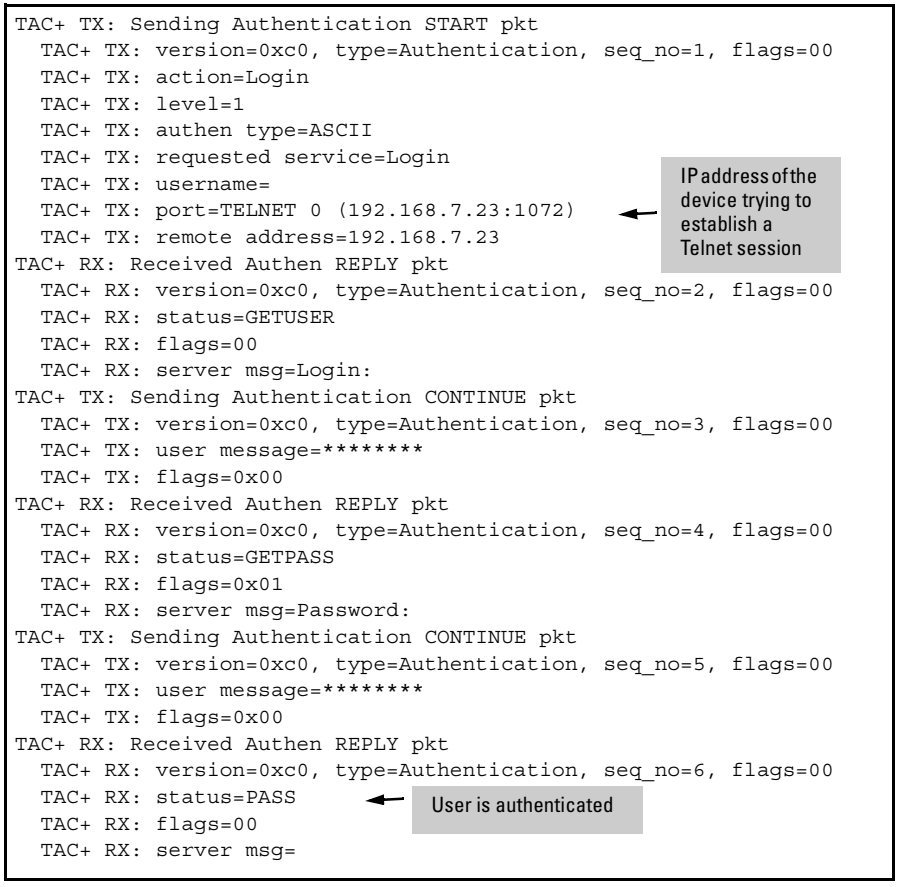


**Figure 2-7. Using the debug tacacs+ Command to Monitor Authentication Through the TACACS+ Server**

# Using SNMP to Manage the ProCurve Secure Router

SNMP is an industry-standard protocol that allows you to manage and monitor a variety of network devices from a central location. Specifically, you can configure these SNMP-compliant devices and apply consistent security and management policies to these devices across your network.

You can also monitor SNMP-compliant devices for conditions requiring administrative attention—for example, a server has gone down, a printer is jammed, or a WAN connection is no longer available. You can track device uptime, link states, and many other device information variables. When a problem occurs, SNMP-compliant devices send an alert message to one or more designated SNMP servers, and you can then take steps to resolve the problem.

## SNMP Architecture

SNMP works in a client-server relationship: SNMP agents, which function as clients, run on managed devices, and the SNMP server is a management application that requests, handles, and analyzes the information from the managed devices. Typically, you access the SNMP server from an SNMP console, or application.

SNMP is considered “simple” because the SNMP agent and the SNMP server use only five basic commands to communicate. However, the SNMP architecture is actually somewhat complicated.

In the SNMP architecture, managed devices such as the ProCurve Secure Router are represented and stored as network objects in a management information base (MIB); the objects are identified in a hierarchical name space containing object identifier (OID) numbers. Within the MIB, network objects can organized into views; the views, in turn, can be assigned to SNMP groups. Group members can then monitor the objects within the view. (See Figure 2-8.)

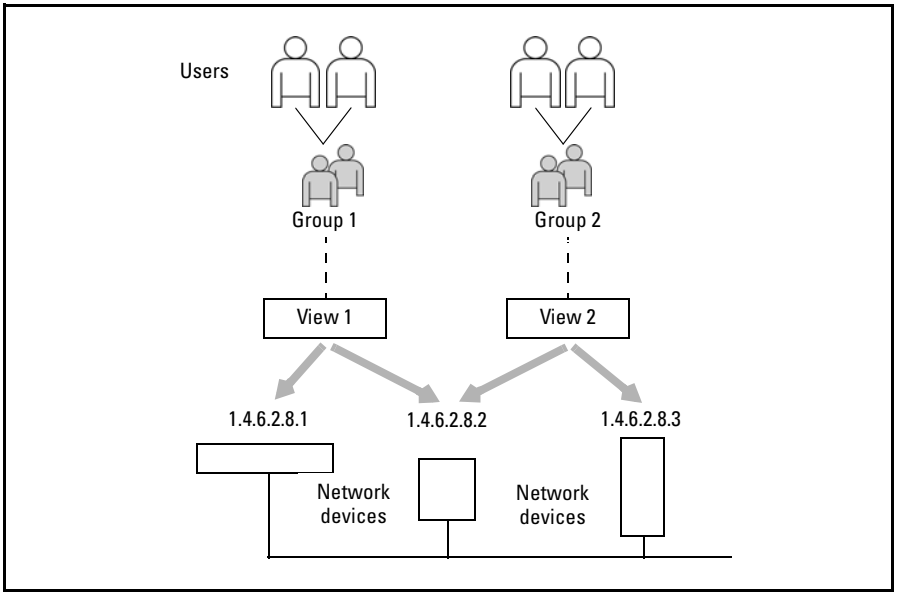


**Figure 2-8. Overview of Managed Objects in a MIB**

## SNMP Versions

Three versions of SNMP are currently implemented in SNMP agents and servers: SNMP v1, v2, and v3.

SNMP versions 1 and 2 use community strings to restrict SNMP access. To segregate types of access, you configure a separate community string for three access levels:

- Read-only—This access level limits the user to reading SNMP information only.
- Read-write—This access level gives the user complete access to SNMP functions, including the ability to make changes on managed devices.
- Trap—A trap allows the managed device to send an unsolicited update packet to the SNMP server. The managed device sends the update packet in response to an internally generated alarm—without being prompted by the SNMP server. In this access level, the SNMP agent sends only the traps that you specify to the SNMP server; the SNMP server receives the trap information but is not allowed to access other information about the SNMP agent—unless you grant the SNMP server an additional access level (such as a read-write community).

SNMP-compliant devices typically use public as the default read-only community and private as the default read-write community. Because many organizations do not change these default settings, their managed devices and SNMP servers are vulnerable to hackers.

In addition, SNMP v1 and v2 do not include security measures to protect the data exchanged between the SNMP agent and the SNMP server: neither the packets nor the community strings are encrypted, and no message integrity measures are provided. As a result, the early versions of SNMP are vulnerable to attacks such as:

- Man-in-the-middle—An attacker can alter in-transit SNMP messages generated on behalf of an authorized user in such a way as to affect management operations. An attacker with read-write access can infiltrate any SNMP-managed device.
- Impersonation—By assuming the identity of an user who has the appropriate authorizations, an attacker can gain read-write access to management operations.
- Reconnaissance—Because early implementations do not encrypt the community string or SNMP packet information, an attacker can eavesdrop on the exchanges between SNMP agents and an SNMP server and collect information about the network or discover the read-write community string.

SNMPv3 addresses the major security flaws in SNMP v1 and v2 by incorporating data authentication and encryption to protect SNMP packets:

- Community string encryption—SNMPv3 requires community string encryption in all packets, protecting against attacks.
- Data integrity—SNMPv3 uses usernames and passwords to determine who can and cannot gain the read-write access necessary to modify information. When the user provides his or her authentication password, the password is converted into a localized key. This key, the SNMP engine timestamp, and the actual message are compressed into a message digest and forwarded with the packet to provide integrity authentication. Therefore, an unauthorized user cannot alter the message in transit.
- Encryption—Along with the username and authentication password, each user is given a privacy password, which is used to encrypt the message packet. SNMP v3 uses encryption algorithms to encrypt the localized key and the SNMP packet.

- Security Levels—SNMP v3 also provides three optional security levels which determine whether the data integrity and encryption described above are used:
  - noAuthNoPriv—This level does not provide authentication (data integrity) or privacy (encryption) and is, therefore, not recommended.
  - AuthNoPriv—This level provides authentication but no privacy.
  - AuthPriv—This level provides both authentication and privacy.

## SNMP Support in the ProCurve Secure Router

The ProCurve Secure Router has always supported SNMP v1 and v2. The J.05 release of the Secure Router OS adds support for SNMP v3. Specifically, the following SNMP commands are new or enhanced in the J.05 release:

- **snmp-server contact**
- **snmp-server engineID**
- **snmp-server group**
- **snmp-server host**
- **snmp-server inform**
- **snmp-server user**
- **show snmp**

Most SNMP functions for the ProCurve Secure Router are controlled by **snmp-server** commands entered from the global configuration context.

You can download MIBs for your SNMP management server from the ProCurve Networking Web site at *http://www.procurve.com*.

## Enabling the SNMP Agent on the ProCurve Secure Router

The ProCurve Secure Router includes an SNMP agent, which allows it to be a managed device in your SNMP management domain. By default, however, the SNMP agent is disabled. To enable this agent, enter the following command from the global configuration mode context:

***Syntax:*** ip snmp agent

To disable the SNMP agent once again, enter:

***Syntax:*** no ip snmp agent

# Configuring SNMP Identity Information

You can enter the **snmp-server** commands in this section to configure the information the ProCurve Secure Router will submit in response to queries from authorized SNMP servers.

## Change the Default Setting for the Router's Chassis ID

The ProCurve Secure Router is identified by a default chassis ID. For most environments, you should accept this default setting. However, if you need to change the default setting, you can use the **snmp-server chassis-id** command. From the global configuration mode context, enter:

***Syntax:*** snmp-server chassis-id <*string*>

Replace ***<string>*** with an alphanumeric string of up to 32 characters. For example, you could enter:

```
ProCurve(config)# snmp-server chassis-id A432692
```

Use the **no** form of the command to return the chassis ID to its default setting, "Chassis ID":

***Syntax:*** no snmp-server chassis-id

## Specify the Router's Location

You can specify the physical location of the ProCurve Secure Router with the **snmp-server location** command. From the global configuration mode context, enter:

***Syntax:*** snmp-server location <*string*>

Replace ***<string>*** with an alphanumeric string of up to 256 characters in length. For example, you might enter:

```
ProCurve(config)# snmp-server location Building1
```

If you want to include spaces in the string, you must enclose the string in quotations marks as shown below.

```
ProCurve(config)# snmp-server location "Floor 8, Network Room"
```

Use the **no** form of the command to remove the location.

***Syntax:*** no snmp-server location

## Specify the SNMP Server Contact Information

In large organizations, management tasks are distributed among a team of IT professionals. The IT professional who manages the SNMP server is probably not the same person who is responsible for managing the ProCurve Secure Router. You can use the **snmp-server contact** command to specify the contact information for the person who is managing the router. Then, if a problem occurs on the router, the SNMP administrator can contact the appropriate person to solve that problem.

You can specify the email address, pager number, phone number, and name for the IT professional who manages the ProCurve Secure Router. From the global configuration mode context, enter:

***Syntax:*** snmp-server contact [email <*address*> | pager <*number*> | phone <*number*> | <*string*>]

Table 2-8 lists the options for the **snmp-server contact** command.

**Table 2-8. Configuration Options for snmp-server contact Command**

| Option | Meaning |
|---|---|
| **email <address>** | Specifies an email address for the person managing the ProCurve Secure Router. |
| **pager <number>** | Specifies a pager number for the person managing the ProCurve Secure Router. |
| **phone <number>** | Specifies a telephone number for the person managing the ProCurve Secure Router. |
| **<string>** | Specifies the name of the person managing the ProCurve Secure Router. The string can be a maximum of 256 characters. |

You can enter the **snmp-server contact** command multiple times to specify the email address, pager number, phone number, and name of the SNMP contact. For example, to specify the contact's name and telephone number, you might enter:

```
ProCurve(config)# snmp-server contact JeffStewart
ProCurve(config)# snmp-server contact phone 555-1212
```

If you want to include spaces in any of the options, you must enclose the information in quotation marks as shown below:

```
ProCurve(config)# snmp-server contact "Jeff Stewart"
```

Use the no form of the command to remove contact information.

***Syntax:*** no snmp-server contact [email | pager | phone | <string>]]

## Specify the SNMP Server Management URL Information

You can use the **snmp-server management-url** command to specify the URL for the router's management software. Again, this information might be helpful to the SNMP administrator if he or she needs to change a setting or view information that is not available through the SNMP console.

From the global configuration mode context, enter:

***Syntax:*** snmp-server management-url <*URL*>

Replace ***<URL>*** with the URL for the management software. For example, you might enter:

ProCurve(config)# snmp-server management-url http://192.168.1.1

Use the **no** form of the command to remove the URL.

***Syntax:*** no snmp-server management-url

You may want to provide additional information about the ProCurve Secure Router's management software. You can use the **snmp-server management-url-label** command to specify a label of up to 255 characters. From the global configuration mode context, enter:

***Syntax:*** snmp-server management-url-label <*label*>

Replace ***<label>*** with information about the management software. For example, you might enter:

ProCurve(config)# snmp-server management-url-label ProCurve Management Software

Use the **no** form of the command to remove the label.

***Syntax:*** no snmp-server management-url-label

## Change the Engine ID for a Local Machine

SNMP v3 requires unique engine IDs for all systems in the SNMP management domain. The ProCurve Secure Router has a default engine ID, and you should not change this ID unless you have a specific reason for doing so. If you inadvertently create two duplicate engine IDs in your SNMP management domain, you will cause problems.

By default, the local snmp-server engine ID is 0000000b03*XXXXXXXXXXXXXX*:

- 0000000b (in the first four octets) identifies the product as a ProCurve Secure Router. (Do *not* change this part of the engine ID.)
- 03 (in the fifth octet) indicates that the remaining digits specify a system MAC address.
- The string of *X*s (in the remaining octets) represents the system MAC address.

To view the current engine ID, enter **show snmp engineID** at the enable command mode context.

If you must change the engineID, enter the following command from the global configuration mode context:

***Syntax:*** snmp-server engineID local <*hex string*>

Replace ***<hex string>*** with an 12-octet hexadecimal representation (24 characters using 0 through 9 and a through f) to define the ProCurve Secure Router in your SNMP management domain.

**Note**

If you do not enter all 12 octets of the engine ID, the Secure Router OS pads the end of the entered string with zeros (least significant bits) until the string is complete.

For example, to change the engine ID to 0000000b05000000000032, enter:

```
ProCurve(config)# snmp-server engineID local 0000000b05000000000032
```

Use the **no** form of the command to return to the default engine ID.

***Syntax:*** no snmp-server engineID local

### Specifying the Engine ID for a Remote Server

When you configure a username to grant a user access to the ProCurve Secure Router, you can specify that the user's account is stored on a remote server. (See "Configure SNMP Users" on page 2-58.) In this case, you must first specify the remote server's engine ID. Enter this command from the global configuration mode context:

***Syntax:*** snmp-server engineID remote <*IP address*> <*hex string*>

Replace ***<hex string>*** with 24 hexadecimal characters.

## Configuring SNMP Views

In SNMP, the network devices to be monitored are configured as views. A *view* consists of one or more network objects that can monitored. When you configure a view, you specify *included* or *excluded* objects. If an object is not specified in the view, it is excluded by default. A given object can be included in or excluded from any number of views, as needed.

An object is identified by its OID in the network's MIB. The OID is a hierarchal string of numbers—for example, 1.4.6.2.8 would identify a specific subtree, and 1.4.6.2.8.* would identify an entire subtree family.

Management access to a view is controlled in two ways:

- Community strings—The community string serves as a password that SNMP users must provide in order to manage the objects in a view. When you create a community string, you specify the view that the community string applies to. (See "Configuring SNMP Traps and Informs" on page 2-60.)
- Group membership—When you create an SNMP group, you specify one or more views that the group (and its member users) has access to. (See "Create an SNMP Group" on page 2-56.)

When you assign views to a group, you can specify each view as one of three types:

- Read view—allows the group members to read (monitor) event notifications received from the network devices within the view
- Write view—allows the group members to write to (perform management functions for) network devices within the view
- Notify view—allows you to configure notify, inform, or trap event notifications for devices within the view

For example, you could create a view named view1 that *includes* a given subtree of OIDs in the MIB, as well as a view named view2 that includes the given subtree as a whole, but *excludes* a portion of the subtree. Then, you could create a group that uses view1 as a read view and view2 as a write view. (See Figure 2-9.)

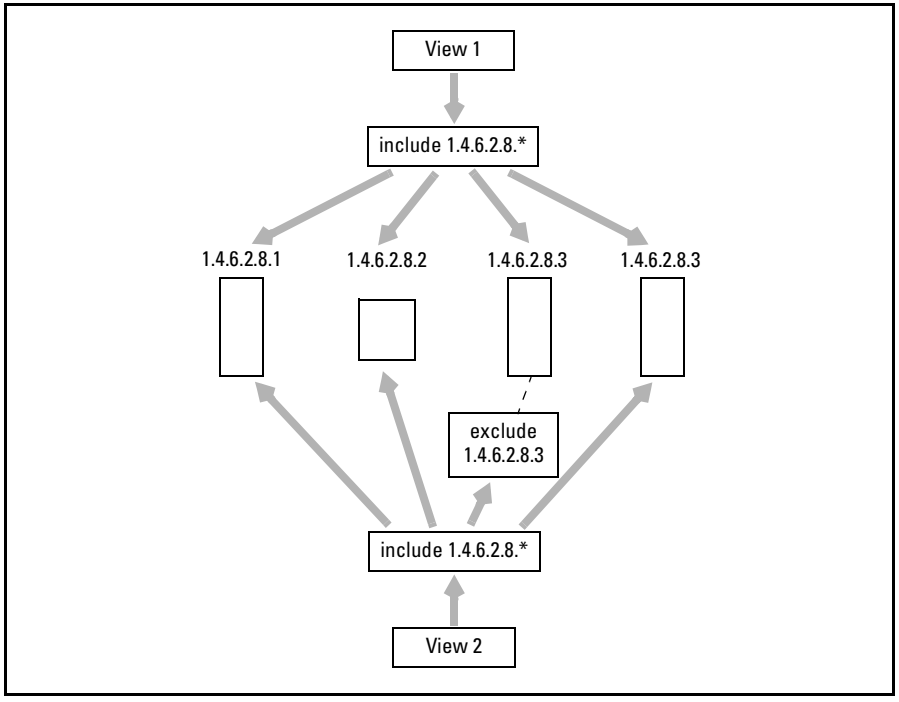


**Figure 2-9. Including or Excluding Objects in a View**

You can apply views in multiple ways as needed. For example, for a group, a given view can be specified as a read, write, or notify view. Or, a given view can be used as a read view for one group and a notify view for another group. You can set up multiple views as needed for your particular environment.

To create or modify an SNMP view for the ProCurve Secure Router, enter the following command from the global configuration mode context:

***Syntax:*** snmp-server view <*viewname*> <*oidtree*> [included | excluded]

Table 2-9 lists the options for the **snmp-server view** command.

**Table 2-9. Configuration Options for snmp-server view Command**

| Option | Meaning |
|---|---|
| **<viewname>** | Specifies the name of the view being created or modified. The name can be a maximum of 32 characters. |
| **<oidtree>** | Specifies the OID to include in or exclude from the view. To identify the subtree, specify a string using numbers, such as 1.4.2.6.8. To specify a subtree family, replace a single subidentifier with an asterisk (*). |
| **excluded** | Indicates that the OID should be excluded from the view. |
| **included** | Indicates that the OID should be included in the view. |

The **snmp-server view** command can include or exclude a group of OIDs.

The following example shows how to create a view called view1 that includes the OID subtree family 1.4.6.2.8:

```
ProCurve(config)# snmp-server view view1 1.4.6.2.8.* included
```

The following example shows how to create a view (named view2) to exclude a specific OID within a subtree family:

```
ProCurve(config)# snmp-server view view2 1.4.6.2.8.3 excluded
ProCurve(config)# snmp-server view view2 1.4.6.2.8.* included
```

Use the **no** form of the command to remove a specified view or a specific OID for the view.

***Syntax:*** no snmp-server view <*viewname*>

## Configuring SNMP Communities

You configure SNMP communities to control the information authorized SNMP servers can view or modify. You can create read-only communities and read-write communities. You can also restrict access to an SNMP view that you have previously configured, and you can use an access control list (ACL) to allow SNMP requests only from authorized SNMP servers (based on their IP address and other supported ACL filters such as protocols). For more information about configuring SNMP views, see “Configuring SNMP Views” on page 2-52. For more information about configuring ACLs, see *Chapter 5: Applying Access Control to Router Interfaces* in the *Advanced Management and Configuration Guide*.

To specify a community string to control access to SNMP information, enter the following command from the global configuration mode context:

***Syntax:*** snmp-server community <*community*> [view <*viewname*>] [ro | rw] [<*listname*>]

Table 2-10 lists the options for the **snmp-server community** command.

**Table 2-10. Configuration Options for snmp-server community Command**

| Option | Meaning |
|---|---|
| **<community>** | Specifies the name of the community string. |
| **ro** | Grants read-only access, allowing the SNMP server to view information. |
| **rw** | Grants read-write access, allowing the SNMP server to both view and modify information. |
| **view <viewname>** | Specifies the view for the community, which identifies the objects available to the community. You must configure the view separately. |
| **<listname>** | Specifies an ACL that limits the SNMP servers that can submit requests to the router. |

The **view <*viewname*>** setting is optional; if you do not specify a view, the community string setting will apply to all of your managed objects. If you want to specify a view, you must enter the **view** option before selecting between the **ro** and **rw** options.

If you do not explicitly specify the community as read-only or read-write, the Secure Router OS creates the community as read-only.

For example, to create a community called CompanyXYZ that uses a previously defined view called WANinterfaces and to assign this community read-write access, enter:

```
ProCurve(config)# snmp-server community CompanyXYZ view WANinterfaces rw
```

Use the **no** form of the command to remove a specified community.

***Syntax:*** no snmp-server community <*community*>

# Configuring SNMP Groups and Users

SNMP groups are used to map SNMP users to SNMP views. That is:

- When you create a group, you will specify one or more views that member users will have access to. A given view can be accessed by more than one group, as needed.
- When you create a user, you will specify the group to which the user belongs. The user's access to views is determined by that group membership.

Figure 2-10 illustrates group memberships.

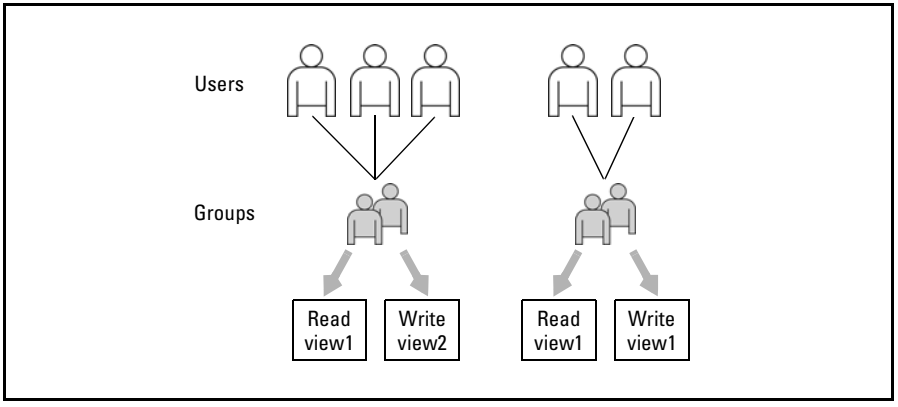


**Figure 2-10. Users Mapped to Views through Groups**

## Create an SNMP Group

You can use the **snmp-server group** command to create a new SNMP group to control access to SNMP information. From the global configuration mode context, enter:

***Syntax:*** snmp-server group <*groupname*> [v1 | v2c | v3 {auth | noauth | priv}] [read <*viewname*>] [write <*viewname*>] [notify <*viewname*>] [access <*listname*>]

**Note**

You can enter multiple options with the **snmp-server group** command, but if you want to use the **access** option to specify an ACL, you must enter this option last.

Table 2-11 lists the options for the **snmp-server group** command.

**Table 2-11. Configuration Options for snmp-server group Command**

| Option | Meaning |
|---|---|
| **<groupname>** | Specifies the name of the SNMP group. The name can be a maximum of 31 characters. |
| **v1 \| v2c \| v3** | Specifies the SNMP security model version. If the version is not specified, version 1 is used. |
| **auth \| noauth \| priv** | Specifies a security level for SNMP v3:<br>• The auth option requires authentication.<br>• The noauth option does not require authentication or encryption.<br>• The priv option requires both authentication and encryption. |
| **read <viewname>** | Specifies the read view to which the SNMP group has rights. |
| **write <viewname>** | Specifies the write view to which the SNMP group has rights. The group can then view and modify information in this view. |
| **notify <viewname>** | Specifies the notify view to which the SNMP group has rights. |
| **access <listname>** | Specifies a standard ACL to control which SNMP server or console group members can use to access SNMP information on the ProCurve Secure Router. |

If no views are specified, the ProCurve Secure Router automatically assigns default read and notify views that have no restrictions.

For example, suppose you want to define the Admins group with the following characteristics:

- uses the SNMP version 3 security model with authentication
- does not use an ACL
- uses the default read-write and notify view entries (no restrictions)

To create this group, you would enter:

```
ProCurve(config)# snmp-server group Admins v3 auth
```

You might want to set up a different group with more limited access. You could assign this group a read-view entry named view1 and a write-view entry named view2 (that is, users in the group would have read privileges for the objects defined in view1 and write privileges for the objects defined in view2). You would enter:

```
ProCurve(config)# snmp-server group LimitedAccess v3 auth read view1 write view2
```

In both examples, the users that you assign to the groups (using the **snmp-server user** command) will have the access to views that are specified in the respective **snmp-server group** commands.

You can also create more than one entry for the same group using different SNMP versions or v3 security options. For example, you could use views to limit the access of Admins who use the less secure SNMP v2c, entering:

```
ProCurve(config)# snmp-server group Admins v2 read view3 write view4
```

Use the **no** form of the command to remove a specified group.

***Syntax:*** no snmp-server group <*groupname*>

## Configure SNMP Users

You use the **snmp-server user** command to create users who can access SNMP information. There are several ways to enter this command. If you want to configure a user on the ProCurve Secure Router, enter the following command from the global configuration mode context:

***Syntax:*** snmp-server user <*username*> <*groupname*> [v1 | v2c | v3 {auth [md5 | sha] <*password*>} | {priv des <*password*>}] [access <*listname*>]

If you want to grant access to a user that is configured on a remote SNMP server, enter the following command from the global configuration mode context:

***Syntax:*** snmp-server user <*username*> <*groupname*> [remote <*SNMP server address*>] [v3 {auth [md5 | sha] <*password*>} {priv des <*password*>}] [access <*listname*>]

**Note**

When entering the **snmp-server user** command, you can include multiple options. If you want to use the **access** option to specify an ACL, you must enter this option last.

Table 2-12 lists the options for the **snmp-server user** command.

**Table 2-12. Configuration Options for snmp-server user Command**

| Option | Meaning |
|---|---|
| **<username>** | Specifies the name of the user on the SNMP host that connects to the managed object. The username can be a maximum of 15 characters. |
| **<groupname>** | Specifies the name of the SNMP group to which the user belongs. |
| **v1 \| v2c \| v3** | Specifies the SNMP security model version. |
| **auth [md5 \| sha] <password>** | For SNMP v3 only, specifies authentication as part of the security level, selects a hash algorithm, and specifies the password:<br>• md5 uses HMAC-MD5-96.<br>• sha uses HMAC-SHA-96. |
| **priv des <password>** | For SNMP v3 only, specifies the privacy part of the security level. Communications are encrypted with the specified password using the CBC-DES algorithm. |
| **remote** | Specifies that the user is created on a remote SNMP server. |
| **<SNMP server address>** | Specifies the IP address of the remote SNMP server on which the user is created. |
| **access <listname>** | Specifies a standard ACL to control which SNMP server or console the user can use to access SNMP information on the ProCurve Secure Router. |

For example, suppose you want to define a user named BobbyW with the following characteristics:

- Assign the user to group SNMPgroup1
- Use the SNMP v3 AuthNoPriv security model
- Use MD5 to encrypt the password and specify the password as passWORD6243

From the global configuration mode context, you would enter:

```
ProCurve(config)# snmp-server user BobbyW SNMPgroup1 v3 auth md5
passWORD6243
```

To define the same user but configure the SNMP v3 security level to use privacy in addition to authentication, enter:

```
ProCurve(config)# snmp-server user BobbyW SNMPgroup1 v3 auth md5
passWORD6243 priv des passWORD1466
```

Use the **no** form of the command to remove a user from a specified group.

***Syntax:*** no snmp-server user <*username*> <*groupname*> [v1 | v2c | v3 {auth [md5 | sha] <*password*>} | {priv des <*password*>}]

***Syntax:*** no snmp-server user <*username*> <*groupname*> [remote <*SNMP server address*>] [v3 {auth [md5 | sha] <*password*>} | {priv des <*password*>}] [access <*listname*>]

## Configuring SNMP Traps and Informs

SNMP traps are used to report an alert or other event about a managed device—for example, a WAN interface goes down, or the device reboots unexpectedly. Traps are one-way notification messages; they are not acknowledged by the receiving SNMP server (which may also be called the trap receiver).

Traps can be configured and enabled by the following router commands:

- **snmp-server enable traps** commands are used to enable and configure SNMP trap generation on a global basis. All users in all groups with a view of the router will receive trap notifications from it.
- **snmp-server host** commands are used to configure SNMP notifications to be received by a specific SNMP host, or server, which is identified by its IP address.

For the **snmp-server host** command, you can configure a second type of message, the inform notification. Inform notifications are similar to trap messages, except that the managed device expects a response from the SNMP server. Because inform notifications require *two-way* communication, the ProCurve Secure Router will repeat the inform message periodically until the SNMP server acknowledges the notification.

### Enabling SNMP Traps

To enable the ProCurve Secure Router to send SNMP traps, enter the following command from the global configuration mode context:

***Syntax:*** snmp-server enable traps [snmp]

If you do not include the **snmp** option, only the system traps are enabled. If you include the **snmp** option, you enable the SNMP traps listed in Table 2-13. (These traps are outlined in Request for Comments [RFC] 1157.)

**Table 2-13. Supported SNMP Traps**

| Trap | Indication |
|---|---|
| **coldStart** | The ProCurve Secure Router has reset, and its configuration may be altered. |
| **warmStart** | The router is reinitializing itself, but the managed objects in its view have not been altered. |
| **linkDown** | An interface has gone from the up state to the down state. |
| **linkUp** | An interface has gone from the down state to the up state. |
| **authenticationFailure** | An SNMP message has been received that failed authentication—for example, a bad community string. |

For example, to enable the SNMP traps, enter:

```
ProCurve(config)# snmp-server enable traps snmp
```

Use the **no** form of the command to disable SNMP traps:

***Syntax:*** no snmp-server enable traps [snmp]

## Specifying Which SNMP Server Receives the Router's Notifications

You use the **snmp-server host** command to configure the SNMP server that will receive SNMP notifications (traps or informs) from the ProCurve Secure Router. (This SNMP server is also sometimes called the SNMP trap receiver.)

**Sending SNMP Traps.** To send traps to a server, from the global configuration mode context, enter:

***Syntax:*** snmp-server host <*ip address*> traps [<*community or username*>] [version 1 <*community*> | version 2c <*community*> | version 3 {auth <*username*> | noauth <*username*> | priv <*username*>}] [snmp]

Specifying the version for the trap receiver is optional; in this case, specify the community or username for the receiver after the **traps** keyword. Otherwise, specify the community or username after the version. Include the **snmp** option to send the SNMP traps in Table 2-13.

**Sending Informs.** To send informs (which require a response) to a server, from the global configuration mode context, enter:

***Syntax:*** snmp-server host <*ip address*> informs [version 1 <*community*> | version 2c <*community*> | version 3 {auth <*username*> | noauth <*username*> | priv <*username*>}] [snmp]

Table 2-14 lists the options for the **snmp-server host** command:

**Table 2-14. Configuration Options for snmp-server host Command**

| Option | Meaning |
|---|---|
| **<ip address>** | Specifies the IP address of the SNMP server. IP addresses should be expressed in dotted decimal notation (for example, 10.10.10.1). |
| **informs** | Enables informs to this SNMP server. |
| **traps** | Enables traps to this SNMP server. |
| **version [1 \| 2c \| 3]** | Specifies the SNMP security model version. If the version is not specified, version 1 is used. |
| **[auth \| noauth \| priv]** | Specifies the security level for SNMP v3:<br>• The auth option requires authentication.<br>• The noauth option does not require authentication or encryption.<br>• The priv option requires authentication with encryption. |
| **<community>** | Specifies the community string. |
| **snmp** | Enables the sending of the SNMP (RFC 1157) notification type. (See Table 2-13 on page 2-61.) |

For example, to send all SNMP traps to the SNMP server at address 10.1.1.1 using community string CommunityXYZ, enter:

```
ProCurve(config)# snmp-server host 10.1.1.1 traps CommunityXYZ snmp
```

## Specify the Response Retry Attempts and Wait Time

You can configure the number of times the ProCurve Secure Router attempts to contact an SNMP server and the amount of time the router waits to receive a response before sending a new request. These settings apply to SNMP inform notifications, which, unlike traps, are *two-way* messages: the managed device that sends the message waits for an acknowledgement from the SNMP server.

From the global configuration mode context, enter:

***Syntax:*** snmp-server inform [retries <*number*>] [timeout <*value*>]

Table 2-15 lists the options for the **snmp-server inform** command:

**Table 2-15. Configuration Options for snmp-server inform Command**

| Option | Meaning |
|---|---|
| **retries <number>** | Specifies the number of retries for a response. The range is from 1 to 100; the default setting is 3. |
| **timeout <value>** | Specifies the time (in seconds) to wait for a response. The range is from 1 to 1,000; the default setting is 5. |

For example, to set the retry count to 10, enter:

```
ProCurve(config)# snmp-server inform retries 10
```

You can combine the retries and timeout options in a single command as shown below.

```
ProCurve(config)# snmp-server inform retries 10 timeout 15
```

## Specify the Source Interface for SNMP

Because each Data Link Layer interface on the ProCurve Secure Router can have a different IP address, you may want to specify a source interface for SNMP. All SNMP originated packets (including traps and get/set requests) will then use the designated interface's IP address.

To specify a source interface for SNMP, enter the following command from the global configuration mode context:

***Syntax:*** snmp-server source-interface <*interface*>

Replace ***<interface>*** with the Data Link Layer interface that should originate SNMP traps. Enter **snmp-server source-interface ?** for a complete list of valid interfaces.

For example, to specify that the Ethernet 0/2 interface should be the source for all SNMP traps and get/set requests, enter:

```
ProCurve(config)# snmp-server source-interface ethernet 0/2
```

## Viewing SNMP Information

You can use **show snmp** commands to view the SNMP identity information and SNMP statistics on the ProCurve Secure Router. From the basic or enable mode context, enter:

```
ProCurve> show snmp
```

Your chassis ID, contact, and management URL information will be displayed, along with information about SNMP packets that have been received by the router.

To view a list of your SNMP users and related settings, enter the following command from the basic or enable mode context:

```
ProCurve# show snmp user
```

To view a list of your SNMP groups, from the enable mode context, enter the following command from the basic or enable mode context:

```
ProCurve# show snmp group
```

To view the current engine ID, enter the following command from the basic or enable mode context:

```
ProCurve# show snmp engineID
```

# The ProCurve Secure Router as an 802.1X Supplicant

Allowing mobile devices unlimited access to a network poses a severe security risk. While it is beneficial to allow employees to plug in and gain access to a company's LAN, there is the potential that unauthorized users may similarly gain access to your network.

Devices can be required to authenticate themselves before they are assigned an IP address on a network and before the access port is opened. The IEEE 802.1X protocol provides a standard for this authentication.

## Enabling Supplicant Functionality

The ProCurve Secure Router can act as an IEEE 802.1X supplicant. You can set the supplicant username and password for access to the protected network using the **port-auth** command.

To enable the router to function as a supplicant:

1. Move to the configuration mode context for the Ethernet interface that you want to use to access the 802.1X-secured network.

   ```
   ProCurve(config)# interface eth 0/1
   ProCurve(config-eth 0/1)#
   ```

2. Configure the supplicant username and password:

   ***Syntax:*** port-auth supplicant username <*username*> password <*password*>

   ```
   ProCurve(config-eth 0/1)# port-auth supplicant username ProCurve password
   ProCurve
   ```

   The default username is "username," and the default password is "password."

3. Enable the interface's supplicant functionality by entering the following:

   ```
   ProCurve(config-eth 0/1)# port-auth supplicant
   ```

As soon as you enable the supplicant functionality, the interface begins to attempt to authenticate itself and establish a connection to the 802.1X-secured network.

## Troubleshooting Supplicant Functionality

If the ProCurve Secure Router is unable to access the 802.1X-secured network, begin troubleshooting by checking the physical connection. Ensure that the 10Base-T or 100Base-T cable is connected and in the proper ports.

Check the supplicant status and make sure that it is enabled and that you have entered the correct username and password. You can do this by entering the following from the enable mode context:

***Syntax:*** show port-auth supplicant [summary | interface <*slot*>/<*port*>]

ProCurve# show port-auth supplicant interface eth 0/1

This command displays the Local Supplicant mode (enabled or disabled), the username and password that are configured, the interface's authorization and connection status. The **summary** option displays all Ethernet interfaces, the status of the supplicant (enabled or disabled), the supplicant's current state, and whether the interface is authorized.

Debug the supplicant interface by entering:

***Syntax:*** debug port-auth [general | packet {both | rx | tx} | supp-sm]

The **general** option displays messages when the port authentication configuration changes. To view information on the packet exchange in transmit-only, receive-only, or both directions, use the **packet** option. The **supp-sm** option displays information on the supplicant state machine.

If you have entered the correct username and password, and you have checked the physical connection and access is still denied, you may need to contact the 802.1X-secured network's administrator. Then determine what other authentication requirements may be needed and ensure that the administrator did not miskey your supplicant username and password.

# Quick Start

This section provides the commands you must enter to quickly configure passwords to protect management access to the ProCurve Secure Router. Only a minimal explanation is provided.

If you need additional information about any of these options, see "Contents" on page 2-1 to locate the section and page number that contains the explanation you need.

## Configure the Enable Mode Password

From the global configuration mode context, enter:

***Syntax:*** enable password [md5] <*password*>

Replace <*password*> with any combination of up to 30 characters. The Message Digest 5 (**md5**) option encrypts the password. If you do not enter this option, the password is stored in clear text in the running-config.

## Configure a Password for the Console Access

By default, you do not have to enter a password to access the ProCurve Secure Router through a console session. To configure a password to protect console access, complete these steps:

1. From the global configuration mode context, enter:

   ProCurve(config)# line console 0

2. Enter the **login** command to require a password for console access.

   ProCurve(config-con0)# login

3. Create a password:

   ***Syntax:*** password [md5] <*password*>

   Replace <*password*> with any combination of up to 30 characters. Use the **md5** option if you want the password encrypted. For example:

   ProCurve(config-con0)#password md5 procurve

   If you do not enter the **md5** option, the password is stored in clear text in the running-config.

# Configuring Remote Access to the ProCurve Secure Router

You can access the ProCurve Secure Router through:

- Telnet
- SSH
- HTTP
- FTP
- Secure Copy (SCP) server

## Configuring an Ethernet Interface

Before you can access the router through a remote location, you must enable at least one interface and provide a physical connection to either a LAN or WAN. This section provides the minimum steps required to configure an Ethernet interface and to connect that interface to your company's LAN. You can then access the router from a workstation on the LAN. For more detailed information about configuring an Ethernet interface, see *Chapter 3: Configuring Ethernet Interfaces*.)

1. Use a 10Base-T or 100Base-T cable to connect the Ethernet port to a device (such as a switch) on your LAN.
2. Open your terminal session software and initiate a console session with the ProCurve Secure Router, using the following parameters:
   - Baud Rate = 9600
   - Parity = None
   - Data Bits = 8
   - Stop Bits = 1
   - Flow Control = None
3. Press **Enter** when you are prompted to start a session with the router. The router basic mode context prompt appears, as shown below:

   ```
   ProCurve>
   ```

4. Access the enable mode context:

   ```
   ProCurve> enable
   ```

5. Access the global configuration mode context:

   ```
   ProCurve# configure terminal
   ```

6. From the global configuration mode context, enter the Ethernet interface configuration mode context:

   ProCurve(config)# interface ethernet 0/<port>

7. Assign the Ethernet interface an IP address.

   ***Syntax:*** ip address <*A.B.C.D*> [<*subnet mask*> | /<*prefix-length*>]

   For example, if you want to assign the Ethernet interface an IP address of 192.168.1.1 with a subnet mask of 255.255.255.0, enter

   ProCurve(config-eth 0/1)# ip address 192.168.1.1 /24

8. Activate the Ethernet interface.

   ProCurve(config-eth 0/1)# no shutdown

9. Save your configuration.

   ProCurve(config-eth 0/1)# do write memory

## Configuring a Password for Telnet Access

By default, you are required to configure a password for Telnet access. In addition, you must configure an enable mode password.

1. From the global configuration mode context, enter the following command:

   ***Syntax:*** line telnet <0–4>

   For example, if you want to configure port 0, enter:

   ProCurve(config)# line telnet 0

   If you want to configure all the Telnet ports, enter:

   ProCurve(config)# line telnet 0 4

2. Configure a password for Telnet access:

   ***Syntax:*** password [md5] <*password*>

   For additional security, use the **md5** option to encrypt the password.

   For example, if you want to create the password as procurve, enter

   ProCurve(config-telnet0)# password md5 procurve

3. Exit to the global configuration mode context and create a password for the enable mode context.

   ***Syntax:*** enable password [md5] <*password*>

**Note**

You can configure an access control list (ACL) to block Telnet access. For instructions on configuring this ACL, see *Chapter 5: Applying Access Control to Router Interfaces* in the *Advanced Management and Configuration Guide*.

## Configuring Local User Lists

You can configure multiple usernames and passwords to be used for FTP, HTTP, and SSH access to the router. From the global configuration mode context, enter:

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

These passwords are stored in the local user lists.

To encrypt *all* the passwords configured on the ProCurve Secure Router, enter the following command from the global configuration mode context:

```
ProCurve(config)# service password-encryption
```

The ProCurve Secure Router automatically supports SSH and FTP access. After you configure a password in the local user list, you can access the router through these methods.

**Enabling HTTP Access.** From the global configuration mode context, enter:

```
ProCurve(config)# ip http server
```

If you want to use Secure Sockets Layer (SSL) to protect the communications between your PC and the router, enter:

```
ProCurve(config)# ip http secure-server
```

**Enabling the SCP Server.** To encrypt files as they are copied to and from the ProCurve Secure Router, enter the following command from the global configuration mode context:

***Syntax:*** ip scp server

# Enabling AAA

If you want to use AAA for authentication, authorization, or accounting, you must first enable the AAA subsystem by entering the following command from the global configuration mode context:

```
ProCurve(config)# aaa on
```

## Configuring Authentication with AAA

1. Create a list of authentication methods, called a named list, for the enable mode context.

   ***Syntax:*** aaa authentication enable default [none | line | enable | {group <*groupname*> | radius | tacacs+}]

   For example, you might enter:

   ```
   ProCurve(config)# aaa authentication enable default enable line
   ```

**Note**

If you specify a RADIUS or TACACS+ server, you must define that server. See "Defining a RADIUS Server" on page 2-76 and "Defining a TACACS+ Server" on page 2-76.

2. Create a named list for the router's access lines (such as the console line and the Telnet lines).

   ***Syntax:*** aaa authentication login [default | <*listname*>] [none | line | enable | local | {group <*groupname*> | radius | tacacs+}]

   Replace <*listname*> with the name that you want to use to refer to the named list that you create. For example, you might enter:

   ```
   ProCurve(config)# aaa authentication login LoginList enable line local
   ```

3. Assign the named list to the console line, Telnet lines, FTP, or Web access. Move to the appropriate line configuration mode context and enter:

   ***Syntax:*** login authentication <*named list*>

   You do not have to complete this step to configure AAA authentication methods for the enable mode.

   Remember to save your configuration changes by entering **write memory** from the enable mode context.

## Configuring Authorization with AAA

Configuring authorization with AAA includes two basic steps:

- Define a named list for authorization. You can define a named list to authorize users to:
  - access the basic mode context or the enable mode context
  - immediately enter the enable mode context when they start a new CLI session
- Assign the named list to a line configuration mode context.

Of course, the AAA subsystem must be enabled, and the TACACS+ server must be defined.

1. To create a named list to authorize access to the basic or enable mode context, enter the following command from the global configuration mode context:

   ***Syntax:*** aaa authorization commands [1 | 15] [default | <*named list*>] group [tacacs+ | <*group name*>] [if-authenticated | none]

   Include **1** or **15** to specify the level of commands for which you want to configure authorization: 1 is for unprivileged access, or basic mode, and 15 is for privileged access, or the enable mode.

   Specify the **default** authorization list, or replace ***<named list>*** to create a named list.

   Use the **group tacacs+** option to specify the default group of TACACS+ servers. Use the **group *<group name>*** if you have created a group of TACACS+ servers.

   Include the **if-authenticated** option to authorize authenticated users. Use the **none** option if authorization is not required. You may want to enter **none** as a second option. That way, if the ProCurve Secure Router cannot contact the TACACS+ server, you will still be able to configure the router.

2. To configure an authorization list for an exec shell, which allows an authenticated user to enter directly into the enable mode context when that user starts a new CLI session, enter the following command from the global configuration mode context:

   ***Syntax:*** aaa authorization exec [default | <*named list*>] [none | if-authenticated] [group {tacacs+ | <*group name*>}]

   Specify the default authorization list, or replace ***<named list>*** with the name of an authorization list.

Include the **if-authenticated** option for authorization to succeed if the user authenticates. Include the **none** option to grant access automatically.

Include the **group tacacs+** option if you want the ProCurve Secure Router to use the TACACS+ server for authorization. Use **group *<groupname>*** to specify a group of remote servers that will verify if a user is authorized to enter the enable mode context. You can specify more than one group of TACACS+ servers. If the servers in one group are unavailable, the ProCurve Secure Router will contact another group. However, if the ProCurve Secure Router contacts a TACACS+ server in the first group and that server does not authorize the user to enter the enable mode context, the ProCurve Secure Router will not attempt to authorize that user with any other TACACS+ groups listed.

3. To enable authorization commands for the console line, enter the following command from the global configuration mode context:

   ***Syntax:*** aaa authorization console

4. Assign the named list to a console, Telnet, or SSH line.
   - To assign a named list that grants access to the basic or enable mode context, enter the following command from the appropriate line configuration mode context:

     ***Syntax:*** authorization commands [1 | 15] [default | <*named list*>]

     Enter **1** to grant access to the basic mode, or enter **15** to grant access to the enable mode.

     Enter **default** to assign the default list, or replace ***<named list>*** with the list that you have created.
   - To assign a named list that allows authorized users to immediately enter the enable mode context when they start a new CLI session, enter the following command from the appropriate line configuration mode context:

     ***Syntax:*** authorization exec [default | <*named list*>]

     Enter **default** if you configured a default named list or replace ***<named list>*** with the name of the list that you created.

**Note**

Take care when you configure authorization for the console line. If you are not careful, you may prohibit yourself from entering commands from the console.

## Configuring Accounting with AAA

Configuring accounting includes two basic steps:

- Configure an accounting named list. You can define accounting named lists to track the following events:
  - a user accesses the basic or enable mode context
  - a user logs in to the router
  - a user establishes an outbound Telnet session
- Apply the accounting named list.

Of course, the AAA subsystem must be enabled, and the TACACS+ server must be defined.

1. To configure a named list that tracks when users access the basic or enable mode context, enter the following command from the global configuration mode context:

   ***Syntax:*** aaa accounting commands [1 |15] [default | <***named list***>] [none | stop-only] [group {tacacs+ | <***group name***>}]

   Specify the level of commands for which you want to generate accounting: **1** is unprivileged access, which is the basic mode, and **15** is privileged access, which is the enable mode.

   Specify the default accounting list, or replace ***<named list>*** to create an accounting list.

   Include the **stop-only** option if you want an accounting record to be generated when the user ends his or her session. Include the **none** option if you do not want an accounting record to be generated. If you specify the **none** option, you cannot include the **group** option (because a TACACS+ server is not required).

   Include the **group tacacs+** option if you want the ProCurve Secure Router to send the accounting information to the default group of TACACS+ servers. Replace **group *<groupname>*** if you want to specify a TACACS+ group that you created. You can specify more than one group.

2. You can configure the ProCurve Secure Router to send updates to the TACACS+ server for either of the following:
   - all new connections or logins
   - outbound Telnet connections

**Note**

You can initiate an outbound Telnet session from both the basic and enable mode context. You simply enter **telnet <A.B.C.D>**, replacing <A.B.C.D> with the IP address of the device that you want to access.

From the global configuration mode context, enter:

***Syntax:*** aaa accounting [exec | connection] [default | <*named list*>] [none | start-stop | stop-only] [group {tacacs+ | <*groupname*>}]

Specify the **exec** option to send records of all new connections, or specify the **connection** option to send records for outbound Telnet connections.

Specify the default accounting list, or replace ***<named list>*** to create an accounting list.

Include the **start-stop** option if you want an accounting record to be generated both when the user begins and ends his or her session. Include the **stop-only** option if you want an accounting record to be generated only when the user ends his or her session. Include the **none** option if you do not want an accounting record generated. If you specify the **none** option, you cannot include the **group** option (because a TACACS+ server is not required).

Include the **group tacacs+** option if you want the ProCurve Secure Router to send the accounting information to the default group of TACACS+ servers. Replace **group *<groupname>*** with a group of TACACS+ servers that you created. You can specify more than one group.

3. Assign the named list to the appropriate line configuration mode context.
   - If you have created a named list to track the users who access the basic or enable mode context, enter:

     ***Syntax:*** accounting commands [1 | 15] [default | <*named list*>]

     Specify the level of commands for which you want to generate accounting: **1** is unprivileged access, which is the basic mode, and **15** is privileged access, which is the enable mode.

     Specify the default accounting list, or replace ***<named list>*** to create an accounting list.

- If you have created a named list to track all connections, or logins, or if you have created a named list to track outbound Telnet connections, enter:

  ***Syntax:*** accounting [connection | exec] [default | <*named list*>]

  Include the **connection** option if you want to track all outbound Telnet connections made from this line. Include the **exec** option if you want to track all login connections made from this line.

  Specify the default accounting list, or replace ***<named list>*** to create an accounting list.

### Defining a RADIUS Server

Define the IP address of the RADIUS server and the key that the ProCurve Secure Router must use to authenticate to the server (if a key is required). From the global configuration mode context, enter:

***Syntax:*** radius-server host <*A.B.C.D*> key <*key*>

Replace ***<A.B.C.D>*** with the RADIUS server's IP address, and replace ***<key>*** with the shared key for the RADIUS server.

### Defining a TACACS+ Server

Define the IP address of the TACACS+ server and the key that the ProCurve Secure Router must use to authenticate to the server (if a key is required). From the global configuration mode context, enter:

***Syntax:*** tacacs-server host <*A.B.C.D*> | *hostname*> <*key*>

Replace ***<A.B.C.D>*** with the server's IP address, or replace ***<hostname>*** with the hostname of the TACACS+ server. Replace ***<key>*** with the shared key.

## Using SNMP to Monitor Network Devices

To configure SNMP, complete these steps:

1. Enable the SNMP agent.

   ***Syntax:*** ip snmp agent

2. Create an SNMP view by entering the following command from the global configuration mode context:

   ***Syntax:*** snmp-server view <*viewname*> <*oidtree*> included | excluded

3. Specify a community string by entering the following command from the global configuration mode context:

   ***Syntax:*** snmp-server community <*community*> [view <*viewname*>] [ro | rw] [<*listname*>]

4. Create an SNMP group by entering the following command from the global configuration mode context:

   ***Syntax:*** snmp-server group <*groupname*> [v1 | v2c | v3 {auth | noauth | priv}] [read <*viewname*>] [write <*viewname*>] [notify <*viewname*>] [access <*listname*>]

5. Create an SNMP user by entering the following command from the global configuration mode context:

   ***Syntax:*** snmp-server user <*username*> <*groupname*> [v1 | v2c | v3 {auth [md5 | sha] <*password*>} {priv des <*password*>}] [access <*listname*>]

6. Specify the source interface for SNMP by entering the following command from the global configuration mode context:

   ***Syntax:*** snmp-server source-interface <*interface*>

7. Enable SNMP traps on the ProCurve Secure Router by entering the following command from the global configuration mode context:

   ***Syntax:*** snmp-server enable traps [snmp]

8. Configure the SNMP host, or server, to receive SNMP notifications (traps and informs). From the global configuration mode context, enter:

   ***Syntax:*** snmp-server host <*ip address*> traps [<*community or username*>] | [version 1 <*community*> | version 2c <*community*> | version 3 {auth <*username*> | noauth <*username*> | priv <*username*>}] [snmp]

   ***Syntax:*** snmp-server host <*ip address*> informs [version 1 <*community*> | version 2c <*community*> | version 3 {auth <*username*> | noauth <*username*> | priv <*username*>}] [snmp]

9. If you have configured the ProCurve Secure Router to send informs, specify the response retry attempts and wait time. From the global configuration mode context, enter:

   ***Syntax:*** snmp-server inform [retries <*number*>] [timeout <*value*>]

## Enabling 802.1X Supplicant Status

To enable the router to function as a supplicant, complete the following steps:

1. Move to the configuration mode context for the Ethernet interface that you want to use to access the 802.1X-secured network.

   ```
   ProCurve(config)# interface eth 0/1
   ProCurve(config-eth 0/1)#
   ```

2. Configure the supplicant username and password:

   ***Syntax:*** port-auth supplicant username <*username*> password <*password*>

   For example, you might enter:

   ```
   ProCurve(config-eth 0/1)# port-auth supplicant username ProCurve password
   ProCurve
   ```

   The default username is username, and the default password is password.

3. Enable the interface's supplicant functionality by entering the following:

   ```
   ProCurve(config-eth 0/1)# port-auth supplicant
   ```