5

RADIUS Authentication and Accounting

Contents

Overview

Feature	Default	Menu	CLI	Web
Configuring RADIUS Authentication	None	n/a	5-6	n/a
Configuring RADIUS Accounting	None	n/a	5-17	n/a
Viewing RADIUS Statistics	n/a	n/a	5-25	n/a

RADIUS (*Remote Authentication Dial-In User Service*) enables you to use up to three servers (one primary server and one or two backups) and maintain separate authentication and accounting for each RADIUS server employed. For authentication, this allows a different password for each user instead of having to rely on maintaining and distributing switch-specific passwords to all users. For accounting, this can help you track network resource usage.

Authentication. You can use RADIUS to verify user identity for the following types of primary password access to the ProCurve switch:

- Serial port (Console)
- Telnet
- SSH
- Web (Series 2600, 2600-PWR, and 2800 switches)
- Port-Access

Note

The switch does not support RADIUS security for SNMP (network management) access or, for the 4100gl and 6108 switches, web browser interface access. For information on blocking unauthorized access through the web browser interface, refer to "Controlling Web Browser Interface Access When Using RADIUS Authentication" on page 5-17.

Accounting. RADIUS accounting on the switch collects resource consumption data and forwards it to the RADIUS server. This data can be used for trend analysis, capacity planning, billing, auditing, and cost analysis.

Terminology

CHAP (Challenge-Handshake Authentication Protocol): A challenge-response authentication protocol that uses the Message Digest 5 (MD5) hashing scheme to encrypt a response to a challenge from a RADIUS server.

EAP (Extensible Authentication Protocol): A general PPP authentication protocol that supports multiple authentication mechanisms. A specific authentication mechanism is known as an EAP type, such as MD5-Challenge, Generic Token Card, and TLS (Transport Level Security).

Host: See **RADIUS Server**.

NAS (Network Access Server): In this case, a ProCurve switch configured for RADIUS security operation.

RADIUS (Remote Authentication Dial In User Service):

RADIUS Client: The device that passes user information to designated RADIUS servers.

RADIUS Host: See RADIUS server.

RADIUS Server: A server running the RADIUS application you are using on your network. This server receives user connection requests from the switch, authenticates users, and then returns all necessary information to the switch. For the ProCurve switch, a RADIUS server can also perform accounting functions. Sometimes termed a *RADIUS host*.

Shared Secret Key: A text value used for encrypting data in RADIUS packets. Both the RADIUS client and the RADIUS server have a copy of the key, and the key is never transmitted across the network.

Switch Operating Rules for RADIUS

- You must have at least one RADIUS server accessible to the switch.
- The switch supports authentication and accounting using up to three RADIUS servers. The switch accesses the servers in the order in which they are listed by **show radius** (page 5-25). If the first server does not respond, the switch tries the next one, and so-on. (To change the order in which the switch accesses RADIUS servers, refer to "Changing RADIUS-Server Access Order" on page 5-29.)
- You can select RADIUS as the primary authentication method for each type of access. (Only one primary and one secondary access method is allowed for each access type.)
- In the ProCurve switch, EAP RADIUS uses MD5 and TLS to encrypt a response to a challenge from a RADIUS server.

General RADIUS Setup Procedure

Preparation:

1. Configure one to three RADIUS servers to support the switch. (That is, one primary server and one or two backups.) Refer to the documentation provided with the RADIUS server application.
2. Before configuring the switch, collect the information outlined below.

Table 5-1. Preparation for Configuring RADIUS on the Switch

- Determine the access methods (console, Telnet, Port-Access (802.1X), SSH, and/or web browser interface) for which you want RADIUS as the primary authentication method. Consider both Operator (login) and Manager (enable) levels, as well as which secondary authentication methods to use (local or none) if the RADIUS authentication fails or does not respond.

```
ProCurve> show authentication

 Status and Counters - Authentication Information

  Login Attempts : 3
  Respect Privilege : Disabled

               | Login      Login      Enable     Enable
  Access Task  | Primary    Secondary  Primary    Secondary
  ------------ + ---------- ---------- ---------- ---------
  Console      | Radius     Local      Radius     Local
  Telnet       | Radius     None       Radius     None
  Port-Access  | EapRadius
  Webui        | Radius     None       Radius     None
  SSH          | Radius     None       Radius     None
  Web-Auth     | ChapRadius
  MAC-Auth     | ChapRadius
```

Console access requires Local as secondary method to prevent lockout if the primary RADIUS access fails due to loss of RADIUS server access or other problems with the server.

Webui, Web-Auth, and Mac-Auth access is available on the 2600, 2600-PWR, and 2800 switches (not on the 4100 and 6108 switches).

Figure 5-1. Example of Possible RADIUS Access Assignments

- Determine the IP address(es) of the RADIUS server(s) you want to support the switch. (You can configure the switch for up to three RADIUS servers.)
- If you need to replace the default UDP destination port (1812) the switch uses for authentication requests to a specific RADIUS server, select it before beginning the configuration process.
- If you need to replace the default UDP destination port (1813) the switch uses for accounting requests to a specific Radius server, select it before beginning the configuration process.
- Determine whether you can use one, global encryption key for all RADIUS servers or if unique keys will be required for specific servers. With multiple RADIUS servers, if one key applies to two or more of these servers, then you can configure this key as the global encryption key. For any server whose key differs from the global key you are using, you must configure that key in the same command that you use to designate that server's IP address to the switch.

- Determine an acceptable timeout period for the switch to wait for a server to respond to a request. ProCurve recommends that you begin with the default (five seconds).
- Determine how many times you want the switch to try contacting a RADIUS server before trying another RADIUS server or quitting. (This depends on how many RADIUS servers you have configured the switch to access.)
- Determine whether you want to bypass a RADIUS server that fails to respond to requests for service. To shorten authentication time, you can set a bypass period in the range of 1 to 1440 minutes for non-responsive servers. This requires that you have multiple RADIUS servers accessible for service requests.

Configuring the Switch for RADIUS Authentication

RADIUS Authentication Commands	Page
aaa authentication	5-8
< console | telnet | ssh | web > < enable | login > radius*	5-8
< local | none >	5-8
[no] radius-server host < *IP-address* >	5-10
[auth-port < *port-number* >]	5-10
[acct-port < *port-number* >]	5-10, 5-20
[key < *server-specific key-string* >]	5-10
[no] radius-server key < *global key-string* >	5-12
radius-server timeout < 1 - 15>	5-12
radius-server retransmit < 1 - 5 >	5-12
[no] radius-server dead-time < 1 - 1440 >	5-14
show radius	5-25
[< host < *ip-address*>]	5-25
show authentication	5-27
show radius authentication	5-27

* The web authentication option for the web browser interface is available on the 2600, 2600-PWR, and 2800 switches running software releases H.08.58 and I.08.60 or greater.

Outline of the Steps for Configuring RADIUS Authentication

There are three main steps to configuring RADIUS authentication:

1. Configure RADIUS authentication for controlling access through one or more of the following
   - Serial port
   - Telnet
   - SSH
   - Web browser interface (2600, 2600-PWR, and 2800 switches running software releases H.08.58 and I.08.60 or greater)
   - Port-Access (802.1X)
2. Configure the switch for accessing one or more RADIUS servers (one primary server and up to two backup servers):

Note

This step assumes you have already configured the RADIUS server(s) to support the switch. Refer to the documentation provided with the RADIUS server documentation.)

   - Server IP address
   - (Optional) UDP destination port for authentication requests (default: 1812; recommended)
   - (Optional) UDP destination port for accounting requests (default: 1813; recommended)
   - (Optional) encryption key for use during authentication sessions with a RADIUS server. This key overrides the global encryption key you can also configure on the switch, and must match the encryption key used on the specified RADIUS server. (Default: null)
3. Configure the global RADIUS parameters.
   - **Server Key:** This key must match the encryption key used on the RADIUS servers the switch contacts for authentication and accounting services unless you configure one or more per-server keys. (Default: null.)
   - **Timeout Period:** The timeout period the switch waits for a RADIUS server to reply. (Default: 5 seconds; range: 1 to 15 seconds.)
   - **Retransmit Attempts:** The number of retries when there is no server response to a RADIUS authentication request. (Default: 3; range of 1 to 5.)

- **Server Dead-Time:** The period during which the switch will not send new authentication requests to a RADIUS server that has failed to respond to a previous request. This avoids a wait for a request to time out on a server that is unavailable. If you want to use this feature, select a dead-time period of 1 to 1440 minutes. (Default: 0—disabled; range: 1 - 1440 minutes.) If your first-choice server was initially unavailable, but then becomes available before the dead-time expires, you can nullify the dead-time by resetting it to zero and then trying to log on again. As an alternative, you can reboot the switch, (thus resetting the dead-time counter to assume the server is available) and then try to log on again.
- **Number of Login Attempts:** This is an **aaa authentication** command. It controls how many times in one session a RADIUS client (as well as clients using other forms of access) can try to log in with the correct username and password. (Default: Three times per session.)

(For RADIUS accounting features, refer to "Configuring RADIUS Accounting" on page 5-17.)

1. Configure Authentication for the Access Methods You Want RADIUS To Protect

This section describes how to configure the switch for RADIUS authentication through the following access methods:

- **Console:** Either direct serial-port connection or modem connection.
- **Telnet:** Inbound Telnet must be enabled (the default).
- **SSH:** To employ RADIUS for SSH access, you must first configure the switch for SSH operation. Refer to "Configuring Secure Shell (SSH)" on page 6-1.
- **Web:** Web browser interface (2600, 2600-PWR, and 2800 switches).

You can also use RADIUS for Port-Based Access authentication. Refer to "Configuring Port-Based Access Control (802.1X)" on page 8-1.

You can configure RADIUS as the primary password authentication method for the above access methods. You will also need to select either **local** or **none** as a secondary, or backup, method. Note that for console access, if you configure **radius** (or **tacacs**) for primary authentication, you must configure **local** for the secondary method. This prevents the possibility of being completely locked out of the switch in the event that all primary access methods fail.

Syntax: aaa authentication < console | telnet | ssh | web > < enable | login > < radius >

Configures RADIUS as the primary password authentication method for console, Telnet, SSH and/or the Web browser interface. (The default primary **< enable | login >** *authentication is* **local**.*)*

[< local | none >]

Provides options for secondary authentication (default: ***none****). Note that for console access, secondary authentication must be* ***local*** *if primary access is not* ***local****. This prevents you from being completely locked out of the switch in the event of a failure in other access methods.*

For example, suppose you have already configured local passwords on the switch, but want to use RADIUS to protect primary Telnet and SSH access without allowing a secondary Telnet or SSH access option (which would be the switch's local passwords):

```
ProCurve(config)# aaa authentication telnet login radius none
ProCurve(config)# aaa authentication telnet enable radius none
ProCurve(config)# aaa authentication ssh login radius none
ProCurve(config)# aaa authentication ssh enable radius none
ProCurve(config)# show authentication

 Status and Counters - Authentication Information

  Login Attempts : 3
  Respect Privilege : Disabled

              | Login      Login      Enable     Enable
  Access Task | Primary    Secondary  Primary    Secondary
  ----------- + ---------- ---------- ---------- ----------
  Console     | Local      None       Local      None
  Telnet      | Radius     None       Radius     None
  Port-Access | Local
  Webui       | Local      None       Local      None
  SSH         | Radius     None       Radius     None
```

The switch now allows Telnet and SSH authentication only through RADIUS.

Figure 5-2. Example Configuration for RADIUS Authentication

Note

In the above example, if you configure the Login Primary method as **local** instead of **radius** (and local passwords are configured on the switch), then you can gain access to either the Operator or Manager level without encountering the RADIUS authentication specified for Enable Primary. Refer to "Local Authentication Process" on page 5-16.

2. Configure the Switch To Access a RADIUS Server

This section describes how to configure the switch to interact with a RADIUS server for both authentication and accounting services.

Note

If you want to configure RADIUS accounting on the switch, go to page 5-17: "Configuring RADIUS Accounting" instead of continuing here.

Syntax: [no] radius-server host < *ip-address* >

Adds a server to the RADIUS configuration or (with ***no****) deletes a server from the configuration. You can configure up to three RADIUS server addresses. The switch uses the first server it successfully accesses. (Refer to "Changing the RADIUS Server Access Order" on page 5-29.)*

[auth-port < *port-number* >]

Optional. Changes the UDP destination port for authentication requests to the specified RADIUS server (host). If you do not use this option with the ***radius-server host*** *command, the switch automatically assigns the default authentication port number. The* ***auth-port*** *number must match its server counterpart. (Default:* **1812***)*

[acct-port < *port-number* >]

Optional. Changes the UDP destination port for accounting requests to the specified RADIUS server. If you do not use this option with the ***radius-server host*** *command, the switch automatically assigns the default accounting port number. The* ***acct-port*** *number must match its server counterpart.(Default: 1813)*

[key < *key-string* >]

Optional. Specifies an encryption key for use during authentication (or accounting) sessions with the specified server. This key must match the encryption key used on the RADIUS server. Use this command only if the specified server requires a different encryption key than configured for the global encryption key.

no radius-server host < *ip-address* > key

Use the **no** *form of the command to remove the key for a specified server.*

For example, suppose you have configured the switch as shown in figure 5-3 and you now need to make the following changes:

1. Change the encryption key for the server at 10.33.18.127 to "source0127".
2. Add a RADIUS server with an IP address of 10.33.18.119 and a server-specific encryption key of "source0119".

```
ProCurve# show radius
 Status and Counters - General RADIUS Information
  Deadtime(min) : 0
  Timeout(secs) : 5
  Retransmit Attempts : 5
  Global Encryption Key :
                    Auth  Acct
  Server IP Addr    Port  Port  Encryption Key
  ---------------- ----- ----- --------------------
  10.33.18.127      1812  1813  TempKey01
```

Figure 5-3. Sample Configuration for RADIUS Server Before Changing the Key and Adding Another Server

To make the changes listed prior to figure 5-3, you would do the following:

```
ProCurve(config)# radius-server host 10.33.18.127 key source0127

ProCurve(config)# radius-server host 10.33.18.119 key source0119

ProCurve(config)# show radius
 Status and Counters - General RADIUS Information
  Deadtime(min) : 0
  Timeout(secs) : 5
  Retransmit Attempts : 5
  Global Encryption Key :

                    Auth  Acct
  Server IP Addr    Port  Port  Encryption Key
  ---------------- ----- ----- ----------------
  10.33.18.127      1812  1813  source0127
  10.33.18.119      1812  1813  source0119
```

Changes the key for the existing server to "source0127"

Adds the new RADIUS server with its required "source0119" key.

Lists the switch's new RADIUS server configuration. Compare this with

Figure 5-4. Sample Configuration for RADIUS Server After Changing the Key and Adding Another Server

To change the order in which the switch accesses RADIUS servers, refer to "Changing RADIUS-Server Access Order" on page 5-29.

3. Configure the Switch's Global RADIUS Parameters

You can configure the switch for the following global RADIUS parameters:

- **Number of login attempts:** In a given session, specifies how many tries at entering the correct username and password pair are allowed before access is denied and the session terminated. (This is a general **aaa authentication** parameter and is not specific to RADIUS.)
- **Global server key:** The server key the switch will use for contacts with all RADIUS servers for which there is not a server-specific key configured by **radius-server host < *ip-address* > key < *key-string* >**. This key is optional if you configure a server-specific key for each RADIUS server entered in the switch. (Refer to "2. Configure the Switch To Access a RADIUS Server" on page 5-10.)
- **Server timeout:** Defines the time period in seconds for authentication attempts. If the timeout period expires before a response is received, the attempt fails.
- **Server dead time:** Specifies the time in minutes during which the switch avoids requesting authentication from a server that has not responded to previous requests.
- **Retransmit attempts:** If the first attempt to contact a RADIUS server fails, specifies how many retries you want the switch to attempt on that server.

Syntax: aaa authentication num-attempts < 1 - 10 >

Specifies how many tries for entering the correct username and password before shutting down the session due to input errors. (Default: 3; Range: 1 - 10).

[no] radius-server

key < *global-key-string* >

Specifies the global encryption key the switch uses with servers for which the switch does not have a server-specific key assignment. This key is optional if all RADIUS server addresses configured in the switch include a server-specific encryption key. (Default: Null.)

dead-time < 1 - 1440 >

Optional. Specifies the time in minutes during which the switch will not attempt to use a RADIUS server that has not responded to an earlier authentication attempt. (Default: 0; Range: 1 - 1440 minutes)

radius-server timeout < 1 - 15 >

Specifies the maximum time the switch waits for a response to an authentication request before counting the attempt as a failure. (Default: 3 seconds; Range: 1 - 15 seconds)

radius-server retransmit < 1 - 5 >

If a RADIUS server fails to respond to an authentication request, specifies how many retries to attempt before closing the session. Default: 3; Range: 1 - 5)

Note

Where the switch has multiple RADIUS servers configured to support authentication requests, if the first server fails to respond, then the switch tries the next server in the list, and so-on. If none of the servers respond, then the switch attempts to use the secondary authentication method configured for the type of access being attempted (console, Telnet, or SSH). If this occurs, refer to "RADIUS-Related Problems" in the Troubleshooting chapter of the Management and Configuration Guide for your switch.

For example, suppose that your switch is configured to use three RADIUS servers for authenticating access through Telnet and SSH. Two of these servers use the same encryption key. In this case your plan is to configure the switch with the following global authentication parameters:

- Allow only two tries to correctly enter username and password.
- Use the global encryption key to support the two servers that use the same key. (For this example, assume that you did not configure these two servers with a server-specific key.)
- Use a dead-time of five minutes for a server that fails to respond to an authentication request.
- Allow three seconds for request timeouts.
- Allow two retries following a request that did not receive a response.

```
ProCurve(config)# aaa authentication num-attempts 2
ProCurve(config)# radius-server key My-Global-Key-1099
ProCurve(config)# radius-server dead-time 5
ProCurve(config)# radius-server timeout 3
ProCurve(config)# radius-server retransmit 2
ProCurve(config)# write mem
```

Figure 5-5. Example of Global Configuration Exercise for RADIUS Authentication

```
ProCurve# show authentication

 Status and Counters - Authentication Information

  Login Attempts : 2
  Respect Privilege : Disabled

              | Login      Login      Enable     Enable
  Access Task | Primary    Secondary  Primary    Secondary
  ----------- + ---------- ---------- ---------- ----------
  Console     | Local      None       Local      None
  Telnet      | Radius     None       Radius     None
  Port-Access | Local
  Webui       | Local      None       Local      None
  SSH         | Radius     None       Radius     None
  Web-Auth    | ChapRadius
  MAC-Auth    | ChapRadius


ProCurve# show radius

 Status and Counters - General RADIUS Information

  Deadtime(min) : 5
  Timeout(secs) : 3
  Retransmit Attempts : 2
  Global Encryption Key : My-Global-Key-1099

                  Auth  Acct
  Server IP Addr  Port  Port  Encryption Key
  --------------- ----- ----- --------------------------------
  10.33.18.127    1812  1813  source0127
  10.33.18.119    1812  1813
  10.33.18.151    1812  1813
```

After two attempts failing due to username or password entry errors, the switch will terminate the session.

Global RADIUS parameters from figure 5-5.

Server-specific encryption key for the RADIUS server that will not use the global encryption key.

These two servers will use the global encryption key.

Figure 5-6. Listings of Global RADIUS Parameters Configured In Figure 5-5

Local Authentication Process

When the switch is configured to use RADIUS, it reverts to local authentication only if one of these two conditions exists:

- "Local" is the authentication option for the access method being used.
- The switch has been configured to query one or more RADIUS servers for a primary authentication request, but has not received a response, and local is the configured secondary option.

For local authentication, the switch uses the Operator-level and Manager-level username/password set(s) previously configured locally on the switch. (These are the usernames and passwords you can configure using the CLI password command, the web browser interface, or the menu interface—which enables only local password configuration).

- If the operator at the requesting terminal correctly enters the username/password pair for either access level (Operator or Manager), access is granted on the basis of which username/password pair was used. For example, suppose you configure Telnet primary access for RADIUS and Telnet secondary access for local. If a RADIUS access attempt fails, then you can still get access to either the Operator or Manager level of the switch by entering the correct username/password pair for the level you want to enter.
- If the username/password pair entered at the requesting terminal does not match either local username/password pair previously configured in the switch, access is denied. In this case, the terminal is again prompted to enter a username/password pair. In the default configuration, the switch allows up to three attempts. If the requesting terminal exhausts the attempt limit without a successful authentication, the login session is terminated and the operator at the requesting terminal must initiate a new session before trying again.

Controlling Web Browser Interface Access When Using RADIUS Authentication

To prevent unauthorized access through the web browser interface, do one or more of the following:

- For Series 2600, 2600-PWR, and Series 2800 switches, configure RADIUS authentication access (software releases H.08.58 and I.08.60 or greater). (Configuring the switch for RADIUS authentication does not affect web browser interface access for the 4100 and 6108 switches.)
- Configure local authentication (a Manager user name and password and, optionally, an Operator user name and password) on the switch.
- Configure the switch's Authorized IP Manager feature to allow web browser access only from authorized management stations. (The Authorized IP Manager feature does not interfere with TACACS+ operation.)
- Disable web browser access to the switch.

Configuring RADIUS Accounting

RADIUS Accounting Commands	Page
[no] radius-server host < *ip-address* >	5-20
[acct-port < *port-number* >]	5-20
[key < *key-string* >]	5-20
[no] aaa accounting < exec | network | system > < start-stop | stop-only> radius	5-23
[no] aaa accounting update periodic < 1 - 525600 > (*in minutes*)	5-24
[no] aaa accounting suppress null-username	5-24
show accounting	5-28
show accounting sessions	5-29
show radius accounting	5-28

Note

This section assumes you have already:

- Configured RADIUS authentication on the switch for one or more access methods
- Configured one or more RADIUS servers to support the switch

If you have not already done so, refer to "General RADIUS Setup Procedure" on page 5-5 before continuing here.

RADIUS accounting collects data about user activity and system events and sends it to a RADIUS server when specified events occur on the switch, such as a logoff or a reboot. The switch supports three types of accounting services:

- **Network accounting:** Provides records containing the information listed below on clients directly connected to the switch and operating under Port-Based Access Control (802.1X):

  - Acct-Session-Id
  - Acct-Status-Type
  - Acct-Terminate-Cause
  - Acct-Authentic
  - Acct-Delay-Time
  - Acct-Input-Packets
  - Acct-Output-Packets
  - Acct-Input-Octets
  - Nas-Port
  - Acct-Output-Octets
  - Acct-Session-Time
  - Username
  - Service-Type
  - NAS-IP-Address
  - NAS-Identifier
  - Called-Station-Id

  (For 802.1X information for the switch, refer to "Configuring Port-Based Access Control (802.1X)" on page 8-1.)

- **Exec accounting:** Provides records holding the information listed below about login sessions (console, Telnet, and SSH) on the switch:

  - Acct-Session-Id
  - Acct-Status-Type
  - Acct-Terminate-Cause
  - Acct-Authentic
  - Acct-Delay-Time
  - Acct-Session-Time
  - Username
  - Service-Type
  - NAS-IP-Address
  - NAS-Identifier
  - Calling-Station-Id

- **System accounting:** Provides records containing the information listed below when system events occur on the switch, including system reset, system boot, and enabling or disabling of system accounting.

  - Acct-Session-Id
  - Acct-Status-Type
  - Acct-Terminate-Cause
  - Acct-Authentic
  - Acct-Delay-Time
  - Username
  - Service-Type
  - NAS-IP-Address
  - NAS-Identifier
  - Calling-Station-Id

The switch forwards the accounting information it collects to the designated RADIUS server, where the information is formatted, stored, and managed by the server. For more information on this aspect of RADIUS accounting, refer to the documentation provided with your RADIUS server.

Operating Rules for RADIUS Accounting

- You can configure up to three types of accounting to run simultaneously: exec, system, and network.
- RADIUS servers used for accounting are also used for authentication.
- The switch must be configured to access at least one RADIUS server.
- RADIUS servers are accessed in the order in which their IP addresses were configured in the switch. Use **show radius** to view the order. As long as the first server is accessible and responding to authentication requests from the switch, a second or third server will not be accessed. (For more on this topic, refer to "Changing RADIUS-Server Access Order" on page 5-29.)
- If access to a RADIUS server fails during a session, but after the client has been authenticated, the switch continues to assume the server is available to receive accounting data. Thus, if server access fails during a session, it will not receive accounting data transmitted from the switch.

Steps for Configuring RADIUS Accounting

1. Configure the switch for accessing a RADIUS server.

   You can configure a list of up to three RADIUS servers (one primary, two backup). The switch operates on the assumption that a server can operate in both accounting and authentication mode. (Refer to the documentation for your RADIUS server application.)

   - Use the same **radius-server host** command that you would use to configure RADIUS authentication. Refer to "2. Configure the Switch To Access a RADIUS Server" on page 5-10.
   - Provide the following:
     - A RADIUS server IP address.
     - Optional—a UDP destination port for authentication requests. Otherwise the switch assigns the default UDP port (1812; recommended).

– Optional—if you are also configuring the switch for RADIUS authentication, and need a unique encryption key for use during authentication sessions with the RADIUS server you are designating, configure a server-specific key. This key overrides the global encryption key you can also configure on the switch, and must match the encryption key used on the specified RADIUS server. For more information, refer to the **key < *key-string* >** parameter on page 5-10. (Default: null)

2. Configure accounting types and the controls for sending reports to the RADIUS server.
   - **Accounting types:** exec (page 5-18), network (page 5-18), or system (page 5-18)
   - **Trigger for sending accounting reports to a RADIUS server:** At session start and stop or only at session stop
3. (Optional) Configure session blocking and interim updating options
   - **Updating:** Periodically update the accounting data for sessions-in-progress
   - **Suppress accounting:** Block the accounting session for any unknown user with no username access to the switch

1. Configure the Switch To Access a RADIUS Server

Before you configure the actual accounting parameters, you should first configure the switch to use a RADIUS server. This is the same as the process described on page 5-10. You need to repeat this step here only if you have not yet configured the switch to use a RADIUS server, your server data has changed, or you need to specify a non-default UDP destination port for accounting requests. Note that switch operation expects a RADIUS server to accommodate both authentication and accounting.

Syntax: [no] radius-server host < *ip-address* >

*Adds a server to the RADIUS configuration or (with **no**) deletes a server from the configuration.*

[acct-port < *port-number* >]

Optional. Changes the UDP destination port for accounting requests to the specified RADIUS server. If you do not use this option, the switch automatically assigns the default accounting port number. (Default: 1813)

[key < *key-string* >]

Optional. Specifies an encryption key for use during accounting or authentication sessions with the specified server. This key must match the encryption key used on the RADIUS server. Use this command only if the specified server requires a different encryption key than configured for the global encryption key.

(For a more complete description of the **radius-server** command and its options, turn to page 5-10.)

For example, suppose you want to the switch to use the RADIUS server described below for both authentication and accounting purposes.

- IP address: 10.33.18.151
- A non-default UDP port number of 1750 for accounting.

For this example, assume that all other RADIUS authentication parameters for accessing this server are acceptable at their default settings, and that RADIUS is already configured as an authentication method for one or more types of access to the switch (Telnet, Console, etc.).

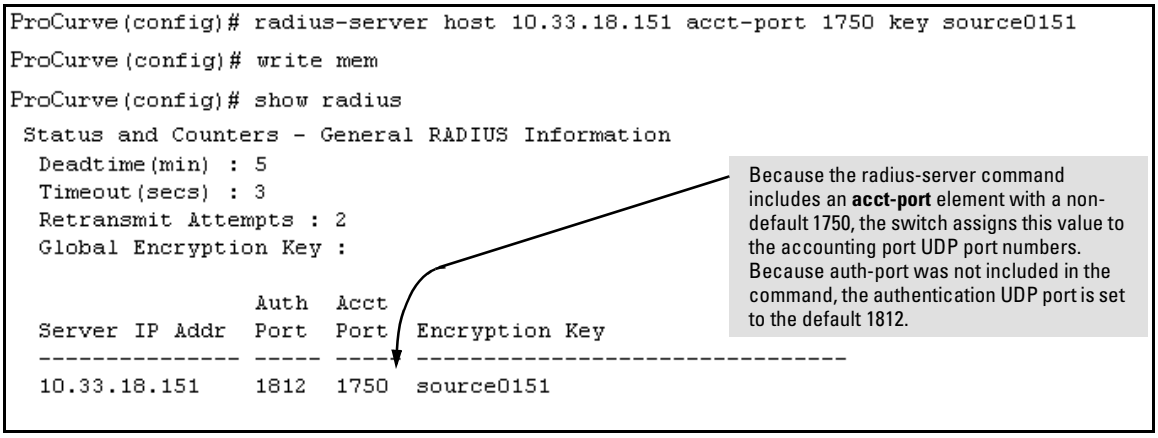

Figure 5-7. Example of Configuring for a RADIUS Server with a Non-Default Accounting UDP Port Number

The radius-server command as shown in figure 5-7, above, configures the switch to use a RADIUS server at IP address 10.33.18.151, with a (non-default) UDP accounting port of 1750, and a server-specific key of "source0151".

2. Configure Accounting Types and the Controls for Sending Reports to the RADIUS Server

Select the Accounting Type(s):

- **Exec:** Use **exec** if you want to collect accounting information on login sessions on the switch via the console, Telnet, or SSH. (See also "Accounting" on page 5-2.)
- **System:** Use **system** if you want to collect accounting data when:
  - A system boot or reload occurs
  - System accounting is turned on or off

  Note that there is no time span associated with using the **system** option. It simply causes the switch to transmit whatever accounting data it currently has when one of the above events occurs.
- **Network:** Use Network if you want to collect accounting information on 802.1X port-based-access users connected to the physical ports on the switch to access the network. (See also "Accounting" on page 2.) For information on this feature, refer to "Configuring Port-Based Access Control (802.1X)" on page 8-1.

Determine how you want the switch to send accounting data to a RADIUS server:

- **Start-Stop:**
  - Send a start record accounting notice at the beginning of the accounting session and a stop record notice at the end of the session. Both notices include the latest data the switch has collected for the requested accounting type (Network, Exec, or System).
  - Do not wait for an acknowledgement.

  The system option (page 5-22) ignores **start-stop** because the switch sends the accumulated data only when there is a reboot, reload, or accounting on/off event.

- **Stop-Only:**
  - Send a stop record accounting notice at the end of the accounting session. The notice includes the latest data the switch has collected for the requested accounting type (Network, Exec, or System).
  - Do not wait for an acknowledgment.

  The system option (page 5-22) always delivers **stop-only** operation because the switch sends the accumulated data only when there is a reboot, reload, or accounting on/off event.

Syntax: [no] aaa accounting < exec | network | system > < start-stop | stop-only > radius

Configures RADIUS accounting type and how data will be sent to the RADIUS server.

For example, to configure RADIUS accounting on the switch with **start-stop** for exec functions and **stop-only** for system functions:

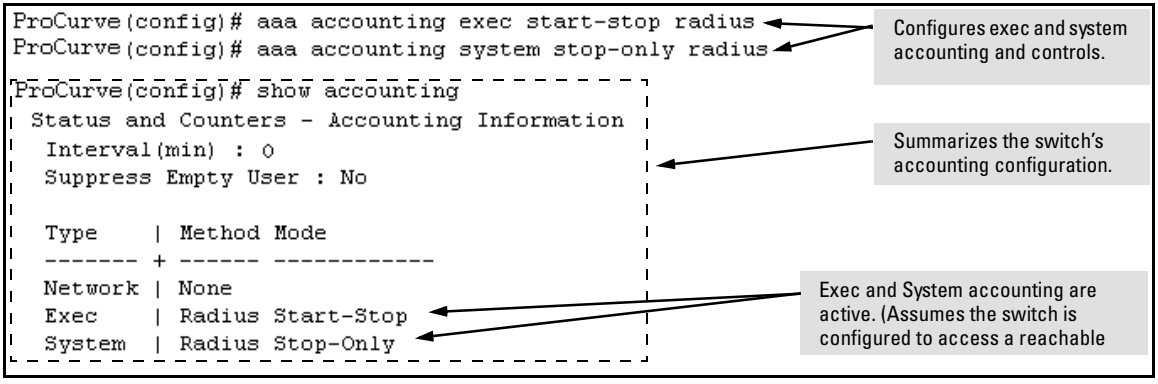

Figure 5-8. Example of Configuring Accounting Types

3. (Optional) Configure Session Blocking and Interim Updating Options

These optional parameters give you additional control over accounting data.

- **Updates:** In addition to using a Start-Stop or Stop-Only trigger, you can optionally configure the switch to send periodic accounting record updates to a RADIUS server.
- **Suppress:** The switch can suppress accounting for an unknown user having no username.

Syntax: [no] aaa accounting update periodic < 1 - 525600 >

Sets the accounting update period for all accounting sessions on the switch. (The **no** *form disables the update function and resets the value to zero.) (Default: zero; disabled)*

Syntax: [no] aaa accounting suppress null-username

Disables accounting for unknown users having no username. (Default: suppression disabled)

To continue the example in figure 5-8, suppose that you wanted the switch to:

- Send updates every 10 minutes on in-progress accounting sessions.
- Block accounting for unknown users (no username).

```
ProCurve(config)# aaa accounting update periodic 10
ProCurve(config)# aaa accounting suppress null-username

ProCurve(config)# show accounting
 Status and Counters - Accounting Information
  Interval(min) : 10
  Suppress Empty User : No

  Type     | Method Mode
  -------- + ------ ------------
  Network  | None
  Exec     | Radius Start-Stop
  System   | Radius Stop-Only
```

Update Period

Suppress Unknown User

Figure 5-9. Example of Optional Accounting Update Period and Accounting Suppression on Unknown User

Viewing RADIUS Statistics

General RADIUS Statistics

Syntax: show radius [host < *ip-addr* >]

Shows general RADIUS configuration, including the server IP addresses. Optional form shows data for a specific RADIUS host. To use **show radius**, *the server's IP address must be configured in the switch, which. requires prior use of the* **radius-server host** *command. (See "Configuring RADIUS Accounting" on page 5-17.)*

```
ProCurve(config)# show radius
 Status and Counters - General RADIUS Information
  Deadtime(min) : 5
  Timeout(secs) : 10
  Retransmit Attempts : 2
  Global Encryption Key : myg10balkey

                   Auth  Acct
  Server IP Addr   Port  Port  Encryption Key
  ---------------- ----- ----- --------------------
  192.33.12.65     1812  1813  my65key
```

Figure 5-10. Example of General RADIUS Information from Show Radius Command

```
ProCurve(config)# show radius host 192.33.12.65
 Status and Counters - RADIUS Server Information
  Server IP Addr : 192.33.12.65
  Authentication UDP Port : 1812          Accounting UDP Port  : 1813
  Round Trip Time         : 2             Round Trip Time      : 7
  Pending Requests        : 0             Pending Requests     : 0
  Retransmissions         : 0             Retransmissions      : 0
  Timeouts                : 0             Timeouts             : 0
  Malformed Responses     : 0             Malformed Responses  : 0
  Bad Authenticators      : 0             Bad Authenticators   : 0
  Unknown Types           : 0             Unknown Types        : 0
  Packets Dropped         : 0             Packets Dropped      : 0
  Access Requests         : 2             Accounting Requests  : 2
  Access Challenges       : 0             Accounting Responses : 2
  Access Accepts          : 2
  Access Rejects          : 0
```

Figure 5-11. RADIUS Server Information From the Show Radius Host Command

Table 5-2. Values for Show Radius Host Output (Figure 5-11)

Term	Definition
Round Trip Time	The time interval between the most recent Accounting-Response and the Accounting-Request that matched it from this RADIUS accounting server.
Pending Requests	The number of RADIUS Accounting-Request packets sent to this server that have not yet timed out or received a response. This variable is incremented when an accounting-Request is sent and decremented due to receipt of an Accounting-Response, a timeout or a retransmission.
Retransmissions	The number of RADIUS Accounting-Request packets retransmitted to this RADIUS accounting server. Retransmissions include retries where the Identifier and Acct-Delay have been updated, as well as those in which they remain the same.
Timeouts	The number of accounting timeouts to this server. After a timeout the client may retry to the same server, send to a different server, or give up. A retry to the same server is counted as a retransmit as well as a timeout. A send to a different server is counted as an Accounting-Request as well as a timeout.
Malformed Responses	The number of malformed RADIUS Accounting-Response packets received from this server. Malformed packets include packets with an invalid length. Bad authenticators and unknown types are not included as malformed accounting responses.
Bad Authenticators	The number of RADIUS Accounting-Response packets which contained invalid authenticators received from this server.
Unknown Types	The number of RADIUS packets of unknown type which were received from this server on the accounting port.
Packets Dropped	The number of RADIUS packets which were received from this server on the accounting port and dropped for some other reason.
Access Requests	The number of RADIUS Access-Requests the switch has sent since it was last rebooted. (Does not include retransmissions.)
Accounting Requests	The number of RADIUS Accounting-Request packets sent. This does not include retransmissions.
Access Challenges	The number of RADIUS Access-Challenge packets (valid or invalid) received from this server.
Access Accepts	The number of RADIUS Access-Accept packets (valid or invalid) received from this server.
Access Rejects	The number of RADIUS Access-Reject packets (valid or invalid) received from this server.
Responses	The number of RADIUS packets received on the accounting port from this server.

RADIUS Authentication Statistics

Syntax: show authentication

Displays the primary and secondary authentication methods configured for the Console, Telnet, Port-Access (802.1X), and SSH methods of accessing the switch. Also displays the number of access attempts currently allowed in a session.

show radius authentication

Displays NAS identifier and data on the configured RADIUS server and the switch's interactions with this server. (Requires prior use of the **radius-server host** *command to configure a RADIUS server IP address in the switch. See "Configuring RADIUS Accounting" on page 5-17.)*

```
ProCurve> show authentication
 Status and Counters - Authentication Information
  Login Attempts : 2
                | Login      Login      Enable     Enable
  Access Task   | Primary    Secondary  Primary    Secondary
  ------------- + ---------- ---------- ---------- ----------
  Console       | Local      None       Local      None
  Telnet        | Radius     Local      Radius     Local
  Port-Access   | Local
  SSH           | Radius     Local      Radius     Local
```

Figure 5-12. Example of Login Attempt and Primary/Secondary Authentication Information from the Show Authentication Command

```
ProCurve(config)# show radius authentication

 Status and Counters - RADIUS Authentication Information

  NAS Identifier : HPswitch
  Invalid Server Addresses : 0

                  UDP
  Server IP Addr  Port  Timeouts   Requests   Challenges Accepts    Rejects
  --------------- ----- ---------- ---------- ---------- ---------- ----------
  192.33.12.65    1812  0          2          0          2          0
```

Figure 5-13. Example of RADIUS Authentication Information from a Specific Server

RADIUS Accounting Statistics

Syntax: show accounting

Lists configured accounting interval, "Empty User" suppression status, accounting types, methods, and modes.

show radius accounting

Lists accounting statistics for the RADIUS server(s) configured in the switch (using the **radius-server host** *command).*

show accounting sessions

Lists the accounting sessions currently active on the switch.

```
ProCurve # show accounting

 Status and Counters - Accounting Information

  Interval(min) : 5
  Suppress Empty User : No

  Type     | Method Mode
  -------- + ------ ------------
  Network  | None
  Exec     | Radius Start-Stop
  System   | Radius Stop-Only
```

Figure 5-14. Listing the Accounting Configuration in the Switch

```
ProCurve # show radius accounting
 Status and Counters - RADIUS Accounting Information
  NAS Identifier : HPswitch
  Invalid Server Addresses : 0

                   UDP
  Server IP Addr   Port  Timeouts   Requests   Responses
  ---------------- ----- ---------- ---------- ----------
  192.33.12.65     1813  0          1          1
```

Figure 5-15. Example of RADIUS Accounting Information for a Specific Server

```
ProCurve # show accounting sessions

Active Accounted actions on CONSOLE, User radius Priv 2,
  Session ID 1, EXEC Accounting record, 00:02:32 Elapsed
```

Figure 5-16. Example Listing of Active RADIUS Accounting Sessions on the Switch

Changing RADIUS-Server Access Order

The switch tries to access RADIUS servers according to the order in which their IP addresses are listed by the **show radius** command. Also, *when you add a new server IP address, it is placed in the highest empty position in the list.*

Adding or deleting a RADIUS server IP address leaves an empty position, but does not change the position of any other server addresses in the list. For example if you initially configure three server addresses, they are listed in the order in which you entered them. However, if you subsequently remove the second server address in the list and add a new server address, the new address will be placed second in the list.

Thus, to move a server address up in the list, you must delete it from the list, ensure that the position to which you want to move it is vacant, and then re-enter it. For example, suppose you have already configured the following three RADIUS server IP addresses in the switch:

```
ProCurve # show radius
 Status and Counters - General RADIUS Information
  Deadtime(min) : 0
  Timeout(secs) : 5
  Retransmit Attempts : 3
  Global Encryption Key :

                  Auth  Acct
  Server IP Addr  Port  Port  Encryption Key
  --------------- ----- ----- --------------------
  10.10.10.1      1812  1813
  10.10.10.2      1812  1813
  10.10.10.3      1812  1813
```

RADIUS server IP addresses listed in the order in which the switch will try to access them. In this case, the server at IP address 10.10.10.1 is first.

Note: If the switch successfully accesses the first server, it does not try to access any other servers in the list, even if the client is denied access by the first server.

Figure 5-17. Search Order for Accessing a RADIUS Server

To exchange the positions of the addresses so that the server at 10.10.10.003 will be the first choice and the server at 10.10.10.001 will be the last, you would do the following:

1. Delete 10.10.10.003 from the list. This opens the third (lowest) position in the list.
2. Delete 10.10.10.001 from the list. This opens the first (highest) position in the list.
3. Re-enter 10.10.10.003. Because the switch places a newly entered address in the highest-available position, this address becomes first in the list.
4. Re-enter 10.10.10.001. Because the only position open is the third position, this address becomes last in the list.

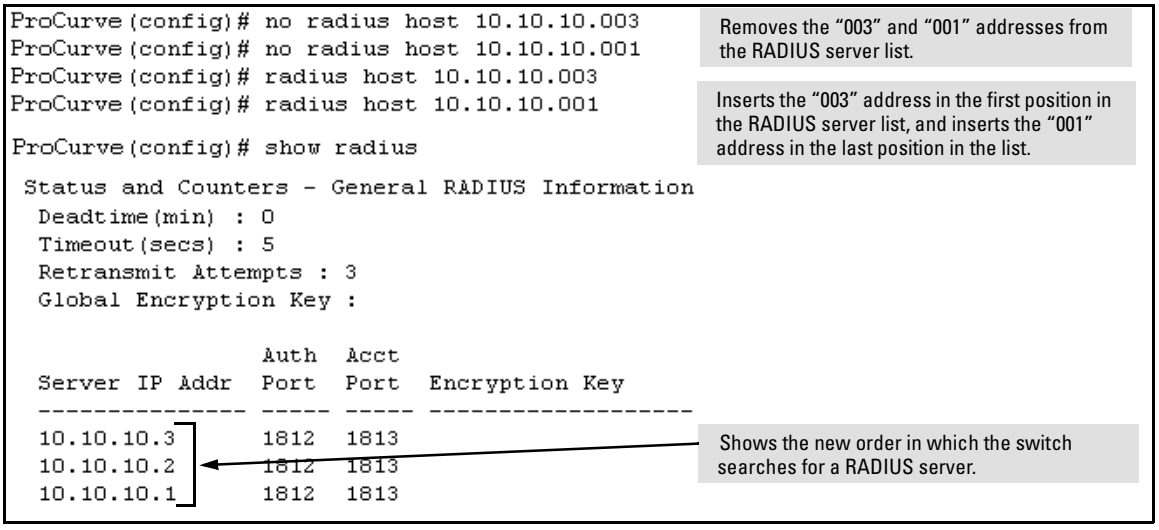

Figure 5-18. Example of New RADIUS Server Search Order

Messages Related to RADIUS Operation

Message	Meaning
`Can't reach RADIUS server < x.x.x.x >.`	A designated RADIUS server is not responding to an authentication request. Try pinging the server to determine whether it is accessible to the switch. If the server is accessible, then verify that the switch is using the correct encryption key and that the server is correctly configured to receive an authentication request from the switch.
`No server(s) responding.`	The switch is configured for and attempting RADIUS authentication, however it is not receiving a response from a RADIUS server. Ensure that the switch is configured to access at least one RADIUS server. (Use **show radius**.) If you also see the message `Can't reach RADIUS server < x.x.x.x >`, try the suggestions listed for that message.
`Not legal combination of authentication methods.`	Indicates an attempt to configure **local** as both the primary and secondary authentication methods. If **local** is the primary method, then **none** must be the secondary method.

— This page is intentionally unused. —