

RADIUS Authentication and Accounting

Contents

Overview	6-3
Authentication Services	6-3
Accounting Services	6-4
RADIUS-Administered CoS and Rate-Limiting	6-4
SNMP Access to the Switch's Authentication Configuration MIB ...	6-4
Terminology	6-5
Switch Operating Rules for RADIUS	6-6
General RADIUS Setup Procedure	6-7
Configuring the Switch for RADIUS Authentication	6-8
Outline of the Steps for Configuring RADIUS Authentication	6-9
1. Configure Authentication for the Access Methods You Want RADIUS To Protect	6-10
2. Enable the (Optional) Access Privilege Option	6-13
3. Configure the Switch To Access a RADIUS Server	6-14
4. Configure the Switch's Global RADIUS Parameters	6-17
Using SNMP To View and Configure	
Switch Authentication Features	6-21
Changing and Viewing the SNMP Access Configuration	6-22
Local Authentication Process	6-24
Controlling Web Browser Interface Access	6-25
Commands Authorization	6-26
Enabling Authorization	6-27
Displaying Authorization Information	6-28
Configuring Commands Authorization on a RADIUS Server	6-28
Using Vendor Specific Attributes (VSAs)	6-28
Example Configuration on Cisco Secure ACS for MS Windows	6-30
Example Configuration Using FreeRADIUS	6-32

VLAN Assignment in an Authentication Session	6-34
Tagged and Untagged VLAN Attributes	6-35
Additional RADIUS Attributes	6-36
Configuring RADIUS Accounting	6-37
Operating Rules for RADIUS Accounting	6-39
Steps for Configuring RADIUS Accounting	6-39
1. Configure the Switch To Access a RADIUS Server	6-40
2. Configure Accounting Types and the Controls for Sending Reports to the RADIUS Server	6-42
3. (Optional) Configure Session Blocking and Interim Updating Options	6-44
Viewing RADIUS Statistics	6-46
General RADIUS Statistics	6-46
RADIUS Authentication Statistics	6-48
RADIUS Accounting Statistics	6-49
Changing RADIUS-Server Access Order	6-50
Messages Related to RADIUS Operation	6-53

Overview

Feature	Default	Menu	CLI	Web
Configuring RADIUS Authentication	None	n/a	6-8	n/a
Configuring RADIUS Accounting	None	n/a	6-37	n/a
Configuring RADIUS Authorization	None	n/a	6-26	n/a
Viewing RADIUS Statistics	n/a	n/a	6-46	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 Services

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
- SFTP/SCP
- Web (8212zl, 5400zl, 4200vl, 2800s as of software version I.08.60, and 2600s as of software version H.08.58 switches)
- Port-Access (802.1X)

The switch also supports RADIUS accounting for Web Authentication and MAC authentication sessions.

Note

The switch does not support RADIUS security for SNMP (network management) access. For information on blocking access through the web browser interface, refer to “Controlling Web Browser Interface Access” on page 6-25.

Accounting Services

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.

RADIUS-Administered CoS and Rate-Limiting

The switches covered in this guide take advantage of vendor-specific attributes (VSAs) applied in a RADIUS server to support these optional, RADIUS-assigned attributes:

- 802.1p (CoS) priority assignment to inbound traffic on the specified port(s) (port-access authentication only)
- Per-Port Rate-Limiting on a port with an active link to an authenticated client (port-access authentication only)

SNMP Access to the Switch’s Authentication Configuration MIB

Beginning with software release K.12.*xx*, the switch’s default configuration allows SNMP access to the hpSwitchAuth MIB (Management Information Base). A management station running an SNMP networked device management application such as ProCurve Manager Plus (PCM+) or HP OpenView can access the switch’s MIB for read access to the switch’s status and read/write access to the switch’s configuration. For more information, including the CLI command to use for disabling this feature, refer to “Using SNMP To View and Configure Switch Authentication Features” on page 6-21.

Terminology

AAA: Authentication, Authorization, and Accounting groups of services provided by the carrying protocol.

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.

CoS (Class of Service): Support for priority handling of packets traversing the switch, based on the IEEE 802.1p priority carried by each packet. (For more on this topic, refer to the “Overview” section in the “Quality of Service (QoS)” chapter in the *Advanced Traffic Management Guide* for your switch.)

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).

EXEC Session: a service (EXEC shell) granted to the authenticated login user for doing management operations on the ProCurve device.

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): a protocol for carrying authentication, authorization, and accounting information between a Network Access Server and shared AAA servers in a distributed dial-in networking environment.

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.

Vendor-Specific Attribute: A vendor-defined value configured in a RADIUS server to specific an optional switch feature assigned by the server during an authenticated client session.

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 6-46). 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 6-50.)
- 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.
- When primary/secondary authentication is set to Radius/Local (for either Login or Enable) and the RADIUS server fails to respond to a client attempt to authenticate, the failure is noted in the Event Log with the message **radius: Can't reach RADIUS server < server-ip-addr >**. When this type of failure occurs, the switch prompts the client again to enter a username and password. In this case, use the local username (if any) and password configured on the switch itself.
- Zero-length usernames or passwords are not allowed for RADIUS authentication, even though allowed by some RADIUS servers.
- TACACS+ is not supported for the web browser interface access.

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 6-1. Preparation for Configuring RADIUS on the Switch

- Determine the access methods (console, Telnet, Port-Access (802.1X), web browser interface and/or SSH) 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(config)# show authentication					Note: The Webui access task shown in this figure is available only on the switches covered in this guide.
Status and Counters - Authentication Information					
Login Attempts : 3					
Respect Privilege : Disabled					
Access Task	Login Primary	Login Secondary	Enable Primary	Enable Secondary	
Console	Radius	Local	Radius	Local	← 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.
Telnet	Radius	Local	Radius	Local	
Port-Access	EapRadius				
Webui	Radius	Local	Radius	Local	
SSH	Radius	Local	Radius	Local	
Web-Auth	ChapRadius				
MAC-Auth	ChapRadius				

Figure 6-1. 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).

RADIUS Authentication and Accounting

Configuring the Switch for RADIUS Authentication

- 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.
 - Optional: Determine whether the switch access level (Manager or Operator) for authenticated clients can be set by a Service Type value the RADIUS server includes in its authentication message to the switch. (Refer to “2. Enable the (Optional) Access Privilege Option” on page 6-13.)
 - Configure RADIUS on the server(s) used to support authentication on the switch.
-

Configuring the Switch for RADIUS Authentication

RADIUS Authentication Commands	Page
aaa authentication	6-10
console telnet ssh web < enable login <local radius>> web-based mac-based <chap-radius peap-radius>	6-10
[local none authorized]	6-10
[login privilege-mode]*	6-13
[no] radius-server host < IP-address >	6-14
[auth-port < port-number >]	6-14
[acct-port < port-number >]	6-14, 6-40
[key < server-specific key-string >]	6-14
[no] radius-server key < global key-string >	6-18
radius-server timeout < 1 - 15 >	6-18
radius-server retransmit < 1 - 5 >	6-18
[no] radius-server dead-time < 1 - 1440 >	6-19
show radius	6-46
[< host < ip-address >]	6-47
show authentication	6-48
show radius authentication	6-49

*The **web** authentication option for the web browser interface is available on the switches covered in this guide.

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
 - Port-Access (802.1X)
 - Web browser interface
2. Enable RADIUS authentication on the switch to override the default authentication operation of automatically assigning an authenticated client to the Operator privilege level. This optional feature applies the privilege level specified by the Service Type value received from the RADIUS server. (Refer to “1. Configure Authentication for the Access Methods You Want RADIUS To Protect” on page 6-10.)
3. 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)
4. 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 actually an **aaa authentication** command. It controls how many times per session a RADIUS client (and 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 6-37.)

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 use RADIUS for SSH access, first configure the switch for SSH operation. Refer to chapter 8, “Configuring Secure Shell (SSH)” .
- **Web:** You can enable RADIUS authentication for web browser interface access to the switch.

You can configure RADIUS as the primary password authentication method for the above access methods. You also need to select either **local**, **none**, or **authorized** as a secondary, or backup, method. Note that for console access, if you configure **radius** (or **tacacs**) for primary authentication, you must config-

ure **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 <local | radius>> web-based | mac-based <chap-radius | peap-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.)

<console | telnet | ssh | web>

[< local | none | authorized >]

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 locked out of the switch in the event of a failure in other access methods.

<<web-based | mac-based >login> <chap-radius | peap-mschap v2>:

Password authentication for web-based or mac-based port access to the switch. Use peap-mschapv2 when you want password verification without requiring access to a plain text password; it is more secure.

Default: **chap-radius**

[none | authorized]: *Provides options for secondary authentication. The none option specifies that a backup authentication method is not used. The authorized option allows access without authentication. (default: none).*

In certain situations, RADIUS servers can become isolated from the network. Users are not able to access the network resources configured with RADIUS access protection and are rejected. To address this situation, configuring the **authorized** secondary authentication method allows users unconditional access to the network when the primary authentication method fails because the RADIUS servers are unreachable.

Caution

Configuring **authorized** as the secondary authentication method used when there is a failure accessing the RADIUS servers allows clients to access the network unconditionally. Use this method with care.

Figure 6-2 shows an example of the **show authentication** command displaying **authorized** as the secondary authentication method for port-access, Web-auth access, and MAC-auth access. Since the configuration of **authorized** means no authentication will be performed and the client has unconditional access to the network, the “Enable Primary” and “Enable Secondary” fields are not applicable (N/A).

```
ProCurve(config)# show authentication

Status and Counters - Authentication Information

Login Attempts : 3
Respect Privilege : Disabled

-----+-----
Access Task | Login      Login      Enable     Enable
             | Primary    Secondary  Primary    Secondary
-----+-----
Console     | Local      None       Local      None
Telnet      | Local      None       Local      None
Port-Access | Local      Authorized N/A        N/A
Webui       | Local      None       Local      None
SSH         | Local      None       Local      None
Web-Auth    | ChapRadius Authorized N/A        N/A
MAC-Auth    | ChapRadius Authorized N/A        N/A
```

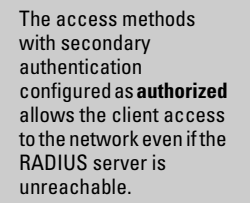


Figure 6-2. Example of AAA Authentication Using Authorized for the Secondary Authentication Method

Suppose you already configured local passwords on the switch, but want RADIUS to protect primary Telnet and SSH access without allowing a secondary Telnet or SSH access option (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

Access Task	Login Primary	Login Secondary	Enable Primary	Enable 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			

Note: The **Webui** access task shown in this figure is available only on the switches covered in this guide.

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

Figure 6-3. Example Configuration for RADIUS Authentication

Note

If you configure the Login Primary method as **local** instead of **radius** (and local passwords are configured on the switch), then clients connected to your network 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 6-24.

2. Enable the (Optional) Access Privilege Option

In the default RADIUS operation, the switch automatically admits any authenticated client to the Login (Operator) privilege level, even if the RADIUS server specifies Enable (Manager) access for that client. Thus, an authenticated user authorized for the Manager privilege level must authenticate again to change privilege levels. Using the optional **login privilege-mode** command overrides

this default behavior for clients with Enable (manager) access. That is, with **privilege-mode** enabled, the switch immediately allows Enable (Manager) access to a client for whom the RADIUS server specifies this access level.

Syntax: [no] aaa authentication login privilege-mode

When enabled, the switch reads the Service-Type field in the client authentication received from a RADIUS server. The following table describes the applicable Service-Type values and corresponding client access levels the switch allows upon authentication by the server.

Service-Type	Value	Client Access Level
Administrative-User	6	Manager
NAS-Prompt-User	7	Operator
Any Other Type	Any Value Except 6 or 7	Access Denied

This feature applies to console (serial port), Telnet, SSH, and web browser interface access to the switch. It does not apply to 802.1X port-access.

Notes: *While this option is enabled, a Service-Type value other than 6 or 7, or an unconfigured (null) Service-Type causes the switch to deny access to the requesting client.*

— Continued on the next page. —

— Continued from the preceding page. —

*The **no** form of the command returns the switch to the default RADIUS authentication operation. The default behavior for most interfaces is that a client authorized by the RADIUS server for Enable (Manager) access will be prompted twice, once for Login (Operator) access and once for Enable access. In the default RADIUS authentication operation, the switch's web browser interface requires only one successful authentication request. For more information on configuring the Service Type in your RADIUS application, refer to the documentation provided with the application.*

3. 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 6-37: “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 6-50.)*

[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.

Note: *Formerly, when you saved the configuration file using Xmodem or TFTP, the RADIUS encryption key information was not saved in the file. This caused RADIUS authentication to break when the startup configuration file was loaded back onto the switch. You now can save the configured RADIUS shared secret (encryption) key to a configuration file by entering the following commands:*

include-credentials
write memory

For more information, see “Saving Security Credentials in a Config File” on page 2-10 in this guide.

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 6-4 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
  Deadttime(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 6-4. Sample Configuration for RADIUS Server Before Changing the Key and Adding Another Server

To make the changes listed prior to figure 6-4, 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 :

Server IP Addr      Auth  Acct
Port               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" (step 1, above).

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

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

Figure 6-5. 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 6-50.

4. 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 "3. Configure the Switch To Access a RADIUS Server" on page 6-14.)
- **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 user-name 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 6-6. Example of Global Configuration Exercise for RADIUS Authentication

RADIUS Authentication and Accounting

Configuring the Switch for RADIUS Authentication

```
ProCurve(config)# show authentication
```

Status and Counters - Authentication Information

Login Attempts : 2
Respect Privilege : Disabled

Access Task	Login Primary	Login Secondary	Enable Primary	Enable 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(config)# show radius

Status and Counters - General RADIUS Information

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

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

Note: The **Webui** access task shown in this figure is available only on the switches covered in this guide.

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

Global RADIUS parameters from figure 6-6.

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 6-7. Listings of Global RADIUS Parameters Configured In Figure 6-6

Using SNMP To View and Configure Switch Authentication Features

Beginning with software release K.12.xxx, SNMP MIB object access is available for switch authentication configuration (hpSwitchAuth) features. This means that the switches covered by this Guide allow, by default, manager-only SNMP read/write access to a subset of the authentication MIB objects for the following features:

- number of primary and secondary login and enable attempts
- TACACS+ server configuration and status
- RADIUS server configuration
- selected 802.1X settings
- key management subsystem chain configuration
- key management subsystem key configuration
- OSPF interface authentication configuration
- local switch operator and manager usernames and passwords

With SNMP access to the hpSwitchAuth MIB enabled, a device with management access to the switch can view the configuration for the authentication features listed above (excluding usernames, passwords, and keys). Using SNMP sets, a management device can change the authentication configuration (*including* changes to usernames, passwords, and keys). Operator read/write access to the authentication MIB is always denied.

Security Notes

All usernames, passwords, and keys configured in the hpSwitchAuth MIB are not returned via SNMP, and the response to SNMP queries for such information is a null string. However, SNMP sets can be used to configure username, password, and key MIB objects.

To help prevent unauthorized access to the switch's authentication MIB, ProCurve recommends enhancing security according to the guidelines under "Switch Access Security" on page 1-3.

If you do not want to use SNMP access to the switch's authentication configuration MIB, then use the **snmp-server mib hpswitchauthmib excluded** command to disable this access, as described in the next section.

If you choose to leave SNMP access to the security MIB open (the default setting), ProCurve recommends that you configure the switch with the SNMP version 3 management and access security feature, and disable SNMP version

2c access. (Refer to “Switch Access Security” on page 1-3.)

Changing and Viewing the SNMP Access Configuration

Syntax: snmp-server mib hpswitchauthmib < excluded | included >

included: *Enables manager-level SNMP read/write access to the switch's authentication configuration (hpSwitchAuth) MIB.*

excluded: *Disables manager-level SNMP read/write access to the switch's authentication configuration (hpSwitchAuth) MIB. (Default: included)*

Syntax: show snmp-server

*The output for this command has been enhanced to display the current access status of the switch's authentication configuration MIB in the **Excluded MIBs** field.*

For example, to disable SNMP access to the switch's authentication MIB and then display the result in the Excluded MIB field, you would execute the following two commands.

```
ProCurve(config)# snmp-server mib hpswitchauthmib excluded
ProCurve(config)# show snmp-server
```

SNMP Communities

Community Name	MIB View	Write Access
public	Manager	Unrestricted

Trap Receivers

Link-Change Traps Enabled on Ports [All] : All

Send Authentication Traps [No] : No

Address	Community	Events Sent in Trap
---------	-----------	---------------------

Excluded MIBs

```
hpSwitchAuthenticationMIB
```

This command disables SNMP security MIB access.

Indicates that SNMP security MIB access is disabled, which is the nondefault setting.

Figure 6-8. Disabling SNMP Access to the Authentication MIB and Displaying the Result

An alternate method of determining the current Authentication MIB access state is to use the **show run** command.

```
ProCurve(config)# show run

Running configuration:

; J8715A Configuration Editor; Created on release #K.12.XX

hostname "ProCurve"
snmp-server mib hpSwitchAuthMIB excluded ] ← Indicates that SNMP access to the
ip default-gateway 10.10.24.55                authentication configuration MIB
snmp-server community "public" Operator      (hpSwitchAuth) is disabled.
vlan 1
  name "DEFAULT_VLAN"
  untagged A1-A24,B1-B4
  ip address 10.10.24.100 255.255.255.0
  exit
password manager
```

Figure 6-9. Using the show run Command to View the Current Authentication MIB Access State

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

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

- Configure the switch to support RADIUS authentication for web browser interface access (Web Authentication, Chapter 7).
- Options for the switches covered in this guide:
 - 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.)
 - Use one of the following methods to disable web browser access to the switch via http (Port 80):

CLI: **no web-management**

Menu Interface—From the Main menu, select the following:

2. Switch Configuration

1. System Information

Web Agent Enabled: No

Commands Authorization

The RADIUS protocol combines user authentication and authorization steps into one phase. The user must be successfully authenticated before the RADIUS server will send authorization information (from the user's profile) to the Network Access Server (NAS). After user authentication has occurred, the authorization information provided by the RADIUS server is stored on the NAS for the duration of the user's session. Changes in the user's authorization profile during this time will not be effective until after the next authentication occurs.

You can limit the services for a user by enabling AAA RADIUS authorization. The NAS uses the information set up on the RADIUS server to control the user's access to CLI commands.

The authorization type implemented on the switches covered in this guide is the "commands" method. This method explicitly specifies on the RADIUS server which commands are allowed on the client device for authenticated users. This is done on a per-user or per-group basis.

Note

The commands authorization will only be executed for commands entered from Telnet, SSH, or console sessions. The Web management interface is not supported.

By default, all users may execute a minimal set of commands regardless of their authorization status, for example, "exit" and "logout". This minimal set of commands can prevent deadlock on the switch due to an error in the user's authorization profile on the RADIUS server.

Enabling Authorization

To configure authorization for controlling access to the CLI commands, enter this command at the CLI.

Syntax: [no] aaa authorization <commands> <radius | none>

Configures authorization for controlling access to CLI commands. When enabled, the switch checks the list of commands supplied by the RADIUS server during user authentication to determine if a command entered by the user can be executed.

radius: *The NAS requests authorization information from the RADIUS server. Authorization rights are assigned by user or group.*

none: *The NAS does not request authorization information.*

For example, to enable the RADIUS protocol as the authorization method:

```
ProCurve(config)# aaa authorization commands radius
```

When the NAS sends the RADIUS server a valid username and password, the RADIUS server sends an Access-Accept packet that contains two attributes—the command list and the command exception flag. When an authenticated user enters a command on the switch, the switch examines the list of commands delivered in the RADIUS Access-Accept packet as well as the command exception flag, which indicates whether the user has permission to execute the commands in the list. See *Configuring the RADIUS Server* on page 6-28.

After the Access-Accept packet is delivered, the command list resides on the switch. Any changes to the user's command list on the RADIUS server are not seen until the user is authenticated again.

Displaying Authorization Information

You can show the authorization information by entering this command:

Syntax: show authorization

Configures authorization for controlling access to CLI commands. When enabled, the switch checks the list of commands supplied by the RADIUS server during user authentication to determine if a command entered by the user can be executed.

An example of the output is shown.

```
ProCurve(config)# show authorization

Status and Counters - Authorization Information

Type      | Method
-----+-----
Commands | RADIUS
```

Figure 6-10. Example of Show Authorization Command

Configuring Commands Authorization on a RADIUS Server

Using Vendor Specific Attributes (VSAs)

Some RADIUS-based features implemented on ProCurve switches use HP VSAs for information exchange with the RADIUS server. RADIUS Access-Accept packets sent to the switch may contain the vendor-specific information. The attributes supported with **commands** authorization are:

- **HP-Command-String:** List of commands (regular expressions) that are permitted (or denied) execution by the user. The commands are delimited by semi-colons and must be between 1 and 249 characters in length. Multiple instances of this attribute may be present in Access-Accept packets. (A single instance may be present in Accounting-Request packets.)
- **HP-Command-Exception:** A flag that specifies whether the commands indicated by the HP-Command-String attribute are permitted or denied to the user. A zero (0) means permit all listed commands and deny all others; a one (1) means deny all listed commands and permit all others.

The results of using the HP-Command-String and HP-Command-Exception attributes in various combinations are shown below.

HP-Command-String	HP-Command-Exception	Description
Not present	Not present	If command authorization is enabled and the RADIUS server does not provide any authorization attributes in an Access-Accept packet, the user is denied access to the server. This message appears: "Access denied: no user's authorization info supplied by the RADIUS server."
Not present	DenyList-PermitOthers(1)	Authenticated user is allowed to execute all commands available on the switch.
Not present	PermitList-DenyOthers(0)	Authenticated user can only execute a minimal set of commands (those that are available by default to any user).
Commands List	DenyList-PermitOthers(1)	Authenticated user may execute all commands except those in the Commands list.
Commands List	PermitList-DenyOthers(0)	Authenticated user can execute only those commands provided in the Commands List, plus the default commands.
Commands List	Not present	Authenticated user can only execute commands from the Commands List, plus the default commands.
Empty Commands List	Not present	Authenticate user can only execute a minimal set of commands (those that are available by default to any user).
Empty Commands List	DenyList-PermitOthers(1)	Authenticated user is allowed to execute all commands available on the switch.
Empty Commands List	PermitList-DenyOthers(0)	Authenticate user can only execute a minimal set of commands (those that are available by default to any user).

You must configure the RADIUS server to provide support for the HP VSAs. There are multiple RADIUS server applications; the two examples below show how a dictionary file can be created to define the VSAs for that RADIUS server application.

Example Configuration on Cisco Secure ACS for MS Windows

It is necessary to create a dictionary file that defines the VSAs so that the RADIUS server application can determine which VSAs to add to its user interface. The VSAs will appear below the standard attributes that can be configured in the application.

The dictionary file must be placed in the proper directory on the RADIUS server. Follow these steps.

1. Create a dictionary file (for example, hp.ini) containing the HP VSA definitions, as shown in the example below.

```
; [User Defined Vendor]
;
; The Name and IETF vendor code and any VSAs MUST be unique.
;
; One or more VSAs named (max 255)
;
; Each named VSA requires a definition section...
;
; Types are STRING, INTEGER, IPADDR
;
; The profile specifies usage, IN for accounting, OUT for
  authorization,
; MULTI if more than a single instance is allowed per
  RADIUS message.
; Combinations are allowed, e.g. "IN", "MULTI OUT",
  "MULT IN OUT"
;
; Enumerations are optional for INTEGER attribute types

[User Defined Vendor]

Name=HP
IETF Code=11
VSA 2=Hp-Command-String
VSA 3=Hp-Command-Exception

[Hp-Command-String]

Type=STRING
Profile=IN OUT

[Hp-Command-Exception]

Type=INTEGER
```

```
Profile=IN OUT
```

```
Enums=Hp-Command-Exception-Types
```

```
[Hp-Command-Exception-Types]
```

```
0=PermitList
```

```
1=DenyList
```

2. Copy the hp.ini dictionary file to c:\program files\cisco acs 3.2\utils (or the \utils directory wherever acs is installed).
3. From the command prompt execute the following command:

```
c:\Program files\CiscoSecure ACS v3.2\utils>  
csutil -addudv 0 hp.ini
```

The zero (0) is the slot number. You will see some processing messages:

```
Adding or removing vendors requires ACS services to be  
re-started. Please make sure regedit is not running as  
it can prevent registry backup/restore operations.
```

```
Are you sure you want to proceed? (Y or N) y
```

```
Parsing [.\hp.ini] for addition at UDV slot [0]
```

```
Stopping any running services
```

```
Creating backup of current config
```

```
Adding Vendor [HP} added as [RADIUS (HP)]
```

```
Done
```

```
Checking new configuration...
```

```
New configuration OK
```

```
Re-starting stopped services
```

4. Start the registry editor (regedit) and browse to HKEY_LOCAL_MACHINE\software\cisco\CiscoAAA v3.2\NAS Vendors tree.

Cisco adds the entry into this tree for each custom vendor. The id is 100 + the slot number used in the previous command (100 + 0, as it was added in slot 0). Look in the key to verify the vendor name and id.

5. Go to:

```
HKEY_LOCAL_MACHINE\software\cisco\CiscoAAA\3.2\  
CSRADIUS\ExtensionPoints\002\AssociatedWithVendors
```

6. Right click and then select **New > key**. Add the vendor Id number that you determined in step 4 (100 in the example).
7. Restart all Cisco services.
8. The newly created HP RADIUS VSA appears only when you configure an AAA client (NAS) to use the HP VSA RADIUS attributes. Select Network Configuration and add (or modify) an AAA entry. In the Authenticate Using field choose RADIUS(HP) as an option for the type of security control protocol.
9. Select **Submit + Restart** to effect the change. The HP RADIUS VSA attributes will appear in Cisco ACS configurations, for example, "Interface Configuration", "Group Setup", "User Setup".

To enable the processing of the HP-Command-String VSA for RADIUS accounting:

1. Select **System Configuration**.
2. Select **Logging**.
3. Select **CSV RADIUS Accounting**. In the Select Columns to Log section, add the HP-Command-String attribute to the Logged Attributes list.
4. Select **Submit**.
5. Select **Network Configuration**. In the AAA Clients section, select an entry in the AAA Client Hostname column. You will go to the AAA Client Setup screen.
6. Check the box for **Log Update/Watchdog Packets from this AAA Client**.
7. Click **Submit + Restart**. You should be able to see the HP-Command-String attribute in the RADIUS accounting reports.

You can enter the commands you wish to allow or deny with the special characters used in standard regular expressions (c, ., \, [list], [^list], *, ^, \$). Commands must be between 1-249 characters in length.

Example Configuration Using FreeRADIUS

1. Create a dictionary file (for example, dictionary.hp) containing HP VSA definitions. An example file is:


```
#
# dictionary.hp
#
# As posted to the list by User <user_email>
#
# Version: $Id: dictionary.hp, v 1.0 2006/02/23 17:07:07
#
VENDOR          Hp          11

# HP Extensions

ATTRIBUTE       Hp-Command-String    2    string    Hp
ATTRIBUTE       Hp-Command-Exception    3    integer   Hp

# Hp-Command-Exception Attribute Values

VALUE           Hp-Command-Exception    Permit-List    0
VALUE           Hp-Command-Exception    Deny-List      1
```

2. Find the location of the dictionary files used by FreeRADIUS (try /usr/local/share/freeradius).
3. Copy dictionary.hp to that location. Open the existing dictionary file and add this entry:
`$ INCLUDE dictionary.hp`
4. You can now use HP VSAs with other attributes when configuring user entries.

VLAN Assignment in an Authentication Session

A switch supports concurrent 802.1X and either Web- or MAC-authentication sessions on a port (with up to 32 clients allowed). If you have configured RADIUS as the primary authentication method for a type of access, when a client authenticates on a port, the RADIUS server assigns an untagged VLAN that is statically configured on the switch for use in the authentication session. (For information on how to configure a user profile on a RADIUS server with the VLAN to be assigned for 802.1X, Web, or MAC authentication, refer to the documentation provided with the RADIUS server application.)

If a switch port is configured to accept multiple 802.1X and/or Web- or MAC-Authentication client sessions, all authenticated clients must use the same port-based, untagged VLAN membership assigned for the earliest, currently active client session. On a port where one or more authenticated client sessions are already running, all clients are on the same untagged VLAN. If the RADIUS server subsequently authenticates a new client, but attempts to re-assign the port to a different, untagged VLAN than the one already in use for the previously existing, authenticated client sessions, the connection for the new client will fail.

Tagged and Untagged VLAN Attributes

When you configure a user profile on a RADIUS server to assign a VLAN to an authenticated client, you can use either the VLAN's name or VLAN ID (VID) number. For example, if a VLAN configured in the switch has a VID of 100 and is named **vlan100**, you could configure the RADIUS server to use either "100" or "vlan100" to specify the VLAN.

After the RADIUS server validates a client's username and password, the RADIUS server returns an Access-Accept packet that contains the VLAN assignment and the following attributes for use in the authentication session:

- **Egress-VLANID:** Configures an optional, egress VLAN ID for either tagged or untagged packets (RFC 4675).
- **Egress-VLAN-Name:** Configures an optional, egress VLAN for either tagged or untagged packets when the VLAN ID is not known (RFC 4675).
- **Tunnel-Type, Tunnel-Medium-Type, and Tunnel-Private-Group-ID:** Tunnel attributes that specify an untagged VLAN assignment (RFC 3580).

Tunnel (untagged VLAN) attributes may be included in the same RADIUS packet as the Egress-VLANID and Egress-VLAN-Name attributes. These attributes are not mutually exclusive.

The switch processes the VLAN information returned from the remote RADIUS server for each successfully 802.1X-, Web-, and MAC-authenticated client (user). The VLAN information is part of the user's profile stored in the RADIUS server's database and is applied if the VLANs exist on the switch.

The support for RADIUS-assigned tagged and untagged VLAN configuration on an authenticated port allows you to use IDM to dynamically configure tagged and untagged VLANs as required for different client devices, such as PCs and IP phones, that share the same switch port.

Additional RADIUS Attributes

The following attributes are included in Access-Request and Access-Accounting packets sent from the switch to the RADIUS server to advertise switch capabilities, report information on authentication sessions, and dynamically reconfigure authentication parameters:

- **MS-RAS-Vendor (RFC 2548):** Allows ProCurve switches to inform a Microsoft RADIUS server that the switches are from ProCurve Networking. This feature assists the RADIUS server in its network configuration.
- **HP-capability-advert:** A ProCurve proprietary RADIUS attribute that allows a switch to advertise its current capabilities to the RADIUS server for port-based (MAC, Web, or 802.1X) authentication; for example, HP VSAs for port QoS, ingress rate-limiting, IDM filter rules, RFC 4675 QoS and VLAN attributes, and RFC 3580 VLAN-related attributes.

The RADIUS server uses this information to make a more intelligent policy decision on the configuration settings to return to the switch for a client session.

- **HP-acct-terminate-cause:** A ProCurve proprietary RADIUS accounting attribute that allows a switch to report to the RADIUS server why an authentication session was terminated. This information allows customers to diagnose network operational problems and generate reports on terminated sessions. This attribute provides extended information on the statistics provided by the acct-terminate-cause attribute.
- **change-of-authorization (RFC 3576: Dynamic Authorization Extensions to RADIUS):** A mechanism that allows a RADIUS server to dynamically terminate or change the authorization parameters (such as VLAN assignment) used in an active client session on the switch. The switch (NAS) does not have to initiate the exchange.

For example, for security reasons you may want to limit the network services granted to an authenticated user. In this case, you can change the user profile on the RADIUS server and have the new authorization settings take effect immediately in the active client session. The change-of-authorization attribute provides the mechanism to dynamically update an active client session with a new user policy that is sent in RADIUS packets.

Configuring RADIUS Accounting

RADIUS Accounting Commands	Page
[no] radius-server host < <i>ip-address</i> >	6-40
[acct-port < <i>port-number</i> >]	6-40
[key < <i>key-string</i> >]	6-40
[no] aaa accounting < exec network system commands > < start-stop stop-only > radius	6-44
[no] aaa accounting update periodic < 1 - 525600 > (<i>in minutes</i>)	6-44
[no] aaa accounting suppress null-username	6-44
show accounting	6-49
show accounting sessions	6-50
show radius accounting	6-50

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 6-7 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 switches covered in this guide support four 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-Authentic | • Acct-Session-Id | • MS-RAS-Vendor |
| • Acct-Delay-Time | • Acct-Session-Time | • NAS-Identifier |
| • Acct-Input-Octets | • Acct-Status-Type | • NAS-IP-Address |
| • Acct-Input-Packets | • Acct-Terminate-Cause | • NAS-Port |
| • Acct-Output-Octets | • Called-Station-Id | • Service-Type |
| • Acct-Output-Packets | • HP-acct-terminate-cause | • Username |

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

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

- **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-Authentic
- Acct-Delay-Time
- Acct-Session-Id
- Acct-Session-Time
- Acct-Terminate-Cause
- Calling-Station-Id
- MS-RAS-Vendor
- NAS-IP-Address
- Service-Type
- Username

- **Commands accounting:** Provides records containing information after the execution of a command.

- **RADIUS accounting with IP attribute:** The RADIUS Attribute 8 (Framed-IP-Address) feature provides the RADIUS server with information about the client's IP address after the client is authenticated. DHCP snooping is queried for the IP address of the client, so DHCP snooping must be enabled for the VLAN of which the client is a member.

When the switch begins communications with the RADIUS server it sends the IP address of the client requesting access to the RADIUS server as RADIUS Attribute 8 (Framed-IP-Address) in the RADIUS accounting request. The RADIUS server can use this information to build a map of usernames and addresses.

It may take a minute or longer for the switch to learn the IP address and then send the accounting packet with the Framed-IP-Address attribute to the RADIUS server. If the switch does not learn the IP address after a minute, it sends the accounting request packet to the RADIUS server without the Framed-IP-Address attribute. If the IP address is learned at a later time, it will be included in the next accounting request packet sent.

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 four types of accounting to run simultaneously: exec, system, network, and commands.
- 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 6-50.)
- 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 “3. Configure the Switch To Access a RADIUS Server” on page 6-14.
- 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 6-14. (Default: null)

2. Configure accounting types and the controls for sending reports to the RADIUS server.
 - **Accounting types:** exec (page 6-38), network (page 6-37), commands (page 6-38), or system (page 6-38)
 - **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 6-14. 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.

Note: When you save the config file using Xmodem or TFTP, the key information is not saved in the file. This causes Radius authentication to fail when the config file is loaded back onto the switch.

(For a more complete description of the **radius-server** command and its options, turn to page 6-14.)

For example, suppose you want 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.).

```
ProCurve(config)# radius-server host 10.33.18.151 acct-port 1750 key source0151
ProCurve(config)# write mem
ProCurve(config)# show radius
Status and Counters - General RADIUS Information
Deadtime(min) : 5
Timeout(secs) : 3
Retransmit Attempts : 2
Global Encryption Key :

Server IP Addr      Auth  Acct  Encryption Key
-----
10.33.18.151      1812  1750  source0151
```

Because the radius-server command includes an **acct-port** element with a non-default 1750, the switch assigns this value to the accounting port UDP port numbers. Because auth-port was not included in the command, the authentication UDP port is set to the default 1812.

Figure 6-11. Example of Configuring for a RADIUS Server with a Non-Default Accounting UDP Port Number

The radius-server command as shown in figure 6-11, 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 Services” on page 6-4.)
- **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 Services” on page 4.)
- **Commands:** When commands authorization is enabled, a record accounting notice is sent after the execution of a command.
- **Web or MAC:** You can also use Web or MAC to collect accounting information.

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, Commands, or System).
- Do not wait for an acknowledgement.

The system option (page 6-42) 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, Commands, or System).
- Do not wait for an acknowledgment.

The system option (page 6-42) 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 | commands > < 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:

```
ProCurve (config)# aaa accounting exec start-stop radius
ProCurve (config)# aaa accounting system stop-only radius
ProCurve (config)# show accounting
Status and Counters - Accounting Information
Interval(min) : 0
Suppress Empty User : No

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

Configures exec and system accounting and controls.

Summarizes the switch's accounting configuration.

Exec and System accounting are active. (Assumes the switch is configured to access a reachable

Figure 6-12. 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 6-12, 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 : Yes

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

The diagram shows a grey rectangular box on the right side of the terminal output. Two arrows originate from this box. The top arrow points to the text 'Interval(min) : 10' in the 'show accounting' output. The bottom arrow points to the text 'Suppress Empty User : Yes' in the same output. The text 'Update Period' is positioned above the top arrow, and 'Suppress Unknown User' is positioned above the bottom arrow.

Figure 6-13. 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 6-37.)*

```
ProCurve(config)# show radius
Status and Counters - General RADIUS Information
  Deadtme(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 6-14. 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 6-15. RADIUS Server Information From the Show Radius Host Command

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.
PendingRequests	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.

Term	Definition
Requests	The number of RADIUS Accounting-Request packets sent. This does not include retransmissions.
AccessChallenges	The number of RADIUS Access-Challenge packets (valid or invalid) received from this server.
AccessAccepts	The number of RADIUS Access-Accept packets (valid or invalid) received from this server.
AccessRejects	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 6-37.)*

ProCurve(config)# show authentication					Note: The Webui access task shown in this figure is available only on the 8212zl switches.
Status and Counters - Authentication Information					
Login Attempts : 2					
Respect Privilege : Disabled					
Access Task	Login Primary	Login Secondary	Enable Primary	Enable 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				

Figure 6-16. 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 : ProCurve.
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 6-17. 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.

```

HPswitch # show accounting

Status and Counters - Accounting Information

Interval(min) : 5
Suppress Empty User : Yes

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

```

Figure 6-18. 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 6-19. 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 6-20. 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 :

Server IP Addr  Auth Port  Acct 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 1.1.1.1 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 6-21. 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.

RADIUS Authentication and Accounting

Changing RADIUS-Server Access Order

```
ProCurve(config)# no radius host 10.10.10.003
ProCurve(config)# no radius host 10.10.10.001
ProCurve(config)# radius host 10.10.10.003
ProCurve(config)# radius host 10.10.10.001

ProCurve(config)# show radius
```

Status and Counters - General RADIUS Information

Deadtime(min) : 0
Timeout(secs) : 5
Retransmit Attempts : 3
Global Encryption Key :

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

Removes the "003" and "001" addresses from the RADIUS server list.

Inserts the "003" address in the first position in the RADIUS server list, and inserts the "001" address in the last position in the list.

Shows the new order in which the switch searches for a RADIUS server.

Figure 6-22. 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 <code>Can't reach RADIUS server < x.x.x.x ></code> , 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.

RADIUS Authentication and Accounting
Messages Related to RADIUS Operation