5

TACACS+ Authentication

Contents

Overview

Feature	Default	Menu	CLI	Web
view the switch's authentication configuration	n/a	—	page 5-9	—
view the switch's TACACS+ server contact configuration	n/a	—	page 5-10	—
configure the switch's authentication methods	disabled	—	page 5-11	—
configure the switch to contact TACACS+ server(s)	disabled	—	page 5-18	—

TACACS+ authentication enables you to use a central server to allow or deny access to the switches covered in this guide (and other TACACS-aware devices) in your network. This means that you can use a central database to create multiple unique username/password sets with associated privilege levels for use by individuals who have reason to access the switch from either the switch's console port (local access) or Telnet (remote access).

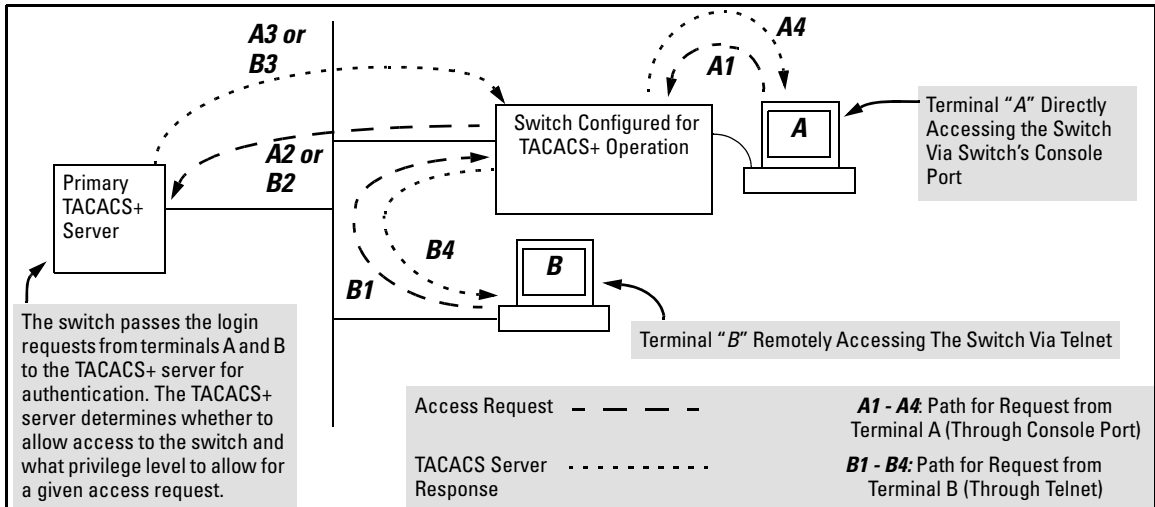**Figure 5-1. Example of TACACS+ Operation**

TACACS+ in the switches covered in this guide manages authentication of logon attempts through either the Console port or Telnet. TACACS+ uses an authentication hierarchy consisting of (1) remote passwords assigned in a TACACS+ server and (2) local passwords configured on the switch. That is, with TACACS+ configured, the switch first tries to contact a designated

TACACS+ server for authentication services. If the switch fails to connect to any TACACS+ server, it defaults to its own locally assigned passwords for authentication control if it has been configured to do so. For both Console and Telnet access you can configure a login (read-only) and an enable (read/write) privilege level access.

TACACS+ does not affect web browser interface access. See "Controlling Web Browser Interface Access" on page 5-28.

Terminology Used in TACACS Applications:

- **NAS (Network Access Server):** This is an industry term for a TACACS-aware device that communicates with a TACACS server for authentication services. Some other terms you may see in literature describing TACACS operation are *communication server, remote access server,* or *terminal server.* These terms apply to a switch when TACACS+ is enabled on the switch (that is, when the switch is TACACS-aware).

- **TACACS+ Server:** The server or management station configured as an access control server for TACACS-enabled devices. To use TACACS+ with a switch covered in this guide and any other TACACS-capable devices in your network, you must purchase, install, and configure a TACACS+ server application on a networked server or management station in the network. The TACACS+ server application you install will provide various options for access control and access notifications. For more on the TACACS+ services available to you, see the documentation provided with the TACACS+ server application you will use.

- **Authentication:** The process for granting user access to a device through entry of a user name and password and comparison of this username/password pair with previously stored username/password data. Authentication also grants levels of access, depending on the privileges assigned to a user name and password pair by a system administrator.

    - **Local Authentication:** This method uses username/password pairs configured locally on the switch; one pair each for manager-level and operator-level access to the switch. You can assign local usernames and passwords through the CLI or web browser inter-

face. (Using the menu interface you can assign a local password, but not a username.) Because this method assigns passwords to the switch instead of to individuals who access the switch, you must distribute the password information on each switch to everyone who needs to access the switch, and you must configure and manage password protection on a per-switch basis. (For more on local authentication, refer to chapter 2, "Configuring Username and Password Security".)

- **TACACS+ Authentication:** This method enables you to use a TACACS+ server in your network to assign a unique password, user name, and privilege level to each individual or group who needs access to one or more switches or other TACACS-aware devices. This allows you to administer primary authentication from a central server, and to do so with more options than you have when using only local authentication. (You will still need to use local authentication as a backup if your TACACS+ servers become unavailable.) This means, for example, that you can use a central TACACS+ server to grant, change, or deny access to a specific individual on a specific switch instead of having to change local user name and password assignments on the switch itself, and then have to notify other users of the change.

General System Requirements

To use TACACS+ authentication, you need the following:

■ A TACACS+ server application installed and configured on one or more servers or management stations in your network. (There are several TACACS+ software packages available.)

■ A switch configured for TACACS+ authentication, with access to one or more TACACS+ servers.

Notes The effectiveness of TACACS+ security depends on correctly using your TACACS+ server application. For this reason, ProCurve recommends that you thoroughly test all TACACS+ configurations used in your network.

TACACS-aware ProCurve switches include the capability of configuring multiple backup TACACS+ servers. ProCurve recommends that you use a TACACS+ server application that supports a redundant backup installation. This allows you to configure the switch to use a backup TACACS+ server if it loses access to the first-choice TACACS+ server.

TACACS+ does not affect web browser interface access. Refer to "Controlling Web Browser Interface Access When Using TACACS+ Authentication" on page 5-28.

General Authentication Setup Procedure

It is important to test the TACACS+ service before fully implementing it. Depending on the process and parameter settings you use to set up and test TACACS+ authentication in your network, you could accidentally lock all users, including yourself, out of access to a switch. While recovery is simple, it may pose an inconvenience that can be avoided. To prevent an unintentional lockout on the switch, use a procedure that configures and tests TACACS+ protection for one access type (for example, Telnet access), while keeping the

other access type (console, in this case) open in case the Telnet access fails due to a configuration problem. The following procedure outlines a general setup procedure.

Note

If a complete access lockout occurs on the switch as a result of a TACACS+ configuration, see "Troubleshooting TACACS+ Operation" in the Trouble-shooting chapter of the *Management and Configuration Guide* for your switch.

1. Familiarize yourself with the requirements for configuring your TACACS+ server application to respond to requests from the switch. (Refer to the documentation provided with the TACACS+ server soft-ware.) This includes knowing whether you need to configure an encryp-tion key. (See "Using the Encryption Key" on page 5-27.)

2. Determine the following:

    - The IP address(es) of the TACACS+ server(s) you want the switch to use for authentication. If you will use more than one server, determine which server is your first-choice for authentication services.
    - The encryption key, if any, for allowing the switch to communicate with the server. You can use either a global key or a server-specific key, depending on the encryption configuration in the TACACS+ server(s).
    - The number of log-in attempts you will allow before closing a log-in session. (Default: 3)

    - The period you want the switch to wait for a reply to an authentication request before trying another server.
    - The username/password pairs you want the TACACS+ server to use for controlling access to the switch.
    - The privilege level you want for each username/password pair administered by the TACACS+ server for controlling access to the switch.
    - The username/password pairs you want to use for local authentication (one pair each for Operator and Manager levels).

3. Plan and enter the TACACS+ server configuration needed to support TACACS+ operation for Telnet access (login and enable) to the switch. This includes the username/password sets for logging in at the Operator (read-only) privilege level and the sets for logging in at the Manager (read/ write) privilege level.

Note on Privilege Levels

When a TACACS+ server authenticates an access request from a switch, it includes a privilege level code for the switch to use in determining which privilege level to grant to the terminal requesting access. The switch interprets a privilege level code of "15" as authorization for the Manager (read/write) privilege level access. Privilege level codes of 14 and lower result in Operator (read-only) access. Thus, when configuring the TACACS+ server response to a request that includes a username/password pair that should have Manager privileges, you must use a privilege level of 15. For more on this topic, refer to the documentation you received with your TACACS+ server application.

If you are a first-time user of the TACACS+ service, ProCurve recommends that you configure only the minimum feature set required by the TACACS+ application to provide service in your network environment. After you have success with the minimum feature set, you may then want to try additional features that the application offers.

4. Ensure that the switch has the correct local username and password for Manager access. (If the switch cannot find any designated TACACS+ servers, the local manager and operator username/password pairs are always used as the secondary access control method.)

Caution

You should ensure that the switch has a local Manager password. Otherwise, if authentication through a TACACS+ server fails for any reason, then unauthorized access will be available through the console port or Telnet.

5. Using a terminal device connected to the switch's console port, configure the switch for TACACS+ authentication *only* for **telnet login** access and **telnet enable** access. At this stage, do not configure TACACS+ authentication for console access to the switch, as you may need to use the console for access if the configuration for the Telnet method needs debugging.

6. Ensure that the switch is configured to operate on your network and can communicate with your first-choice TACACS+ server. (At a minimum, this requires IP addressing and a successful **ping** test from the switch to the server.)

7. On a remote terminal device, use Telnet to attempt to access the switch. If the attempt fails, use the console access to check the TACACS+ configuration on the switch. If you make changes in the switch configuration, check Telnet access again. If Telnet access still fails, check the

configuration in your TACACS+ server application for mis-configurations or missing data that could affect the server's interoperation with the switch.

8. After your testing shows that Telnet access using the TACACS+ server is working properly, configure your TACACS+ server application for console access. Then test the console access. If access problems occur, check for and correct any problems in the switch configuration, and then test console access again. If problems persist, check your TACACS+ server application for mis-configurations or missing data that could affect the console access.

9. When you are confident that TACACS+ access through both Telnet and the switch's console operates properly, use the **write memory** command to save the switch's running-config file to flash.

Configuring TACACS+ on the Switch

Before You Begin

If you are new to TACACS+ authentication, ProCurve recommends that you read the "General Authentication Setup Procedure" on page 5-5 and configure your TACACS+ server(s) before configuring authentication on the switch.

The switch offers three command areas for TACACS+ operation:

■ **show authentication** and **show tacacs:** Displays the switch's TACACS+ configuration and status.

■ **aaa authentication:** A command for configuring the switch's authentication methods

■ **tacacs-server:** A command for configuring the switch's contact with TACACS+ servers

CLI Commands Described in this Section

Command	Page
show authentication	5-9
show tacacs	5-10
aaa authentication	5-11 through 5-17
console	
Telnet	
num-attempts <1-10 >	
tacacs-server	5-18
host < *ip-addr* >	5-18
key	5-22
timeout < 1-255 >	5-23

Viewing the Switch's Current Authentication Configuration

This command lists the number of login attempts the switch allows in a single login session, and the primary/secondary access methods configured for each type of access.

Syntax: show authentication

This example shows the default authentication configuration.

```
ProCurve> show authentication
 Status and Counters - Authentication Information
  Login Attempts : 3

              Login      Login       Enable     Enable
  Access Task Primary    Secondary   Primary    Secondary
  ----------- --------   ----------  --------   ----------
  Console     Local      None        Local      None
  Telnet      Local      None        Local      None
```

Configuration for login and enable access to the switch through the switch console port.

Configuration for login and enable access to the switch through Telnet.

Figure 5-2. Example Listing of the Switch's Authentication Configuration

Viewing the Switch's Current TACACS+ Server Contact Configuration

This command lists the timeout period, encryption key, and the IP addresses of the first-choice and backup TACACS+ servers the switch can contact.

Syntax: show tacacs

For example, if the switch was configured for a first-choice and two backup TACACS+ server addresses, the default timeout period, and **paris-1** for a (global) encryption key, **show tacacs** would produce a listing similar to the following:

```
                ProCurve # show tacacs
First-Choice      Status and Counters - TACACS Information
TACACS+ Server      Timeout : 5
                    Encryption Key : paris-1
Second-Choice       Server IP Addr  Opens   Closes  Aborts  Errors  Pkts Rx  Pkts Tx
TACACS+ Server      --------------  ------  ------  ------  ------  -------  -------
                    10.30.248.100   0       0       0       0       0        0
Third-Choice        10.30.248.156   0       0       0       0       0        0
TACACS+ Server      10.30.248.105   0       0       0       0       0        0
```

Figure 5-3. Example of the Switch's TACACS+ Configuration Listing

Configuring the Switch's Authentication Methods

The **aaa authentication** command configures access control for the following access methods:

■   Console

■   Telnet

■   SSH

■   Web

■   Port-access (802.1X)

However, TACACS+ authentication is only used with the console, Telnet, or SSH access methods. The command specifies whether to use a TACACS+ server or the switch's local authentication, or (for some secondary scenarios) no authentication (meaning that if the primary method fails, authentication is denied). The command also reconfigures the number of access attempts to allow in a session if the first attempt uses an incorrect username/password pair.

Using the Privilege-Mode Option for Login

When using TACACS+ to control user access to the switch, you must first login with your username at the Operator privilege level using the password for Operator privileges, and then login again with the same username but using the Manger password to obtain Manager privileges. You can avoid this double login process by entering the **privilege-mode** option with the **aaa authentication login** command to enable TACACS+ for a single login. The switch authenticates your username/password, then requests the privilege level (Operator or Manager) that was configured on the TACACS+ server for this username/password. The TACACS+ server returns the allowed privilege level to the switch. You are placed directly into Operator or Manager mode, depending on your privilege level.

```
ProCurve(config) aaa authentication login privilege-mode
```

The **no** version of the above command disables TACACS+ single login capability.

Syntax: aaa authentication

< console | telnet | ssh | web | port-access >

Selects the access method for configuration.

< enable>

*The server grants privileges at the Manager privilege
level.*

<login [privilege-mode] >

*The server grants privileges at the Operator privilege
level. If the* **privilege-mode** *option is entered, TACACS+ is
enabled for a single login. The authorized privilege level
(Operator or Manager) is returned to the switch by the
TACACS+ server.*
Default: Single login disabled.

< local | tacacs | radius >

Selects the type of security access:
local — *Authenticates with the Manager and Operator
password you configure in the switch.*
tacacs — *Authenticates with a password and other
data configured on a TACACS+ server.*
radius — *Authenticates with a password and other
data configured on a RADIUS server.*

[< local | none >]

*If the primary authentication method fails, determines
whether to use the local password as a secondary method
or to disallow access.*

aaa authentication num-attempts < 1-10 >

*Specifies the maximum number of login attempts allowed in
the current session. Default: 3*

Authentication Parameters

Table 5-1.   AAA Authentication Parameters Parameters

Name	Default	Range	Function
console, Telnet, SSH, web or port-access	n/a	n/a	Specifies the access method used when authenticating. TACACS+ authentication only uses the console, Telnet or SSH access methods.

Name	Default	Range	Function
enable	n/a	n/a	Specifies the Manager (read/write) privilege level for the access method being configured.
login <privilege-mode>	privilege-mode disabled	n/a	**login:** Specifies the Operator (read-only) privilege level for the access method being configured. The **privilege-mode** option enables TACACS+ for a single login. The authorized privilege level (Operator or Manager) is returned to the switch by the TACACS+ server.

local
- or -
tacacs
	local	n/a	Specifies the primary method of authentication for the access method being configured.
			    local: Use the username/password pair configured locally in the switch for
			        the privilege level being configured
			  tacacs: Use a TACACS+ server.

local
- or -
none
	none	n/a	Specifies the secondary (backup) type of authentication being configured.
			    local: The username/password pair configured locally in the switch for the
			        privilege level being configured
			  none: No secondary type of authentication for the specified method/privilege path. **(Available only if the primary method of authentication for the access being configured is local.)**
			
			Note: If you do not specify this parameter in the command line, the switch automatically assigns the secondary method as follows:
			• If the primary method is **tacacs**, the **only** secondary method is **local**.
			• If the primary method is **local**, the default secondary method is **none**.

num-attempts	3	1 - 10	In a given session, specifies how many tries at entering the correct username/password pair are allowed before access is denied and the session terminated.

Configuring the TACACS+ Server for Single Login

In order for the single login feature to work correctly, you need to check some entries in the User Setup on the TACACS+ server.

In the User Setup, scroll to the Advanced TACACS+ Settings section. Make sure the radio button for "Max Privilege for any AAA Client" is checked and the level is set to 15, as shown in Figure 5-4. Privileges are represented by the numbers 0 through 15, with zero allowing only Operator privileges (and requiring two logins) and 15 representing root privileges. The root privilege level is the only level that will allow Manager level access on the switch.
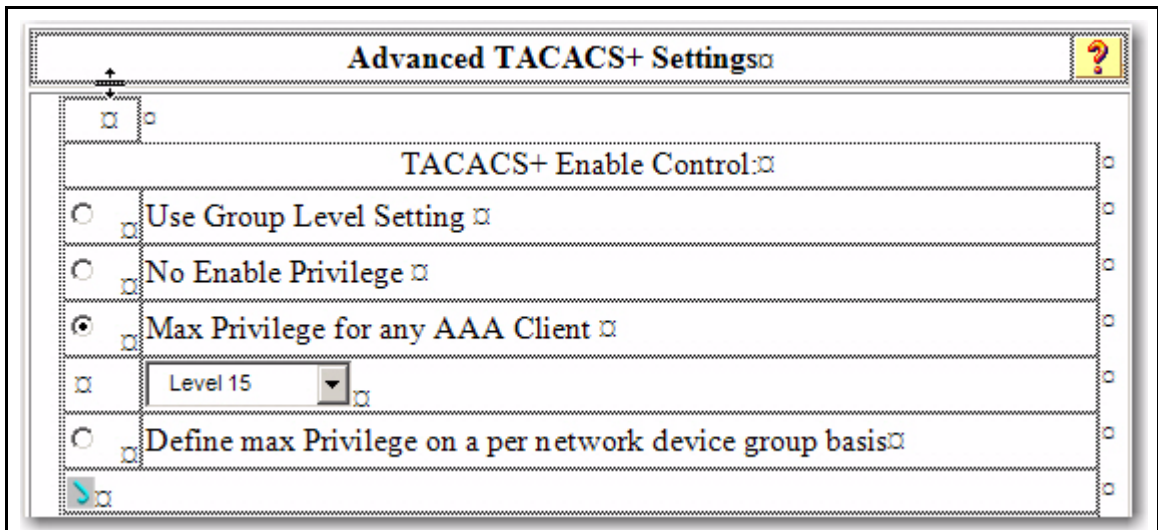
Figure 5-4. Advanced TACACS+ Settings Section of the TACACS+ Server User Setup

Then scroll down to the section that begins with "Shell" (See Figure 5-5). Check the Shell box.

Check the Privilege level box and set the privilege level to 15 to allow "root" privileges. This allows you to use the single login option.

Figure 5-5. The Shell Section of the TACACS+ Server User Setup

As shown in the next table, login and enable access is always available locally through a direct terminal connection to the switch's console port. However, for Telnet access, you can configure TACACS+ to deny access if a TACACS+ server goes down or otherwise becomes unavailable to the switch.

Table 5-2.   Primary/Secondary Authentication Table

Access Method and Privilege Level	Authentication Options		Effect on Access Attempts
	Primary	Secondary	
Console — Login	local	none*	Local username/password access only.
	tacacs	local	If Tacacs+ server unavailable, uses local username/password access.
Console — Enable	local	none	Local username/password access only.
	tacacs	local	If Tacacs+ server unavailable, uses local username/password access.
Telnet — Login	local	none*	Local username/password access only.
	tacacs	local	If Tacacs+ server unavailable, uses local username/password access.
	tacacs	none	If Tacacs+ server unavailable, denies access.
Telnet — Enable	local	none	Local username/password access only.
	tacacs	local	If Tacacs+ server unavailable, uses local username/password access.
	tacacs	none	If Tacacs+ server unavailable, denies access.

Caution Regarding the Use of Local for Login Primary Access

During local authentication (which uses passwords configured in the switch instead of in a TACACS+ server), the switch grants read-only access if you enter the Operator password, and read-write access if you enter the Manager password. For example, if you configure authentication on the switch with Telnet Login Primary as Local and Telnet Enable Primary as Tacacs, when you attempt to Telnet to the switch, you will be prompted for a local password. If you enter the switch's local Manager password (or, if there is no local Manager password configured in the switch) you can bypass the TACACS+ server authentication for Telnet Enable Primary and go directly to read-write (Manager) access. Thus, for either the Telnet or console access method, configuring Login Primary for Local authentication while configuring Enable Primary for TACACS+ authentication is not recommended, as it defeats the purpose of using the TACACS+ authentication. If you want Enable Primary log-in attempts to go to a TACACS+ server, then you should configure both Login Primary and Enable Primary for Tacacs authentication instead of configuring Login Primary to Local authentication.

For example, here is a set of access options and the corresponding commands to configure them:

Console Login (Operator or Read-Only) Access: Primary using TACACS+ server.
Secondary using Local.

```
ProCurve (config)# aaa authentication console login tacacs local
```

Console Enable (Manager or Read/Write) Access: Primary using TACACS+ server.
Secondary using Local.

```
ProCurve (config)# aaa authentication console enable tacacs local
```

Telnet Login (Operator or Read-Only) Access: Primary using TACACS+ server.
Secondary using Local.

```
ProCurve (config)# aaa authentication Telnet login tacacs local
```

Telnet Enable (Manager or Read/Write Access: Primary using TACACS+ server.
Secondary using Local.

```
ProCurve (config)# aaa authentication telnet enable tacacs local
```

Deny Access and Close the Session After Failure of Two Consecutive Username/Password Pairs:

```
ProCurve (config)# aaa authentication num-attempts 2
```

Configuring the Switch's TACACS+ Server Access

The tacacs-server command configures these parameters:

■ **The host IP address(es)** for up to three TACACS+ servers; one first-choice and up to two backups. Designating backup servers provides for a continuation of authentication services in case the switch is unable to contact the first-choice server.

■ **An optional encryption key.** This key helps to improve security, and must match the encryption key used in your TACACS+ server application. In some applications, the term "secret key" or "secret" may be used instead of "encryption key". If you need only one encryption key for the switch to use in all attempts to authenticate through a TACACS+ server, configure a global key. However, if the switch is configured to access multiple TACACS+ servers having different encryption keys, you can configure the switch to use different encryption keys for different TACACS+ servers.

■ **The timeout value** in seconds for attempts to contact a TACACS+ server. If the switch sends an authentication request, but does not receive a response within the period specified by the timeout value, the switch resends the request to the next server in its Server IP Addr list, if any. If the switch still fails to receive a response from any TACACS+ server, it reverts to whatever secondary authentication method was configured using the **aaa authentication** command (local or none; see "Configuring the Switch's Authentication Methods" on page 5-11.)

Note　　As described under "General Authentication Setup Procedure" on page 5-5, ProCurve recommends that you configure, test, and troubleshoot authentication via Telnet access before you configure authentication via console port access. This helps to prevent accidentally locking yourself out of switch access due to errors or problems in setting up authentication in either the switch or your TACACS+ server.

Syntax: tacacs-server host < *ip-addr* > [key < *key-string* >]

Adds a TACACS+ server and optionally assigns a server-specific encryption key.

[no] tacacs-server host < *ip-addr* >

Removes a TACACS+ server assignment (including its server-specific encryption key, if any).

tacacs-server key <*key-string*>

Enters the optional global encryption key.

[no] tacacs-server key

Removes the optional global encryption key. (Does not affect any server-specific encryption key assignments.)

tacacs-server timeout < 1-255 >

Changes the wait period for a TACACS server response. (Default: 5 seconds.)

Note on Encryption Keys

Encryption keys configured in the switch must exactly match the encryption keys configured in TACACS+ servers the switch will attempt to use for authentication.

If you configure a global encryption key, the switch uses it only with servers for which you have not also configured a server-specific key. Thus, a global key is more useful where the TACACS+ servers you are using all have an identical key, and server-specific keys are necessary where different TACACS+ servers have different keys.

If TACACS+ server "X" does not have an encryption key assigned for the switch, then configuring either a global encryption key or a server-specific key in the switch for server "X" will block authentication support from server "X".

Name	Default	Range
host <*ip-addr*> [key <*key-string*>	none	n/a

Specifies the IP address of a device running a TACACS+ server application. Optionally, can also specify the unique, per-server encryption key to use when each assigned server has its own, unique key. For more on the encryption key, see "Using the Encryption Key" on page 5-27 and the documentation provided with your TACACS+ server application.

You can enter up to three IP addresses; one first-choice and two (optional) backups (one second-choice and one third-choice).

Use **show tacacs** to view the current IP address list.

If the first-choice TACACS+ server fails to respond to a request, the switch tries the second address, if any, in the show tacacs list. If the second address also fails, then the switch tries the third address, if any.

(See figure 5-3, "Example of the Switch's TACACS+ Configuration Listing" on 5-10.)

The priority (first-choice, second-choice, and third-choice) of a TACACS+ server in the switch's TACACS+ configuration depends on the order in which you enter the server IP addresses:

1. When there are no TACACS+ servers configured, entering a server IP address makes that server the first-choice TACACS+ server.

2. When there is one TACACS+ serves already configured, entering another server IP address makes that server the second-choice (backup) TACACS+ server.

3. When there are two TACACS+ servers already configured, entering another server IP address makes that server the third-choice (backup) TACACS+ server.

- The above position assignments are fixed. Thus, if you remove one server and replace it with another, the new server assumes the priority position that the removed server had. For example, suppose you configured three servers, A, B, and C, configured in order:

  First-Choice: A
  Second-Choice: B
  Third-Choice: C

- If you removed server B and then entered server X, the TACACS+ server order of priority would be:

  First-Choice: A
  Second-Choice: X
  Third-Choice: C

- If there are two or more vacant slots in the TACACS+ server priority list and you enter a new IP address, the new address will take the vacant slot with the highest priority. Thus, if A, B, and C are configured as above and you (1) remove A and B, and (2) enter X and Y (in that order), then the new TACACS+ server priority list would be X, Y, and C.

- The easiest way to change the order of the TACACS+ servers in the priority list is to remove all server addresses in the list and then re-enter them in order, with the new first-choice server address first, and so on.

To add a new address to the list when there are already three addresses present, you must first remove one of the currently listed addresses.

See also "General Authentication Process Using a TACACS+ Server" on page 5-24.

Name	Default	Range
key <*key-string*>	none (null)	n/a

Specifies the optional, global "encryption key" that is also assigned in the TACACS+ server(s) that the switch will access for authentication. This option is subordinate to any "per-server" encryption keys you assign, and applies only to accessing TACACS+ servers for which you have not given the switch a "per-server" key. (See the **host <*ip-addr*> [key <*key-string*>** entry at the beginning of this table.)

For more on the encryption key, see "Using the Encryption Key" on page 5-27 and the documentation provided with your TACACS+ server application.

timeout <1 - 255>	5 sec	1 - 255 sec

Specifies how long the switch waits for a TACACS+ server to respond to an authentication request. If the switch does not detect a response within the timeout period, it initiates a new request to the next TACACS+ server in the list. If all TACACS+ servers in the list fail to respond within the timeout period, the switch uses either local authentication (if configured) or denies access (if **none** configured for local authentication).

Adding, Removing, or Changing the Priority of a TACACS+ Server.

Suppose that the switch was already configured to use TACACS+ servers at 10.28.227.10 and 10.28.227.15. In this case, 10.28.227.15 was entered first, and so is listed as the first-choice server:

```
ProCurve# show tacacs
 Status and Counters - TACACS Information
  Timeout : 5
  Encryption Key :     First-Choice TACACS+ Server

  Server IP Addr  Closes    Aborts    Errors    Pkts Rx   Pkts Tx
  -------------   --------  --------  --------  --------  --------
  10.28.227.15    0         0         0         0         0
  10.28.227.10    0         0         0         0         0
```

Figure 5-6. Example of the Switch with Two TACACS+ Server Addresses Configured

To move the "first-choice" status from the "15" server to the "10" server, use the **no tacacs-server host <*ip-addr*>** command to delete both servers, then use **tacacs-server host <*ip-addr*>** to re-enter the "10" server first, then the "15" server.

The servers would then be listed with the new "first-choice" server, that is:

```
                                The "10" server is now the "first-choice" TACACS+ authentication device.

ProCurve# show tacacs
  Status and Counters - TACACS Information
   Timeout : 5
   Encryption Key :
   Server IP Addr  Opens    Closes   Aborts   Errors   Pkts Rx  Pkts Tx
   --------------  -------- -------- -------- -------- -------- --------
   10.28.227.10    0        0        0        0        0        0
   10.28.227.15    0        0        0        0        0        0
```

Figure 5-7. Example of the Switch After Assigning a Different "First-Choice" Server

To remove the 10.28.227.15 device as a TACACS+ server, you would use this command:

```
ProCurve(config)# no tacacs-server host 10.28.227.15
```

Configuring an Encryption Key. Use an encryption key in the switch if the switch will be requesting authentication from a TACACS+ server that also uses an encryption key. (If the server expects a key, but the switch either does not provide one, or provides an incorrect key, then the authentication attempt will fail.) Use a *global encryption key* if the same key applies to all TACACS+ servers the switch may use for authentication attempts. Use a *per-server encryption key* if different servers the switch may use will have different keys. (For more details on encryption keys, see "Using the Encryption Key" on page 5-27.)

To configure **north01** as a global encryption key:

```
ProCurve(config) tacacs-server key north01
```

To configure **north01** as a per-server encryption key:

```
ProCurve(config)# tacacs-server host 10.28.227.63 key
north01
```

An encryption key can contain up to 100 characters, without spaces, and is likely to be case-sensitive in most TACACS+ server applications.

To delete a global encryption key from the switch, use this command:

```
ProCurve(config)# no tacacs-server key
```

To delete a per-server encryption key in the switch, re-enter the tacacs-server host command without the key parameter. For example, if you have **north01** configured as the encryption key for a TACACS+ server with an IP address of 10.28.227.104 and you want to eliminate the key, you would use this command:

```
ProCurve(config)# tacacs-server host 10.28.227.104
```

Note   You can save the encryption key in a configuration file by entering this command:

```
Procurve(config)# tacacs-server key <keystring>
```

The `<keystring>` parameter is the encryption key in clear text.

Note   The **show tacacs** command lists the global encryption key, if configured. However, to view any configured per-server encryption keys, you must use **show config** or **show config running** (if you have made TACACS+ configuration changes without executing **write mem**).

Configuring the Timeout Period. The timeout period specifies how long the switch waits for a response to an authentication request from a TACACS+ server before either sending a new request to the next server in the switch's Server IP Address list or using the local authentication option. For example, to change the timeout period from 5 seconds (the default) to 3 seconds:

```
ProCurve(config)# tacacs-server timeout 3
```

How Authentication Operates

General Authentication Process Using a TACACS+ Server

Authentication through a TACACS+ server operates generally as described below. For specific operating details, refer to the documentation you received with your TACACS+ server application.
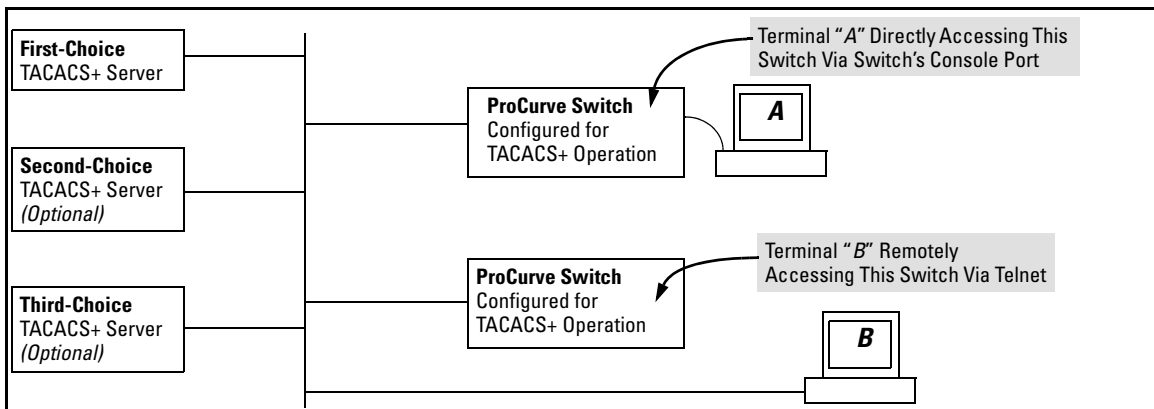

Figure 5-8. Using a TACACS+ Server for Authentication

Using figure 5-8, above, after either switch detects an operator's logon request from a remote or directly connected terminal, the following events occur:

1. The switch queries the first-choice TACACS+ server for authentication of the request.

    • If the switch does not receive a response from the first-choice TACACS+ server, it attempts to query a secondary server. If the switch does not receive a response from any TACACS+ server, then it uses its own local username/password pairs to authenticate the logon request. (See "Local Authentication Process" on page 5-26.)

    • If a TACACS+ server recognizes the switch, it forwards a username prompt to the requesting terminal via the switch.

2. When the requesting terminal responds to the prompt with a username, the switch forwards it to the TACACS+ server.

3. After the server receives the username input, the requesting terminal receives a password prompt from the server via the switch.

4. When the requesting terminal responds to the prompt with a password, the switch forwards it to the TACACS+ server and one of the following actions occurs:

    •   If the username/password pair received from the requesting terminal matches a username/password pair previously stored in the server, then the server passes access permission through the switch to the terminal.

    •   If the username/password pair entered at the requesting terminal does not match a username/password pair previously stored in the server, access is denied. In this case, the terminal is again prompted to enter a username and repeat steps 2 through 4. In the default configuration, the switch allows up to three attempts to authenticate a login session. If the requesting terminal exhausts the attempt limit without a successful TACACS+ authentication, the login session is terminated and the operator at the requesting terminal must initiate a new session before trying again.

Local Authentication Process

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

■ "Local" is the authentication option for the access method being used.

■ TACACS+ is the primary authentication mode for the access method being used. However, the switch was unable to connect to any TACACS+ servers (or no servers were configured) AND **Local** is the secondary authentication mode being used.

(For a listing of authentication options, see table 5-2, "Primary/Secondary Authentication Table" on 5-16.)

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, access is granted.

■ If the username/password pair entered at the requesting terminal does not match either username/password pair previously configured locally 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.

Note   The switch's menu allows you to configure only the local Operator and Manager passwords, and not any usernames. In this case, all prompts for local authentication will request only a local password. However, if you use the CLI or the web browser interface to configure usernames for local access, you will see a prompt for both a local username and a local password during local authentication.

Using the Encryption Key

General Operation

When used, the encryption key (sometimes termed "key", "secret key", or "secret") helps to prevent unauthorized intruders on the network from reading username and password information in TACACS+ packets moving between the switch and a TACACS+ server. At the TACACS+ server, a key may include both of the following:

■ **Global key:** A general key assignment in the TACACS+ server application that applies to all TACACS-aware devices for which an individual key has not been configured.

■ **Server-Specific key:** A unique key assignment in the TACACS+ server application that applies to a specific TACACS-aware device.

Note   Configure a key in the switch only if the TACACS+ server application has this exact same key configured for the switch. That is, if the key parameter in switch "X" does not exactly match the key setting for switch "X" in the TACACS+ server application, then communication between the switch and the TACACS+ server will fail.

Thus, on the TACACS+ server side, you have a choice as to how to implement a key. On the switch side, it is necessary only to enter the key parameter so that it exactly matches its counterpart in the server. For information on how to configure a general or individual key in the TACACS+ server, refer to the documentation you received with the application.

Encryption Options in the Switch

When configured, the encryption key causes the switch to encrypt the TACACS+ packets it sends to the server. When left at "null", the TACACS+ packets are sent in clear text. The encryption key (or just "key") you configure in the switch must be identical to the encryption key configured in the corresponding TACACS+ server. If the key is the same for all TACACS+ servers the switch will use for authentication, then configure a global key in the switch. If the key is different for one or more of these servers, use "server-specific" keys in the switch. (If you configure both a global key and one or more per-server keys, the per-server keys will override the global key for the specified servers.)

For example, you would use the next command to configure a global encryption key in the switch to match a key entered as **north40campus** in two target TACACS+ servers. (That is, both servers use the same key for your switch.) Note that you do not need the server IP addresses to configure a global key in the switch:

```
ProCurve(config)# tacacs-server key north40campus
```

Suppose that you subsequently add a third TACACS+ server (with an IP address of 10.28.227.87) that has **south10campus** for an encryption key. Because this key is different than the one used for the two servers in the previous example, you will need to assign a server-specific key in the switch that applies only to the designated server:

```
ProCurve(config)# tacacs-server host 10.28.227.87 key
south10campus
```

With both of the above keys configured in the switch, the **south10campus** key overrides the **north40campus** key only when the switch tries to access the TACACS+ server having the 10.28.227.87 address.

Controlling Web Browser Interface Access When Using TACACS+ Authentication

Configuring the switch for TACACS+ authentication does not affect web browser interface access. To prevent unauthorized access through the web browser interface, do one or more of the following:

■ 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 by going to the System Information screen in the Menu interface and configuring the **Web Agent Enabled** parameter to **No**.

Messages Related to TACACS+ Operation

The switch generates the CLI messages listed below. However, you may see other messages generated in your TACACS+ server application. For information on such messages, refer to the documentation you received with the application.

CLI Message	Meaning
Connecting to Tacacs server	The switch is attempting to contact the TACACS+ server identified in the switch's **tacacs-server** configuration as the **first-choice** (or only) TACACS+ server.
Connecting to secondary Tacacs server	The switch was not able to contact the **first-choice** TACACS+ server, and is now attempting to contact the next (secondary) TACACS+ server identified in the switch's **tacacs-server** configuration.
Invalid password	The system does not recognize the username or the password or both. Depending on the authentication method (**tacacs** or **local**), either the TACACS+ server application did not recognize the username/password pair or the username/password pair did not match the username/password pair configured in the switch.
No Tacacs servers responding	The switch has not been able to contact any designated TACACS+ servers. If this message is followed by the **Username** prompt, the switch is attempting local authentication.
Not legal combination of authentication methods	**For console access,** if you select **tacacs** as the primary authentication method, you must select **local** as the secondary authentication method. This prevents you from being locked out of the switch if all designated TACACS+ servers are inaccessible to the switch.
Record already exists	When resulting from a **tacacs-server host** <*ip addr*> command, indicates an attempt to enter a duplicate TACACS+ server IP address.

Operating Notes

■   If you configure Authorized IP Managers on the switch, it is not necessary to include any devices used as TACACS+ servers in the authorized manager list. That is, authentication traffic between a TACACS+ server and the switch is not subject to Authorized IP Manager controls configured on the switch. Also, the switch does not attempt TACACS+ authentication for a management station that the Authorized IP Manager list excludes because, independent of TACACS+, the switch already denies access to such stations.

■ When TACACS+ is not enabled on the switch—or when the switch's only designated TACACS+ servers are not accessible— setting a local Operator password without also setting a local Manager password does not protect the switch from manager-level access by unauthorized persons.

■ When using the **copy** command to transfer a configuration to a TFTP server, any optional, server-specific and global encryption keys (page 5-18) in the TACACS configuration will not be included in the transferred file. Otherwise, a security breach could occur, allowing access to the TACACS+ username/password information.