Chapter 3
Securing Access

This chapter outlines the physical installation and network connection for the HP 9304M, HP 9308M, and HP 6308M-SX routing switches and the HP 6208M-SX switch.

The HP 9304M, HP 9308M, and HP 6308M-SX routing switches and the HP 6208M-SX switch provide the following methods for securing access to the device. You can use one or more of these methods:

- Local user accounts
- Enable passwords (for CLI access)
- Telnet password (for CLI access through Telnet only)
- RADIUS authentication server (for CLI access only)
- TACACS or TACACS+ authentication server (for CLI access only)
- SNMP community strings (the default access method for the Web management interface)

Table 3.3.1 lists the default authentication methods and the methods that are supported for each type of management access to the device.

Table 3.1: Access Authentication Methods

Access Method	Default Authentication Method	Supported Authentication Methods
Serial access to CLI	None	None
"Enable" access to the Privileged EXEC and CONFIG levels of the CLI	None	• TACACS/TACACS+ • RADIUS • Local user accounts • "Enable" password • Telnet password • IP address list

Table 3.1: Access Authentication Methods (Continued)

Access Method	Default Authentication Method	Supported Authentication Methods
Telnet access to the CLI	None	• Access Control Lists (ACLs) • TACACS/TACACS+ • RADIUS • Local user accounts • "Enable" password • Telnet password • IP address list
Web management access	SNMP read or read-write community strings	• Access Control Lists (ACLs) • Local user accounts • SNMP read or read-write community strings • IP address list

The following sections describe how to configure each of these methods.

NOTE: If you want to authenticate access using local user accounts, a TACACS/TACACS+ server, or a RADIUS server, you must configure an authentication method list for each type of access to which these methods applies. See "Configuring Authentication-Method Lists" on page 3-24.

Restricting Remote Access to the Device Using Access Control Lists

You can use standard ACLs to control the following types of management access to an HP device:

- Telnet
- Web
- SNMP

To configure access control for these access methods:

1. Configure an ACL with the IP addresses you want to allow to access the device
2. Configure a Telnet access group, web access group, and SNMP community strings. Each of these configuration items accepts an ACL as a parameter. The ACL contains entries that identify the IP addresses that can use the access method.

Use the methods in the following sections to configure management access based on ACLs.

Controlling Telnet Access

To use ACLs to control Telnet access, use the following method.

USING THE CLI

To configure an ACL and use it to control Telnet access to the device, enter commands such as the following:

```
HP9300(config)# access-list 10 deny host 209.157.22.32 log
HP9300(config)# access-list 10 deny 209.157.23.0 0.0.0.255 log
HP9300(config)# access-list 10 deny 209.157.24.0 0.0.0.255 log
HP9300(config)# access-list 10 deny 209.157.25.0/24 log
HP9300(config)# access-list 10 permit any
HP9300(config)# telnet access-group 10
HP9300(config)# write mem
```

Syntax: telnet access-group <num>

The <num> parameter specifies the number of a standard ACL and must be from 1 – 99.

These commands configure ACL 10, then apply the ACL as the access list for Telnet access. The device will allow Telnet access to all IP addresses except those listed in ACL 10.

To configure a more restrictive ACL, create permit entries and do not add an entry to permit all at the end of the ACL. Here is an example:

```
HP9300(config)# access-list 10 permit host 209.157.22.32
HP9300(config)# access-list 10 permit 209.157.23.0 0.0.0.255
HP9300(config)# access-list 10 permit 209.157.24.0 0.0.0.255
HP9300(config)# access-list 10 permit 209.157.25.0/24
HP9300(config)# telnet access-group 10
HP9300(config)# write mem
```

The ACL in this example permits access only to the IP addresses in the permit entries and denies access from all other IP addresses.

Controlling Web Access

To use ACLs to control Web access, use the following method.

USING THE CLI

To configure an ACL list and use it to control Web access to the device, enter the following commands:

```
HP9300(config)# access-list 12 deny host 209.157.22.98 log
HP9300(config)# access-list 12 deny 209.157.23.0 0.0.0.255 log
HP9300(config)# access-list 12 deny 209.157.24.0/24 log
HP9300(config)# access-list 12 permit any
HP9300(config)# web access-group 12
HP9300(config)# write mem
```

Syntax: web access-group <num>

The <num> parameter specifies the number of a standard ACL and must be from 1 – 99.

These commands configure ACL 12, then apply the ACL as the access list for Web access. The device denies Web management access from the IP addresses listed in ACL 12 and permits Web management access from all other IP addresses. Without the last ACL entry for permitting all packets, this ACL would deny Web management access from all IP addresses.

NOTE: In this example, the **web access-group 10** command could have been used to apply the ACL configured in the example for Telnet access. You can use the same ACL multiple times.

Controlling SNMP Access

To use ACLs to control SNMP access, use the following method.

NOTE: The syntax for using ACLs for SNMP access is different from the syntax for controlling Telnet and web access using ACLs.

USING THE CLI

To configure an ACL list and use it to control SNMP access to the device, enter the following commands:

```
HP9300(config)# access-list 25 deny host 209.157.22.98 log
HP9300(config)# access-list 25 deny 209.157.23.0 0.0.0.255 log
HP9300(config)# access-list 25 deny 209.157.24.0 0.0.0.255 log
HP9300(config)# access-list 30 deny 209.157.25.0 0.0.0.255 log
HP9300(config)# access-list 30 deny 209.157.26.0/24 log
HP9300(config)# access-list 30 permit any
HP9300(config)# snmp-server community public ro 25
HP9300(config)# snmp-server community private rw 30
HP9300(config)# write mem
```

Syntax: snmp-server community <string> ro | rw <num>

The <string> parameter specifies the SNMP community string the user must enter to gain SNMP access.

The **ro** parameter indicates that the community string is for read-only (“get”) access. The **rw** parameter indicates the community string is for read-write (“set”) access.

The <num> parameter specifies the number of a standard ACL and must be from 1 – 99.

These commands configure ACLs 25 and 30, then apply the ACLs to community strings.

ACL 25 is used to control read-only access using the “public” community string. ACL 30 is used to control read-write access using the “private” community string.

Restricting Remote Access to the Device to Specific IP Addresses

By default, an HP device does not control remote management access based on the IP address of the managing device. You can restrict remote management access to a single IP address for the following types of access:

- Web – controls access to the Web management interface
- Telnet – controls in-band CLI access
- SNMP – controls SNMP access from SNMP applications such as HP TopTools for Switches & Hubs or HP OpenView

In addition, if you want to restrict all three types of access to the same IP address, you can do so using a single command, as shown below.

NOTE: As an alternative to using this method, you can configure Access Control Lists (ACLs) to secure CLI, Telnet, and SNMP access to the device. See “Restricting Remote Access to the Device Using Access Control Lists” on page 3-2.

USING THE CLI TO RESTRICT REMOTE ACCESS TO A SPECIFIC IP ADDRESS

The following examples show the CLI commands for restricting remote access. You can specify only one IP address with each command. However, you can enter each command ten times to specify up to ten IP addresses.

To restrict Web access to the host with IP address 209.157.22.26, enter the following command:

```
HP9300(config)# web-client 209.157.22.26
```

Syntax: [no] web-client <ip-addr>

To restrict Telnet access to the host with IP address 209.157.22.39, enter the following command:

```
HP9300(config)# telnet-client 209.157.22.39
```

Syntax: [no] telnet-client <ip-addr>

To restrict SNMP access to the host with IP address 209.157.22.14, enter the following command:

```
HP9300(config)# snmp-client 209.157.22.14
```

Syntax: [no] snmp-client <ip-addr>

To restrict Telnet, Web, and SNMP management access to the host with IP address 209.157.22.69, you can enter three separate commands (one for each access type, as shown above) or you can enter the following command:

```
HP9300(config)# all-client 209.157.22.69
```

Syntax: [no] all-client <ip-addr>

USING THE WEB MANAGEMENT INTERFACE

You cannot restrict remote management access to specific IP addresses using the Web management interface.

Configuring the SNMP Community Strings

The default passwords for Web management access are actually the SNMP community strings configured on the device.

- The default read-only community string is “public”. To open a read-only Web management session, enter “get” and “public” for the user name and password.
- There is no default read-write community string. Thus, by default, you cannot open a read-write management session using the Web management interface. You first must configure a read-write community string using the CLI. Then you can log on using “set” as the user name and the read-write community string you configure as the password.

You can configure as many additional read-only and read-write community strings as you need. The number of strings you can configure depends on the memory on the device. There is no practical limit.

The Web management interface supports only one read-write session at a time. When a read-write session is open on the Web management interface, opening another session allows only read-only access, even if the subsequent session login is “set” with a valid read-write password.

NOTE: If you delete the startup-config file, the device automatically re-adds the default “public” read-only community string the next time you load the software.

To change the SNMP community strings, use the following method.

NOTE: As an alternative to the SNMP community strings, you can configure local user accounts or ACLS for Web management access to the device. See “Configuring Local User Accounts” on page 3-13 or “Restricting Remote Access to the Device Using Access Control Lists” on page 3-2.

Encryption

The software automatically encrypts SNMP community strings. Users with read-only access or who do not have Enable access cannot display the strings. For users with read-write or Enable access, the strings are encrypted in the CLI but are shown in the clear in the Web management interface.

Encryption is enabled by default. You can disable encryption for individual strings or trap receivers if desired.

Adding an SNMP Community String

To add a community string, use either of the following methods. When you add a community string, you can specify whether the string is encrypted or clear. By default, the string is encrypted.

USING THE CLI

To add an encrypted community string, enter commands such as the following:

```
HP9300(config)# snmp-server community private rw
HP9300(config)# write mem
```

Syntax: snmp-server community [0 | 1] <string> ro | rw

The **0 | 1** parameter specifies whether you want the software to encrypt the string (**1**) or show the string in the clear (**0**). The default is **1**.

The <string> parameter specifies the community string name. The string can be up to 32 characters long.

The **ro | rw** parameter specifies whether the string is read-only (**ro**) or read-write (**rw**).

The command in the example above adds the read-write SNMP community string “private”. When you save the new community string to the startup-config file (using the **write mem** command), the software adds the following command to the file:

snmp-server community 1 *<encrypted-string>* **rw**

To add an non-encrypted community string, you must explicitly specify that you do not want the software to encrypt the string. Here is an example:

```
HP9300(config)# snmp-server community 0 private rw
HP9300(config)# write mem
```

The command in this example adds the string “private” in the clear, which means the string is displayed in the clear. When you save the new community string to the startup-config file, the software adds the following command to the file:

snmp-server community 0 private rw

Displaying the SNMP Community Strings

USING THE CLI

To display the configured community strings, enter the following command at any CLI level:

```
HP9300(config)# show snmp server
```

Syntax: show snmp server

See the *Command Line Interface Reference* for an example of the information displayed by the command.

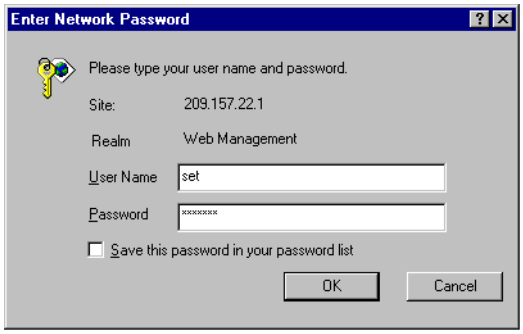
NOTE: If display of the strings is encrypted, the strings are not displayed. Encryption is enabled by default.

USING THE WEB MANAGEMENT INTERFACE

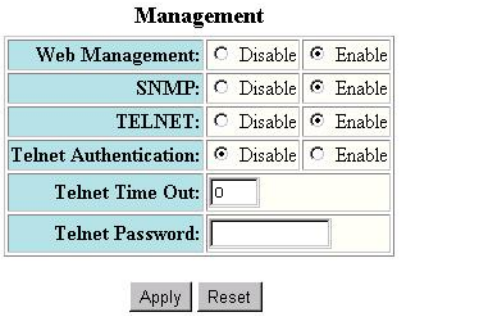
NOTE: To make configuration changes, including changes involving SNMP community strings, you must first configure a read-write community string using the CLI. Alternatively, you must configure another authentication method and log on to the CLI using a valid password for that method.

1. Log on to the device using a valid user name and password for read-write access. The System configuration panel is displayed.

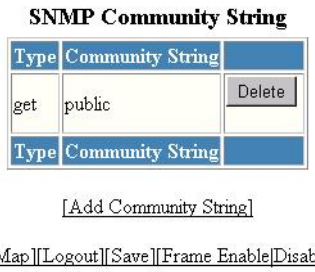
NOTE: If you have configured the device to secure Web management access using local user accounts, you must instead enter the user name and password of one of the user accounts. See “Configuring Local User Accounts” on page 3-13.



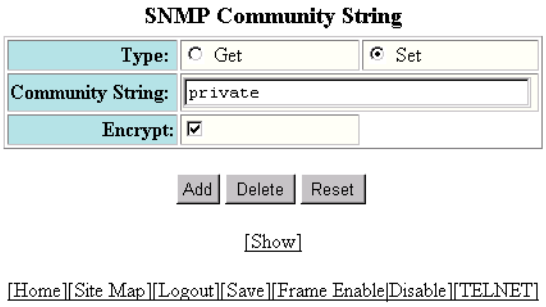
2. Select the Management link from the System configuration panel to display the following panel.



3. Select the Community String link to display the SNMP Community String panel, as shown in the following example. This example shows the table listed for a system that is configured only with the default read-only community string “public”.



4. Select the Add Community String link to display a panel such as the following.



5. Select the community string type:
   - Select Get for a read-only string.
   - Select Set for a read-write string.
6. Enter the community string in the Community String field.
7. Select the Encrypt checkbox to remove the checkmark if you want to disable encryption of the string display. Encryption prevents other users from seeing the string in the CLI or Web management interface. If you disable encryption, other users can view the community string. Encryption is enabled by default.

   To re-enable encryption, select the checkbox to place a checkmark in the box.
8. Click the Add button to save the change to the device's running-config file.
9. Repeat steps 5 – 7 for each string you want to add. You can add as many strings as you need. The limit depends only on the available system memory.
10. Select the Save link at the bottom of the dialog. Select Yes when prompted to save the configuration change to the startup-config file on the device's flash memory.

Disabling Web Management

If you want to prevent access to the device through the Web management interface, you can disable the Web management interface.

NOTE: As soon as you make this change, the device stops responding to Web management sessions. If you make this change using your Web browser, your browser can contact the device, but the device will not reply once the change takes place.

USING THE CLI

To disable the Web management interface, enter the following command:

```
HP9300(config)# no web-management
```

To re-enable the Web management interface, enter the following command:

```
HP9300(config)# web-management
```

Syntax: [no] web-management

USING THE WEB MANAGEMENT INTERFACE

1. Log on to the device using a valid user name and password for read-write access. The System configuration panel is displayed.
2. Select the Management link from the System configuration panel to display the Management panel.
3. Click Disable next to Web Management.

4. Click the Apply button to save the change to the device's running-config file.
5. Select the Save link at the bottom of the dialog. Select Yes when prompted to save the configuration change to the startup-config file on the device's flash memory.

Disabling Password Authentication on the Web Management Interface

If you wish, you can disable the password authentication feature of the Web management interface. When you disable password authentication, users are not prompted to enter a password when they log into the Web management interface. Since any user would then be able to gain access to the device and change system settings, you should carefully consider the implications of turning off password authentication.

USING THE CLI

To disable password authentication for the Web management interface, enter the following commands:

```
HP9300(config)# aaa authentication web-server default none
HP9300(config)# web-management allow-no-password
```

USING THE WEB MANAGEMENT INTERFACE

You cannot disable password authentication for Web management access using the Web management interface.

Disabling Telnet or SNMP Access

The simplest way to ensure against unauthorized Telnet or SNMP access to the device is to disable Telnet or SNMP.

NOTE: If you disable Telnet access, you will not be able to access the CLI except through a serial connection to the management module.

Disabling Telnet Access

Telnet access is enabled by default. You can use Telnet to access the CLI on the device over the network. If you do not plan to use the CLI over the network and want to disable Telnet access to prevent others from establishing CLI sessions with the device, use one of the following methods.

NOTE: If you do not want to disable Telnet but you do want to secure Telnet access, you can configure ACLS, local user accounts, RADIUS parameters, and TACACS/TACACS+ authentication for the device. See the following sections:

"Restricting Remote Access to the Device Using Access Control Lists" on page 3-2

"Configuring Local User Accounts" on page 3-13

"Configuring for TACACS/TACACS+ Authentication" on page 3-15

"Configuring for RADIUS Authentication" on page 3-20

USING THE CLI

To disable Telnet operation, enter the following command:

```
HP9300(config)# no telnet-server
```

To re-enable Telnet operation, enter the following command:

```
HP9300(config)# telnet-server
```

Syntax: [no] telnet-server

USING THE WEB MANAGEMENT INTERFACE

1. Log on to the device using a valid user name and password for read-write access. The System configuration panel is displayed.
2. Select the Management link from the System configuration panel to display the Management panel.
3. Click Disable next to TELNET.
4. Click the Apply button to save the change to the device's running-config file.
5. Select the Save link at the bottom of the dialog. Select Yes when prompted to save the configuration change to the startup-config file on the device's flash memory.

Disabling SNMP Access

SNMP is enabled by default on all HP devices. SNMP is required if you want to manage an HP device using an SNMP network management application such as HP TopTools for Switches & Hubs or HP OpenView.

To disable SNMP, use one of the following methods.

USING THE CLI

To disable SNMP management of a device:

```
HP9300(config)# snmp disable
```

To later re-enable SNMP management of the device:

```
HP9300(config)# no snmp disable
```

Syntax: [no] snmp disable

USING THE WEB MANAGEMENT INTERFACE

1. Log on to the device using a valid user name and password for read-write access. The System configuration panel is displayed.
2. Select the Management link from the System configuration panel to display the Management panel.
3. Click Disable next to SNMP.
4. Click the Apply button to save the change to the device's running-config file.
5. Select the Save link at the bottom of the dialog. Select Yes when prompted to save the configuration change to the startup-config file on the device's flash memory.

Setting a Telnet Password

By default, the device does not require a user name or password when you log in to the CLI using Telnet. You can assign a password for Telnet access using one of the following methods.

USING THE CLI

To set the password "letmein" for Telnet access to the CLI, enter the following command at the global CONFIG level:

```
HP9300(config)# enable telnet password letmein
```

Syntax: [no] enable telnet password <string>

USING THE WEB MANAGEMENT INTERFACE

1. Log on to the device using a valid user name and password for read-write access. The System configuration panel is displayed.
2. Select the Management link from the System configuration panel to display the Management panel.
3. Enter the password in the Telnet Password field.
4. Click the Apply button to save the change to the device's running-config file.

5. Select the Save link at the bottom of the dialog. Select Yes when prompted to save the configuration change to the startup-config file on the device's flash memory.

Setting the Enable Passwords

You can set one password for each of the following levels of Enable access:

- Super User – Allows complete read-and-write access to the system. This is generally for system administrators and is the only password level that allows you to configure passwords.
- Port Configuration – Allows read-and-write access for specific ports but not for global (system-wide) parameters.
- Read Only – Allows access to the Privileged EXEC mode and CONFIG mode but only with read access.

You can assign a password to each level of Enable access to the CLI. You also can configure up to 16 user accounts consisting of a user name and password, and assign each user account to one of the three access levels. See "Configuring Local User Accounts" on page 3-13.

NOTE: You must use the CLI to assign an Enable password. You cannot assign a password using the Web management interface.

If you configure user accounts in addition to Enable passwords, the device will validate a user's access attempt using one or both methods (local user account or Enable password), depending on the order you specify in the authentication-method lists. See "Configuring Authentication-Method Lists" on page 3-24.

USING THE CLI

To set passwords:

1. At the opening CLI prompt, enter the following command to change to the Privileged level of the EXEC mode:

   ```
   HP9300> enable
   HP9300#
   ```

2. Access the CONFIG level of the CLI by entering the following command:

   ```
   HP9300# configure terminal
   HP9300(config)#
   ```

3. Enter the following command to set the super-user password:

   ```
   HP9300(config)# enable super-user-password <text>
   ```

   NOTE: You must set the super-user password before you can set other types of passwords.

4. Enter the following commands to set the port configuration and read-only passwords:

   ```
   HP9300(config)# enable port-config-password <string>
   HP9300(config)# enable read-only-password <string>
   ```

NOTE: If you forget your super-user password, see "How to Recover From a Lost Password" on page 2-13.

USING THE WEB MANAGEMENT INTERFACE

You cannot set the Enable passwords using the Web Management interface.

Augmenting CLI Command Privilege Levels

Each CLI privilege level provides access to specific areas of the CLI by default:

- Full access provides access to all commands and displays.
- Port-configuration access gives access to:
  - The User EXEC and Privileged EXEC levels, and the port-specific parts of the CONFIG level
  - All interface configuration levels
- Read-only access gives access to:
  - The User EXEC and Privileged EXEC levels

You can grant additional access to a privilege level in the CLI, on an individual command basis. To grant the additional access, you specify the privilege level you are enhancing, the CLI level that contains the command, and the individual command.

To augment a CLI privilege level, use one of the following methods.

NOTE: This feature applies only to the CLI. You cannot augment privilege levels for the Web management interface.

USING THE CLI

To enhance the port-configuration privilege level so users also can enter IP commands at the global CONFIG level, enter the following command:

```
HP9300(config)# privilege configure level 4 ip
```

In this command, configure specifies that the enhanced access is for a command at the global CONFIG level of the CLI. The **level 4** parameter indicates that the enhanced access is for privilege level 4 (port-configuration). All users with port-configuration privileges will have the enhanced access. The **ip** parameter indicates that the enhanced access is for the IP commands. Users who log in with valid port-configuration level user names and passwords can enter commands that begin with “ip” at the global CONFIG level.

Syntax: [no] privilege <cli-level> level <privilege-level> <command-string>

The <cli-level> parameter specifies the CLI level and can be one of the following values:

- **exec** – EXEC level; for example, `HP9300> or HP9300#`
- **configure** – CONFIG level; for example, `HP9300(config)#`
- **interface** – Interface level; for example, `HP9300(config-if-6)#`
- **virtual-interface** – Virtual-interface level; for example, `HP9300(config-vif-6)#`
- **rip-router** – RIP router level; for example, `HP9300(config-rip-router)#`
- **ospf-router** – OSPF router level; for example, `HP9300(config-ospf-router)#`
- **dvmrp-router** – DVMRP router level; for example, `HP9300(config-dvmrp-router)#`
- **pim-router** – PIM router level; for example, `HP9300(config-pim-router)#`
- **bgp-router** – BGP4 router level; for example, `HP9300(config-bgp-router)#`
- **port-vlan** – Port-based VLAN level; for example, `HP9300(config-vlan)#`
- **protocol-vlan** – Protocol-based VLAN level

The <privilege-level> indicates the privilege level you are augmenting.

The **level** parameter specifies the privilege-level. You can specify one of the following:

- **0** – Full read-write access (super-user)
- **4** – Port-configuration access
- **5** – Read-only access

The <command-string> parameter specifies the command you are allowing users with the specified privilege level to enter. To display a list of the commands at a CLI level, enter "?" at that level's command prompt.

USING THE WEB MANAGEMENT INTERFACE

You cannot augment access privilege levels using the Web management interface.

Configuring Local User Accounts

You can define up to 16 local user accounts to control the following types of access to the HP 9304M, HP 9308M, HP 6208M-SX, and HP 6308M-SX:

- Telnet access through the CLI
- Enable access through the EXEC level and CONFIG levels of the CLI
- Web-browser access through the Web management interface

The user accounts provide greater flexibility for controlling management access to devices than the Enable passwords and SNMP community strings. You can continue to use the Enable passwords and the SNMP community strings as a secondary means of access authentication. Alternatively, you can choose not to use user accounts and instead continue to use only the Enable passwords and community strings. The local access feature is backward compatible with configuration files that contain Enable passwords. See "Setting the Enable Passwords" on page 3-11.

If you configure user accounts, you also need to configure an authentication-method list for each type of access listed above. See "Configuring Authentication-Method Lists" on page 3-24.

For each user account, you specify the user name. You also can specify the following parameters:

- A password
- The privilege level, which can be one of the following:
  - Full read-write access (super-user). This is the default.
  - Port-configuration access
  - Read-only access

Configuring a User Account

To configure a user account, use one of the following methods.

USING THE CLI

To configure a user account, enter a command such as the following at the global CONFIG level of the CLI.

```
HP9300(config)# username wonka password willy
```

This command adds a user account for a super-user with the user name "wonka" and the password "willy", with privilege level super-user. This user has full access to all configuration and display features.

NOTE: If you configure user accounts, you must add a user account for super-user access before you can add accounts for other access levels. You will need the super-user account to make further administrative changes.

```
HP9300(config)# username waldo privilege 5 password whereis
```

This command adds a user account for user name “waldo”, password “whereis”, with privilege level read-only. Waldo can look for information but cannot make configuration changes.

Syntax: [no] username <user-string> privilege <privilege-level> password | nopassword <password-string>

The privilege parameter specifies the privilege-level. You can specify one of the following:

- **0** – Full access (super-user)
- **4** – Port-configuration access
- **5** – Read-only access

The default privilege level is **0**. If you want to assign full access to the user account, you can enter the command without “**privilege 0**", as shown in the command example above.

The **password | nopassword** parameter indicates whether the user must enter a password. If you specify **password**, enter the string for the user's password.

NOTE: You must be logged on with super-user access (privilege level 0, or with a valid Enable password for super-user access) to add user accounts or configure other access parameters.

To display user account information, enter the following command:

```
HP9300(config)# show users
```

Syntax: show users

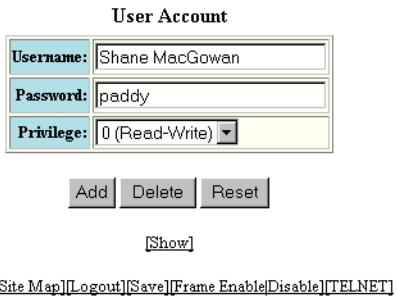
USING THE WEB MANAGEMENT INTERFACE

To configure a user account using the Web management interface, use the following procedure.

NOTE: Before you can add a user account using the Web management interface, you must enable this capability by entering the **password any** command at the global CONFIG level of the CLI.

---

1. Log on to the device using a valid user name and password for read-write access. The System configuration dialog is displayed.
2. Select the Management link from the System configuration panel to display the Management panel.
3. Select the User Account link.
   - If any user accounts are already configured on the device, the account information is listed in a table. Select the Add User Account link to display the following panel. Notice that the password display is encrypted. If you want the passwords to be displayed in clear text, you can use the CLI to disable encryption of password displays. See “Password Encryption” on page 3-15.
   - If the device does not have any user accounts configured, the following panel is displayed.



4. Enter the user name in the User Name field. The name cannot contain blanks.
5. Enter the password in the Password field. The password cannot contain blanks.

6. Select the access privilege level from the Privilege pulldown menu. You can select one of the following:
   - 0 (Read-Write) – equivalent to super-user access. The user can display and configure everything.
   - 4 (Port-Config) – allows the user to configure port parameters but not global parameters.
   - 5 (Read-Only) – allows the user to display information but not to make configuration changes.
7. Click the Add button to save the change to the device's running-config file.
8. Repeat steps 4 – 7 for each user account. You can add up to 16 accounts.
9. Select the Save link at the bottom of the dialog. Select Yes when prompted to save the configuration change to the startup-config file on the device's flash memory.

Password Encryption

When you configure a password, then save the configuration to the HP device's flash memory, the password is also saved to flash as part of the configuration file. By default, the passwords are encrypted so that the passwords cannot be observed by another user who displays the configuration file. Even if someone observes the file while it is being transmitted over TFTP, the password is encrypted.

To disable password encryption, use the following CLI method.

NOTE: You cannot disable password encryption using the Web management interface.

USING THE CLI

If you want to remove the password encryption, you can disable encryption by entering the following command:

```
HP9300(config)# no service password-encryption
```

Syntax: [no] service password-encryption

USING THE WEB MANAGEMENT INTERFACE

You cannot disable password encryption using the Web management interface.

Configuring for TACACS/TACACS+ Authentication

You can use the security protocol Terminal Access Controller Access Control System (TACACS) or TACACS+ to authenticate CLI access to the HP 9304M, HP 9308M, HP 6208M-SX, and HP 6308M-SX.

The TACACS/TACACS+ protocol defines how authentication, authorization, and accounting information is sent between the switch or routing switch and an authentication database on a TACACS/TACACS+ server. TACACS/TACACS+ services are maintained in a database, typically on a UNIX workstation or PC with a TACACS/TACACS+ server running.

When you configure an HP device to use a TACACS/TACACS+ server for authentication, the device prompts users who are trying to access the CLI for a user name and password, then verifies the password with the TACACS/TACACS+ server.

NOTE: TACACS/TACACS+ authentication is supported only for CLI access. You cannot authenticate Web management or SNMP access to an HP device using TACACS/TACACS+. When you configure authentication-method lists for TACACS/TACACS+ authentication, you must specify a separate list for Telnet CLI access and for "enable" CLI access to the Privileged EXEC level and CONFIG levels of the CLI.

How TACACS+ Differs from TACACS

TACACS is a simple UDP based access control protocol originally developed by BBN for MILNET. TACACS+ is an enhancement to TACACS and uses TCP to ensure reliable delivery.

TACACS+ is an enhancement to the TACACS security protocol. TACACS+ improves on TACACS by separating the functions of authentication, authorization, and accounting (AAA) and by encrypting all traffic between the HP device and the TACACS+ server. TACACS+ allows for arbitrary length and content authentication exchanges,

which allow any authentication mechanism to be utilized with the HP device. TACACS+ is extensible to provide for site customization and future development features, and it uses a TCP based access control protocol to ensure reliable delivery. The protocol allows the HP device to request very precise access control and allows the TACACS+ server to respond to each component of that request.

NOTE: TACACS+ provides for authentication, authorization, and accounting, but an implementation or configuration is not required to employ all three. Each one serves a unique purpose that alone is useful, and together can be quite powerful.

Configuration Considerations

- You must deploy at least one TACACS/TACACS+ server in your network.
- The switch and the routing switches support authentication using only a single TACACS/TACACS+ server.
- TACACS+ accounting is not supported.
- You can select only one primary authentication method for each type of access to a device (CLI through Telnet, CLI Privileged EXEC and CONFIG levels, Web, and SNMP). For example, you can select TACACS+ as the primary authentication method for Telnet CLI access, but you cannot also select RADIUS authentication as a primary method for the same type of access. However, you can configure up to six secondary authentication methods for each access type.
- Up to three concurrent TACACS/TACACS+ client authentications are supported.

Configuring the Switch or Routing Switch for TACACS/TACACS+ Authentication

If you want to authenticate access using local user accounts, a TACACS/TACACS+ server, or a RADIUS server, you must configure an authentication method list for each type of access to which these methods apply. For example, to use TACACS+ to secure Telnet access to the CLI, you must configure an authentication-method list specifically for Telnet access.

Within an authentication-method list, you can specify the primary authentication method and up to six secondary authentication methods. The device tries the secondary authentication methods in the order you specify as backups in case the primary method fails due to an authentication error.

For TACACS/TACACS+ authentication, you also must identify the TACACS/TACACS+ server.

The following sections show how to identify the TACACS/TACACS+ server and to configure authentication method lists to use TACACS or TACACS+ as the primary authentication method.

Identifying the TACACS/TACACS+ Server

To use a TACACS/TACACS+ server to authenticate access to an HP device, you must identify the server to the HP device.

USING THE CLI

To identify a TACACS server that has the IP address 209.94.6.191 and identify the server's UDP port number it uses for TACACS authentication traffic as port 1800, enter the following command:

```
HP9300(config)# tacacs-server host 207.94.6.191 auth-port 1800
HP9300(config)# write mem
```

Syntax: tacacs-server <ip-addr> | <hostname> [auth-port <number>]

The only required parameter is the IP address or host name of the server.

NOTE: To specify the server's host name instead of its IP address, you must first identify a DNS server using the **ip dns server-address** <ip-addr> command at the global CONFIG level. See “Enabling Domain Name Server (DNS) Resolver” on page 8-7.

The **auth-port** parameter specifies the UDP (for TACACS) or TCP (for TACACS+) port number of the authentication port on the server. The default port number is 49.

Optionally, you also can change the server key, timeout, retransmit, and dead-time values, as shown in the following command examples.

```
HP9300(config)# tacacs-server key rkwong
HP9300(config)# tacacs-server timeout 5
HP9300(config)# tacacs-server retransmit 5
HP9300(config)# tacacs-server dead-time 5
HP9300(config)# write mem
```

NOTE: If you erase the **tacacs-server** command, make sure you also erase the **aaa** command. Otherwise, when you exit from the CONFIG mode or from a TELNET session, the system continues to believe it is TACACS/TACACS+ enabled and you will not be able to access the system.

Syntax: tacacs-server [key <key-string>] [timeout <number>] [retransmit <number>] [dead-time <number>]

The **key** parameter specifies the value that the HP device sends to the server when trying to authenticate user access. The TACACS+ server uses the key to determine whether the HP device has authority to request authentication from the server. The key can be from 1 – 16 characters in length.

NOTE: The **key** parameter applies only to TACACS+ servers, not to TACACS servers. If you are configuring for TACACS authentication, do not configure a key on the TACACS server and do not enter a key on the HP device.

The **timeout** parameter specifies how many seconds the switch or routing switch waits for a response from the TACACS/TACACS+ server before either retrying the authentication request, or determining that the TACACS/TACACS+ server is unavailable and moving on to the next authentication method in the authentication-method list. The timeout can be from 1 – 15 seconds. The default is 3 seconds.

The **retransmit** parameter specifies how many times the HP device will resend an authentication request when the TACACS/TACACS+ server does not respond. The retransmit value can be from 1 – 5 times. The default is 3 times.

The **dead-time** parameter is not used in this software release. When the software allows multiple authentication servers, this parameter will specify how long the HP device waits for the primary authentication server to reply before deciding the server is dead and trying to authenticate using the next server. The dead-time value can be from 1 – 5 seconds. The default is 3.

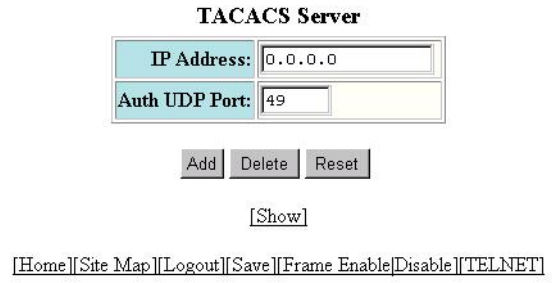
USING THE WEB MANAGEMENT INTERFACE

1. Log on to the device using a valid user name and password for read-write access. The System configuration panel is displayed.
2. Select the TACACS link from the System configuration panel to display the TACACS panel.
3. If needed, change the Authentication port and Accounting port. (The default values work in most networks.)
4. Enter the key if applicable.

   NOTE: The **key** parameter applies only to TACACS+ servers, not to TACACS servers. If you are configuring for TACACS authentication, do not configure a key on the TACACS server and do not enter a key on the HP device.

5. Click Apply if you changed any TACACS/TACACS+ parameters.

6. Select the TACACS Server link.
   - If any TACACS/TACACS+ servers are already configured on the device, the servers are listed in a table. Select the Add TACACS Server link to display the following panel.
   - If the device does not have any TACACS servers configured, the following panel is displayed.



7. Enter the server's IP address in the IP Address field.
8. If needed, change the Authentication port. (The default values work in most networks.)
9. Click the Add button to save the change to the device's running-config file.
10. Select the Save link at the bottom of the dialog. Select Yes when prompted to save the configuration change to the startup-config file on the device's flash memory.
11. Go to the next section. You must configure an authentication method list for each type of access you want to use (Telnet, Enable, Web, SNMP). See the beginning of "Configuring the Authentication-Method Lists" on page 3-18 for descriptions of the access levels.

Configuring the Authentication-Method Lists

To configure authentication-method lists for TACACS/TACACS+ access to the CLI, use one of the following methods.

NOTE: For examples of how to define authentication-method lists for types of authentication other than TACACS/TACACS+, see "Configuring Authentication-Method Lists" on page 3-24.

USING THE CLI

To configure the authentication-method lists for "enable" and Telnet CLI access to both use TACACS/TACACS+ as the primary authentication method, enter the following commands. Notice that one of these commands uses the **tacacs** keyword and the other uses the **tacacs+** keyword. You can use either keyword. Each keyword specifies both TACACS and TACACS+.

```
HP9300(config)# aaa authentication enable default tacacs enable
HP9300(config)# aaa authentication login default tacacs+ line
HP9300(config)# write mem
```

Syntax: aaa authentication snmp-server | web-server | enable | login default <method1> [<method2>] [<method3>] [<method4>] [<method5>] [<method6>] [<method7>]

The **snmp-server | web-server | enable | login** parameter specifies the type of access this authentication-method list controls. You can configure one authentication-method list for each type of access.

NOTE: TACACS/TACACS+ and RADIUS are supported only for **enable** and **login**.

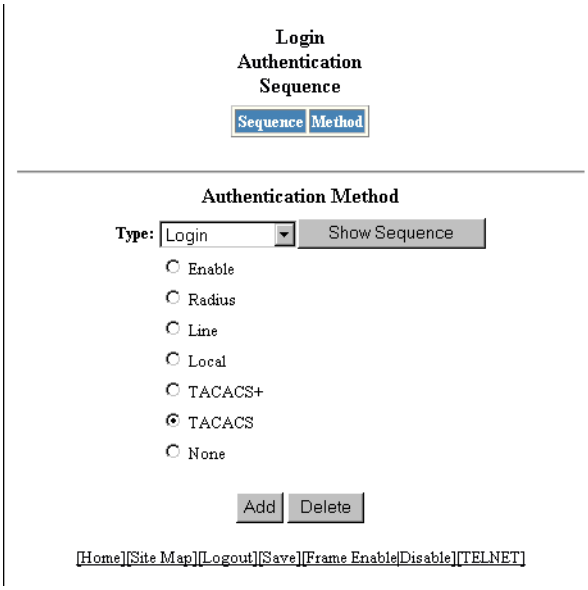
The **default** parameter is required and indicates that this is the default authentication-method list for this type of access.

The <method1> parameter specifies the primary authentication method. The remaining optional <method> parameters specify the secondary methods to try if an error occurs with the primary method. See “Configuring Authentication-Method Lists” on page 3-24.

USING THE WEB MANAGEMENT INTERFACE

To configure the device to use a TACACS/TACACS+ server to authenticate attempts to log in through the CLI:

1. Log on to the device using a valid user name and password for read-write access. The System configuration panel is displayed.
2. Select the Management link to display the Management panel.
3. Select the Authentication Methods link to display the Login Authentication Sequence panel, as shown in the following example.



4. Select the type of access for which you are defining the authentication method list from the Type field’s pulldown menu. Each type of access must have a separate authentication-method list. For example, to define the authentication-method list for logging in to the CLI, select Login.
5. Select the primary authentication method by clicking on the radio button next to the method. For example to use a TACACS+ server as the primary means of authentication for logging on to the CLI, select TACACS+.
6. Click the Add button to save the change to the device’s running-config file. The access type and authentication method you selected are displayed in the table at the top of the dialog. Each time you add an authentication method for a given access type, the software assigns a sequence number to the entry. When the user tries to log in using the access type you selected, the software tries the authentication sources in ascending sequence order until the access request is either approved or denied. Each time you add an entry for a given access type, the software increments the sequence number. Thus, if you want to use multiple authentication methods, make sure you enter the primary authentication method first, the secondary authentication method second, and so on.

   If you need to delete an entry, select the access type and authentication method for the entry, then click Delete.
7. Select the Save link at the bottom of the dialog. Select Yes when prompted to save the configuration change to the startup-config file on the device’s flash memory.

Configuring for RADIUS Authentication

The security methods described in the previous sections secure access on a system-by-system basis. You must configure and administer security individually for each HP switch and routing switch (HP 9304M, HP 9308M, HP 6208M-SX, and HP 6308M-SX). However, if your network contains a RADIUS server, you can configure all the HP switches and routing switches to use the RADIUS server to authenticate access.

You can use your RADIUS server to secure the following types of access to the HP device:

- Login access through Telnet to the CLI using a super-user password.
- Enable access to the CLI's privileged and CONFIG modes using a super-user password.

NOTE: HP devices do not support RADIUS authentication for read-only and port-configuration passwords or for Web management access.

Implementation Notes

- A RADIUS server is required.
- Each switch or routing switch can use only one RADIUS server.
- Up to three concurrent RADIUS client authentications are supported.
- RADIUS Accounting is not supported.
- Only default method lists are supported.

Basic Configuration Steps

To configure RADIUS authentication, perform the following steps:

1. Access the CONFIG mode using your super-user password, or access the Web management interface with read-write access.
2. Enter the RADIUS server's IP address.
3. Optionally, change the UDP port on the RADIUS server used for authentication traffic. (The default port is 1645.)
4. Enable authentication for Telnet access.
5. Configure an authentication method list for Telnet access.
6. Configure an authentication method list for Enable access.
7. Save the RADIUS configuration information to the startup-config file on the flash memory.

USING THE CLI

Here is an example of how to configure RADIUS authentication.

```
HP9300> enable
```

<<enter super-user password if defined>>

```
HP9300# configure terminal
HP9300(config)#   radius-server host 209.157.22.99
HP9300(config)#   radius-server key abcd1234
HP9300(config)#   enable telnet authentication
HP9300(config)#   aaa authentication login default radius line
HP9300(config)#   aaa authentication enable default radius enable
HP9300(config)#   write memory
```

NOTE: If you erase the **radius-server** command, make sure you also erase the **aaa** command. Otherwise, when you exit from the CONFIG mode or from a TELNET session, the system continues to believe it is RADIUS-enabled and you will not be able to access the system.

Syntax: radius-server host <ip-addr> | <server-name> [auth-port <number>] [acct-port <number>]

The **host** <ip-addr> **|** <server-name> parameter is either an IP address or an ASCII text string.

The <auth-port> parameter is the Authentication port number; it is an optional parameter. The default is 1645.

The <acct-port> parameter is the Accounting port number; it is an optional parameter. The default is 1646.

Syntax: radius-server [key <key-string>] [timeout <number>] [retransmit <number>] [dead-time <number>]

The key <key-string> parameter is the encryption key; valid key string length is from 1 – 16.

The **timeout** <number> is how many seconds to wait before declaring a RADIUS server timeout for the authentication request. The default timeout is 3 seconds. The range of possible timeout values is from 1 – 15.

The **retransmit** <number> is the maximum number of retransmission attempts. When an authentication request times out, the HP software will retransmit the request up to the maximum number of retransmissions configured. The default retransmit value is 3 retries. The range of retransmit values is from 1 – 5.

The **dead-time** parameter is not used in this software release. When the software allows multiple authentication servers, this parameter will specify how long the HP device waits for the primary authentication server to reply before deciding the server is dead and trying to authenticate using the next server. The dead-time value can be from 1 – 5 seconds. The default is 3.

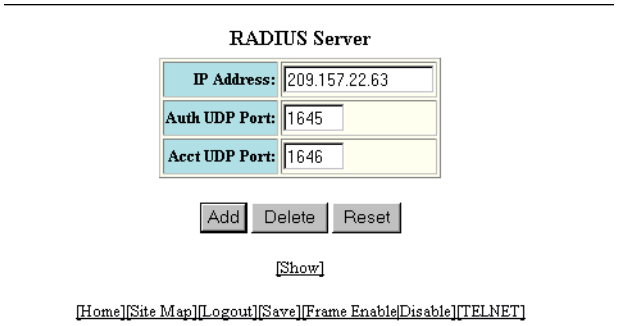
Syntax: aaa authentication login | enable default <method1> [<method2>] [<method3>] [<method4>] [<method5>] [<method6>] [<method7>]

After configuring the RADIUS parameters, you need to configure authentication-method lists. See “Configuring Authentication-Method Lists” on page 3-24.

USING THE WEB MANAGEMENT INTERFACE

1. Log on to the device using a valid user name and password for read-write access. The System configuration panel is displayed.
2. Select the RADIUS link from the System configuration panel to display the RADIUS panel.
3. Change the retransmit interval, time out, and dead time if needed.
4. Enter the authentication key if applicable.
5. Click Apply if you changed any RADIUS parameters.

6. Select the RADIUS Server link.
   - If any RADIUS servers are already configured on the device, the servers are listed in a table. Select the Add RADIUS Server link to display the following panel.
   - If the device does not have any RADIUS servers configured, the following panel is displayed.

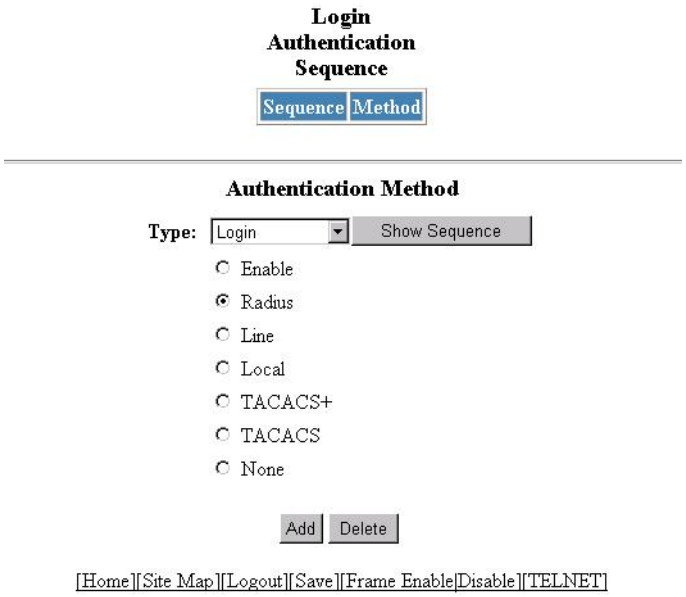


7. Enter the server's IP address in the IP Address field.
8. If needed, change the Authentication port and Accounting port. (The default values work in most networks.)
9. Click Home to return to the System configuration panel, then select the Save link at the bottom of the dialog. Select Yes when prompted to save the configuration change to the startup-config file on the device's flash memory.
10. Go to "Configuring the Authentication-Method Lists" on page 3-23. You must configure an authentication method list for each type of access you want to use (Telnet, Enable, Web, SNMP). See the beginning of "Configuring Local User Accounts" on page 3-13 for descriptions of the access levels.

Configuring the Authentication-Method Lists

To configure the device to use a RADIUS server to authenticate attempts to log in through the CLI:

1. Log on to the device using a valid user name and password for read-write access. The System configuration dialog is displayed.
2. Select the Management link to display the Management panel.
3. Select the Authentication Methods link to display the Login Authentication Sequence panel, as shown in the following example.



4. Select the type of access for which you are defining the authentication method list from the Type field's pulldown menu. Each type of access must have a separate authentication-method list. For example, to define the authentication-method list for logging in to the CLI, select Login.
5. Select the primary authentication method by clicking on the radio button next to the method. For example to use a RADIUS server as the primary means of authentication for logging on to the CLI, select RADIUS.
6. Click the Add button to save the change to the device's running-config file. The access type and authentication method you selected are displayed in the table at the top of the dialog. Each time you add an authentication method for a given access type, the software assigns a sequence number to the entry. When the user tries to log in using the access type you selected, the software tries the authentication sources in ascending sequence order until the access request is either approved or denied. Each time you add an entry for a given access type, the software increments the sequence number. Thus, if you want to use multiple authentication methods, make sure you enter the primary authentication method first, the secondary authentication method second, and so on.

   If you need to delete an entry, select the access type and authentication method for the entry, then click Delete.
7. Select the Save link at the bottom of the dialog. Select Yes when prompted to save the configuration change to the startup-config file on the device's flash memory.

Configuring Authentication-Method Lists

For each access level (Telnet, Enable, Web server, and SNMP server), you can configure an authentication-method list to specify the order in which the device consults authentication sources for access levels. To configure an authentication-method list, you specify the access level and the order in which the authentication methods are used. For each authentication-method list, you specify the order in which the device tries one or more of the following authentication methods:

- TACACS or TACACS+ server – Authenticate based on the database on a TACACS or TACACS+ server.
- RADIUS server – Authenticate based on the database on the RADIUS server.
- Line – Authenticate locally based on the Telnet login password.
- Enable – Authenticate locally based on the Enable password.
- Local – Authenticate locally based on the user accounts configured on the device.
- None – Do not perform authentication.

NOTE: The TACACS/TACACS+, RADIUS, and line authentication methods are not supported for Web access or SNMP access.

NOTE: You do not need an authentication-method list to secure access based on ACLs or a list of IP addresses. See “Restricting Remote Access to the Device Using Access Control Lists” on page 3-2 and “Restricting Remote Access to the Device to Specific IP Addresses” on page 3-4.

CLI Access

For CLI access, you must configure access-method lists if you want the device to authenticate access using user accounts or a RADIUS server. Otherwise, the device will authenticate using only the Enable passwords.

Web Management Access

The Web server access level controls access to the device through the Web management interface. By default (when no authentication-method list is configured for Web management access), the device authenticates access through the Web management interface using the SNMP access levels and associated community strings.

- For read-only access, you can use the user name “get” and the password “public”. The default read-only community string is “public”.
- There is no default read-write community string. Thus, by default, you cannot open a read-write management session using the Web management interface. You first must configure a read-write community string using the CLI. Then you can log on using “set” as the user name and the read-write community string you configure as the password. See “Configuring the SNMP Community Strings” on page 3-5.

If you configure an access-method list for Web server access and specify “local” as the first authentication method, users who attempt to access the device using the Web management interface must supply a user name and password configured in one of the user accounts on the device. The user cannot access the device by entering “set” or “get” and the corresponding SNMP community string.

Authentication Algorithm

When you configure an authentication-method list for an access level, you can specify up to seven authentication methods. If the first authentication method is successful, the software grants access and stops the authentication process. If the access is rejected by the first authentication method, the software denies access and stops checking.

However, if an error occurs with an authentication method, the software tries the next method on the list, and so on. For example, if the first authentication method is the RADIUS server but the link to the server is down, the software will try the next authentication method in the list.

NOTE: If an authentication method is working properly and the password (and user name, if applicable) is not known to that method, this is not an error. The authentication attempt stops, and the user is denied access.

The software will continue this process until either the authentication method is passed or the software reaches the end of the method list. If the super-user password is not rejected after all the access methods in the list have been tried, access is granted.

USING THE CLI

Example 1: The following example shows how to configure authentication-method lists for the CLI and Web management access. In this example, the primary authentication method for each is "local". The device will authenticate access attempts using the locally configured user names and passwords first.

To configure an access method list for the Web management interface, enter a command such as the following:

```
HP9300(config)# aaa authentication web-server default local
```

This command configures the device to use the local user accounts to authenticate access to the device through the Web management interface. If the device does not have a user account that matches the user name and password entered by the user, the user is not granted access.

To configure the CLI to use the local user accounts to authenticate access, enter the following commands:

```
HP9300(config)# aaa authentication login default local
HP9300(config)# aaa authentication enable default local
HP9300(config)# write mem
```

The first command configures access authentication for logging in to the CLI through Telnet. The second command configures access authentication for accessing the Privileged EXEC and CONFIG levels of the CLI.

Example 2: To configure the device to consult a RADIUS server first for CLI Enable access (access to the Privileged EXEC and CONFIG levels) then consult the local user accounts if the RADIUS server is unavailable, enter the following command:

```
HP9300(config)# aaa authentication enable default radius local
HP9300(config)# write mem
```

Syntax: [no] aaa authentication snmp-server | web-server | enable | login default <method1> [<method2>] [<method3>] [<method4>] [<method5>] [<method6>] [<method7>]

The **snmp-server | web-server | enable | login** parameter specifies the type of access this authentication-method list controls. You can configure one authentication-method list for each type of access.

NOTE: TACACS/TACACS+ and RADIUS are supported only for **enable** and **login**.

The <method1> parameter specifies the primary authentication method. The remaining optional <method> parameters specify the secondary methods to try if an error occurs with the primary method. A method can be one of the values listed in the Method Value column in Table 3.3.2.

Table 3.2: Authentication Method Values

Method Value	Description
tacacs or tacacs+	A TACACS/TACACS+ server. You can use either parameter. Each parameter supports both TACACS and TACACS+. You also must identify the server to the device using the **tacacs-server** command. See "Configuring for TACACS/TACACS+ Authentication" on page 3-15.
radius	A RADIUS server. You also must identify the server to the device using the **radius-server** command. See "Configuring for RADIUS Authentication" on page 3-20.

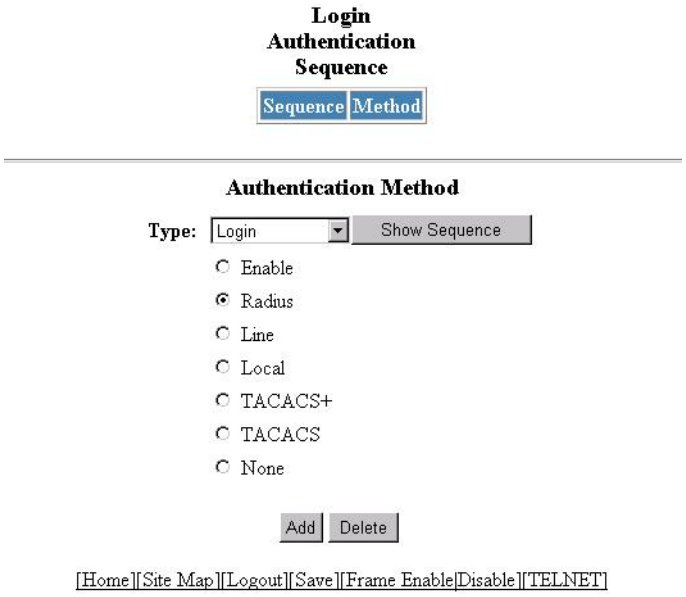
Table 3.2: Authentication Method Values (Continued)

Method Value	Description
local	A local user name and password you configured on the device. Local user names and passwords are configured using the **username…** command. See "Configuring a User Account" on page 3-13.
line	The password you configured for Telnet access. The Telnet password is configured using the **enable telnet password…** command. See "Setting a Telnet Password" on page 3-10.
enable	The super-user "enable" password you configured on the device. The enable password is configured using the **enable super-user-password…** command. See "Setting the Enable Passwords" on page 3-11.
none	No authentication is used. The device automatically permits access.

USING THE WEB MANAGEMENT INTERFACE

To configure the device to use a RADIUS server to authenticate attempts to log in through the CLI:

1. Log on to the device using a valid user name and password for read-write access. The System configuration panel is displayed.
2. Select the Management link to display the Management panel.
3. Select the Authentication Methods link to display the Login Authentication Sequence panel, as shown in the following example.



4. Select the type of access for which you are defining the authentication method list from the Type field's pulldown menu. Each type of access must have a separate authentication-method list. For example, to define the authentication-method list for logging into the CLI, select Login.
5. Select the primary authentication method by clicking on the radio button next to the method. For example to use a RADIUS server as the primary means of authentication for logging on to the CLI, select RADIUS.

6. Click the Add button to save the change to the device's running-config file. The access type and authentication method you selected are displayed in the table at the top of the dialog. Each time you add an authentication method for a given access type, the software assigns a sequence number to the entry. When the user tries to log in using the access type you selected, the software tries the authentication sources in ascending sequence order until the access request is either approved or denied. Each time you add an entry for a given access type, the software increments the sequence number. Thus, if you want to use multiple authentication methods, make sure you enter the primary authentication method first, the secondary authentication method second, and so on.

   If you need to delete an entry, select the access type and authentication method for the entry, then click Delete.

7. Select the Save link at the bottom of the dialog. Select Yes when prompted to save the configuration change to the startup-config file on the device's flash memory.