Chapter 2
Installation

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

Unpacking a System

Package Contents

For a list of included parts, please refer to the *Read Me First* document shipped with your HP device.

General Requirements

To manage a switch or routing switch, you need the following items for serial connection to the device:

- A management station, such as a PC running a terminal emulation application.
- A straight-through EIA/TIA DB-9 serial cable (M/F), which is provided with your HP switch or routing switch.

Use the serial connection to perform basic configuration tasks including assigning an IP address and network mask to the system. This information is required for managing the system using the Web management interface or using the CLI through Telnet.

WARNING: Do not use the handles on the power supply units to lift or carry the HP 9304M or 9308M routing switch.

Installation Procedures

Summary

Follow the steps listed below to install your routing switch. Details for each of the steps highlighted below are provided in the balance of this chapter.

1. **Preparing the installation site (page 2-4)**. Ensure that the physical environment that will host the routing switch has the proper cabling and ventilation.
2. **Chassis-based devices only – Installing (or Removing) Optional Modules (page 2-4**). There are several optional modules designed for any of the module slots on the HP 9304M and HP 9308M routing switches. Depending on where you will install the routing switch, it may be easier to install the modules first. However, the modules are “hot swappable”, and can be installed or removed after the routing switch is mounted and powered-on.

   NOTE: If you are installing a second Redundant Management module, see “Using Redundant Management Modules” on page 3-1 for complete installation, configuration, and management instructions for this module.

3. **Chassis-based devices only – (Optional) Installing (or Removing) Redundant Power Supplies (page 2-6)**. The HP 9304M can hold one or two power supplies. The HP 9308M can hold up to four power supplies. If you have a power supply to install, it may be easier to install it before mounting the routing switch, although the power supplies are “hot swappable”, and can be installed or removed after the routing switch is mounted and powered-on.

   CAUTION: Remove the power cord from a power supply before you install it in or remove it from the routing switch. Otherwise, damage to the power supply or the routing switch could result. (The routing switch can be running while a power supply is being installed or removed, *but the power supply itself should not be connected to a power source*.)

4. **Verifying Proper Operation (page 2-9)**. Verify that the system and module LEDs are registering the proper LED state after power-on of the system.
5. **Attaching a PC or Terminal (page 2-10)**. A terminal or PC serial port connection is all that is required to support configuration on the routing switch.
6. **Assign a Permanent Password (page 2-12)**. No default password is assigned to HP devices. For additional access security, assign a password.
7. **Assign Permanent IP Addresses (page 2-13)**. Before attaching equipment to the device, assign an interface IP address to the sub-net on which it will be located. Initial IP address assignment is done using the Command Line Interface (CLI) with either a direct serial connection or using Telnet with a direct terminal-to-device LAN connection. The subsequent IP address assignments used with routing switches can be done via Telnet or the Web management interface.
8. **Mounting the Device (page 2-15)**. HP switches and routing switches support both desktop and rack-mount installation.
9. **Connecting Power to the Device (page 2-17).** Once the device is physically installed, plug the device into a nearby power source in keeping with regulatory requirements outlined in this manual.
10. **Connecting Network Devices (page 2-18)**. Once the device is powered on and IP addresses are assigned, the device is ready to accept network equipment.
11. **Verifying Proper Connections (page 2-20)**. Test IP connectivity to other devices by pinging them and tracing routes.
12. **Managing the device (page 2-21)**. Continue configuring the device using the CLI or the Web management interface.

13. **Securing Access to the Device (page 2-23)**. Enhance device security by configuring user accounts, passwords, authentications (RADIUS, TACACS, or TACACS+), and SNMP communities.
14. **Chassis-based devices only – Swapping Modules (page 2-45)**. If you are removing a module and placing a module of another type in its slot, you need to reconfigure the chassis slot for the module.

Installation Precautions

Follow these precautions when installing an HP switch or routing switch:

WARNING: The HP 9304M chassis exceeds 40 lbs. (18 kg), or 47.7 lbs.(21.6 kg) when fully populated with modules and power supplies. Also, the HP 9308M chassis exceeds 55 lbs. (24.9 kg) or 69.1 lbs. (31.3 kg) when fully populated with modules and power supplies. TWO OR MORE PEOPLE ARE REQUIRED WHEN LIFTING, HANDLING, OR MOUNTING THESE ROUTING SWITCHES.

WARNING: Do not use the handles on the power supply units to lift or carry the routing switch.

WARNING: The rack or cabinet housing the switch or routing switch should be adequately secured to prevent it from becoming unstable and/or falling over.

WARNING: Devices installed in a rack or cabinet should be mounted as low as possible, with the heaviest device at the bottom and progressively lighter devices installed above.

CAUTION:

- Make sure that the power source circuits are properly grounded, then use the power cord supplied with the device to connect it to the power source.

  If the installation requires a different power cord than the one supplied with the device, be sure to use a power cord displaying the mark of the safety agency that defines the regulations for power cords in your country. The mark is your assurance that the power cord can be used safely with the device.
- Ensure that the device does not overload the power circuits, wiring, and over-current protection. To determine the possibility of overloading the supply circuits, add together the ampere ratings of all devices installed on the same circuit as the switch or routing switch. Compare this total with the rating limit for the circuit. The maximum ampere ratings are usually printed on the devices, near their AC power connectors.
- Do not install the device in an environment where the operating ambient temperature might exceed 40 degrees C (104 degrees F).
- Make sure the air flow around the front, sides, and back of the device is not restricted.
- To provide additional safety and proper airflow to the device, make sure that slot cover plates are installed on all chassis slots that do not have either a module or power supply installed.

1. Preparing the Installation Site

Cabling Infrastructure

Ensure that the proper cabling is installed in the site. See “Hardware Overview” on page 6-1 for a summary of supported cabling types and their specifications.

Installation Location

Before installing the device, plan its location and orientation relative to other devices and equipment. Allow at least three inches (3") of space at the front of the device for the twisted-pair, fiber-optic and power cabling. Also, a minimum of three inches (3") of space should be allowed between the sides and the back of the device and walls or other obstructions.

2. Installing (or Removing) Optional Modules (chassis only)

Installing Modules

To install a module in the chassis, do the following:

1. Put on an ESD wrist strap and attach the clip end to a metal surface (e.g. an equipment rack) to act as ground.

   WARNING: To avoid risk of shock, do not attach the clip end to the air flow panel of the power supply.

2. Remove the blank face plate from the slot in which the module is to be installed. Place the blank face plate in a safe place for future use.
3. Remove the module from its packaging.
4. Insert the module into the chassis slot and glide the card along the card guide until the card ejectors on the front of the module touch the chassis.

   CAUTION: To avoid hardware damage during installation, be careful to properly line up the edges of the module board with the guides built into the module slot on the chassis.

   NOTE: Modules for the 9308M slide in vertically with the module label (e.g. ProCurve 9300) and port number 1 at the top (Figure 2.3). Modules for the 9304M slide in horizontally with the module label (e.g. ProCurve 9300) and port number 1 on the left (Figure 2.4).

5. Push the ejectors toward the center of the module until they are flush with the front panel of the module. The module will be fully seated in the backplane.
6. Tighten the two screws at either end of the module.

   CAUTION: If you do not use one or more of the slots, make sure that a slot cover plate is still attached over each unused slot for safe operation and proper system cooling.

   NOTE: If installing a module into a slot *previously occupied by a different type of module*, you must use the CLI to configure the new module (with the CLI command, **module *<slot number> <module type>***) and then use the **write memory** command to save the configuration and the **reload** command to reset the routing switch. See “Swapping Modules (chassis platforms only)” on page 2-45. If the slot has never contained a module or you are swapping in exactly the same type of module, you do not need to enter these commands.

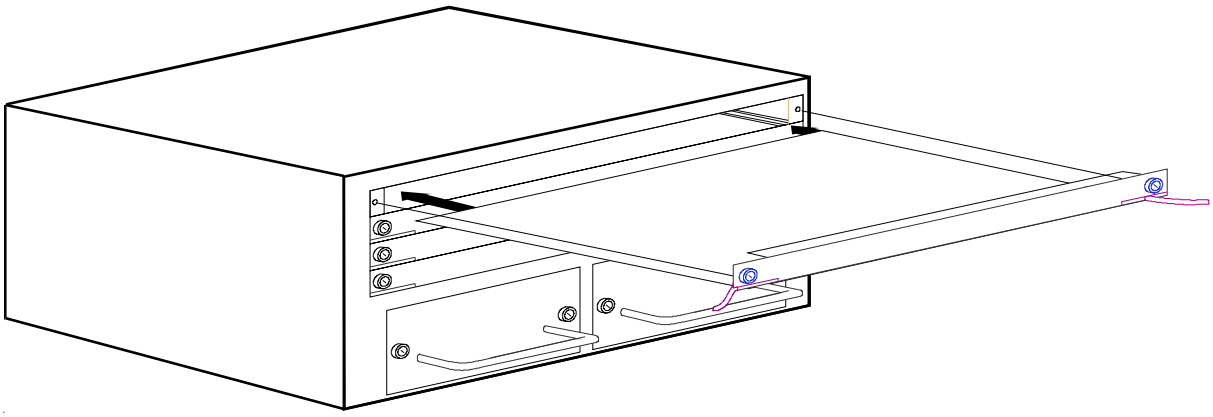


Figure 2.1 Installing a Module

Removing Modules

To remove a module from the chassis, do the following:

1. Put on an ESD wrist strap and attach the clip end to a metal surface (e.g. an equipment rack) to act as ground.

WARNING: To avoid risk of shock, do not attach the clip end to the air flow panel of the power supply.

2. Loosen the two screws on the module.
3. Pull the card ejectors towards you, and away from the module front panel. The card will unseat from the backplane.
4. Pull the module out of the chassis and place in an anti-static bag for storage.
5. Cover the slot with the blank face plate that shipped with the chassis.

CAUTION: If you remove a module and do not replace it, cover the slot opening with one of the blank plates you received with the routing switch to provide additional safety and airflow for the system.

NOTE: Modules can be installed and removed when the unit is powered on (hot swap). There is no need to power the system down. You do not need to change the slot's configuration unless you plan to insert a different type of module. See "Swapping Modules (chassis platforms only)" on page 2-45.

3. Installing (or Removing) Redundant Power Supplies (chassis only)

Determining Power Supply Status

If you are replacing a power supply that has failed and you are not sure which supply has failed, enter the following command at any CLI command prompt:

show chassis

This command displays status information for the fans and the power supplies. The power supplies are numbered in the display. The power supply numbers correspond to the following positions. These positions assume you are facing the front of the chassis, not the rear.

Table 2.1: Power Supply Positions in Chassis Devices

Product	Power Supply 1 Position	Power Supply 2 Position	Power Supply 3 Position	Power Supply 4 Position
HP 9304M	left side	right side	n/a	n/a
HP 9308M	bottom	second from bottom	second from top	top

Installing Power Supplies

To install a power supply in the chassis, do the following:

CAUTION: Power supplies are hot swappable but they should be disconnected from AC power before being installed or removed. That is, the routing switch can be running while a power supply is being installed or removed, but the power supply itself *should not be connected* to a power source. Otherwise, damage to the power supply or the routing switch could result.

1. Use a screwdriver to remove the blank power supply face plate. This will expose the empty power supply slot.
2. Remove the power supply from its packaging.
3. Holding the bar on the front panel of the power supply, insert the power supply into the empty power supply slot using the module guides provided on either side of the compartment.

CAUTION: Carefully follow the mechanical guides on each side of the power supply slot and make sure the power supply is properly inserted in the guides. Never insert the power supply upside down.

4. Continue to slide the power supply towards the back of the chassis until the two metal rods and the connector make contact with the back connector. Then push the power supply until the front panel of the power supply is flush with the rest of the chassis.
5. Use a screwdriver to tighten the two screws on either side of the power supply.
6. Connect the power cord to the front of the power supply.
7. Connect the power plug into an outlet.

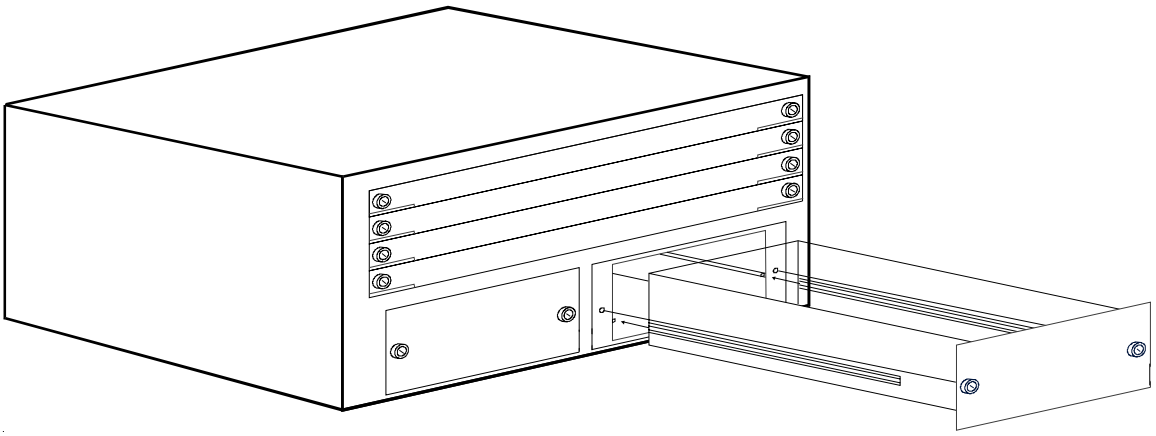


Figure 2.2 Installing a Power Supply

Removing Power Supplies

To remove a power supply module from the chassis, do the following:

CAUTION: Power supplies are hot swappable but they should be disconnected from AC power before being installed or removed. That is, the routing switch can be running while a power supply is being installed or removed, but the power supply itself *should not be connected* to a power source. Otherwise, damage to the power supply or the routing switch could result.

1. Unplug the power supply AC power cord from the outlet.
2. Disconnect the power cord from the power supply.
3. Use a screwdriver to loosen the screws on either side of the power supply.
4. Holding the bar on the front panel of the power supply, pull outward, disconnecting the power supply from the backplane.
5. Continue to pull the power supply until it is removed from the chassis.
6. Place the power supply in an anti-static bag for storage.
7. Cover the power supply slot with the blank power supply cover that came with the unit.
8. Use a screwdriver to tighten the screws.

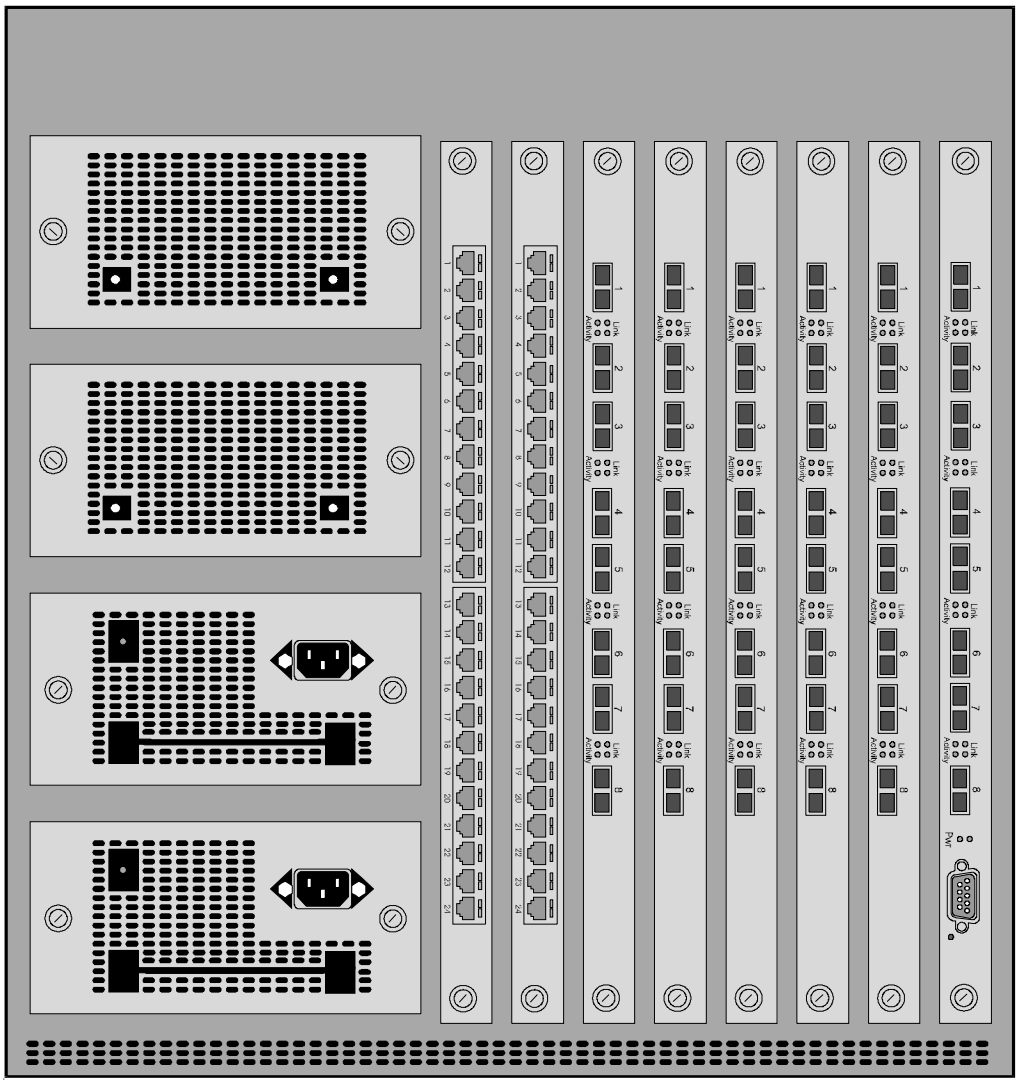


Figure 2.3 Example of the front panel of an HP 9308M routing switch

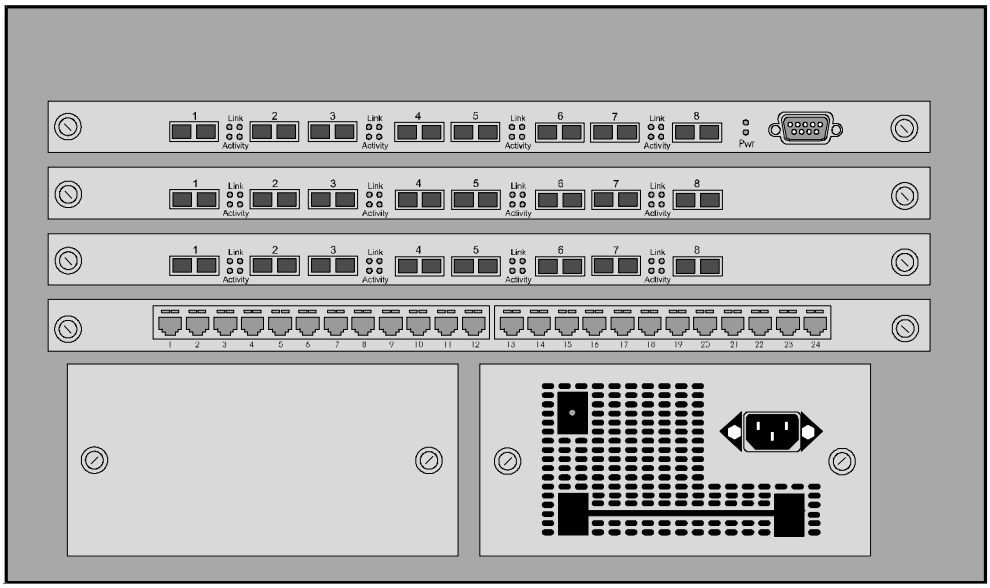


Figure 2.4 Example of the front panel of an HP 9304M routing switch

4. Verifying Proper Operation

After you have installed any modules or redundant power supplies, but before mounting the routing switch in its network location, you should first verify that it is working properly by plugging it into a power source and verifying that it passes its self test.

NOTE: Chassis only – If your device has more than one power supply installed, repeat this procedure for each power supply.

---

1. Connect the power cord supplied with the switch to the power connector found on the power supply on the front of the device.
2. Insert the other end into a properly grounded electrical outlet.

NOTE: The devices do not have power switches. They are powered on when the power cord is connected to the device and to a power source.

If your installation requires a different power cord than that supplied with the device, be sure to obtain a power cord displaying the mark of the safety agency that defines the regulations for power cords in your country. The mark is your assurance that the power cord can be used safely with the device.

---

3. Verify proper operation by observing the LEDs:
   - Chassis devices – Make sure the LED on each power supply is a solid green. Also make sure that some of the port LEDs on each module momentarily light up. The LEDs indicate that the device is performing diagnostics. After the diagnostics are complete, the LEDs will be dark except for the ones that are attached by cables to other devices. If the links on these cables are good and the connected device is powered on, the link LEDs will light.

   NOTE: If all of the LEDs on a module do not light up during the diagnostics, this does not indicate an error. Only some of the LEDs are lighted during the diagnostics.

- Fixed-port devices – All the port LEDs should flash momentarily, usually in sequence, while the device performs diagnostics. After the diagnostics are complete, the LEDs will be dark except for the ones that are attached by cables to other devices. If the links on these cables are good and the connected device is powered on, the link LEDs will light.

For more details on specific LED conditions after system start-up, see “LEDs” on page 6-9.

5. Attaching a PC or Terminal

To assign an IP address, you must have access to the ***Command Line Interface (CLI)***. The CLI is a text-based interface that can be accessed through a direct serial connection to the device and through Telnet connections. The CLI is described in detail in “Command Line Interface Commands” on page B-1.

HP switches and routing switches have a default IP address and subnet mask of 209.157.22.254 and 255.255.255.0 when shipped from the factory. You need to assign a permanent IP address using the CLI. You can access the CLI by attaching a serial cable to the Console port. After you assign an IP address, you can access the system through Telnet or the Web management interface.

Attaching a PC or Terminal Using a Serial Port

To attach a management station using the serial port:

1. Connect a PC or terminal to the serial port of the system via the (serial) console cable. The serial port is a male DB-9 connector. Generally, a PC port will require a cable with a female DB-9 connector. Terminal connections will vary, requiring either a DB-9 or DB-25 connector, male or female.

   A console cable is provided with your switch or routing switch. Cable pin-outs and signalling for the serial cable are shown in Figure 2.5 and Figure 2.6.

2. If you are using a PC for a terminal, run a terminal emulation program on the PC.
3. Set the terminal or PC terminal emulation program to the parameters shown below:
   - Baud: 9600 bps
   - Data bits: 8
   - Parity: None
   - Stop bits: 1
   - Flow control: None

Attaching a PC or Terminal Using a Direct LAN Connection

To attach a management station using a direct LAN connection:

NOTE: Use this procedure if you are unable to make the serial connection described above.

NOTE: The switch or routing switch was shipped from the factory with a default IP address and subnet mask of 209.157.22.254 and 255.255.255.0.

1. Directly connect the LAN port on a Telnet-capable terminal device such as a laptop or desktop PC to one of the following:
   - In a chassis device, port 1 in slot 1
   - In a fixed-port device, port 1
2. Configure the terminal device with an IP address and subnet mask that assigns the terminal to the same subnet as the switch or routing switch's IP address for port 1, slot 1 (chassis devices) or port 1 (fixed-port devices). For example, if the port's IP address is the factory default (209.157.22.254 and 255.255.255.0), you can use 209.157.22.1 and 255.255.255.0.

3. From the DOS prompt, enter **telnet <ip address>** to access the switch or routing switch CLI, where <ip address> is the IP address for the switch or routing switch port.

When you establish the serial connection to the device, press Enter to display the CLI prompt for your switch or routing switch. For example:

```
HP9304>

HP9308>

HP6308>

HP6208>
```

If you see one of these prompts, you are now connected to the system and can proceed to “Assigning a Permanent Password” on page 2-12.

NOTE: For simplicity, CLI examples for both the 9304M or 9308M show the command prompt `HP9300`. This command prompt represents both the 9304M or 9308M unless otherwise noted. Command prompts that are specific to the 6208M-SX or 6308M-SX show `HP6208` or `HP6308`.

You can customize the prompt by changing the system name. See “Entering System Administration Information” on page 8-4.

If you do not see one of these prompts:

1. Make sure the cable is securely connected to your PC and to the HP device.
2. Check the settings in your terminal emulation program. In addition to the session settings listed above, make sure the terminal emulation session is running on the same serial port you attached to the HP device.

The EIA/TIA 232 serial communication port serves as a connection point for management by a PC or SNMP workstation. HP switches and routing switches come with a standard male DB-9 connector, shown in Figure 2.5.

Pin Assignment	Pin Number	Switch Signal
DB-9 male	1	Not Used
	2	TXD (output)
	3	RXD (input)
	4	Not Used
	5	GND
	6	Not Used
	7	CTS (input)
	8	RTS (output)
	9	Not Used

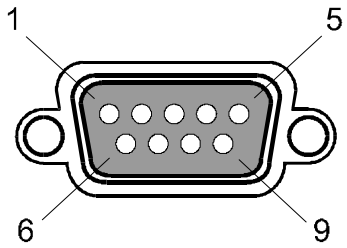


Figure 2.5 Serial port pin and signalling details

Most PC serial ports also require a cable with a female DB-9 connector. Terminal connections will vary, requiring either a DB-9 or DB-25 connector, male or female. Serial cable options between an HP switch or routing switch and a PC terminal are shown in Figure 2.6.

NOTE: As indicated in Figure 2.5 and Figure 2.6, some of the wires should not be connected. If you do connect the wires that are labeled "Not Used" or "Not Connected", you might get unexpected results with some terminals.

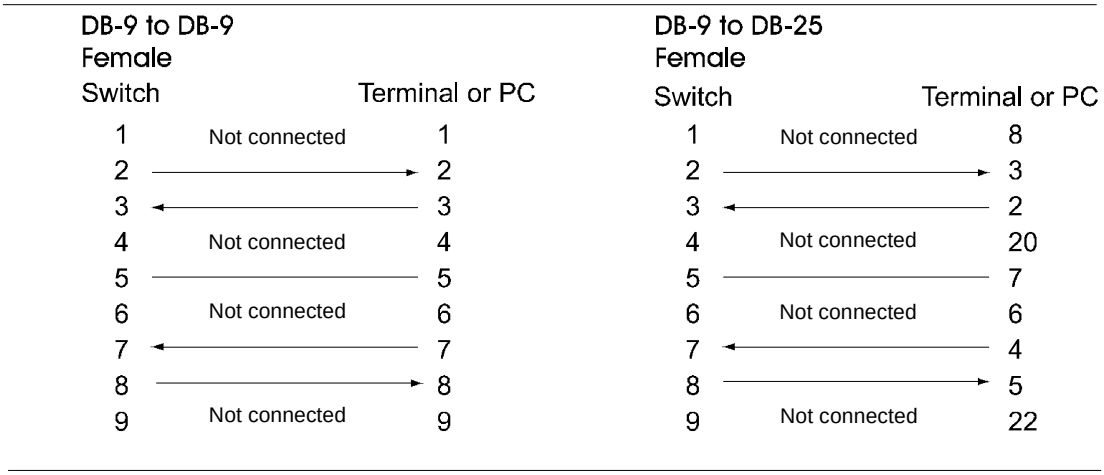


Figure 2.6 Serial port signal directions

6. Assigning a Permanent Password

You must use the CLI to assign a password. A password cannot be assigned through the Web management interface.

The CLI contains the following access levels:

- ***User EXEC level*** – The level you enter when you first start a CLI session. At this level, you can view some system information but you cannot configure system or port parameters.
- ***Privileged EXEC level*** – This level is also called the Enable level and can be secured by a password. You can perform tasks such as manage files on the flash module, save the system configuration to flash, and clear caches at this level.
- ***CONFIG level*** – The configuration level. This level lets you configure the system's IP address and configure switching and routing features. To access the CONFIG mode, you must already be logged in to the Privileged level of the EXEC mode.

By default, there are no CLI passwords. To secure CLI access, you must assign passwords.

NOTE: You must use the CLI to assign a password. You cannot assign a password using the Web management interface or an SNMP network management application.

You can set the following levels of Enable passwords:

- 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. *You must set a super user password before you can set other types of 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.

How To Assign a Password

When you first connect to the CLI, you are at the User EXEC level of the CLI. This is the first level of the CLI. The next level is the Privileged EXEC level. You need to get to the global CONFIG level of the CONFIG command structure to assign a permanent password.

To reach the global CONFIG level and assign passwords, use the following steps:

1. At the opening prompt, enter the following command to go from the User EXEC level to the Privileged EXEC level:

   ```
   HP9300> enable
   ```

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

   ```
   HP9300# configure terminal              Privileged EXEC Level
   HP9300(config)#                         Global CONFIG Level
   ```

3. To set the super-user password:

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

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

4. To set the port-configuration and read-only passwords:

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

How to Recover From a Lost Password

Recovery from a lost password requires direct access to the serial port and a system reset of the device.

NOTE: You can perform this procedure only from the CLI.

To recover from a lost password:

1. Start a CLI session over the serial interface to the device.
2. Reboot the device.
3. At the initial boot prompt at system start-up enter **b** to initiate boot monitor mode.
4. Enter **no password** at the prompt. This command cannot be abbreviated.
5. Enter **boot system flash primary**. This will cause the device to bypass the system password check.
6. After the console prompt reappears, assign a new password.

7. Assign a Permanent IP Address

Before you can manage the switch or routing switch over your network, you must assign at least one IP address to the device. (For more information on IP addressing, see chapter 9, "Configuring IP and IP/RIP" in the *Advanced Configuration and Management Guide* included on the CD-ROM shipped with your device.)

Routing Switches

Before attaching an HP routing switch to your network, you must assign an interface IP address to the sub-net on which the routing switch will be located. For subsequent addresses, you also can use the CLI through Telnet or use the Web management interface.

Using a serial connection is the recommended method for assigning the first IP address on a routing switch. (You also can use Telnet with a direct, terminal-to-device LAN connection if necessary—see “Attaching a PC or Terminal Using a Direct LAN Connection” on page 2-10.)

On the 9304M and 9308M, you can configure up to 24 IP interfaces on each port, virtual interface, and loopback interface. On the 6308M-SX routing switch, you can increase this amount to up to 64 IP sub-net addresses per port by increasing the size of the subnet-per-interface table. See “Modifying System Parameter Default Settings” on page 8-69.

The following procedure shows how to add an IP address and mask to a routing switch port.

1. At the opening CLI prompt, enter **enable**.

   ```
   HP9300> enable
   ```

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

   ```
   HP9300# configure terminal              Privileged EXEC Level
   HP9300(config)#                         Global CONFIG Level
   ```

3. Delete the factory-set IP address from port 1 (or 1/1 on chassis devices) by entering the following commands:

   ```
   HP9300(config)# int e 1/1
   HP9300(config-if-1/1)# no ip address 209.157.22.254 255.255.255.0
   ```

4. Set the IP and mask addresses.

   ```
   HP9300(config)# int e 1/5
   HP9300(config-if-1/5)# ip address 192.22.3.44 255.255.255.0
   ```

NOTE: You can use the syntax, **ip address <ip address /sub-net mask length>** if you know the sub-net mask length. In the above example, you could enter **ip address 192.22.3.44/24**.

Syntax: enable [<password>]

Syntax: configure terminal

Syntax: [no] ip address <ip-addr> <mask> [secondary]

or

[no] ip address <ip-addr>/<mask-bits> [secondary]

Use the **secondary** parameter if you have already configured an IP address within the same sub-net on the interface.

Switches

Using a serial connection is the recommended method for assigning the IP address on a switch. (You also can use Telnet with a direct, terminal-to-device LAN connection if necessary—see “Attaching a PC or Terminal Using a Direct LAN Connection” on page 2-10.)

To assign an IP Address to the 6208M-SX switch:

1. At the opening CLI prompt, enter **enable**.

   ```
   HP6208> enable [<password>]
   ```

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

   ```
   HP6208# configure terminal              Privileged EXEC Level
   HP6208(config)#                         Global CONFIG Level
   ```

3. Delete the factory-set IP address from the switch by entering the following command:

   ```
   HP6208(config)# no ip address 209.157.22.254 255.255.255.0
   ```

4. Set the IP and mask addresses for the switch.

   ```
   HP6208(config)# ip address 192.22.3.44 255.255.255.0
   ```

5. Set a default gateway address for the switch.

```
HP6208(config)# ip default-gateway 192.22.3.1
```

NOTE: You do not need to assign a default gateway address for single sub-net networks.

Syntax: enable [<password>]

Syntax: configure terminal

Syntax: [no] ip address <ip-addr> <mask>

or

[no] ip address <ip-addr>/<mask-bits>

Syntax: ip default-gateway <ip address>

8. Mounting the Device

The HP switch and routing switches can be installed on a desktop or in a rack.

WARNING: The HP 9304M chassis exceeds 40 lbs. (18 kg), or 47.7 lbs.(21.6 kg) when fully populated with modules and power supplies. Also, the HP 9308M chassis exceeds 55 lbs. (24.9 kg) or 69.1 lbs. (31.3 kg) when fully populated with modules and power supplies. TWO OR MORE PEOPLE ARE REQUIRED WHEN LIFTING, HANDLING, OR MOUNTING THESE ROUTING SWITCHES.

WARNING: Do not use the handles on the power supply units to lift or carry a routing switch.

WARNING: Make sure the rack or cabinet housing the routing switch is adequately secured to prevent it from becoming unstable and/or falling over.

WARNING: Mount the devices you install in a rack or cabinet as low as possible, with the heaviest device at the bottom and progressively lighter devices installed above. HP recommends that the HP 9304M or 9308M be installed at the bottom of the rack or installed with a shelf and mounting brackets.

Desktop Installation

1. Set the device on a flat desktop, table, or shelf. Use a sturdy surface in an uncluttered area. You may want to secure the networking cables and power cord to the table legs or other part of the surface structure to help prevent people from tripping over them.
2. Make sure that adequate ventilation is provided for the system—a minimum of three inches (3") clearance is recommended on all sides.

NOTE: Make sure the air flow is unrestricted around the front, sides, and back of the switch or routing switch.

3. Proceed to “Connecting Power to the Device” on page 2-17.

Rack Mount Installation – Chassis

NOTE: You need a #2 Phillips-head screwdriver for installation.

1. Remove the rack mount kit from the shipping carton. There will be two L-shaped mounting brackets and mounting screws.
2. Attach the mounting brackets to the sides of the routing switch as illustrated in Figure 2.7.
3. Attach the system in the rack as illustrated in Figure 2.7.
4. Proceed to “Connecting Power to the Device” on page 2-17.

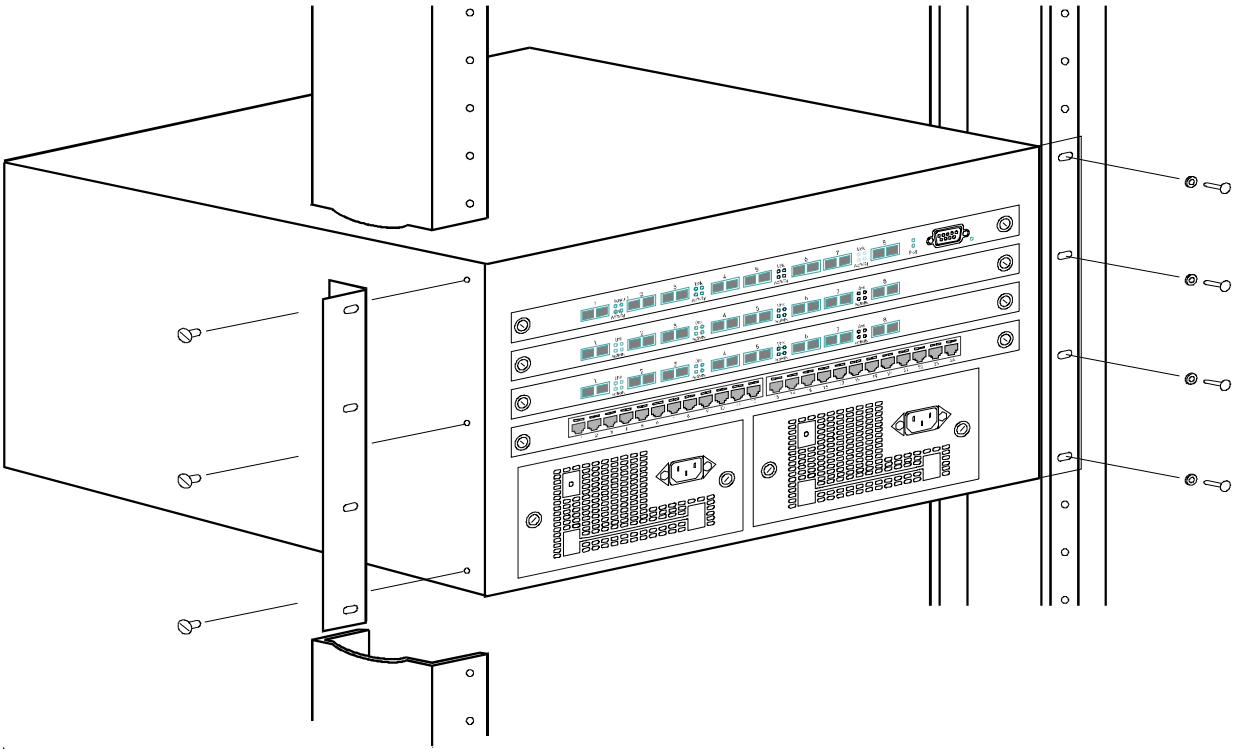


Figure 2.7 Installing a 9304M routing switch in a rack mount

Rack Mount Installation – HP 6208M-SX or HP 6308M-SX

NOTE: You need a #2 Phillips-head screwdriver for installation.

1. Remove the rack mount kit from the shipping carton. The kit contains two L-shaped mounting brackets and mounting screws.
2. Attach the mounting brackets to the sides of the device as illustrated in Step 2 of Figure 2.8.
3. Attach the device in the rack as illustrated in Step 3 of Figure 2.8.
4. Proceed to "Connecting Power to the Device" below.

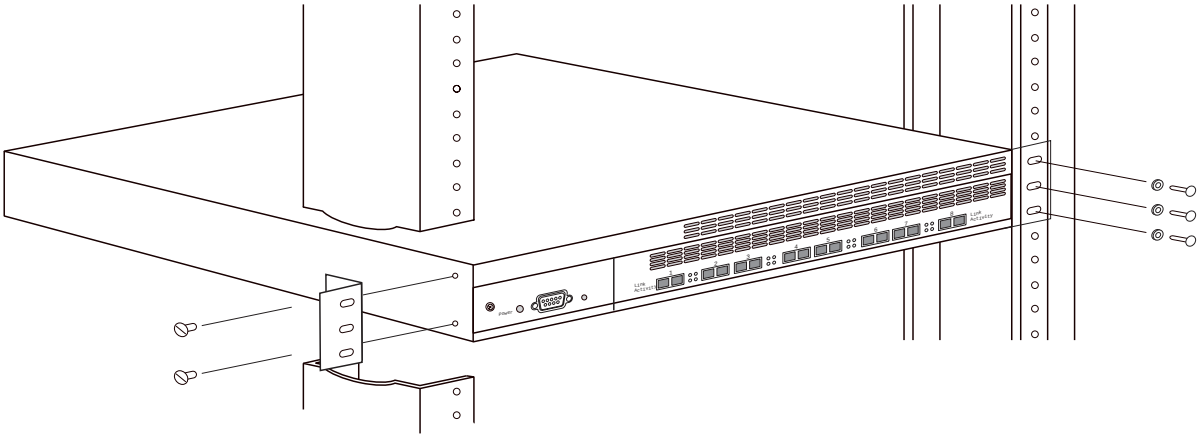


Figure 2.8 Installing an HP 6208M-SX or HP 6308M-SX in a rack mount

9. Connecting Power to the Device

With physical installation of the switch or routing switch complete, it is now time to power up the system and connect the network devices.

CAUTION: There is no separate on/off power switch for the device. The device is powered on when the power cord is connected to a power supply and to a power source. To turn the system off, simply unplug the power cord(s).

CAUTION: The power sockets should be installed near the device and should be easily accessible.

CAUTION: If your installation requires a different power cord than the one supplied with the device, be sure to use a power cord displaying the mark of the safety agency that defines the regulations for power cords in your country. The mark is your assurance that the power cord can be used safely with the system.

1. For a chassis device, ensure that all modules and power supplies are properly inserted, and that no module slots or power supply slots are uncovered.

   WARNING: Electrical shock hazard. Never allow any part of your body to be inside the chassis when the chassis is connected to a power source or to the network.

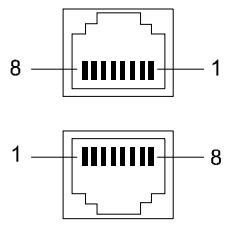
2. Remove the power cord from the shipping package.
3. Attach the AC power cord to the AC connector on the front panel of chassis devices or the rear panel of fixed-port devices. If more than one power supply is installed, attach a power cord for each power supply.
4. Insert the power cord plug(s) into the appropriate outlet(s).

10. Connecting Network Devices

HP switches and routing switches can support connections to other vendors' routers, switches, and hubs as well as to other HP switches, routing switches, and hubs.

Connectors

- 10/100BaseTX ports come with RJ45 jacks for standard unshielded twisted pair (UTP/Category 5) cable connections.
- 100BaseFX ports come equipped with MT-RJ connectors.
- 1000BaseSX ports come equipped with SC connectors.
- 1000BaseLX ports come equipped with SC connectors.



Pin assignment	10BaseT		100BaseTX	
	Pin#	MDI-X ports	Pin #	MDI-X ports
	1	RD+	1	RD+
	2	RD-	2	RD-
	3	TD+	3	TD+
	4	Not Used	4	CMT
	5	Not Used	5	CMT
	6	TD-	6	TD-
	7	Not Used	7	CMT
	8	Not Used	8	CMT

Figure 2.9 Pin assignment and signalling for 10BaseTX and 100BaseTX ports

Cable Length

Table 2.1 Cable length summary table

	Fiber Type	Core Diameter (microns)	Modal Bandwidth (MHz*km)	Minimum Range (meters)
1000Base-SX	MMF	62.5	160	2 – 200[a]
	MMF	62.5	200	2 – 275[b]
	MMF	50	400	2 – 500
	MMF	50	500	2 – 550[c]
1000Base-LX	MMF	62.5	500	2 – 550
	MMF	50	400	2 – 550
	MMF	50	500	2 – 550
	SMF	9	n/a	2 – 5000

a.The TIA 568 building wiring standard specifies 160/500 MHz*km MMF (Multimode Fiber).
b.The international ISO/IEC 11801 building wiring standard specifies 200/500 MHz*km MMF.
c.The ANSI Fibre Channel specification specifies 500/500 MHz*km 50 micron MMF and 500/500 MHz*km fiber has been proposed for addition to ISO/IEC 11801.

- 100BaseTX: Cable length should not exceed 100 meters in keeping with the IEEE 802.3 standard.
- 100BaseFX: Cable length should not exceed 2 kilometers.
- 1000BaseSX: Cable length should not exceed 550 meters when operating with multi-mode cabling.
- 1000BaseLX:
  - Cable length of 2 – 440 meters is supported on 62.5 µm multi-mode fiber (MMF) cabling.
  - Cable length of 2 – 550 meters is supported on 50 µm multi-mode fiber (MMF) cabling.
  - Cable length of 2 – 5000 meters is supported on 9 µm single-mode fiber (SMF) cabling.

NOTE: Cable installation and network configuration will affect overall transmission capability. The numbers provided above represent the accepted recommendations of the various standards. For network-specific recommendations, consult your local HP reseller or system engineer.

Connecting to Other Routers, Switches, Ethernet or Fast Ethernet Hubs

For UTP connections to Ethernet or Fast Ethernet hubs, a 10/100 Mbps switch or another HP switch or routing switch, a crossover cable is required (Figure 2.10). If the hub is equipped with an uplink port, it will require a straight-through cable versus a crossover cable.

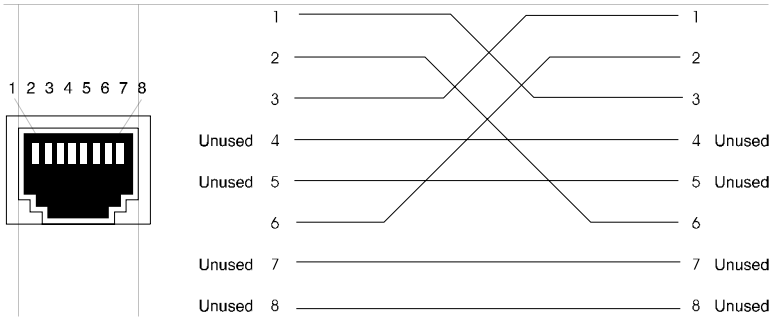


Figure 2.10 UTP crossover cable

Connecting to Workstations, Servers or Routers

Straight-through UTP cabling is required for direct UTP attachment to workstations, servers, or routers via network interface cards (NICs).

Fiber cabling with SC connectors is required for direct attachment to Gigabit NICs or switches and routers.

Troubleshooting Network Connections

- For the indicated port, verify that both ends of the cabling, at the switch or routing switch and the connected device, are snug.
- Verify the connected device and the switch or routing switch are both powered on and operating correctly.
- Verify that you have used the correct cable type for the connection:
  - For twisted-pair connections to an end node, use straight-through cabling.
  - For fiber-optic connections, verify that the transmit port on the switch or routing switch is connected to the receive port on the connected device, and that the receive port on routing switch is connected to the transmit port on the connected device.
- Verify that the port has not been disabled through a configuration change. You can use the CLI or if you have configured an IP address on the routing switch, you can use the Web management interface.
- If the other procedures don't resolve the problem, try using a different port or a different cable.

11. Verifying Proper Connections

After you install the network cables, you can test network connectivity to other devices by pinging those devices. You also can perform trace routes.

Pinging an IP Address

To verify that an HP device can reach another device through the network, enter a command such as the following at any level of the CLI on the HP device:

```
HP9300> ping 192.33.4.7
```

Syntax: ping <ip address>|<hostname> [count <num>] [timeout <msec>] [ttl <num>] [size <byte>] [no-fragment] [quiet] [verify] [data <1 – 4 byte hex>]

See "ping" on page B-67 for information about its parameters.

Tracing a Route

To determine the path through which an HP device can reach another device, enter a command such as the following at any level of the CLI on the HP device:

```
HP9300> traceroute 192.33.4.7
```

Syntax: traceroute <host IP address> [minttl <value> maxttl <value> timeout <value>]

The CLI displays trace route information for each hop as soon as the information is received. See “traceroute” on page B-68 for information about its command syntax.

12. Managing the Device

You can manage an HP device using the following applications:

- Command Line Interface (CLI) – a text-based interface accessible through a direct serial connection or a Telnet session.
- Web management interface – A GUI-based management interface accessible through an HTTP (web browser) connection.
- SNMP network management application – An application such as HP TopTools for Switches & Hubs or HP OpenView.

Logging on Through the CLI

Once an IP address is assigned to the HP switch or to an interface on the HP routing switch, you can access the CLI either through the direct serial connection to the device or through a local or remote Telnet session.

You can initiate a local Telnet or SNMP connection by attaching a straight-through RJ-45 cable to a port and specifying the assigned management station IP address.

The commands in the CLI are organized into the following levels:

- User EXEC level – Lets you display information and perform basic tasks such as pings and traceroutes.
- Privileged EXEC level – Lets you use the same commands as those at the User EXEC level plus configuration commands that do not require saving the changes to the system-config file.
- CONFIG level – Lets you make configuration changes to the device. To save the changes across reboots, you need to save them to the system-config file. The CONFIG level contains sub-levels for individual ports, for VLANs, for routing protocols, and other configuration areas.

NOTE: By default, any user who can open a serial or Telnet connection to the HP device can access all these CLI levels. To secure access, you can configure Enable passwords or local user accounts, and you can configure the device to use a RADIUS or TACACS/TACACS+ server for authentication. See “Securing Access to the Device” on page 2-23.

To display a list of available commands or command options, enter "?" and press Enter, or press Tab. If you have not entered part of a command at the command prompt, all the commands supported at the current CLI level are listed. If you enter part of a command, then enter "?" or press Tab, the CLI lists the options you can enter at this point in the command string.

The CLI supports command completion, so you do not need to enter the entire name of a command or option. As long as you enter enough characters of the command or option name to avoid ambiguity with other commands or options, the CLI understands what you are typing.

The CLI supports the following line editing commands. To enter a line-editing command, use the CTRL-key combination for the command by pressing and holding the CTRL key, then pressing the letter associated with the command.

Table 2.2: CLI Line-Editing Commands

Ctrl-Key Combination	Description
Ctrl-A	Moves to the first character on the command line.
Ctrl-B	Moves the cursor back one character.
Ctrl-C	Escapes and terminates command prompts and ongoing tasks (such as lengthy displays), and displays a fresh command prompt.
Ctrl-D	Deletes the character at the cursor.
Ctrl-E	Moves to the end of the current command line.
Ctrl-F	Moves the cursor forward one character.
Ctrl-K	Deletes all characters from the cursor to the end of the command line.
Ctrl-L; Ctrl-R	Repeats the current command line on a new line.
Ctrl-N	Enters the next command line in the history buffer.
Ctrl-P	Enters the previous command line in the history buffer.
Ctrl-U; Ctrl-X	Deletes all characters from the cursor to the beginning of the command line.
Ctrl-W	Deletes the last word you typed.
Ctrl-Z	Exits to the CLI level above.

For a complete list of CLI commands and syntax information for each command, see “Command Line Interface Commands” on page B-1.

Logging On Through the Web Management Interface

To use the Web management interface, open a web browser and enter the IP address of the HP device in the Location or Address field. The web browser contacts the HP device and displays a login dialog, as shown in Figure 2.11.

NOTE: If you are unable to connect with the switch or routing switch through a web browser due to a proxy problem, it may be necessary to set your web browser to direct Internet access instead of using a proxy. For information on how to change a proxy setting, refer to the online help provided with your web browser.

Figure 2.11 Web management interface login dialog

By default, you can use the user name "get" and the default read-only password "public" for read-only access. However, for read-write access, you must enter "set" for the user name, and enter a read-write community string that you have configured on the device for the password. There is no default read-write community string. You must add one. See “Configuring the SNMP Community Strings” on page 2-26.

As an alternative to using the SNMP community strings to log in, you can configure the device to secure Web management access using local user accounts, a RADIUS authentication server, or a TACACS/TACACS+ server. See “Securing Access to the Device” on page 2-23.

13. Securing Access to the Device

The HP 9304M, 9308M, and 6308M-SX routing switches and the 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 2.3 lists the default authentication methods and the methods that are supported for each type of management access to the device.

Table 2.3: 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
Telnet access to the CLI	None	• TACACS/TACACS+ • RADIUS • Local user accounts • "Enable" password • Telnet password • IP address list
Web management access	SNMP read or read-write community strings	• 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 2-41.

Use the following procedures to secure CLI and Web management access to the HP device.

You can access and change many of the system-level parameters, including access control parameters, from the Web management interface’s system configuration sheet, shown in Figure 2.12. The Web management procedures describe how to access the system configuration sheet.

NOTE: This window shows the options available on an HP 9304M or HP 9308M routing switch. The windows for the 6308M-SX routing switch and 6208M-SX switch contain some differences. Regardless of the differences, all switches and routing switches contain a link for the Management option, which you use for setting up access.

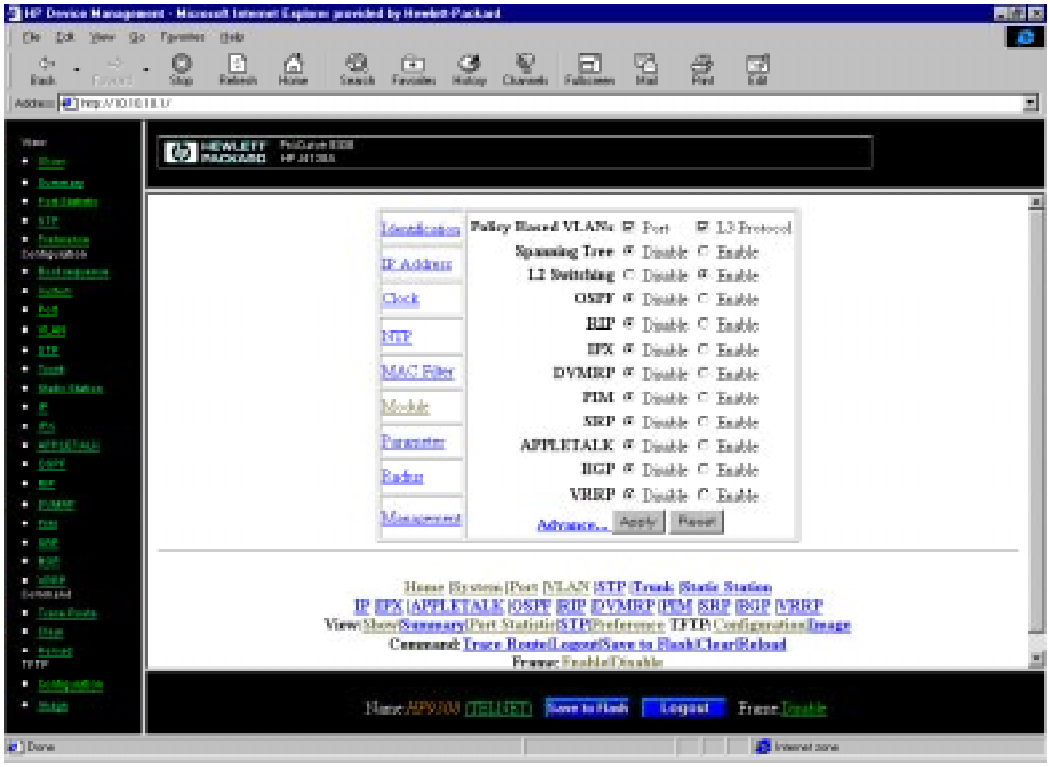


Figure 2.12 Example system configuration sheet on the Web management interface

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.

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.

- 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 for Web management access to the device. See “Configuring Local User Accounts” on page 2-32.

USING THE CLI

To add the read-only community string "look", enter the following commands:

```
HP9300(config)# snmp-server community look ro
HP9300(config)# write mem
```

Syntax: snmp-server community <string> ro

To add or change the read-write community string to "touch", enter the following command:

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

Syntax: snmp-server community <string> rw

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

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

Syntax: show snmp-server

See “show snmp-server” on page B-249 for an example of the information displayed by the command.

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. Enter the HP device's management IP address in the Location or Address field of your web browser.
2. When the Login dialog is displayed, enter "set" as the user name and a read-write community string as the password.
3. Click OK. The HP Device Management window is displayed. This window shown below is the Device Management window for options available on routing switches. The window for switches does not contain Layer 3 (routing) options but does contain some other options. Switches and routing switches all contain the Management link, which you need for this procedure.
4. Select Management from the system configuration sheet, which is the table in the middle of the display. The following panel is displayed.

NOTE: In this example and other examples of Web management interface screens, the Frame option has been disabled to emphasize the data entry fields on the screens.

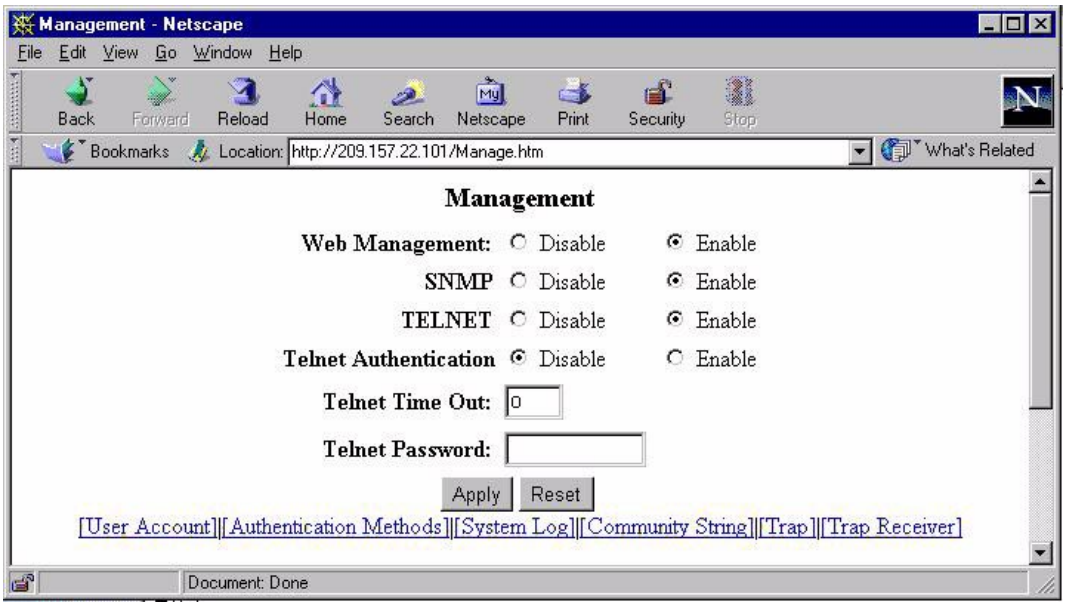


Figure 2.13 Management panel

5. Select the Community String link, located in the row of options at the bottom of the panel. The Community String panel is displayed.
6. Edit the community strings, then select Apply to assign the changes.

Disabling Web Management

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

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. Select the System link to display the system configuration sheet as shown in Figure 2.12.
2. Select the Management link.
3. Select Disable next to Web Management.
4. Select the Apply button to assign the change.

NOTE: As soon as you assign this change, the device stops responding to the browser session. The browser can contact the device, but the device will not reply.

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 local user accounts, RADIUS parameters, and TACACS/TACACS+ authentication for the device. See the following sections:

"Configuring Local User Accounts" on page 2-32

"Configuring for TACACS/TACACS+ Authentication" on page 2-34

"Configuring for RADIUS Authentication" on page 2-39

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. Select the System link to display the system configuration sheet as shown in Figure 2.12.
2. Select the Management link.
3. Select Disable next to Telnet.
4. Click the Apply button to assign the change.

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:

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

syntax: [no] snmp disable

USING THE WEB MANAGEMENT INTERFACE

To enable or disable SNMP management of a device:

1. Select the System link to display the system configuration sheet as shown in Figure 2.12.
2. Select the Management link.
3. Select Disable next to SNMP.
4. Select the Apply button to assign the changes.

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>

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 2-32.

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 2-41.

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
   ```

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 can set the password for Telnet access using the Web management interface.

1. Select the System link to display the system configuration sheet as shown in Figure 2.12.
2. Select the Management link.
3. Enter the password in the Telnet Password field.
4. Select the Apply button to assign the change.

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 and press Return.

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, 9308M, 6208M-SX, and 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 2-29.

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 2-41.

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 username
```

Syntax: show username

USING THE WEB MANAGEMENT INTERFACE

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

1. Select the System link to display the system configuration sheet as shown in Figure 2.12.
2. Select the User Account link, located in the row of links beneath the entry fields. The User Account panel is displayed.

Figure 2.14 User Account panel

3. Enter the user name in the Username field.
4. Enter the password in the Password field.
5. Select the privilege level from the Privilege field's pulldown menu.
6. Click the Add button to assign the change.
7. Select the Show User Account link to verify the new user account. Notice that the password display is encrypted.
8. Go to "Configuring Authentication-Method Lists" on page 2-41. 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 2-32 for descriptions of the access levels.

NOTE: 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 2-34.

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, 9308M, 6208M-SX, and 6308M-SX.

The TACACS/TACACS+ protocol defines how authentication, authorization, and accounting information are 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 TCP based access control protocol to ensure reliable delivery. The protocol allows the HP device to request very fine grained 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 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 8-6.

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. Select the System link to display the system configuration sheet as shown in Figure 2.12.
2. Select the TACACS link to display the TACACS panel.
3. Change the retransmit interval, time out, and dead time if needed.
4. Enter the authentication key if applicable.

   NOTE: The key applies only to TACACS+, not to TACACS. Do not enter a key if you are using TACACS.

5. Click Apply.
6. Select the TACACS Server link to display the following panel.

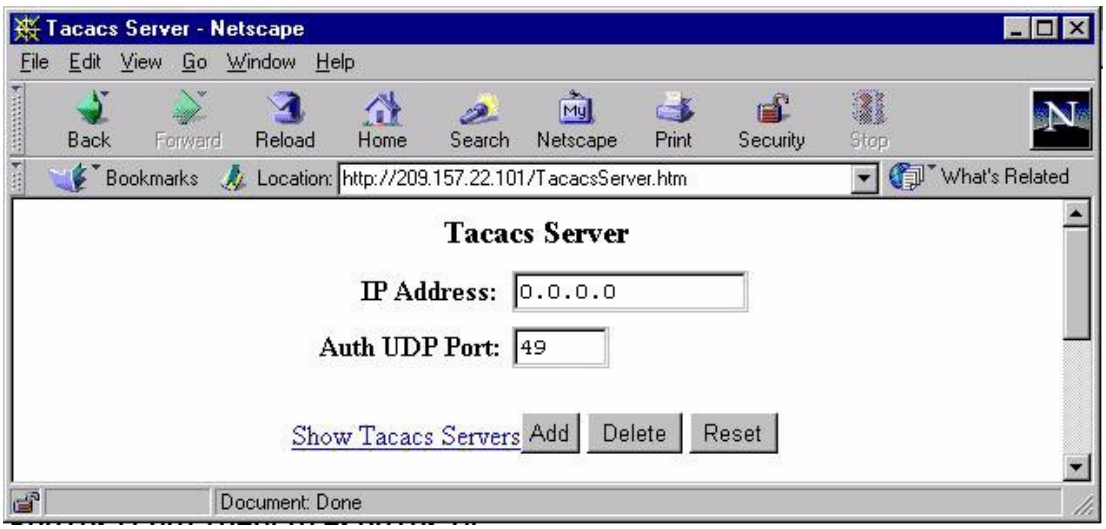


Figure 2.15 TACACS Server panel

7. Enter the TACACS server's IP address.
8. If needed, change the Authentication port. (The default values work in most networks.)

NOTE: Although the field name is "Auth UDP Port", the field applies equally to TACACS (UDP) or TACACS+ (TCP).

9. Click Add to apply the change.
10. Go to "Configuring the Authentication-Method Lists" on page 2-37. 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 2-32 for descriptions of the access levels.

Configuring the Authentication-Method Lists

To configure authentication-method lists for "enable" and Telnet 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 2-41.

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 2-41.

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. Select the System link to display the system configuration sheet as shown in Figure 2.12.
2. Select the Management link.
3. Select the Authentication Methods link from the row of links under the entry fields. The Login Authentication Sequence panel is displayed, as shown in the following example.

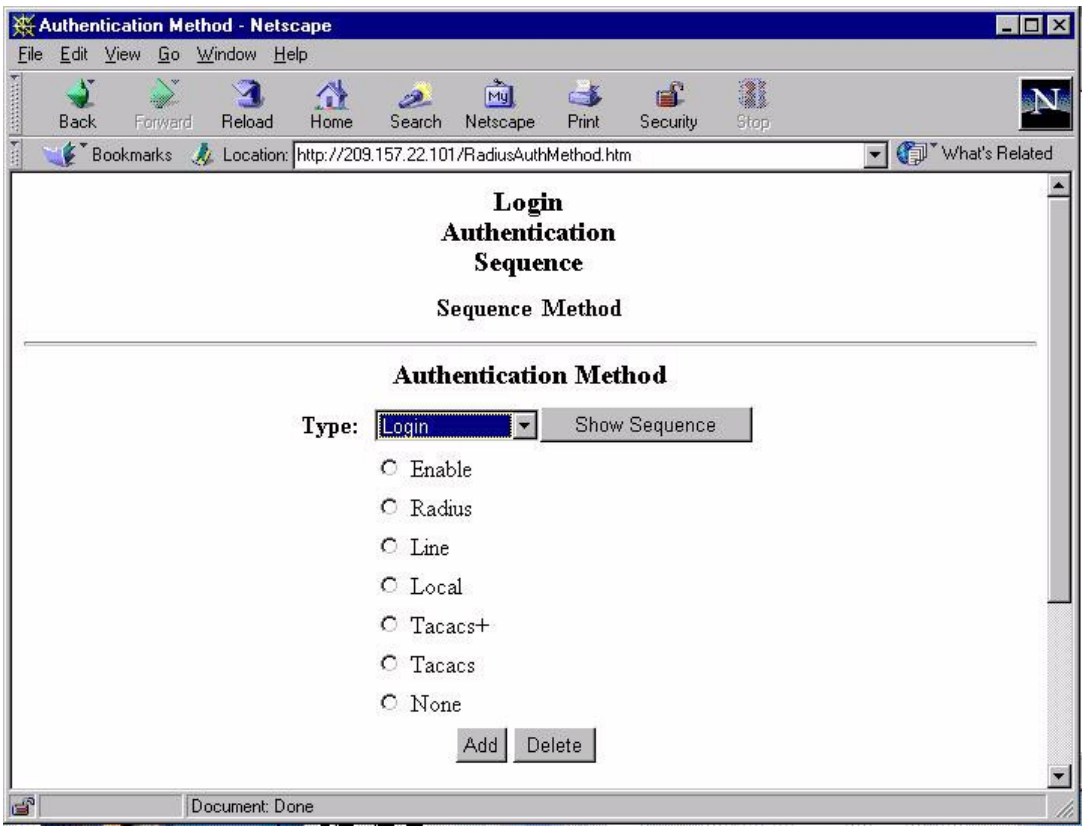


Figure 2.16 Login Authentication Sequence panel

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 Add to assign the change. The authentication method you selected is listed under "Sequence Method", in the upper portion of the panel.
7. Select the secondary authentication method from the Type field's pulldown menu. The device will try the secondary method if the first method is unavailable or results in an error. For example, to authenticate CLI logins using a local user account if the TACACS/TACACS+ server is unavailable, select Local.

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

---

8. Click Add. Repeat step 7 for each additional authentication method. You can select from one to all seven methods.

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, 9308M, 6208M-SX, and 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.

Implementation Notes

- A RADIUS server is required.
- Each switch or router 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 configuration 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 209.157.22.99 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 <IP-addr|server-name> [auth-port <number>] [acct-port <number>]

The **<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]

See “Configuring Authentication-Method Lists” on page 2-41 for more information about authentication-method lists.

USING THE WEB MANAGEMENT INTERFACE

1. Select the System link to display the system configuration sheet as shown in Figure 2.12.
2. Select the RADIUS link 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.
6. Select the Radius Server link to display the following panel.

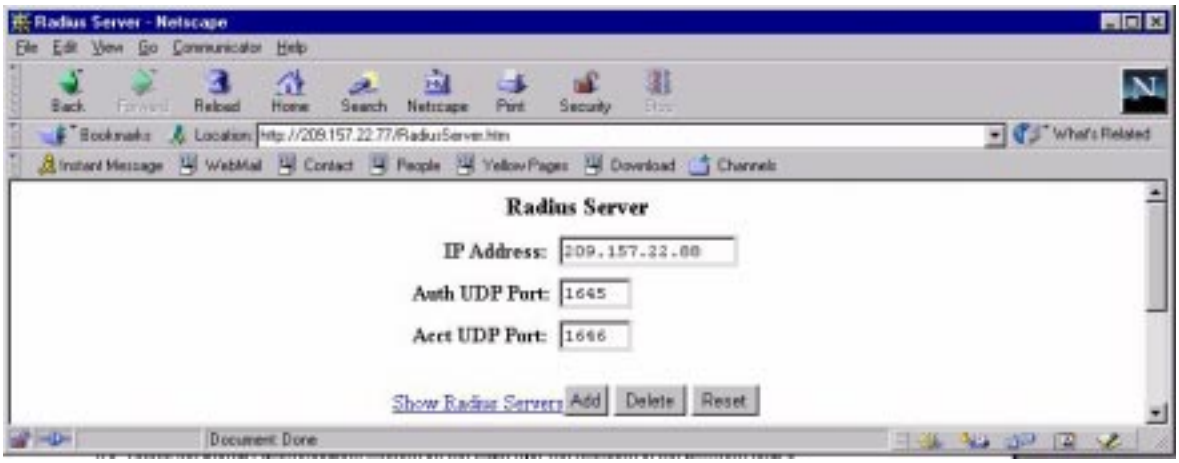


Figure 2.17 RADIUS Server panel

7. Enter the RADIUS server’s IP address.
8. If needed, change the Authentication port and Accounting port. (The default values work in most networks.)
9. Click Add to apply the change.

10. Go to “Configuring Authentication-Method Lists” on page 2-41. 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 2-32 for descriptions of the access levels.

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 a list of IP addresses. See “Restricting Remote Access to the Device to Specific IP Addresses” on page 2-25.

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 2-26.

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 2.4.

Table 2.4: 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 2-34.
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 2-39.
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 2-32.
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 2-29.
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 2-29.
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. Select the System link to display the system configuration sheet as shown in Figure 2.12.
2. Select the Management link.
3. Select the Authentication Methods link from the row of links under the entry fields. The Login Authentication Sequence panel is displayed, as shown in the following example.

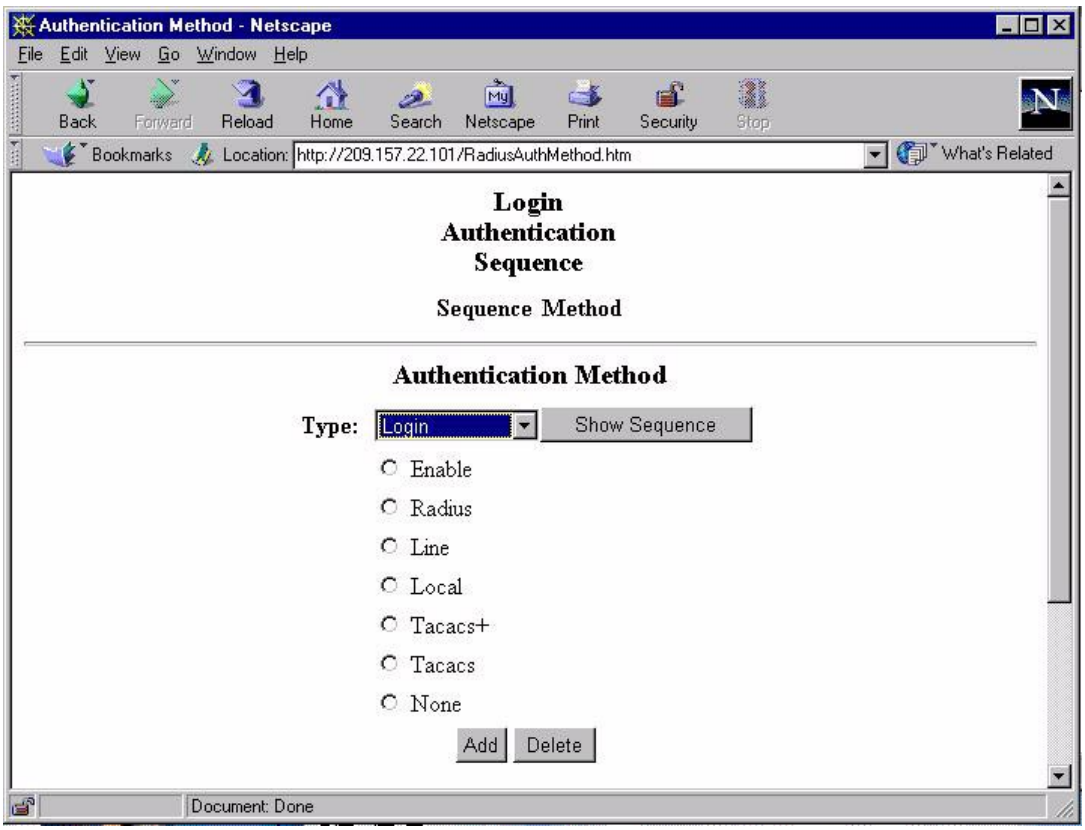


Figure 2.18 Login Authentication Sequence panel

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 Add to assign the change. The authentication method you selected is listed under "Sequence Method", in the upper portion of the panel.
7. Select the secondary authentication method from the Type field's pulldown menu. The device will try the secondary method if the first method is unavailable or results in an error. For example, to authenticate CLI logins using a local user account if the RADIUS server is unavailable, select Local.

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

---

8. Click Add. Repeat step 7 for each additional authentication method. You can select from one to all seven methods.

14. Swapping Modules (chassis platforms only)

After you physically insert a module into a chassis, you need to enter the location and type of module in the software, unless you either reboot the device or are replacing one module with another of the same type.

- Slots on the HP9304M are numbered 1 – 4, from top to bottom.
- Slots on the HP9308M are numbered 1 – 8, from left to right.

See “Slot and Port Numbers” on page 6-8 for more information about slot and port numbering.

NOTE: If the slot has never contained a module or you are swapping in exactly the same type of module, you do not need to use the **module** command. The slot requires configuration only if it has already been configured for another type of module.

USING THE CLI

To add a module to a chassis:

```
HP9300(config)# module 3 24-port-copper-module
```

Syntax: module <slot-number> <module-type>

The <slot number> parameter indicates the chassis slot number.

The <module type> parameter can be one of the following. You can, of course, take advantage of the CLI’s support for abbreviated command and parameter names.

NOTE: Some module strings apply to more than one module. This is because the slot configuration does not differ based on the physical layer. For example, a slot does not distinguish between an 8-port LX Fiber module and 8-port SX Fiber module. However, the software does indicate the physical layer type when you display module information. For example, the output of the **show module** command indicates the physical layer types of each module.

Table 2.5: Module Options

Module Type	Part Number and Description	Module String
Redundant Management modules	J4845A HP ProCurve 9300 GigLX Redundant Management Module (8-port)	8-port-gig-management-module
	J4846A HP ProCurve 9300 GigSX Redundant Management Module (8-port)	8-port-gig-management-module
	J4847A J4847A HP ProCurve 9300 Redundant Management Module (0-port)	0-port-management-module

Table 2.5: Module Options

Module Type	Part Number and Description	Module String
Management modules	J4141A ProCurve 9300 10/100 Management Module (16-port)	16-port-copper-management-module
	J4144A HP ProCurve 9300 Gigabit SX Management Module (8-port)	8-port-gig-management-module
	J4146A HP ProCurve 9300 Gigabit 4LX/ 4SX Management Module (8-port)	8-port-gig-management-module
Unmanaged modules	J4140A HP ProCurve 9300 10/100 Module (24-port)	24-port-copper-module
	J4142A HP ProCurve 9300 100Base FX Module (24-port MT-RJ)	24-port-100fx-module
	J4143A HP ProCurve 9300 Gigabit SX Module (8-port)	8-port-gig-module
	J4145A HP ProCurve 9300 Gigabit 4LX/ 4SX Module (8-port)	8-port-gig-module
	J4844A HP ProCurve 9300 GigLX Module (8-port)	8-port-gig-module

USING THE WEB MANAGEMENT INTERFACE

To assign a module to a chassis platform:

1. Select the Module link from the System configuration sheet. The Module panel showing all the modules installed in the chassis will appear. Figure 2.19 shows an example.
2. Select the Add Module link from the bottom of the Module panel to display the panel shown in Figure 2.20.
3. Select the slot number in which the module will reside from the Slot field's pulldown menu.
4. Select the module type from the Module Type field's pulldown menu.
5. Select the Add button to assign the module.

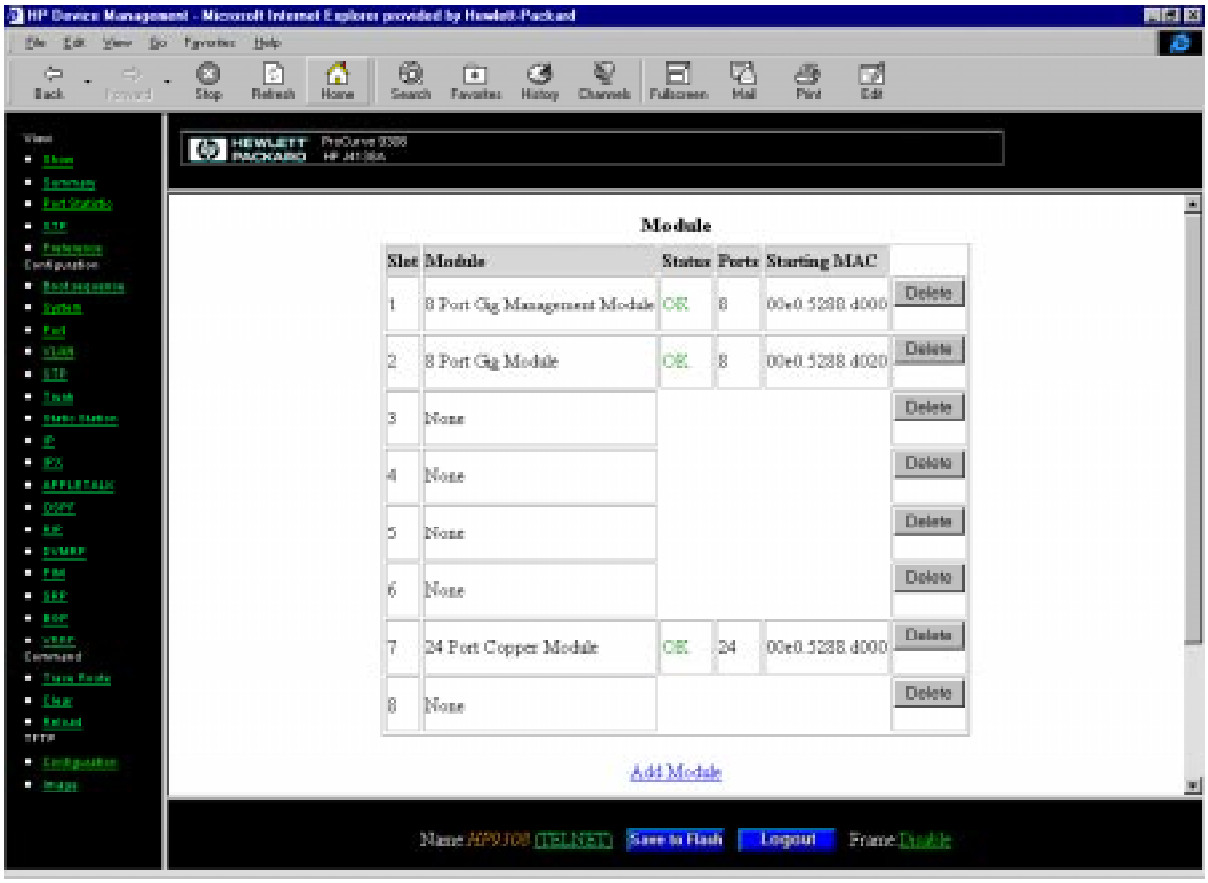


Figure 2.19 Module panel

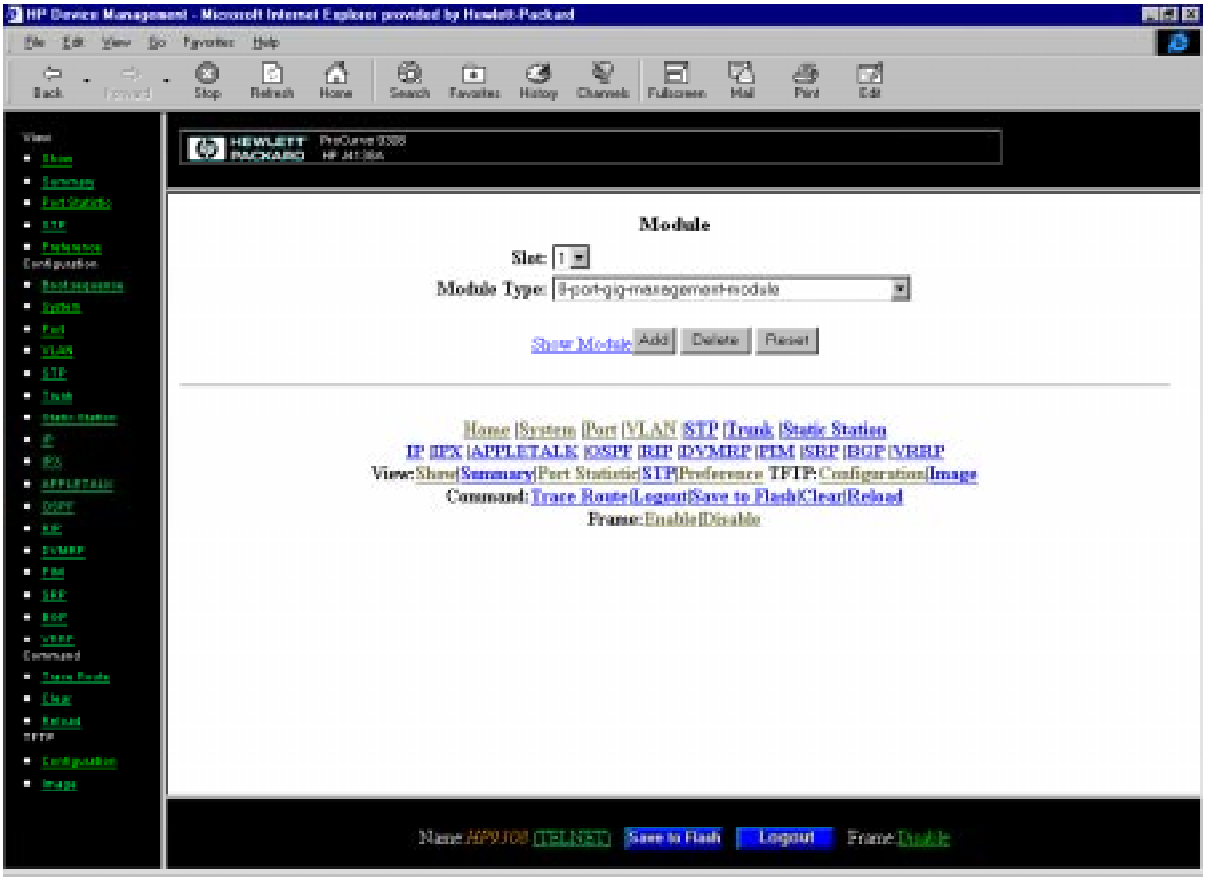


Figure 2.20 Panel for adding a module

15. Next Steps

Once the initial installation steps are completed, you can proceed with enabling routing protocols and configuring specific features on the switch or routing switches as described in “Configuring Basic Features” on page 8-1.

Configuration details for all routing protocols and advanced VLAN features can be found in the *ProCurve Advanced Configuration and Management Guide*.