Chapter 7
Configuring Basic and Advanced Features

This chapter addresses configuration of non-protocol features of the HP 9304M AND 9308M routing switches using the CLI and Web management interface.

A summary of all CLI commands highlighted in this chapter can be found in **Appendix B**.

The following items are covered in this chapter:

- Configuring System Parameters
- Configuring Port Parameters
- Configuring Spanning Tree Protocol
- Configuring Static MAC Entries
- Configuring Trunk Groups

Configuring Basic System Parameters

The HP 9304M and 9308M come configured with a number of default parameters that allow the user to begin using the basic features of the system immediately.

Many of the advanced features such as VLANs or routing protocols for the router must first be enabled at the system (global) level before they can be configured.

When configuring with the CLI, the user will find these system level parameters at the Global CONFIG level of the CLI.

When using the Web management interface, the user configures the system level parameters on the System configuration sheet (**Figure 7.1**) by selecting the System link found on the main menu.

NOTE: Before assigning or modifying any router parameters, the user should assign the IP sub-net (interface) addresses for each port via the System configuration sheet.

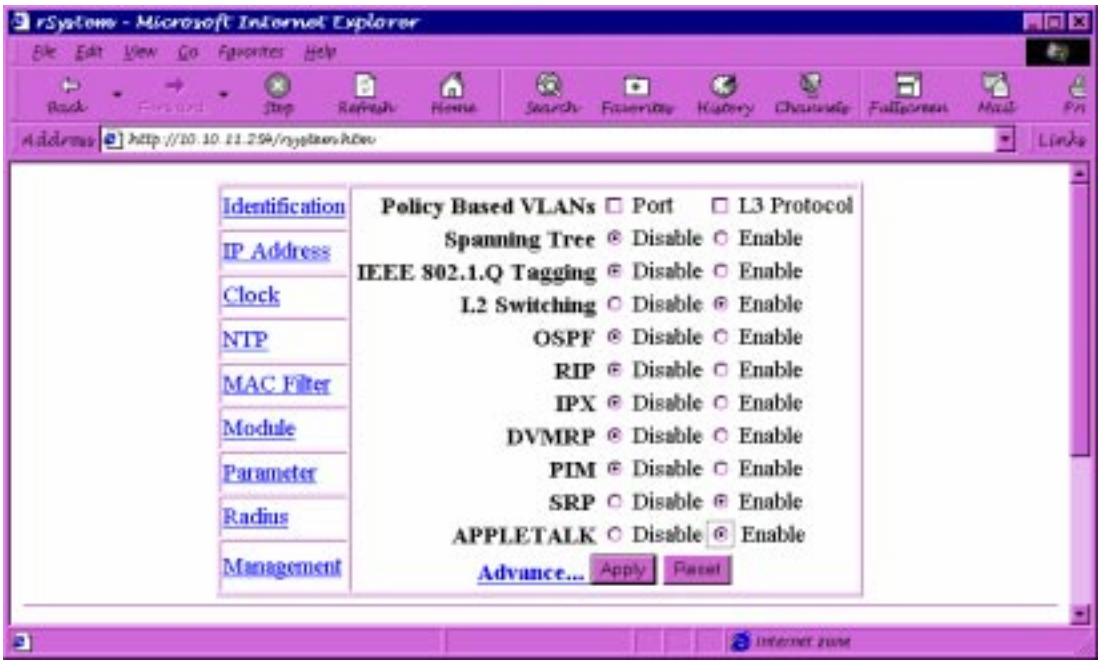

Figure 7.1 System configuration sheet for routing switches

The user can do the following configurations from the System configuration sheet:

- Enter system administration information
- Assign IP sub-net (interface) addresses and masks
- Enable or disable SNMP operation
- Assign a SNMP trap receiver station to collect traps
- Modify SNMP traps generated
- Modify events collected in the SNMP event log
- Modify the community string
- Define a MAC address filter
- Set the system clock

- Establish a reference network time protocol (NTP) server
- Enable port-based and/or layer 3 protocol VLANs
- Enable or disable protocols–OPSF, IP/RIP, IPX, DVMRP, PIM, SRP, AppleTalk
- Enable or disable Spanning Tree Protocol
- Enable or disable IEEE 802.1q VLAN tagging
- Enable or disable Telnet
- Modify telnet timeout period
- Modify telnet password
- Enable or disable layer 2 switching
- Add or delete module
- Assign a mirror port
- Modify system parameter default settings
- Modify events collected in a system log
- Enable or disable web management
- Assign RADIUS support

Entering System Administration Information

A system name, contact and location for the routing switch can be entered and saved locally in the configuration file for future reference. This information is not required for system operation but is suggested.

Up to 32 alphanumeric characters can be used in defining the system name, contact or location.

USING THE CLI

To define a system name, system contact and location:

```
HP9300(config)# chassis name oakland
Oakland(config)# snmp-server contact jack london
Oakland(config)# snmp-server location oakcabldg519
Oakland(config)# end
Oakland# write memory
```

syntax: chassis name <text>, snmp-server contact <text>, snmp-server location <text>

USING THE WEB MANAGEMENT INTERFACE

To define a system name, system contact or location:

1. Select the identification link from the System configuration sheet. The panel seen in **Figure 7.2** will appear.
2. Enter system **name, contact** and **location** information.
3. Select the **apply** button to save the changes.

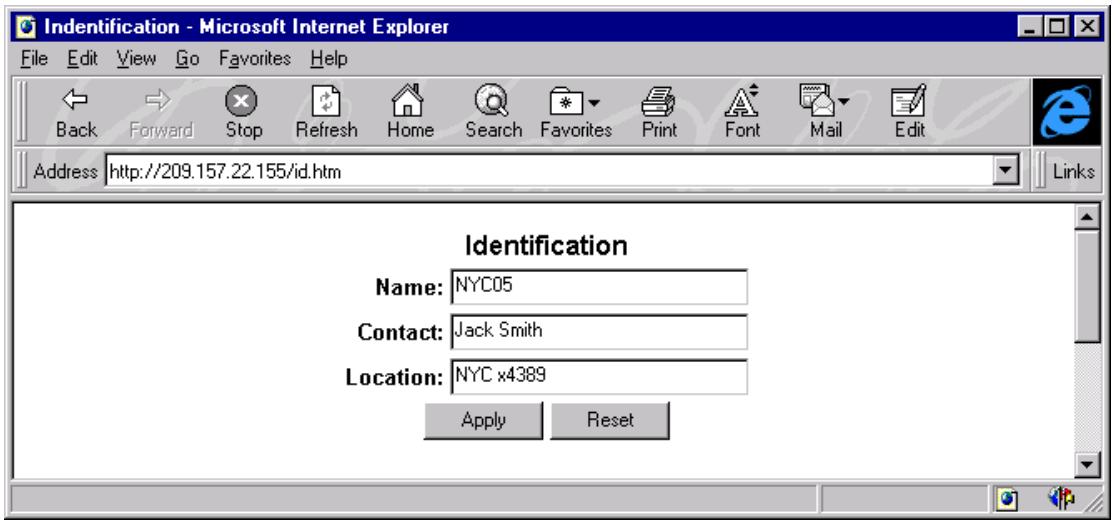

Figure 7.2 Management panel for assigning system contact information and access parameters

Assigning IP Sub-net Addresses

Before attaching equipment or a management station to ports on the router, the user needs to assign individual sub-net IP addresses and masks to each of the ports. By default no IP addresses are assigned.

USING THE CLI

To assign an IP address and mask to a router interface the user would enter the following:

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

NOTE: To define elements for an interface, the user needs to specify the interface by the port number of the module that is being configured as well as the chassis slot number in which the module resides (e.g. ***interface e <slot/port>***) as seen in the above command.

---

syntax: ip address <ip address> <ip mask> OR ip address <ip address /sub-net mask length>

NOTE: The syntax, ***ip address <ip address /sub-net mask length>*** can also be used if the sub-net mask length is known by the user. In the above example, the user would have entered ***ip address 192.22.3.44/24***.

USING THE WEB MANAGEMENT INTERFACE

To assign an IP address and mask to a router interface:

1. Select the IP address link from the System configuration sheet.
2. Select the **slot** and **port** to which the IP address is being assigned.
3. Enter the **IP address**.
4. Enter the sub-net **mask**.
5. Select the **secondary** option if this is not the first IP address being assigned to this interface.
6. Select the **add** button to assign the address to the interface.

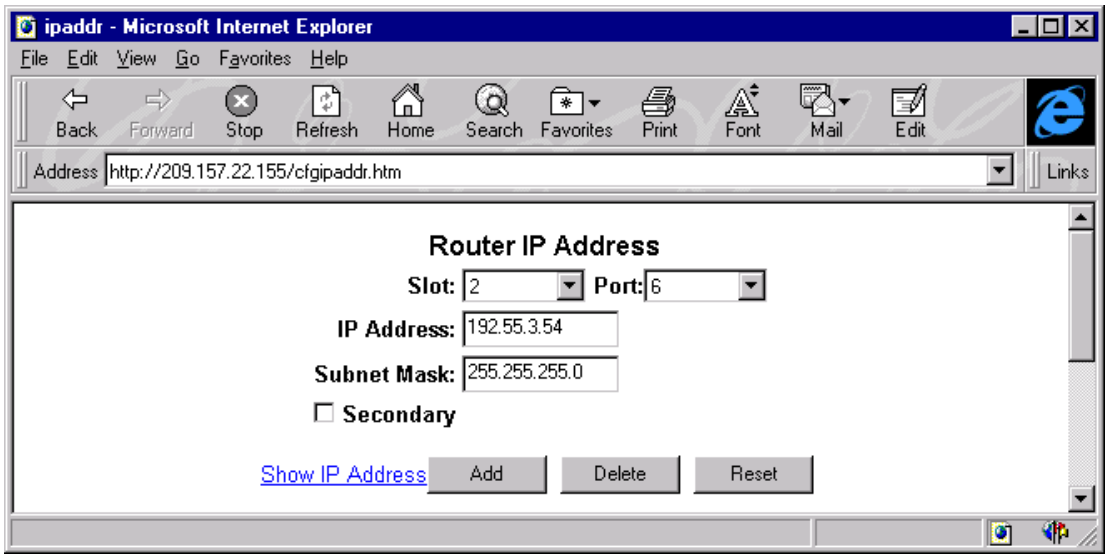

Figure 7.3 Assigning an IP address

Enabling or Disabling SNMP Operation

A user can enable or disable SNMP operation at the system level. SNMP management is by default enabled.

USING THE CLI

To disable SNMP management on a routing switch, the user would enter the following:

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

To later re-enable SNMP management on a routing switch, the user would enter the following:

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

syntax: [no] snmp disable

USING THE WEB MANAGEMENT INTERFACE

To enable or disable SNMP management on a routing switch, the user would do the following:

1. Select the system link. The System configuration sheet will appear.
2. Select the management link. The panel shown in **Figure 7.4** will appear.
3. Enable or disable **SNMP**.
4. Select the **apply** button to assign the change.

Assigning a SNMP Station to Collect Traps

To activate a station as a trap receiver, enter the IP address of the target SNMP station. Up to ten stations can be assigned to operate simultaneously as trap receivers. After assigning the SNMP station IP address, the user should then enter the community string. By default, no community string values will be assigned.

USING THE CLI

To assign a trap receiver, the user would do the following:

```
HP9300(config)# snmp-server trap-receiver 192.22.3.33 public
```

syntax: snmp-server trap-receiver <ip address> <communitystring>

NOTE: In the above example, 'public' refers to the community string.

USING THE WEB MANAGEMENT INTERFACE

To assign a station to act as trap receiver, the user would do the following:

1. Select the management link from the System configuration sheet. The panel seen in **Figure 7.4** will appear.
2. Select the trap receiver link. The panel shown in **Figure 7.5** will appear.
3. Enter the **IP address** of the station that is to serve as the trap receiver.
4. Enter the **community string**.

   NOTE: The community string is initially set with the CLI. The value entered here should match that configured via the CLI.

5. Select the **add** button to assign the changes.

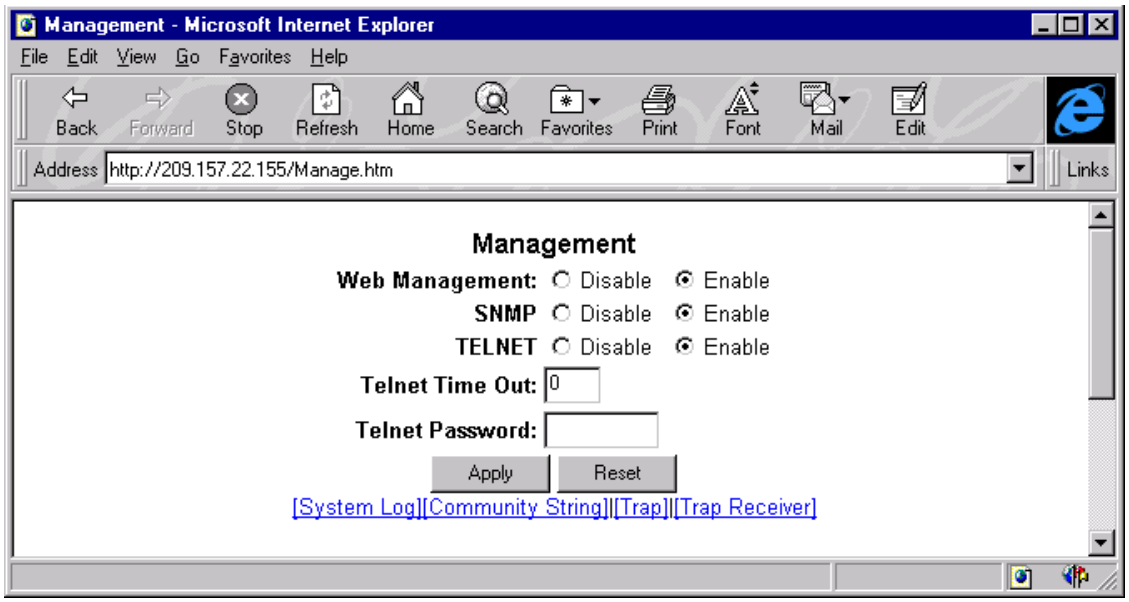

Figure 7.4 Management panel for assigning system contact information and access parameters

Figure 7.5 Trap receiver assignment panel

Modifying SNMP Traps Generated

The HP routing switches come with SNMP trap generation enabled. The user can later modify the traps generated as well as disable the generation of traps altogether.

The following traps are generated on the routing switches: SNMP authentication key, power supply failure, cold start, link up, link down, bridge new root, bridge topology change, locked address violation, addition or deletion of modules and notification of enabling or disabling of OPSF and SRP.

NOTE: By default, all SNMP traps are enabled at system startup.

USING THE CLI

To stop ***link down*** occurrences from being reported, the user would enter the following:

```
HP9300(config)# no snmp-server trap link-down
```

NOTE: For more details on the syntax of this command, please refer to its description in **Appendix B**.

USING THE WEB MANAGEMENT INTERFACE

To modify the SNMP traps generated for a system:

1. Select the management link from the System configuration sheet. The panel seen in **Figure 7.4** will appear.
2. Select the trap link. The panel shown in **Figure 7.6** will appear noting all possible traps and their current state–enabled or disabled.
3. Select the **disable** or **enable** button next to the trap that is to be to modified.
4. Select the **apply** button to save the changes.

Figure 7.6 SNMP trap configuration panel for routing switches

Modifying the Community String

The user can modify the community string for increased security as well as indicate the access type as either public (read only) or private (read/write). A community string can be composed of up to 32 alphanumeric characters.

USING THE CLI

To assign the community string of planet1 with a read access only, the user would enter the following:

```
HP9300(config)# snmp-server community planet1 ro
```

To assign the community string of planet1 with a read/write access, the user would enter the following:

```
HP9300(config)# snmp-server community planet1 rw
```

syntax: `snmp-server community <communitystring> <rw | ro>`

USING THE WEB MANAGEMENT INTERFACE

The community string and access type can only be defined with the CLI. When using the web browser, the user must make sure that the same access type is defined for the Web management interface by selecting the community string link found on the System configuration sheet.

In **Figure 7.7**, the user has configured the web management interface to allow read only access.

.

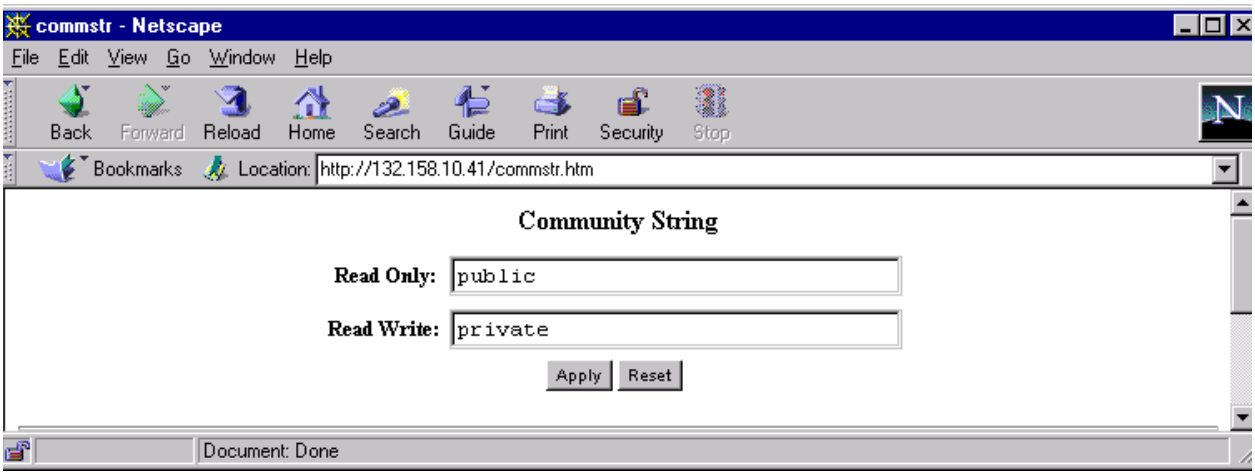

Figure 7.7 Community string configuration panel for defining access

Defining a MAC Address Filter

To define a MAC filter, the user would enter the following:

USING THE CLI

```
HP9300(config)# mac filter 1 deny 1543.6734.366e any snap eq 806
```

syntax: mac filter <index> <permit|deny> <any | H.H.H> <any | H.H.H> <etype | IIc | snap> <operator> <frame type>, *where H = 4 digits as seen in the above example*.

USING THE WEB MANAGEMENT INTERFACE

To define a MAC filter, the user would do the following:

1. Select the MAC filter link from the System configuration sheet. The panel seen in **Figure 7.8** will appear.
2. Select the **permit** or **deny** action.
3. Enter the **source address** and **mask**.
4. Enter the **destination address** and **mask**.

5. Select the **frame type**. The hex number for the frame type should be entered.
6. Select an **operator** to filter by protocol type as well.
7. Enter a **protocol**.
8. Select the **add** button to assign the filter.

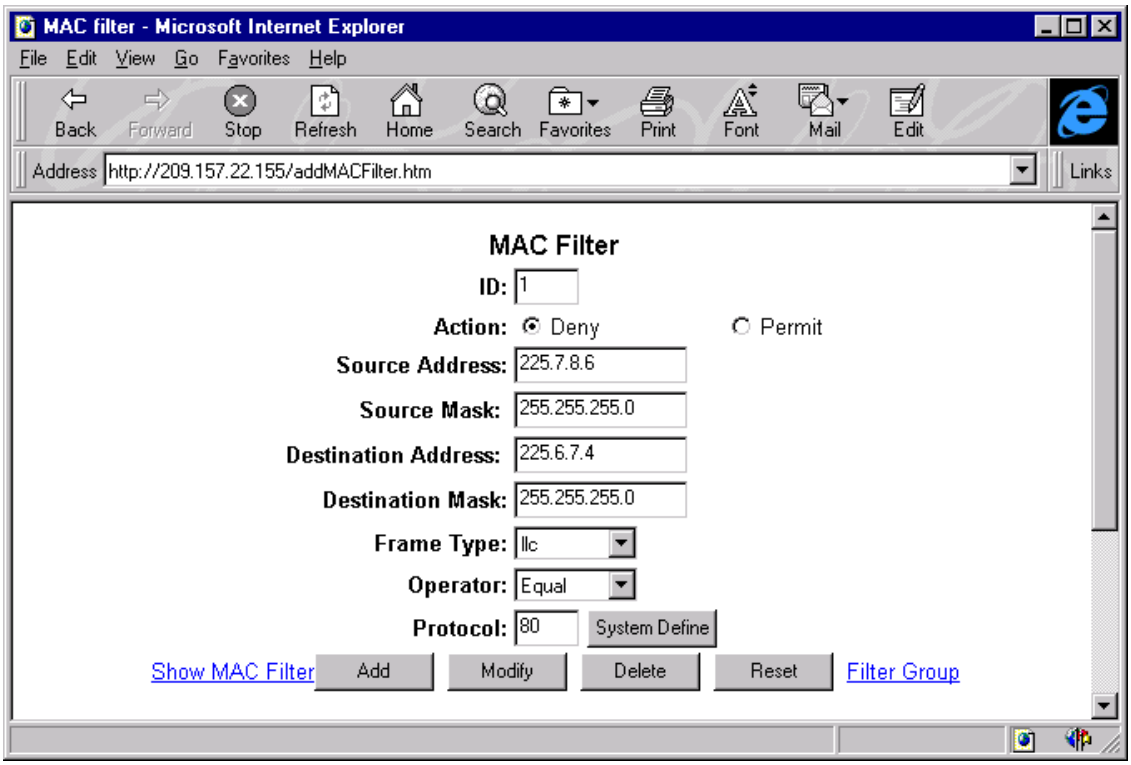

Figure 7.8 Defining a MAC filter

Setting the System Clock

The system clock can be modified for a routing switch. The time and date are set with this command. The time zone is set separately using the clock time zone option. Clock settings are not saved over power cycles; however, the user configure the system to reference a NTP server at power up which can provide a reference time for the routing switch. This server will then automatically download the correct time reference for the network.

For more details on this, refer to the **Establishing a Reference NTP Server** section.

USING THE CLI

To set the system time and date (e.g. 10:15 on October 15, 1998), the user would enter the following:

```
HP9300# clock set 10:15:05 10-15-98
```

syntax: clock set <hh:mm:ss> <mm-dd-yy | mm-dd-yyyy>

USING THE WEB MANAGEMENT INTERFACE

To set the system clock for a routing switch, the user would enter the following:

1. Select the clock link from the System configuration sheet. The panel shown in **Figure 7.9** will appear.
2. Select a **time zone**.
3. Enable or disable **daylight savings**, as appropriate.

4. Enter the current **date**.
5. Enter the current **time**.
6. Select the **apply** button.

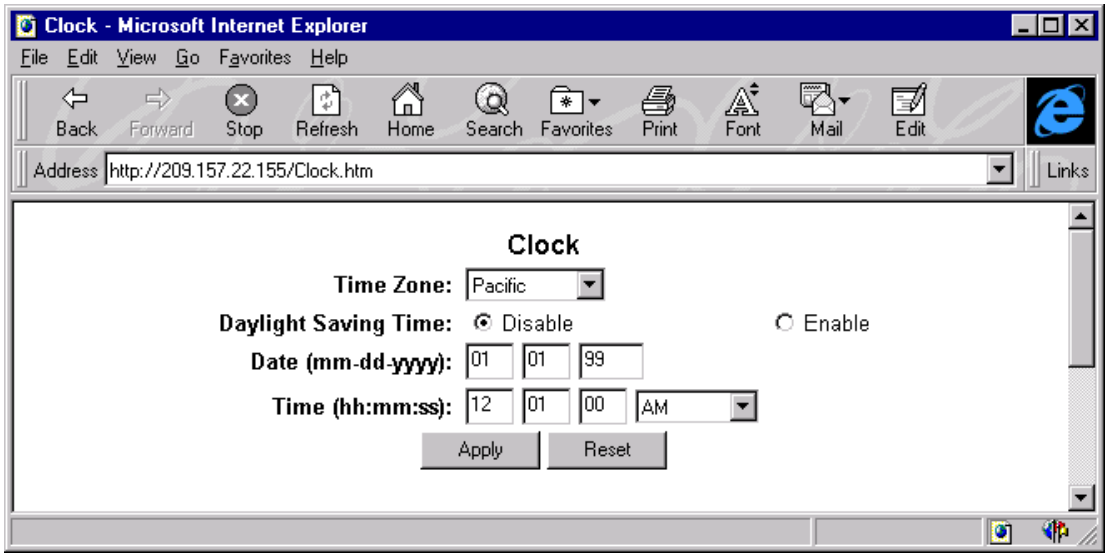

Figure 7.9 Setting the system clock

Establishing a Reference Network Time Protocol (NTP) Server

A SNTP server can be referenced to provide clocking for a routing switch. How often clock updates are sought can also be configured the user.

USING THE CLI

To define a SNTP server (IP address 192.87.5.59) to act as the clock reference for a routing switch, the user would enter the following:

```
HP9300(config)# sntp server 192.87.5.59
```

syntax: sntp server <ip address | hostname>

USING THE WEB MANAGEMENT INTERFACE

To establish a reference NTP server for the system, the user would do the following:

1. Select the NTP link from the System configuration sheet. The panel shown in **Figure 7.10** will appear.
2. Enter the **IP address** of the NTP server.
3. Select the appropriate **version** from the pull down menu.
4. Select the **add** button to assign the changes.

USING THE CLI

To configure the routing switch to poll for clock updates from a SNTP server every 15 minutes, the user would enter the following:

```
HP9300(config)# sntp poll-interval 900
```

syntax: sntp poll-interval <1-65535>

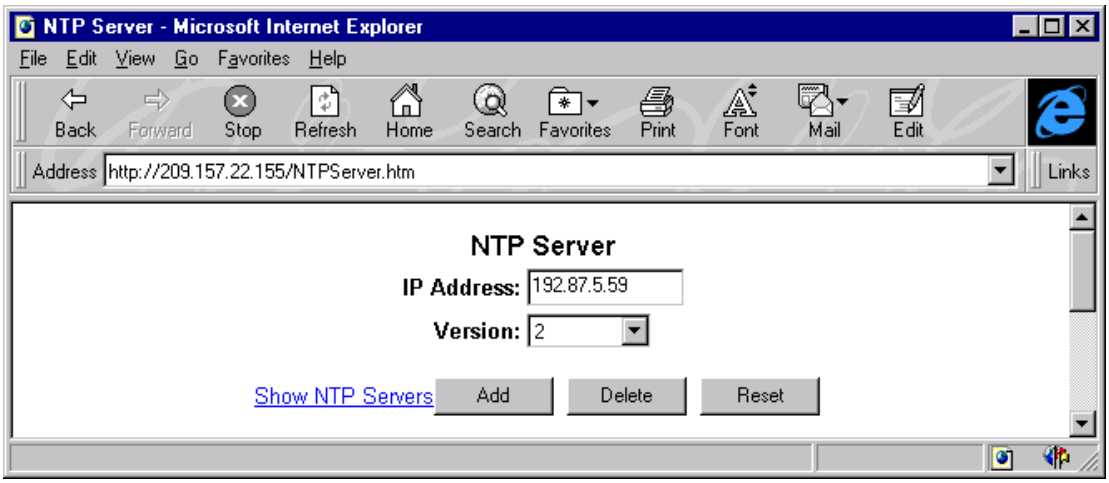

Figure 7.10 Defining a NTP server for a system

Enabling Port-Based and Layer 3 Protocol VLANs

Port and protocol VLANs must first be enabled at the system (global) level before they can be configured at the VLAN level. For details on configuring VLANs, once enabled, refer to **Chapter 14**.

USING THE CLI

When using the CLI, port and protocol-based VLANs are created by entering one of the following commands at the global CONFIG level of the CLI.

To enable a port-based VLAN, the user enters the following command:

```
HP9300(config)# vlan 1
```

Once the VLANs are enabled on the system, the user can create port-based VLANs by entering the following command:

```
HP9300(config)# vlan <1-4095>
```

To create a protocol based VLAN, the user would enter one of the following commands, depending on the protocol VLAN to be defined: appletalk-proto, decnet-proto, ip-proto, ipx-proto, ip-subnet, ipx-network, netbios-proto or other-proto.

```
HP9300(config)# appletalk-proto
```

NOTE: In both examples above, the VLAN enable commands will launch the user into the VLAN level where ports are assigned.

USING THE WEB MANAGEMENT INTERFACE

To enable port-based VLANs on the routing switch:

1. Select the system link from the main menu. The System configuration sheet will appear (**Figure 7.1**).
2. Select the box next to the **port** option next to the policy-based VLANs heading.

To enable protocol-based VLANs on the routing switch:

1. Select the system link from the main menu and the System configuration panel will appear.
2. Select the box next to the **L3 protocol** option next to the policy-based VLANs heading.
3. Select the **apply** button to assign the changes.

Enabling or Disabling Protocols

HP routing switches support all of the following protocols–IP, IPX, OSPF, RIP, DVMRP, PIM, SRP and AppleTalk. IP is by default, active on the router at startup. All other protocols must be enabled at the system level before being configured at the interface level.

In some cases a system reset is required before a protocol is activated on the router. For specific details about this and configuration details on the protocols, refer to their individual chapters.

USING THE CLI

To enable a protocol on a routing switch, the user would enter 'router' at the global CONFIG level, followed by the protocol to be enabled, as shown in the example below which enables OSPF:

```
HP9300(config)# router ospf
HP9300(config)# end
HP9300# write mem
HP9300# reload
```

syntax: router <rip|appletalk|ospf|ipx|srp|dvmrp|pim>

NOTE: The following protocols will require a system reset before the protocol will be active on the system: PIM, DVMRP, RIP and SRP. To reset a system, select the reset option under the File menu (Web) or enter the ***reload*** command at the privileged level of the CLI.

USING THE WEB MANAGEMENT INTERFACE

To enable protocols on a routing switch, the user would do the following:

1. Select the system link from the main menu.
2. Select the **enable** option next to the protocol(s) to be enabled.
3. Select the **save to flash** button.
4. Select the reset link from the main menu to reset the system.

   NOTE: The reset step is not required for AppleTalk and OSPF protocols to become active.

5. Select the **apply** button to assign the change.

Enabling or Disabling the Spanning Tree Protocol (STP)

The STP (IEEE 802.1d bridge protocol) is supported on all routing switches. STP detects and eliminates logical loops in the network. It will also ensure that the least cost path is taken when multiple paths exist between ports or VLANs. Should the selected path fail, STP will search for, and then establish, an alternate path to prevent or limit retransmission of data. STP is by default disabled.

For details on configuring STP at the system level, refer to the **Configuring Spanning Tree Protocol** section of this chapter.

For details on configuring STP on port-based VLANs, refer to **Chapter 14: Configuring VLANs**.

USING THE CLI

To enable STP for all ports on a routing switch, the user would enter the following:

```
HP9300(config)# spanning tree
```

syntax: [no] spanning-tree

USING THE WEB MANAGEMENT INTERFACE

1. Select the system link from the main menu.
2. Select enable next to the **Spanning Tree** option.
3. Select the **apply** button to assign the changes.

Enabling IEEE 802.1Q VLAN Tagging

The VLAN tagging feature allows HP routing switches to support the switching of multiple port-based VLANs across the same physical segment. The default value for this feature is disabled.

NOTE: This parameter is only valid for port-based VLANs.

USING THE CLI

There is no need to enable IEEE tagging at the system level when using the CLI. Tagging is done at the interface level only. For details on assigning tagged ports, refer to the section on **Configuring Port Parameters**.

USING THE WEB MANAGEMENT INTERFACE

When using the Web management interface, VLAN tagging must be enabled at the system (global) level before a port can be tagged at the port (interface) level.

To enable VLAN tagging, the user would do the following:

1. Select the system link from the main menu. The System configuration sheet will appear.
2. Enable the **IEEE 802.1Q tagging** option.
3. Select the **apply** button to assign the change.

Enabling or Disabling Telnet

A user can enable or disable Telnet access at the system level. Telnet access is by default enabled.

USING THE CLI

To disable Telnet operation on a routing switch, the user would enter the following:

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

syntax: [no] telnet-server

USING THE WEB MANAGEMENT INTERFACE

1. Select the system link. The System configuration sheet will appear.
2. Select the management link. The panel shown in **Figure 7.4** will appear.
3. Disable **Telnet**.
4. Select the **apply** button to assign the change.

Modifying Telnet Timeout

A user can modify the period of time that an idle Telnet session will remain before it is automatically logged off. Telnet access is by default enabled. The default timeout value is 0 seconds.

NOTE: To close a Telnet session, the user would enter the ***logout command***.

USING THE CLI

To set a Telnet session to log off after it is idle for 3 minutes, the user would enter the following:

```
HP9300(config)# telnet-timeout 180
```

syntax: telnet-timeout <0-240>

USING THE WEB MANAGEMENT INTERFACE

To set a Telnet session to log off after it is idle for 3 minutes, the user would enter the following:

1. Select the management link on the System configuration sheet. The panel seen in **Figure 7.4** will appear.
2. Verify that Telnet is enabled.
3. Enter a value between 0 and 240 for **telnet time out**.
4. Select the **apply** button to assign the change.

Modifying the Telnet Password

A user can assign a password for Telnet session access. A password can comprise up to 32 alphanumeric characters.

USING THE CLI

To assign a telnet password of secretsalso, the user would enter the following:

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

syntax: enable telnet password <text>

USING THE WEB MANAGEMENT INTERFACE

To assign or modify a Telnet password for a system, the user would do the following:

1. Select the management link on the System configuration sheet. The panel seen in **Figure 7.4** will appear.
2. Verify that Telnet is enabled.
3. Enter a alphanumeric string of up to 32 characters for the **Telnet password**.
4. Select the **apply** button to assign the change.

Enabling or Disabling Layer 2 Switching

HP routing switches support Layer 2 switching. Those protocols not supported on the router will be switched, when this option is enabled. If IPX routing is not enabled, then IPX traffic will be switched also. By default, layer 2 switching is enabled.

USING THE CLI

To disable layer 2 switching on a routing switch, the user would enter the following:

```
HP9300(config)# route-only
HP9300(config)# exit
HP9300# write mem
HP9300# reload
```

To re-enable layer 2 switching on a routing switch, the user would enter the following:

```
HP9300(config)# no route-only
HP9300(config)# exit
HP9300# write mem
HP9300# reload
```

syntax: [no] route-only

USING THE WEB MANAGEMENT INTERFACE

To enable or disable layer 2 switching on a router, the user would:

1. Select the system link from the main menu. The System configuration sheet will appear.
2. Enable or disable the **L2 switching** option.
3. Select the **apply** button to assign the changes.
4. Select the save to flash link from the main menu.
5. Select reset to reboot the system.

Adding or Deleting Modules

When adding modules to a chassis, the user needs to enter the location and type of module. Slot number will be a value between 1 and 4 for a four-slot chassis and 1 and 8 for an eight-slot chassis. Possible modules types are:

- J4141A HP ProCurve 9300 10/100 with management (16 port)
- J4144A HP ProCurve 9300 Gigabit SX management module (8 port)
- J4146A HP ProCurve 9300 Gigabit 4LX/4SX management module (8 port)
- J4140A HP ProCurve 9300 10/100 module (24 port)
- J4142A HP ProCurve 9300 100Base FX module (24 port MT-RJ)
- J4143A HP ProCurve 9300 Gigabit SX module (8 port)
- J4145A HP ProCurve 9300 Gigabit 4LX/4SX module (8 port)

USING THE CLI

To add a module to a chassis, the user would enter the following:

```
HP9300(config)# module <slot number> <module type>
```

syntax: module <slot number> <module type>

USING THE WEB MANAGEMENT INTERFACE

To assign a module to a chassis platform, the user would do the following:

1. Select the module link from the System configuration sheet. A summary panel showing all existing modules installed on the chassis will appear (**Figure 7.11)**.
2. Select the add module link from the module summary panel.
3. Select the **slot** number in which the module will reside from the pull down menu.
4. Select the module **type** from the pull down menu.
5. Select the **add** button to assign the module.

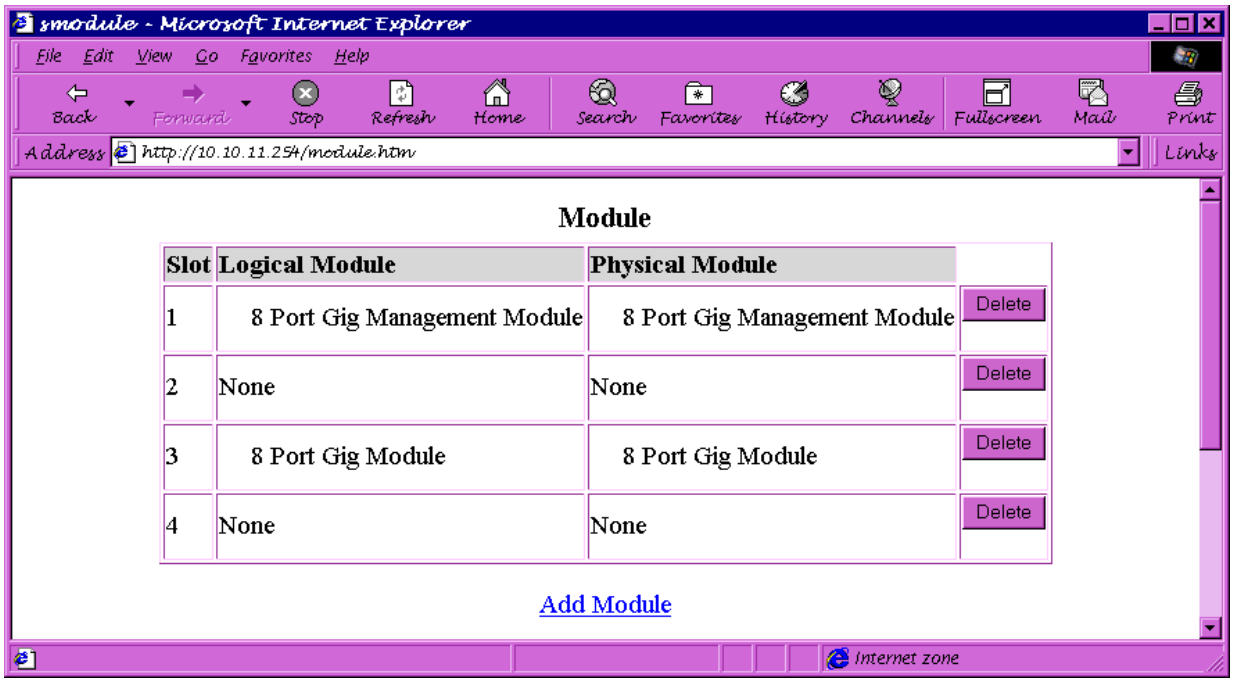

Figure 7.11 Summary module panel

Modifying System Parameters Default Settings

HP routing switches come with a number of system level parameters that come pre-configured with default values. The user can modify the following parameters to adjust to specific network needs via a single point:

- MAC address entries
- Layer 2 Port VLANs supported on a system
- Layer 3 Protocol VLANs supported on a system
- Layer 4 sessions supported
- IP cache size
- ARP entries
- IP routes
- IP route filters
- Static routes
- IGMP
- DVMRP routes
- IPX/SAP entries
- IPX/RIP entries
- IPX/SAP filters
- IPX/RIP filters
- IPX forwarding filters
- AppleTalk routes
- AppleTalk zones

USING THE CLI

When using the CLI, the user would use the ***system...***command found at the global CONFIG level of the CLI to configure the above parameters. For a detailed listing of exact command syntax and possible ranges for the parameters, refer to **Appendix B**.

USING THE WEB MANAGEMENT INTERFACE

To modify system parameters, the user would do the following:

1. Select the parameter link found on the System configuration sheet and the panel shown in **Figures 7.12** and **7.13** will appear.
2. Select the **modify** button next to the parameter to be changed.
3. Enter the new value for the parameter.
4. Select the **add** button to assign the changes

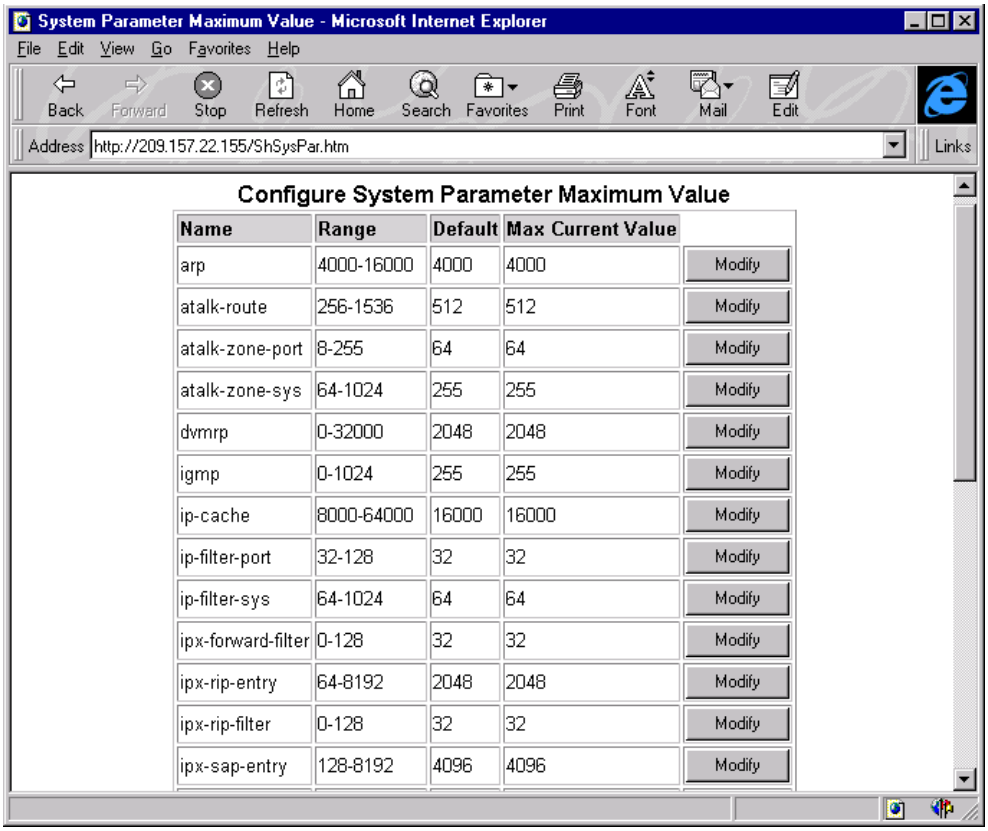

Figure 7.12 System parameter configuration panel (1 of 2)

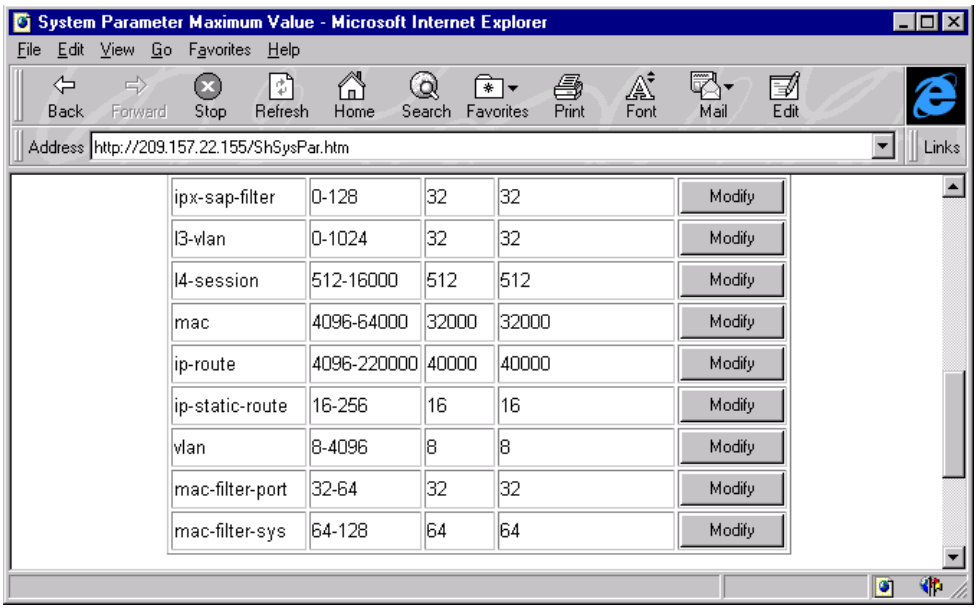

Figure 7.13 System parameter configuration panel (2 of 2)

Modifying Events Collected in the System Log

SNMP traps generated can be saved locally on a routing switch for later review by enabling the system log. Once the system log is enabled, the user can select the type of SNMP events saved to the system log. The user can select or deselect the following categories of events to be saved to an event log: alert, critical, debugging, emergency, error, information, notification and warning.

Up to 100 entries can be stored in the event log. The default value is 50.

USING THE CLI

To establish an event log that will save 75 SNMP traps entries locally on the routing switch, the user would enter the following:

```
HP9300(config)# logging on
HP9300(config)# logging 75
```

syntax: logging <on|off>

syntax: logging <1-100>

NOTE: To disable logging of events the user would enter the ***logging off*** command at the global CONFIG level.

NOTE: The user can later view the events saved on the routing switch by entering the ***show logging*** command. To clear all entries in the event log, the user can select the ***clear logging*** CLI command.

USING THE WEB MANAGEMENT INTERFACE

To enable the collection of SNMP traps in an event log on a local routing switch, the user would:

1. Select the management link found on the System configuration sheet. The panel seen in **Figure 7.4** will appear.
2. Select the system log link. The panel shown in **Figure 7.14** will appear.
3. Select enable next to the **logging** option.
4. To modify the number of entries saved in the event log, enter a value between 1 and 100, for the **buffer size**.
5. Enter the **IP address** of the local system.
6. Select the type of **facility** from the pull down menu.
7. Select the boxes next to the **accept severity** criteria that is to be reported to the event log. A check mark will appear.

NOTE: Criteria with unchecked boxes will not be reported to the event log.

8. Select the **apply** button to assign the change(s).

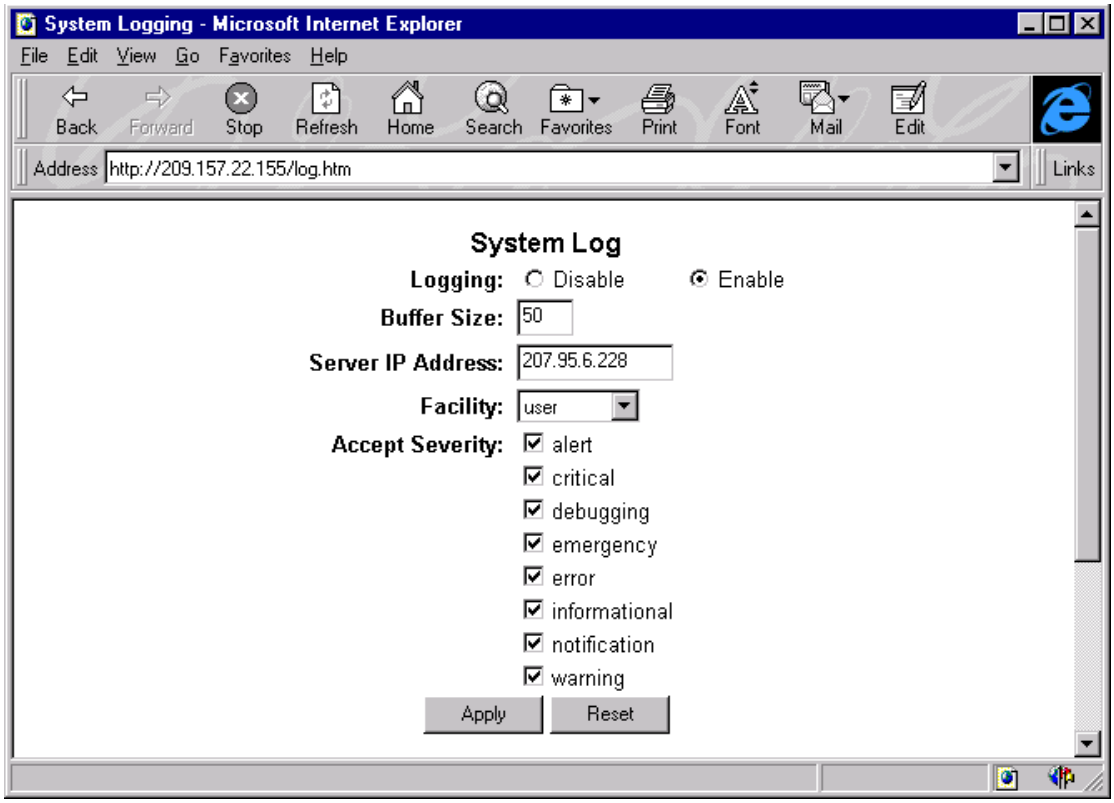

Figure 7.14 System log entry panel to define SNMP traps saved locally

NOTE: The user can later view the events by selecting the system log link from the show panel. The show panel is reached by selecting the show link from the main menu. To clear all entries in the event log, the user can select the clear link from the main menu. The user then selects the box next to the system logging option found on that panel.

Enabling or Disabling Web Management Access

A user can enable or disable the web management interface on a routing switch. By default this feature is enabled on a system.

USING THE CLI

To disable the web management interface on a routing switch, the user would enter the following:

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

syntax: [no] web-management

USING THE WEB MANAGEMENT INTERFACE

1. Select the management link found on the System configuration sheet. The panel seen in **Figure 7.4** will appear.
2. Enable or disable **web management**.
3. Select the **apply** button to assign the change.

Assigning RADIUS Authentication Support

RADIUS is a distributed security system that provides multiple levels of security options to create a very secure dial-in access authentication system. RADIUS is a standard defined by the Internet Engineering Task Force (IETF) and is quickly being adopted throughout the networking industry.

RADIUS combines several security systems:

- Multiple-use password system – A user enters the same password each time he or she logs onto the system. This is a standard password protection system that uses a user ID and password. This system is widely deployed but is vulnerable to attack because multiple-use passwords can be stolen, or even guessed by a computer program using a dictionary, and then used to break into a network.
- Challenge/response system – A system based on single-use passwords. This system usually is accomplished with a special hand-held device that accepts the challenge and computes the correct response. This authentication capability can be distributed among multiple authentication servers for greater security.
- Configuration script – A configuration script dynamically configures a port with optional source destination filters. Each user's network access can be controlled by a set of rules tailored to the individual user, restricting the user to specific areas of the network.

RADIUS is a UDP-based protocol for AAA (authentication, authorization, and accounting) purposes. It provides better security, allowing a company to set up a policy that can be applied at a single administered network point. HP routing switches provide support for RADIUS Authentication with multiple-use password. RADIUS servers can be used to authenticate Telnet or console log ons.

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 routing switch. However, if your network contains a RADIUS server, you can configure all the HP 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 routing switch:

- Login access through Telnet to the CLI using a super-user password.
- Enable access to the CLI using a super-user password.

NOTE: The routing switch does not support RADIUS authentication for read-only and port-configuration passwords.

Authentication Method List

The routing switch authenticates super-user passwords according to an ***authentication-method*** list that you define. The authentication-method list specifies the order in which the routing switch tries the following methods for authenticating a super-user password:

- RADIUS server – Authenticate based on the database on the RADIUS sever.
- Line – Authenticate locally based on the Telnet login password.
- Enable – Authenticate locally based on the Enable password.
- None – Do not perform authentication.

You can specify one, two, three, or all four of these 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 sever but the link to the server is down, the software will try the next authentication method in the list.

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.

NOTE: The software uses separate authentication-method lists for Telnet access and Enable access.

NOTE: The default authentication method is "none". If you configure a RADIUS server, make sure you also configure an authentication-method list.

To use RADIUS within the network, the user must:

1. Access the routing switch using your super-user password.
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.

NOTE: To configure RADIUS authentication, you must access the system using your super-user password.

Configuration Notes

- A RADIUS server is required within the network and only one RADIUS server is supported.
- Only default method lists are supported. The authentication methods are RADIUS server, telnet password, super-user password and no authentication. A default method list can be defined using the above named methods.
- Three concurrent RADIUIS client authentications are allowed.
- Once RADIUS is enabled on a routing switch, all subsequent log ons (e.g. Telnet logins, Privileged (read-write) access, and SNMP access) will be authenticated by the RADIUS server.
- RADIUS accounting is not supported.
- Only default method lists are supported.

USING THE CLI

To assign a server with an IP address of 192.5.19.59 to act as the radius server and enable the radius server to authenticate telnet access, the user would enter the following:

```
HP9300 (config)# radius-server 192.5.19.59
HP9300 (config)# enable telnet authenticate
HP9300 (config)# aaa authenticate login default radius line
HP9300 (config)# aaa authenticate enable default radius line
HP9300 (config)# write memory
```

syntax: radius-server <IP address | name> [auth-port <number>] [acct-port <number>]

syntax: aaa authentication <login|enable> default <method1> [method2] [method3] [method4]

NOTE: When defining the RADIUS server, either an **IP address** or **hostname** (text string) can be entered.

The user can define an **authentication port** number for the RADIUS server. It is optional. The default value for this parameter is 1645.

The user can also define an **accounting port** number for the RADIUS server. It is optional. The default value for this parameter is 1646.

To define an authentication key, the user would enter the following:

HP9300 (config)# radius-server codeword timeout 7 retransmit 5

syntax: radius-server [key <key string>] [timeout <number>] [retransmit <number>]

NOTE: The user can assign an **authentication key** using the values between 1 and 16.

A **timeout** value can be set for the RADIUS server. This value can any number between 1 and 20. The timeout value is the number of seconds a routing switch will wait for a response from a RADIUS server to an authentication request. The default timeout is 3 seconds.

A **retransmit** value can also be set for the RADIUS server. It defines the maximum number of times an authentication request will be forwarded to the RADIUS server for validation before it is timed out.

The default retransmit value is 3 seconds. The possible retransmit value is between 1 and 6.

USING THE WEB MANAGEMENT INTERFACE

To define a system as a RADIUS server, the user would do the following:

1. Select the radius link from the System configuration sheet. The panel seen in **Figure 7.15** will appear.
2. Select the radius server link. The panel seen in **Figure 7.16** will appear.
3. Enter the **IP address** of the system to serve as the RADIUS server for the network.
4. Modify the **auth** (authentication) **UDP port** value if desired.
5. Modify the **acct** (accounting) **UDP port** value if desired.
6. Select the **add** button to assign the change.

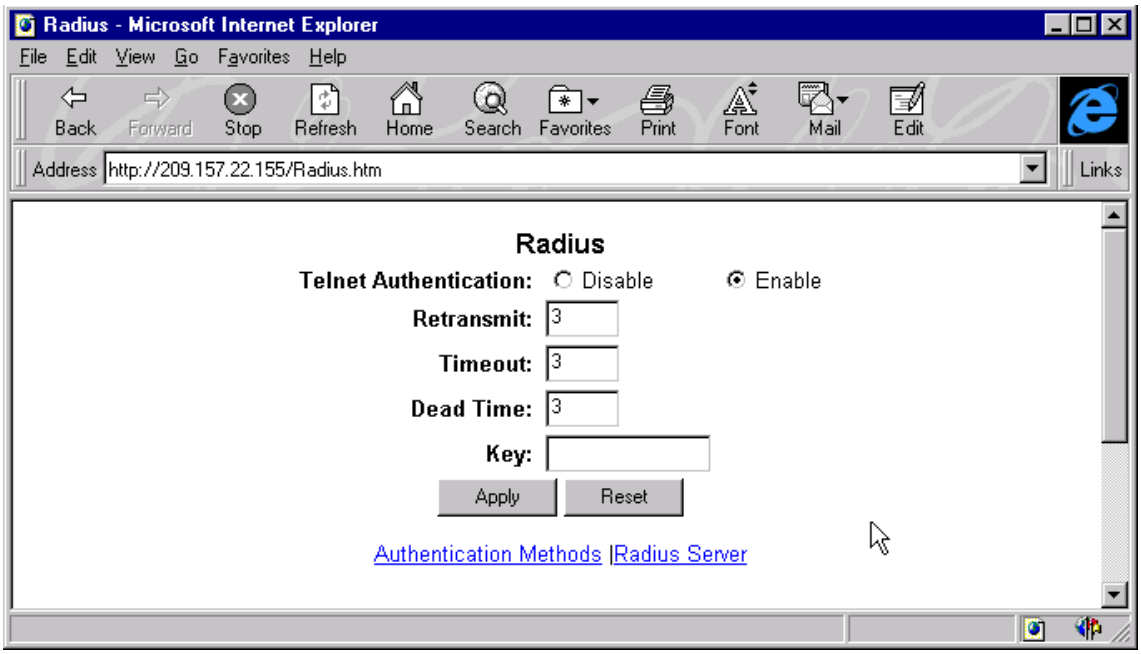

Figure 7.15 Global parameter entry and display panel for radius servers

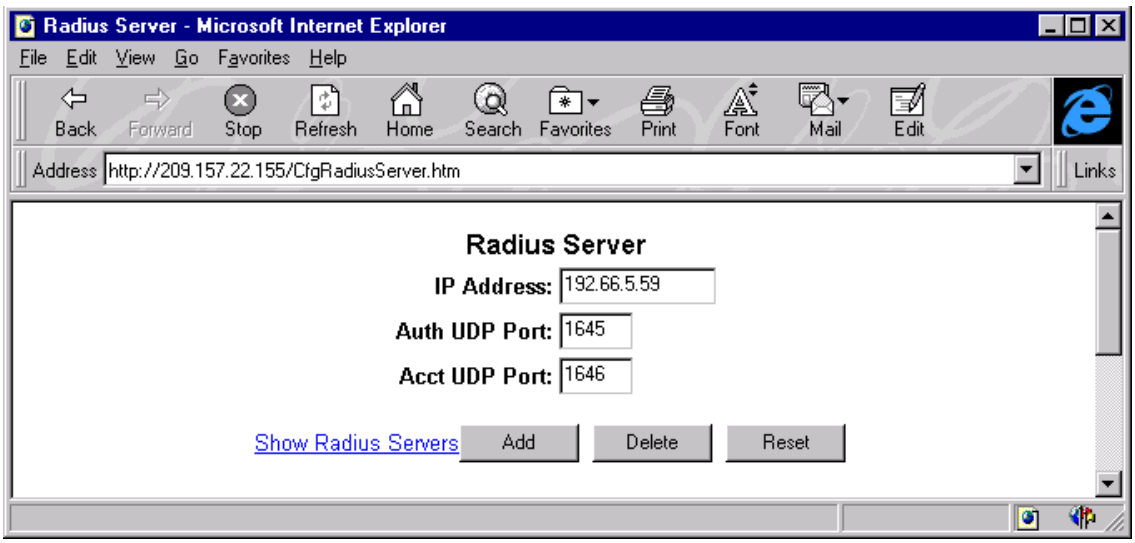

Figure 7.16 Defining a network server to act as radius server for the network

To assign the authentication method used by the RADIUS server, the user would do the following:

1. Select the radius link on the System configuration sheet.
2. Select the authentication methods link from the radius configuration panel. The panel seen in **Figure 7.17** will appear.
3. Select the **type** of activity to be monitored by the RADIUS server from the pull down menu.
4. Select the **show sequence** button to display which authentication methods are configured for the system.
5. Select the **authentication method** to be used:enable, radius, line or none.
6. Select the **add** button to assign the change.

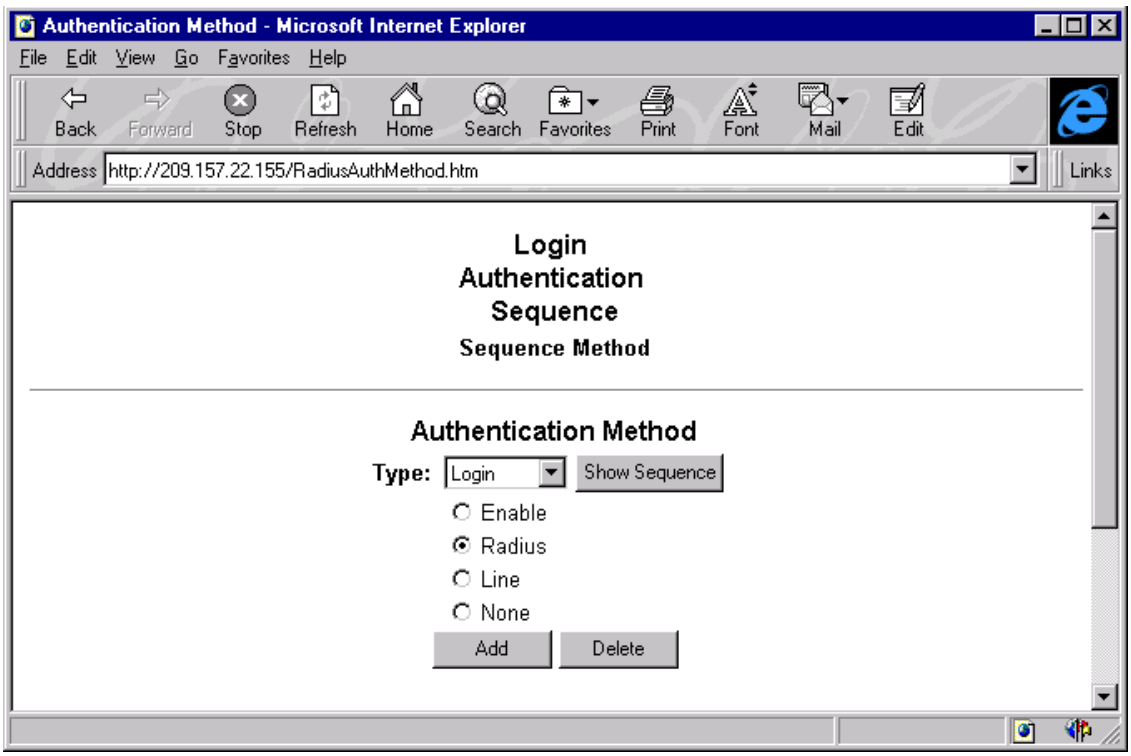

Figure 7.17 Defining the type of authentication method for a radius server

Configuring Port Parameters

The current port configuration for all ports will be displayed when the user selects the Port link from the main menu. To modify a specific port's configuration, the user must select the modify button beside a given port's configuration summary and the panel shown in **Figure 7.18** will appear.

The user can make the following configuration changes to a port:

- Modify port speed
- Assign a port name
- Modify port duplex mode
- Disable or enable port status
- Enable or disable flow control
- Enable or disable auto-negotiate
- Modify port priority (QoS)
- Enable or disable port monitoring
- Enable or disable lock address and define its parameters
- Assign IEEE (802.1q) tagging
- Enable or disable Spanning Tree Protocol (STP)

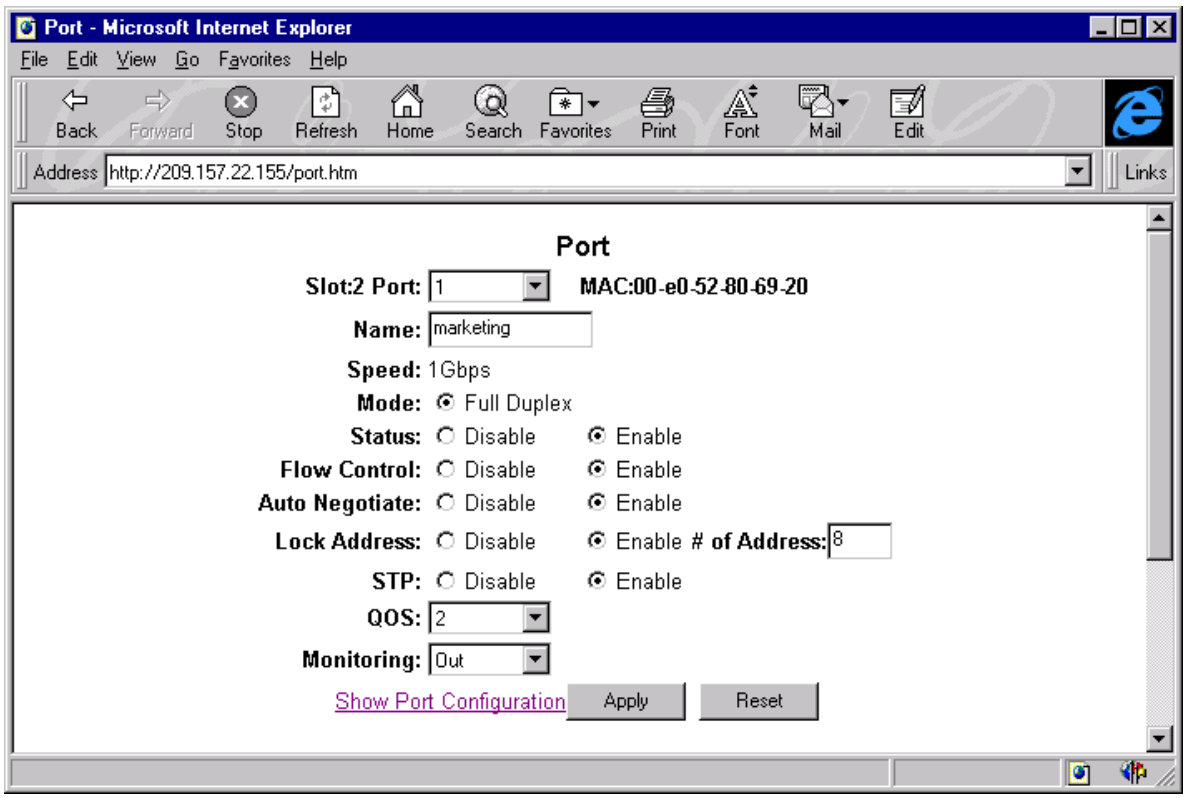

Figure 7.18 Port configuration sheet

NOTE: The IEEE Tagging option will only be seen on the Port configuration sheet when tagging is enabled at the system level and a VLAN is defined on the system.

NOTE: The port speed option of **1 Gbps** will only display when a 1000BaseSX or 1000BaseLX/SX gigabit module is resident in the routing switch. Additionally, only the full-duplex mode will be seen. When an Ethernet module is being configured, the options will be 10/100 Auto, 10 Mbps and 100Mbps.

Modifying Port Speed

Each of the 10/100BaseTX ports is designed to auto-sense and auto-negotiate the speed and mode of the connected device. Should the attached device not support this operation, you can manually enter the port speed to operate at either 10 Mbps or 100 Mbps. The default value for 10/100BaseTX ports is 10/100 auto-sense.

The 100BaseFX ports operate in the full-duplex mode at 100 Mbps only and cannot be modified.

The 1000BaseSX and 1000BaseLX ports operate in the full-duplex mode at 1 gigabit only and cannot be modified.

USING THE CLI

To change the port speed of interface 8 (slot 2) from the default of 10/100 auto-sense to 10 Mbps operating at full-duplex, enter the following:

```
HP9300(config)# interface e 2/8
HP9300(config-if-2/8)# speed-duplex 10-full
```

syntax: speed-duplex <10-full | 10-half | 100-full | 100-half | auto>

USING THE WEB MANAGEMENT INTERFACE

To modify port speed:

1. Select the port link from the main menu. A port summary panel will appear.
2. Select the **modify** button next to the port that is to be modified. The configuration panel seen in **Figure 7.18** will appear.
3. Select the **speed** and **mode** options and make the appropriate changes.
4. Select the **apply** button to assign the new configuration.

NOTE: Remember, before leaving the screen, the **apply** button must be selected for the port parameters to be assigned. Additionally, the configuration changes must be saved to flash (via the File menu) for the changes to be preserved over a power cycle.

Assigning a Port Name

A port name can be assigned to help identify a segment in the network.

USING THE CLI

To assign a name to a port, the user would enter the following:

```
HP9300(config)# interface e 2/8
HP9300(config-if-2/8)# port-name pdtmarketing
```

syntax: port-name <text>

USING THE WEB MANAGEMENT INTERFACE

1. Select the port link from the main menu.
2. Enter a **name** for the port.
3. Select the **apply** button to assign the change.

Modifying Port Duplex Mode

This allows a port to be configured to accept either full-duplex (bi-directional) or half-duplex (uni-directional) traffic. This option is only available when a port is configured to operate at 10 or 100 Mbps. The 1000BaseSx and 1000BaseLx ports only operate at full-duplex.

USING THE CLI

Port duplex mode and port speed are modified by the same command.

To change the port speed of interface 8 (slot 2) from the default of 10/100 auto-sense to 10 Mbps operating at full-duplex, the user would enter the following:

```
HP9300(config)# interface e 2/8
HP9300(config-if-2/8)# speed-duplex 10-full
```

syntax: speed-duplex <10-full | 10-half | 100-full | 100-half | auto>

USING THE WEB MANAGEMENT INTERFACE

To modify port duplex, the user would do the following:

1. Select the port link from the main menu. A port summary panel will appear.
2. Select the **modify** button next to the port that is to be modified. The configuration panel seen in **Figure 7.18** will appear.
3. Select the desired port **mode** option.
4. Select the **apply** button to assign the new configuration.

NOTE: Remember, before leaving the screen, the **apply** button must be selected for the port parameters to be assigned. Additionally, the configuration changes must be saved to flash (via the File menu) for the changes to be preserved over a power cycle.

Disable or Enable Port Status

The port can be made inactive (disable) or active (enable) by selecting the appropriate option under the **status** parameter. The default value for a port is enabled.

USING THE CLI

To disable port 8 on module 1 of a chassis, enter the following:

```
HP9300(config)# interface e 1/8
HP9300(config-if-1/8)# disable
```

syntax: <disable | enable>

USING THE WEB MANAGEMENT INTERFACE

To disable or enable a port:

1. Select the Port link from the main menu. A port summary panel will appear.
2. Select the **modify** button next to the port that is to be modified. The configuration panel seen in **Figure 7.18** will appear.
3. Select either enable or disable option next to the **status** option.
4. Select the **apply** button to assign the new configuration.

NOTE: Remember, before leaving the screen, the **apply** button must be selected for the port parameters to be assigned. Additionally, the configuration changes must be saved to flash (via the File menu) for the changes to be preserved over a power cycle.

Enable or Disable Flow Control

The user can option full-duplex ports on a system to operate with or without flow control (802.3x). Flow control is on, by default, at startup.

USING THE CLI

To disable flow control on full-duplex ports on a system, enter the following:

```
HP9300 (config)# no flow-control
```

To turn the feature back on, the user would enter the command:

```
HP9300 (config)# flow-control
```

syntax: [no] flow-control

USING THE WEB MANAGEMENT INTERFACE

To disable or enable flow control on full-duplex ports on a system, enter the following:

1. Select the port link from the main menu. A port summary panel will appear.
2. Select the **modify** button next to the port that is to be modified. The configuration panel seen in **Figure 7.18** will appear.
3. Select either enable or disable option next to the **flow control** option.
4. Select the **apply** button to assign the new configuration.

NOTE: Remember, before leaving the screen, the **apply** button must be selected for the port parameters to be assigned. Additionally, the configuration changes must be saved to flash (via the File menu) for the changes to be preserved over a power cycle.

Enable or Disable Auto-Negotiate

The user can enable auto-negotiating on a gigabit interface in accordance with the flow control specification 802.3x. Both sides of the gigabit circuit need to be configured with this option for it to operate.

NOTE: This feature is only seen on the Port configuration sheet for gigabit ports.

USING THE CLI

To enable auto-negotiation on gigabit interface 17 (slot 2) on router1, enter the following:

```
Router1(config)# int e 2/17
Router1(config-if-2/17)# auto-gig
```

To disable auto-negotiation on gigabit interface 17 (slot 2), enter the following:

```
Router1(config-if-2/17)# no auto-gig
```

syntax: [no]auto-gig

USING THE WEB MANAGEMENT INTERFACE

To enable or disable auto-negotiation on a gigabit port, the user would:

1. Select the port link from the main menu. A port summary panel will appear.
2. Select the **modify** button next to the port that is to be modified. The configuration panel seen in **Figure 7.18** will appear.
3. Select either enable or disable option next to the **auto-negotiate** option.
4. Select the **apply** button to assign the new configuration.

NOTE: Remember, before leaving the screen, the **apply** button must be selected for the port parameters to be assigned. Additionally, the configuration changes must be saved to flash (via the File menu) for the changes to be preserved over a power cycle.

Modify Port Priority (QOS)

This feature is one of the Selectable Quality of Service (QoS) options available on routing switches. It allows a given MAC address, port or VLAN to be given a higher priority than other comparable entities. Up to eight levels of priority can be assigned with 0 being the lowest priority and 7 the highest, however; only 4 queues are supported internal to the platform. The following assignments will yield the following priorities:

- Configured priority value of 0 or 1 assigns an internal priority queue of 0
- Configured priority value of 2 or 3 assigns an internal priority queue of 1
- Configured priority value of 4 or 5 assigns an internal priority queue of 2
- Configured priority value of 6 or 7 assigns an internal priority queue of 3

NOTE: The default value for port priority is zero.

USING THE CLI

EXAMPLE: To assign a priority to port 5 of a module resident in slot 1 of a chassis, enter the following:

```
HP9300(config)# interface e 1/5
HP9300(config-if-1/5)# priority 5
```

syntax: priority <0-7>

USING THE WEB MANAGEMENT INTERFACE

To assign or enable a port:

1. Select the port link from the main menu. A port summary panel will appear.
2. Select the **modify** button next to the port that is to be modified. The configuration panel seen in **Figure 7.18** will appear.
3. Select the appropriate value form the **qos** pull down menu.
4. Select the **apply** button to assign the new configuration.

NOTE: Remember, before leaving the screen, the **apply** button must be selected for the port parameters to be assigned. Additionally, the configuration changes must be saved to flash (via the File menu) for the changes to be preserved over a power cycle.

Enable or Disable Port Monitoring

This allows a user to select a port to be monitored for diagnosed by a designated mirror port. A user can configure incoming, outgoing or both incoming and outgoing traffic to be monitored on the port. The default value for this feature is disabled.

NOTE: The mirror port feature must be enabled at the system level before monitoring can be done on an individual port.

USING THE CLI

EXAMPLE: To turn on monitoring and diagnose both incoming and outgoing traffic for port 5 of a module resident in slot 1 of the chassis, enter the following:

```
HP9300(config)# interface e 1/5
HP9300(config-if-1/5)# monitor both
```

syntax: monitor <input | output | both>

USING THE WEB MANAGEMENT INTERFACE

To enable monitoring and diagnose both incoming and outgoing traffic on a port, the user would do the following:

1. Select the port link from the main menu and the port summary panel will appear.
2. Select the **modify** button next to the port that is to be modified. The configuration panel seen in **Figure 7.18** will appear.
3. Select both from the **monitoring** pull down menu.
4. Select the **apply** button to assign the new configuration.

NOTE: Remember, before leaving the screen, the **apply** button must be selected for the port parameters to be assigned. Additionally, the configuration changes must be saved to flash (via the File menu) for the changes to be preserved over a power cycle.

Locking a Port to Restrict Address Access

This allows a user to limit the number of devices that have access to a specific port. Access violations will be reported as a SNMP trap. By default this feature is disabled. A maximum of 2,048 entries can be specified for access. The default address count is eight.

USING THE CLI

EXAMPLE: To enable lock address for port 2 on module 3, and place a limit of 15 entries, the user would enter:

```
HP9300(config)# lock e 3/2 addr 15
```

syntax: lock-address ethernet <slot/port number> [addr-count <number>]

USING THE WEB MANAGEMENT INTERFACE

To enable lock address on a port:

1. Select the Port link from the main menu. A port summary panel will appear.
2. Select the **modify** button next to the port that is to be modified. The configuration panel seen in **Figure 7.18** will appear.
3. Select enable next to the **lock address** option.
4. Enter the maximum number of entries that will be allowed access to the port in the **# lock address** field if a value other than the default value of 8 is desired.
5. Select the **apply** button to assign the new configuration.

Assign IEEE (802.1Q) Tagging to a Port

When a port is tagged, it allows communication among the different VLANs to which it is assigned. A common use for this might be to place an email server that multiple groups may need access to on a tagged port, that in turn, is resident in all VLANs that members need access to the server. By default this feature is disabled.

For details on configuring port-based VLANs refer to **Chapter 13**.

USING THE CLI

When using the CLI, ports are defined as either tagged or untagged at the VLAN level.

EXAMPLE: A user wants to make port 5 (slot 2), a member of port-based VLAN 4, a tagged port, so she or he enters the following:

```
HP9300 (config)# vlan 4

HP9300 (config-vlan-4)# tagged e 2/5
```

syntax: tagged-ethernet <slot/port >

USING THE WEB MANAGEMENT INTERFACE

To configure a port as tagged, the user would do the following:

1. Select the Port link from the main menu. A port summary panel will appear.
2. Select the **modify** button next to the port that is to be modified. The configuration panel seen in **Figure 7.18** will appear.
3. Enable **IEEE Tagging**.
4. Select the **apply** button to assign the new configuration.

NOTE: To assign tagging to a port, both the port-based VLAN and IEEE (802.1Q) tagging options must be enabled on the System configuration sheet first.

Enabling Monitoring on a Port

Monitoring traffic on a port is a two step process. First the user must enable a port to act as the mirror port and then secondly he or she must identify the port on which the traffic is to be monitored (i.e. the monitor port).

USING THE CLI

EXAMPLE: A user wants to diagnose the input and output on traffic on port 3 on a module in slot 4 of a routing switch via port 1 in slot 4, to do so the user would enter the following:

```
HP9300(config)# mirror-port e 1/4

HP9300(config)# interface e 4/3

HP9300(config-if-4/3)# monitor both
```

syntax: mirror-port ethernet <slot/port>

NOTE: To monitor just the input traffic the user would enter 'in' instead of 'both' in the above command. To monitor the output traffic the user would enter 'out' instead of 'both' in the above command.

USING THE WEB MANAGEMENT INTERFACE

A user wants to diagnose the input and output on traffic on port 3 on a module in slot 4 via port 1 of the same module, to do so the user would:

1. Select the advance... link frm the System configuraton sheet.
2. Select the value of 4 from the mirror slot pull down menu and the value of 1 from the mirror port pull down menu. This will establish port 1 of the module found in slot 4 on the chassis as the mirror port.
3. Select the **apply** button to assign the changes.
4. Select the port link and the port summary panel will appear.
5. Select the **modify** button next to the 4/3 slot/port combination. The port configuration panel will appear.
6. Select **both** from the **monitoring** pull down menu to initiate diagnosis on both input and output traffic on port 3.
7. Select the **apply** button to assign the changes.

Configuring STP

STP (IEEE 802.1d bridge protocol) is supported on all routing switches. When active, it will detect and eliminate logical loops in the network. It will also ensure that the most efficient path is taken when multiple paths exist between ports or VLANs. Should the selected path fail, STP will search for and then establish an alternate path to prevent or limit retransmission of data. By default, this feature is disabled on routing switches.

NOTE: If a routing switch is configured to operate without VLANs, then the STP bridge parameters will apply to all ports. However, the user can individually configure the STP values—priority and path cost. If a system is configured to operate with VLANs, then the STP bridge parameters seen in **Figure 7.19** can individually be configured or globally applied to each port-based VLAN on the system.

NOTE: Spanning Tree must be enabled at the system level before any of its parameters can be modified.

USING THE CLI

To enable spanning tree on a routing switch, the user would enter the following:

```
HP9300 (config)# span
```

syntax: span [ethernet <portnumber> path-cost <value> priority <value>] forward-delay <value> hello-time <value> maximum-age <time> priority <value>

NOTE: The user can also modify global and port STP parameters at the same time the feature is enabled or separately as shown in the next section example and in the syntax above.

USING THE WEB MANAGEMENT INTERFACE

Spanning tree is enabled on the System configuration sheet.

Modifying Bridge and Port STP Parameters

The user can modify the following STP Parameters:

1. Modify bridge parameters—forward delay, maximum age, hello time and priority
2. Modify port parameters—priority and path cost

Bridge Parameters

Listed below is a description of the bridge parameters noting their possible and default values.

- Forward Delay: The period of time a bridge will wait (the listen and learn period) before forwarding data packets. Possible values are 4 to 30 seconds. The default value is15.
- Maximum Age: The interval a bridge will wait for receipt of a hello packet before initiating a topology change. Possible values are 6 to 40 seconds. The default value is 20.
- Hello Time: The interval of time between each configuration BPDU sent by the root bridge. Possible values are 1 to 10 seconds. The default value is 2.
- Priority: A parameter used to identify the root bridge in a network. The bridge with the lowest value has the highest priority and is the root. Possible values are 0-65,535. The default value is 32,678.

Port Parameters

STP port parameters—priority and path cost come pre-configured with default values. If the default parameters meet your network requirements, no other action is required.

Listed below is a description of the STP port parameters noting their possible and default values.

- Port Priority**:** This parameter can be used to assign a higher (or lower) priority to a port. This will give a port forwarding preference over lower priority ports within a VLAN or on the routing switch (when no VLANs are configured for the system); in the event traffic is re-routed. Ports are re-routed based on their priority, with the highest value being routed first. Possible values are 0 to 255. The default value is 128.

- Path Cost: This parameter can be used to assign a higher or lower path cost to a port. This value can be used to bias traffic toward or away from a certain path during periods of rerouting. For example, if you wish to bias traffic away from a certain port, you would assign it a higher value than other ports within the VLAN or all other ports (when VLANs are not active on the routing switch). Possible values are 0 to 65535 and the default values are 1000/port speed for half-duplex ports and 1000/port speed)/2 for full-duplex ports.

USING THE CLI

The user wants to enable spanning tree on a system in which no port-based VLANs are active and change the hello-time from the default value of 2 to 8 seconds. Additionally, the user wants to change the path and priority costs for port 5 only. The user would enter the following commands.

```
HP9300 (config)# span hello-time 8
```

```
HP9300 (config)# span ethernet 5 path-cost 15 priority 64
```

syntax: span [ethernet <portnumber> path-cost <value> priority <value>] forward-delay <value> hello-time <value> maximum-age <time> priority <value>

USING THE WEB MANAGEMENT INTERFACE

To modify the bridge parameters, the user should do the following:

1. Select the **modify** button next to the STP bridge summary panel. The entry panel seen in **Figures 7.19** will appear.
2. Enter the desired changes and select the **apply** button to save the changes.

To modify the STP port parameters, the user should do the following:

1. Select the **modify** button next to the STP port summary panel. The entry panel seen in **Figure 7.19** will appear.
2. Enter the desired changes to the priority and path cost fields, seen at the bottom of the screen, and select the **apply port STP** button to save the changes.

NOTE: If the user wants to save the priority and path costs of one port to all other ports on the routing switch within a VLAN, the user can select the **apply to all ports** button.

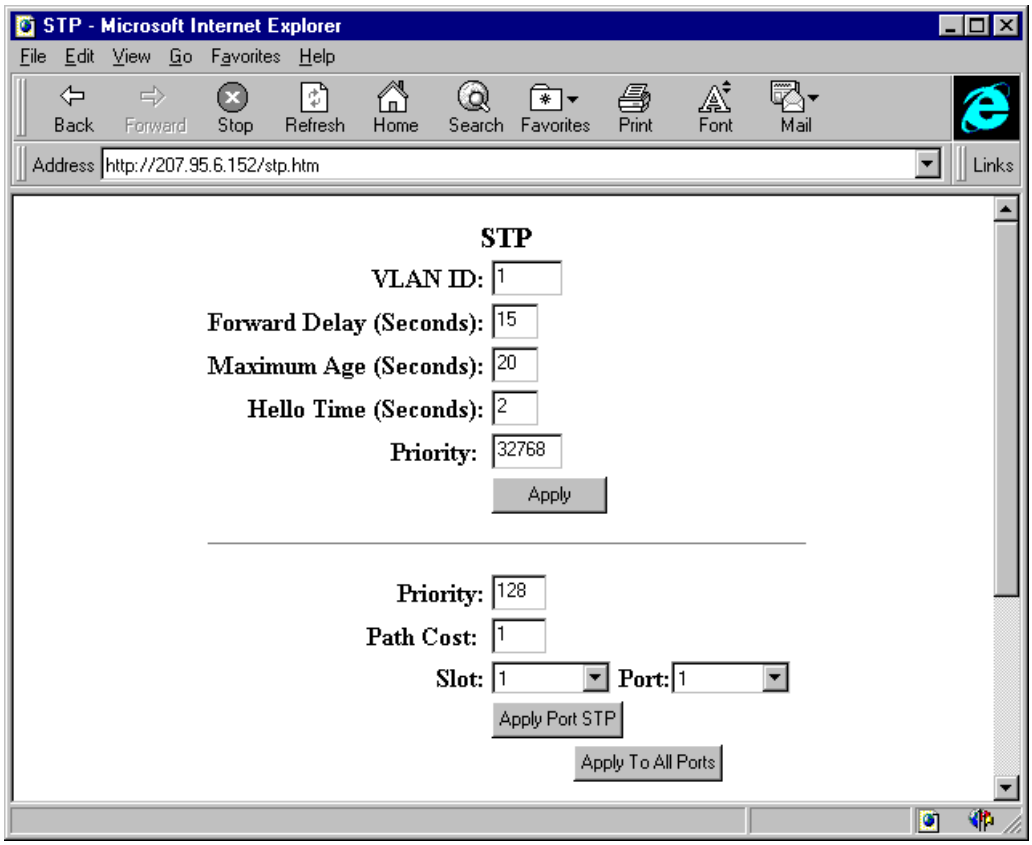

Figure 7.19 STP configuration panel

Configuring Static MAC Entries

Static MAC addresses can be assigned to routing switches.

NOTE: HP routing switches also support the assignment of static IP Routes, static ARP and static RARP entries. For details on configuring these types of static entries, please refer to **Chapter 8: Configuring IP and IP/RIP**.

The user can manually input the MAC address of a device to prevent it from being aged out of the system address table.

This option can be used to prevent traffic from a specified device, such as a server, from flooding the network with traffic when it is down. Additionally, the static MAC address entry is used to assign higher priorities to specific MAC addresses. VLAN membership (VLAN ID) can also be defined for the static MAC entry.

HP routing switches support up to 32,000 addresses with a default setting of 16,000 addresses.

USING THE CLI

To add a static entry for a server with a MAC address of 1145.5563.67FF and a priority of 7 to port 2 of module 1 of a routing switch, the user would enter the following:

```
HP9300(config)# static 1145.5563.67FF e 1/2 priority 7
```

syntax: static <mac address> ethernet <slot/port> priority <0-7>

USING THE WEB MANAGEMENT INTERFACE

1. Select static station from the main menu. The panel shown in **Figure 7.20** will appear.

   NOTE: If static MAC address entries already exist, a summary panel will appear when the user selects static station. The user can then get to the static station entry panel, by selecting add static station.

2. Enter the 12-digit **MAC address** of the device requiring a static entry.
3. Enter the device **VLAN ID**, if it is a member of a port-based VLAN.
4. Select the **slot** and **port** number of the segment upon which the equipment is attached.
5. Select a QoS (priority) level between 0 and 7 from the pull down menu.
6. Select the **add** button.

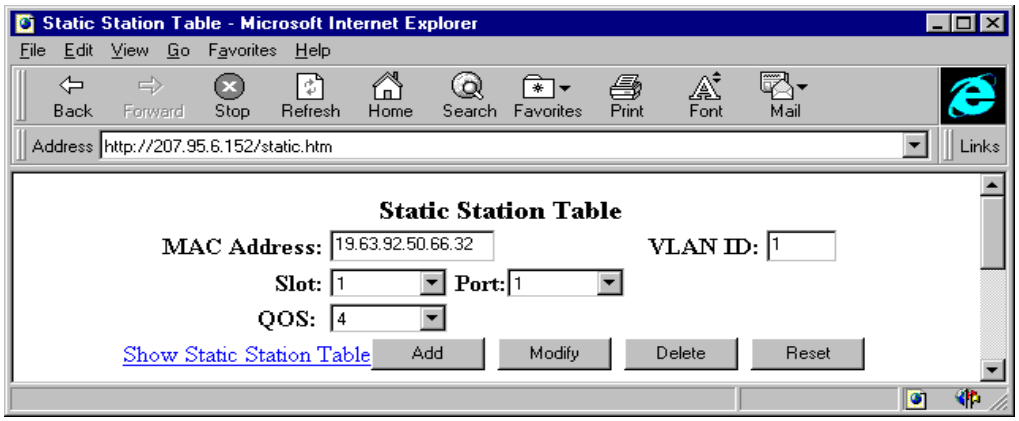

Figure 7.20 Assign a static MAC address

Trunk Groups

Overview

The Trunk Group feature allows multiple high-speed load-sharing links to be established between two routing switches or between a routing switch and a server. This feature allows two or four ports to be configured as a trunk group, supporting transfer rates of up to 4 Gbps of bi-directional traffic.

In addition to enabling load sharing of traffic, trunk groups provide redundant, alternate paths for traffic should any of the segments fail. The default value for this feature is disabled.

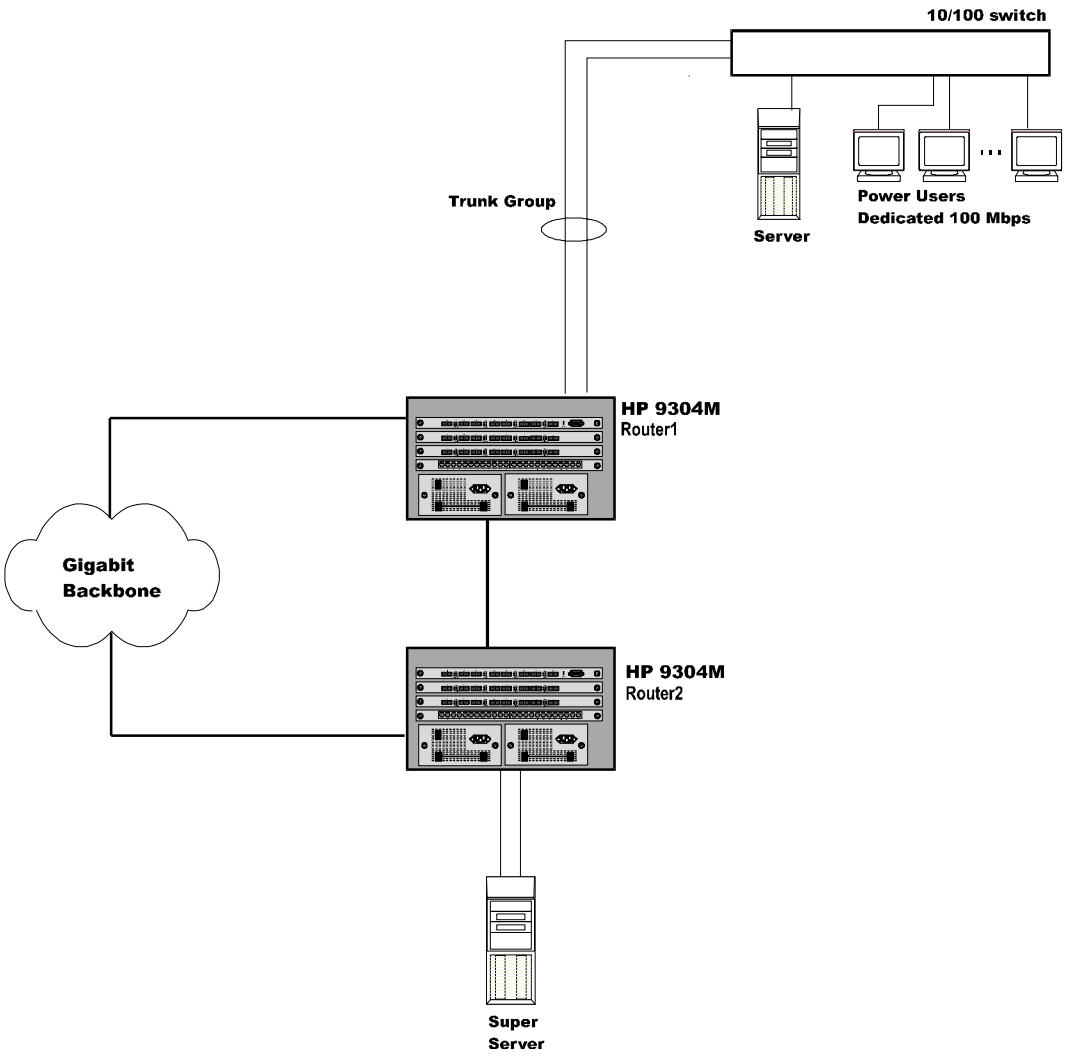

Figure 7.21 Trunk Group application within an HP routing switch network

Trunk Group Connectivity to a Server

To support termination of a trunk group, the server must have either multiple network interface cards (NICs) or a quad interface card installed. The trunk server is designated as a server with multiple adapters or a single adapter with multiple ports that share the same MAC and IP address.

Trunk Group Rules

- Up to four trunk groups may be assigned
- Trunk group port assignment should always start with the lead port. The lead port is always the lowest number in the following port ranges:
  - 1-4, 5-8, 9-12, 13-16 and 17-18 and 21-24
- Port assignment must be contiguous
- Port assignment cannot be across multiple trunk group boundaries, e.g. ports 4 and 5 cannot be in the same trunk group
- All trunk group member properties must match the lead port of the trunk group with respect to the following parameters:
  - Port tag type (untagged or tagged port)
  - Port speed and duplex
  - QoS priority

Trunk Group Configuration and Start-Up Notes

The following steps must also be followed in configuring trunk groups:

1. Disconnect the cables from those ports on both systems that are to be used in the trunk group. Do not configure the trunk groups with cables connected.
2. Configure the trunk group on one of the two routing switches involved in the configuration. Save this configuration to flash and reboot the system.
3. Follow the same process outlined in step 2 for the other routing switch of the trunk group connection.
4. Once both systems are reset (re-booted) and operational, reconnect the cables to those ports that are now configured as trunk groups, starting with the first port (lead port) of each trunk group.
5. To verify the connection is operational, use the ***show trunk*** command.

EXAMPLE: The user wants to build a 200 Mbps trunk group between two routing switches (Router1 and Router2) and a 200 Mbps trunk group from Router 2 to a local server as seen in **Figure 7.21**.

USING THE CLI

To configure the trunk group link between the two routing switches:

```
Router1(config)# trunk switch e 2/5 e 2/7
Trunk is created for next power cycle.
Please save configuration to flash and reboot.
Router1(config)# write mem
Copy_runConfig_startConfig
Wrote 2208 characters to configuration file router1.cfg
Router1(config)# exit
Router1# reload
```

To configure the trunk group link between Router2 and the server:

```
Router2(config)# trunk server e 1/2 e 1/4
Trunk is created for next power cycle.
Please save configuration to flash and reboot.
Router2(config)# write mem
Copy_runConfig_startConfig
Wrote 2208 characters to configuration file router2.cfg
```

NOTE: The text shown in italics in the CLI text above and below, represents messages echoed to the screen in answer to the CLI commands entered.

The user would then configure the trunk group to the server.

```
Router2(config)# trunk server ethernet 4/17 to 4/18
Trunk is created for next power cycle.
Please save configuration to flash and reboot.
Router2(config)# write mem
Copy_runConfig_startConfig
Wrote 1108 characters to configuration file router.cfg
Router2(config)# exit
Router2# reload
```

syntax: trunk <server|switch> ethernet <port number> to <port number>

NOTE: For server-to-client traffic, the server chooses the port for sending to the destination client. All traffic gets switched by hardware as a normal trunk operation.

For client-to-server traffic, all packets are addressed to the server's MAC address and will be switched across the separate links in a trunk group based on the client's source address.

USING THE NETWORK MANAGEMENT INTERFACE

To configure ports 5 to 8 as a trunk group between two routing switches or a routing switch and a server, enter the following:

1. Select trunk from the main menu. The Trunk Group configuration sheet will display on the screen as seen in **Figure 7.22**.
2. Select a slot/port range (2/5-2/8) from the **trunk group** pull down menu.
3. Select the number of ports within that range (e.g. 2 or 4) that you want to operate as part of a trunk group.
4. Select **server** if the other end of the trunk group will be a server. If the other end of the connection is a routing switch, do not to select this parameter.
5. Select the **add** button and the **save to flash** button, and then re-boot the system using the reset link from the main menu. The configuration of trunk groups is complete for this system.

NOTE: The reset button, will not reset the routing switch. The reset button is a browser feature that will clear changes made to the screen before they are applied. To re-boot a system, the user should select the reset link seen in the main menu.

---

6. If the other end of the trunk group is a routing switch, log in to the other system and follow the same process noted in steps 1, 2, 3 and 5 above.

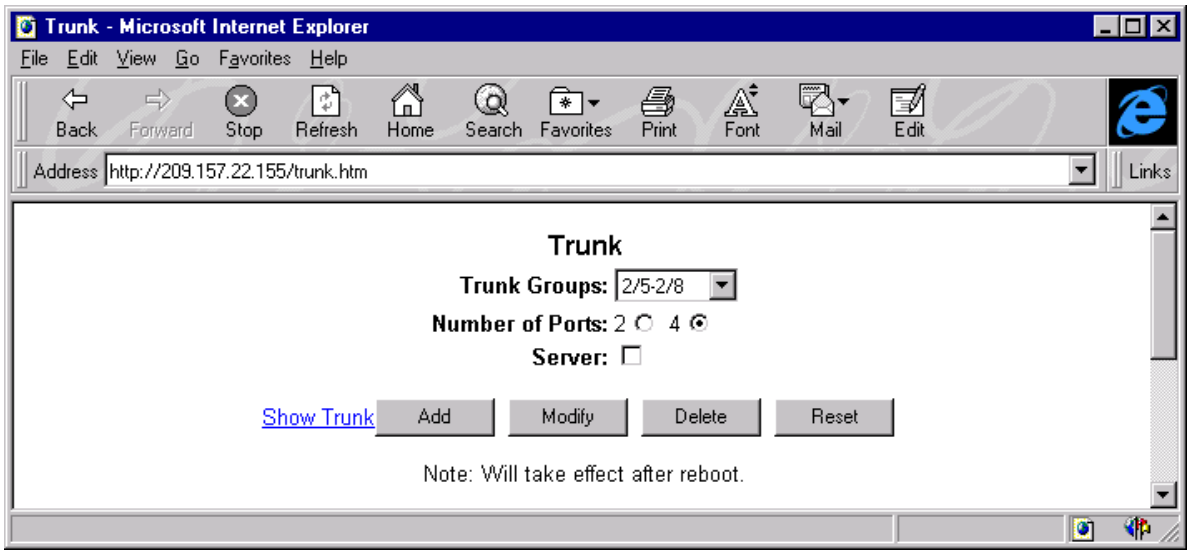

Figure 7.22 Trunk group configuration sheet

To delete a trunk group, the user would do the following:

1. Select Trunk from the main menu.
2. Select the **slot/port range** (e.g. port 2/5-2/8) to be removed.
3. Select the **delete** button and then re-boot the system by selecting the reset link from the main menu. The selected trunk group will now be inactive on this end of the path.

NOTE: If the other end of the trunk group is a routing switch, log in to the other system and follow the same process noted in steps 1 through 3 above.

To modify port membership in a trunk group, the user would do the following:

1. Select trunk from the main menu.
2. Reselect the desired **number of ports** to be included in that trunk group.
3. Select the **modify** button and then the reset link from the main menu to re-boot the system.

NOTE: If the other end of the trunk group is a routing switch, log in to the other system and follow the same process noted in steps 1 through 3 above.