Chapter 8
Configuring IP and IP/RIP

This chapter covers how to configure IP and IP/RIP protocols on HP routing switches using the CLI and Web management interface.

A summary of all CLI commands mentioned in this chapter, noting syntax along with possible values and default values, can be found in **Appendix B**.

Overview of IP/RIP

IP/RIP is a distance-vector protocol. IP/RIP routers transmit and receive RIP updates to and from neighboring routers. These updates, which include a copy of a router's entire routing table are sent out every 30 seconds by default. The frequency of these updates can be modified.

The **routing table** for RIP stores only the best route to a destination. The best path is defined as the destination path with the fewest hops. If information is received that indicates another route as the best path to a given destination, then that route will become the new route and will replace the previously stored entry. This information is then relayed to all other IP/RIP routers.

Each entry in the IP/ RIP routing table includes the destination address, the next hop address and a metric. The metric is equal to the number of hops required to reach a destination.

The IP/RIP protocol supported on HP routing switches supports the following RIP types:

- Version 1
- V1 compatible V2
- Version 2

IP/RIP Features

RIP includes a number of features that help stabilize its performance in the wake of rapidly changing network conditions–**hop count limits, hold downs, split horizons** and **poison reverse updates**.

Hop Count Limit

A maximum of 15 hops is supported by IP/RIP. Any destination that is greater than 15 hops away is considered unreachable. Although limiting to larger networks, it prevents endless loops in the network.

Hold Downs

A hold-down instructs routers to delay (hold down) action upon update messages received from routes believed inactive. The period of time is generally longer than the time required to update the entire network of a routing change. This safeguard prevents a removed or bad route from being reinstated in error.

Split Horizons

Split horizons are designed to prevent routing loops from being generated by adjacent routers. This feature is of particular value when a router's path to a given router is via another router. Split horizons allow a routing broadcast to be modified so that those routers with intermediate routers in their path to a destination router, are not seen as a path to the destination router by the intermediate router.

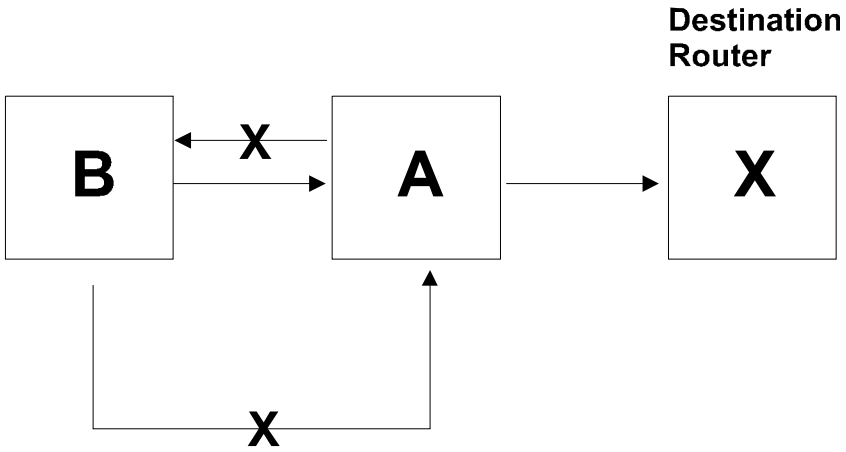

Figure 8.1 Split horizon in action

For example, in **Figure 8.1**, without split horizon operating, router A could see router B as a path to router X. However, if A were to route to B to reach router X, a loop would occur. A split horizon modifies a routing broadcast so that the intermediate router does not treat the source router as a path to the destination router.

Poison Reverse Updates

Poison reverse updates are used to prevent larger loops within the network by setting the metric (cost) of neighboring routes to infinity. This will prevent two hop loops.

IP/RIP Default Route Learning and Advertising

HP routing switches can learn and advertise default IP/RIP routes. This feature can be enabled on a global or interface basis. By default, this feature is disabled.

Priority for learning of IP/RIP routes is in the following order:

1. Static IP/RIP routes.
2. IP/RIP routes learned from RIP.
3. IP/RIP routes learned from OSPF.

Configuring IP and IP/RIP

By default, the IP protocol is active on all HP routing switches at initial start-up so there is no need to enable the protocol. However, the user does need to assign IP addresses.

Static routes, IP filters and the DNS and UDP helper features are all components of the IP protocol. Additionally, the protocol comes with system (global) and interface level parameters that can be modified to better suit the needs of the network.

The following actions can be done at the IP and RIP levels of the CLI or from the IP and RIP configuration sheets of the Web management interface:

1. Enable IP/RIP
2. Assign IP addresses to router interfaces.
3. Modify global IP parameters (optional).
4. Modify interface IP parameters (optional).
5. Define static IP routes (optional).
6. Assign Static ARP and RARP entries (optional)
7. Define IP filters (optional).
8. Configure UDP helper (optional).
9. Define IP/RIP route filters (optional).
10. Define IP/RIP route filter groups (optional).
11. Modify the RIP global default parameters–metric value, update time parameters (optional).
12. Enable redistribution if non-RIP routes are to be imported into the router.
13. Set up the redistribution table, via the permit and deny commands, if non-RIP routes are to be imported into the router.
14. Modify or enable interface parameters–RIP type or poison reverse (optional).

Dynamic IP/RIP Configuration

This features allows an HP routing switch to apply key IP/RIP configuration changes immediately without requiring a system reset. A summary of those parameters is highlighted below:

- Enabling or disabling of RIP
- Adding a static route
- Enabling RARP or Proxy ARP
- Adding static ARP or RARP entries
- Setting the ARP cache aging value
- Enabling ICMP Router Discovery Protocol (IRDP)
- Adding a Relay BootP server address
- Setting RIP transmit intervals
- Assignment of RIP type–V1, V2 or V1/V2 compatible
- Activating RIP poison reverse

Enabling IP/RIP

The IP/RIP protocol is disabled by default. It must be enabled on the HP routing switch, and the system must be reset before the protocol can be used.

USING THE CLI

To enable RIP, the user would enter the following:

```
HP9300 (config)# router rip
HP9300 (config)# exit
HP9300# write mem
HP9300# reload
```

syntax: router rip

NOTE: In the above example, the system is reset to enable the IP/RIP protocol. It is recommended that the user configure all elements of the protocol, before resetting the system.

USING THE WEB MANAGEMENT INTERFACE

1. Select the system link from the main menu.
2. Enable the **IP/RIP** option.
3. Select the save to flash link from the main menu.
4. Select the **reset** option from the File menu.

Assigning IP addresses

Before attaching equipment to the routing switch, the user needs to assign individual sub-net IP addresses and masks for each of the ports based on the desired and current network topology.

USING THE CLI

To assign an IP address for interface 1 (slot 2), the user would enter the following commands:

```
HP9300(config)# interface ethernet 2/1
HP9300(config-if-2/1)# ip address 192.45.6.1 255.255.255.0
```

NOTE: The use can also enter the IP address and mask in the following manner:
`HP9300(config-if-2/1)# ip address 192.45.6.1/24`

NOTE: Before exiting to make an assignment for the remaining ports, the user would configure the parameters for that interface. For details on configuring interface parameters, please refer to the **Modify Interface Parameters** section.

USING THE WEB MANAGEMENT INTERFACE

To assign an IP address, the user would enter the following commands:

1. Select the IP address link from the System configuration sheet.

   NOTE: If at least one IP address is already defined on the system, then a summary panel will appear first and the user will then need to select the add IP address link.

2. Select the **slot/port** combination to which the address is to be assigned.
3. Enter the **IP address** of the sub-net.
4. Enter the **sub-net mask**.

5. Select the **secondary** box if the IP address being defined is not the first address assigned to this interface.
6. Select the **add** button to assign the address.

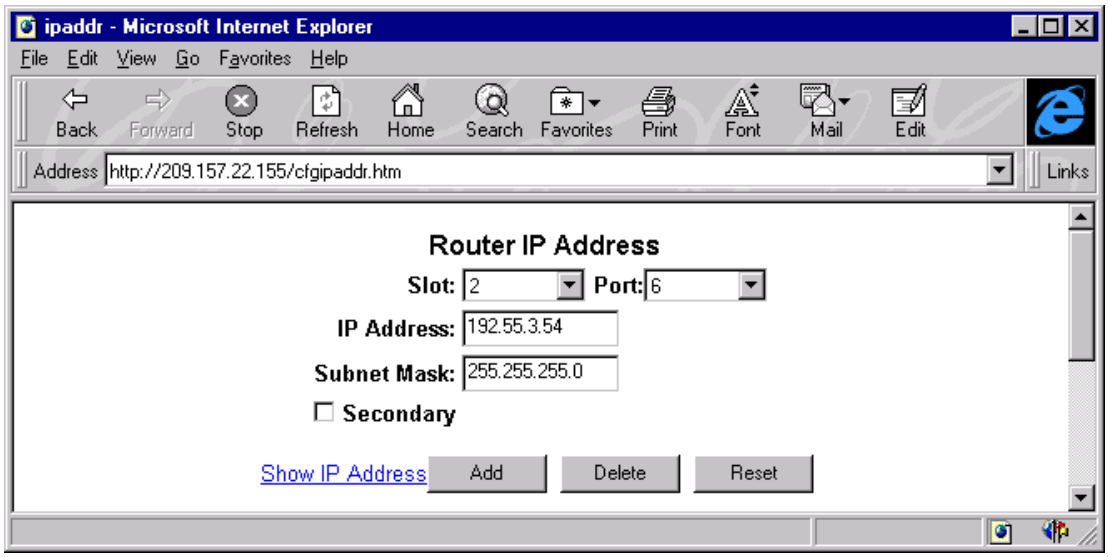

Figure 8.2 Assigning an IP address to an interface

Modifying Global IP and IP/RIP Parameters (optional)

A number of parameters can be modified for the IP protocol on a global basis. Each of these parameters comes with a default setting and does not need to be modified unless specific network requirements deem it.

A list and description of each global parameter is noted below:

- Modify the maximum number of hops for a BootP relay server
- Modify the ARP aging period
- Modify the time-to-live (TTL) threshold
- Enable or disable IRDP
- Enable or disable load sharing
- Enable or disable proxy ARP
- Enable or disable RARP
- Configure global static ARP or RARP entries
- Configure static IP routes
- Enable IP policy
- Enable or disable broadcast forward (UDP Helper)

Modifying the Maximum Number of Hops to a BootP Relay Server

An HP routing switch can support the relay of BootP requests to a BootP server outside of its network. The user can modify the maximum number of hops that a request will traverse to a BootP server. The parameter value ranges from 1 to 15 hops. The default value is 4 hops.

USING THE CLI

To modify the maximum number of hops supported (e.g. 10), the user would enter the following:

```
HP9300(config)# bootp-relay-max-hops 10
```

syntax: bootp-relay-max-hops <1-15>

USING THE WEB MANAGEMENT INTERFACE

To modify the maximum number of hops supported, the user would enter the following:

1. Select the IP link from the main menu. The panel shown in **Figure 8.3** will appear.
2. Enter a value between 1 and 15 into the **BOOTP relay maximum hop** field.
3. Select the **apply** button to assign the changes.

Modifying the ARP Aging Period

This parameter defines how long an ARP entry will remain active in the ARP cache before it is aged out. The parameter value ranges from 0 to 240 minutes. The zero value results in no address aging. The default value is 10 minutes.

USING THE CLI

To modify the ARP aging parameter to 20 minutes, the user would enter:

```
HP9300(config)# ip arp-age 20
```

syntax: ip arp-age <0-240>

USING THE WEB MANAGEMENT INTERFACE

1. Select the IP link from the main menu. The panel shown in **Figure 8.3** will appear.
2. Enter a value between 0 and 240 into the **ARP age** field.
3. Select the **apply** button to assign the changes.

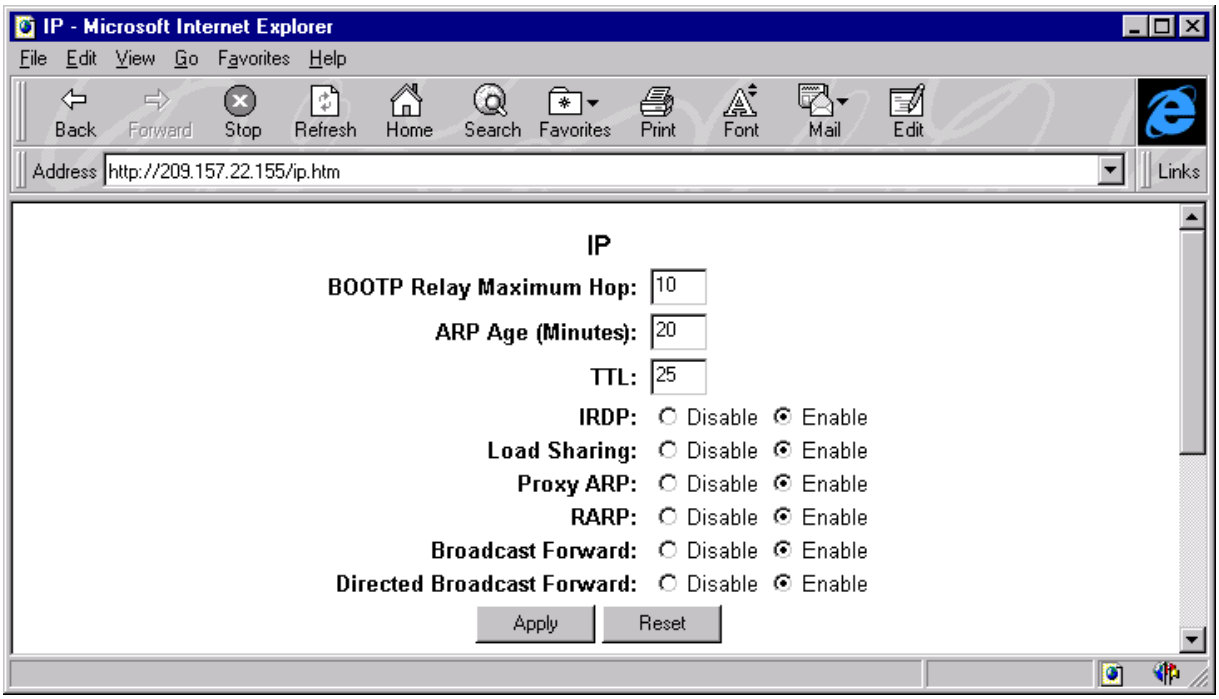

Figure 8.3 IP configuration sheet

Modifying the TTL Threshold

This parameter defines how long a packet will remain alive on the network. The range is between 1 and 255 hops. The default value for this parameter is 64 hops.

USING THE CLI

To modify the TTL threshold to 25, the user would enter the following:

```
HP9300(config)# ip ttl 25
HP9300(config)# exit
```

syntax: ip ttl <1-255>

USING THE WEB MANAGEMENT INTERFACE

1. Select the IP link from the main menu. The panel shown in **Figure 8.3** will appear.
2. Enter a value between 1 and 255 into the **TTL** field.
3. Select the **apply** button to assign the changes.

Enabling or Disabling IRDP

IRDP allows HP routing switches to dynamically learn about routes on other networks. The router will advertise its IP addresses to other routers on the network and answer queries from those routers. The default value for this feature is enabled.

USING THE CLI

To enable IRDP on a router, the user would enter:

```
HP9300(config)# ip irdp
```

syntax: [no] ip irdp

USING THE WEB MANAGEMENT INTERFACE

1. Select the IP link from the main menu. The panel shown in **Figure 8.3** will appear.
2. Enable **IRDP**.
3. Select the **apply** button to assign the changes.

Enable or Disable Load Sharing

This feature allows traffic to be sent across multiple paths of equal cost, to a destination resulting in a faster transmission. This feature is available when using the OSPF routing protocol. This feature is by default disabled.

USING THE CLI

To enable load sharing for OSPF, the user would enter:

```
HP9300(config)# ip load
```

syntax: [no] ip load-sharing

USING THE WEB MANAGEMENT INTERFACE

1. Select the IP link from the main menu and the panel shown in **Figure 8.3** will appear.
2. Enable the **load sharing** option.
3. Select the **apply** button to assign the changes.

NOTE: For more details on configuring OSPF, please refer to **Chapter 9**.

Disabling or Enabling Proxy ARP

This feature enables or disables a router as proxy for devices on its sub-nets. As proxy, the router will respond to ARP requests from other devices on the network. By default, this feature is enabled on the router.

USING THE CLI

To enable proxy ARP, the user would enter:

```
HP9300(config)# ip proxy-arp
```

syntax: [no] ip proxy-arp

USING THE WEB MANAGEMENT INTERFACE

1. Select the IP link from the main menu and the panel shown in **Figure 8.3** will appear.
2. Enable the **proxy ARP** option.
3. Select the **apply** button to assign the changes.

Enable or Disable RARP

The user can enable or disable Reverse Address Resolution Protocol (RARP) on the routing switch. RARP allows retrieval of an IP address associated with a given MAC address. By default this feature is enabled.

USING THE CLI

To enable the RARP, the user would enter:

```
HP9300(config)# ip rarp
```

syntax: [no] ip rarp

USING THE WEB MANAGEMENT INTERFACE

1. Select the IP link from the main menu. The panel shown in **Figure 8.3** will appear.
2. Enable the **RARP** option.
3. Select the **apply** button to assign the changes.

Enabling or Disabling Broadcast Forward

The user would enable broadcast forward to allow UDP helper assignments to be made. This command is used in conjunction with the UDP helper feature to define the type of application traffic (port number socket) that is being forwarded to the server. By default this feature is enabled.

NOTE: Additional configuration is required to configure the UDP helper feature. For more details on configuring that feature, refer to the **Configuring UDP Helper** section.

USING THE CLI

To enable the broadcast forwarding of snmp-traps, the user would enter the following:

```
HP9300 (config)# ip forward-protocol udp snmp-trap
```

syntax: ip forward-protocol udp <UDP application type>

The following port socket options are defined:

number	echo	snmp-trap
bootpc	mobile-ip	tacacs
bootps	netbios-dgm	talk
discard	netbios-ns	
dnsix	ntp	
tftp	snmp	

In addition, the user can specify any UDP application by using the number option listed above.

NOTE: By default, when an IP helper address is configured on an interface, UDP broadcast forwarding is enabled for the following UDP packets: bootps, domain, tftp, time, netbios-dgm, netbios-ns and tacacs.

USING THE WEB MANAGEMENT INTERFACE

1. Select the IP link from the main menu. The panel shown in **Figure 8.3** will appear.
2. Enable the **broadcast forward** option.
3. Select the **apply** button to assign the changes.

NOTE: To define the ports to be forwarded, the user should select the UDP helper link from the IP configuration sheet.

Defining Static IP routes

The user can manually input static IP routes by entering a destination IP address and mask along with the IP address of the next hop router. The user can also assign the default router as the destination by entering 0.0.0.0 0.0.0.0.

HP routing switches can support up to 64 static routes with a default setting of 16.

USING THE CLI

To enter static IP route 1 with a destination address of 192.0.0.0 255.0.0.0 and a next hop router IP address of 195.0.0.0 on interface 6 (slot 2), the user would enter the following:

```
HP9300(config)# int e 2/6
```

```
HP9300(config-if-2/6)# ip route 1 192.0.0.0 255.0.0.0 195.0.0.0
```

syntax: ip route <index> <destination IP address> <destination mask> <next hop IP address>

USING THE WEB MANAGEMENT INTERFACE

1. Select the static route option from the IP configuration sheet. The static route entry panel, shown in **Figure 8.4** will appear.

NOTE: If static routes already exist on the router, then the static route summary panel will appear instead. The user should then select the add static route link to reach the Static Route entry panel.

2. Enter the IP address in the **network** field.
3. Enter the IP **mask**.
4. Enter the address of the **next hop** router that provides access to that destination.
5. Enter a default **metric** for that route if a value other than that configured at the interface level is desired.
6. Select the **add** button to save the entry to the static route table.

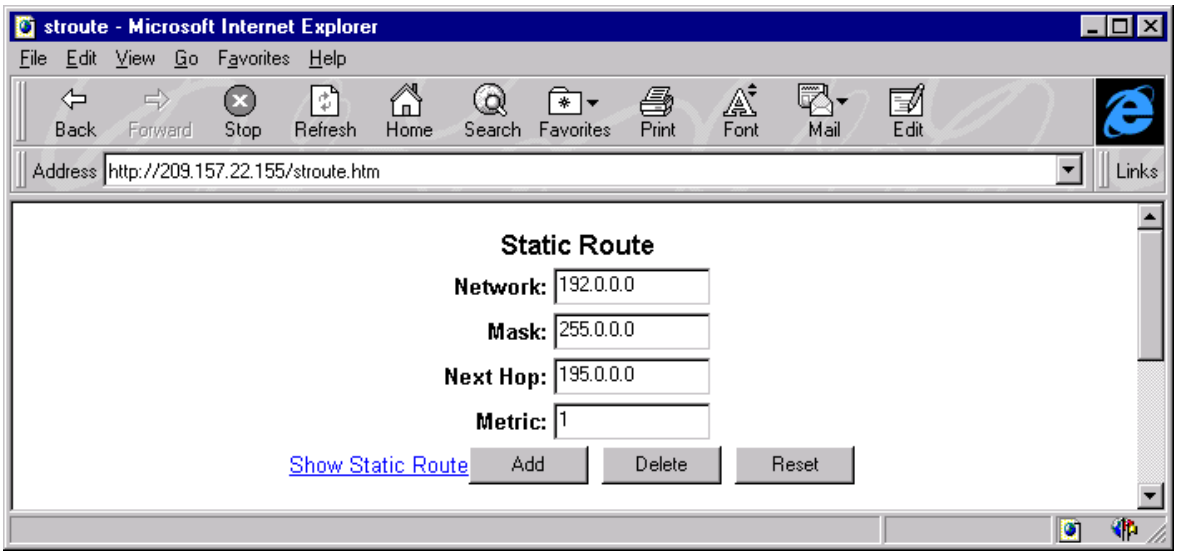

Figure 8.4 Defining an IP static route

Assigning Static ARP and RARP entries (optional)

The user can assign up to 16,000 static ARP and RARP entries on a chassis router and up to 64 on a stackable router.

USING THE CLI

To assign **static ARP** entries on a chassis system, the user would enter:

```
HP9300(config)# arp 1 192.53.4.2 1245.7654.2348 e 2/4
```

syntax: arp <number> <ip address> <mac address> ethernet <slot/port>

USING THE WEB MANAGEMENT INTERFACE

1. Select static ARP from the IP configuration sheet. The panel shown in **Figure 8.5** will appear.

NOTE: If any static ARP entries are defined on the router, the static ARP summary panel will appear first. The user will then need to select add static ARP.

2. Enter **IP address**.
3. Enter **MAC address**.

4. Select the **slot/port** that the static ARP entry is to be assigned to from the pull down menus.
5. Select the **add** button to save the entry to the static ARP table.

NOTE: You must be directly linked to an IP interface for which you are defining a static ARP.

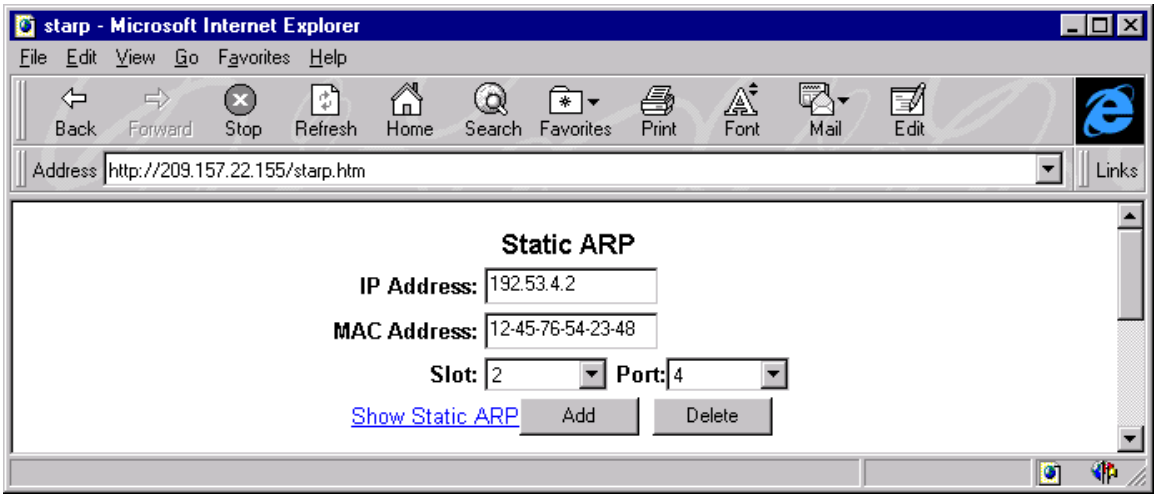

Figure 8.5 Static ARP entry panel

USING THE CLI

To assign a **static IP RARP** entry for static routes on an HP routing switch:

```
HP9300(config)# rarp 1 1245.7654.2348 192.53.4.2
```

syntax: rarp <number> <mac address>.<ip address> ethernet <slot/port>

USING THE WEB MANAGEMENT INTERFACE

1. Select static RARP from the IP configuration sheet. The panel shown in **Figure 8.6** will appear.

NOTE: If any static RARP entries are defined on the router, the static RARP summary panel will appear first. The user will then need to select add static RARP.

2. Enter **MAC address**.
3. Enter **IP address**.
4. Select the **add** button to save the entry to the static RARP table.

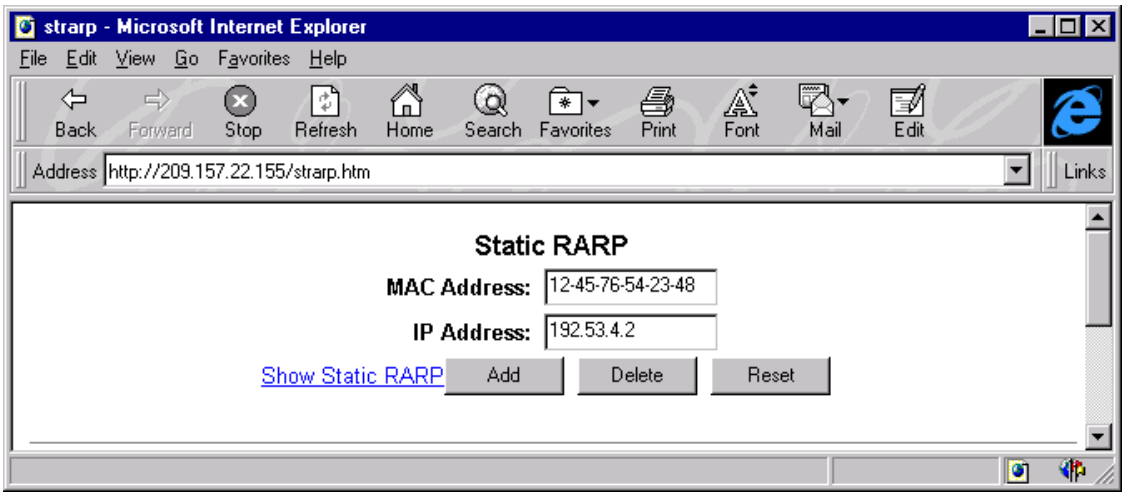

Figure 8.6 Static RARP entry panel

Assigning IP and IP/RIP Filters

The user can define IP and IP/RIP filters on a global basis and assign filters on an interface basis. Filters can also be defined for imported routes (redistribution). The following filters are discussed in this section:

- Define IP Filters
- Assign IP filter groups to interfaces
- Define IP/RIP Filters
- Assign IP/RIP filter groups to all interfaces
- Define IP/RIP neighbor filters
- Define IP/RIP redistribution filters

Defining IP filters (optional)

Filtering of IP routes is supported to provide enhanced security in the network.

An IP filter can be defined with the following possible criteria—source address, source mask, destination address, destination mask, protocol and TCP or UDP port number (bgp, ftp, pop3, smtp, telnet, www). The router supports either a permit or deny action on the filters.

IP filters can be defined for all of the following protocols: ICMP, IGMP, IGRP, OSPF, TCP and UDP.

When filtering on TCP and UDP, an operator and port number must also be supplied. The following operator and port numbers are supported:

Operator values:

- eq (equals)
- gt (greater than)
- lt (less than)
- neq (not equal to)

Port numbers:

- bgp
- ftp
- pop3
- smtp
- telnet
- www
- <protocol number>

USING THE CLI

EXAMPLE 1: To enter an IP filter that globally accepts all FTP traffic without regard to network orientation, the user would use the wildcard value ‘any' in place of an IP address and enter the following:

```
HP9300(config)# ip filter 1 permit any any tcp eq ftp
```

EXAMPLE 2: To enter an IP filter that only accepts FTP traffic from a specific network, the user would enter the following:

```
HP9300(config)# ip filter 1 permit 192.38.5.54 255.255.255.0 195.38.5.53
255.255.255.0 tcp eq ftp
```

syntax: ip filter <filterID> <permit | deny> <source ip address | any> <source mask | any> <destination ip address | any> <destination mask | any> <protocol> [<established> <operator> <port range>]; *items in brackets apply to TCP only*

USING THE WEB MANAGEMENT INTERFACE

To add an IP filter:

1. Select the IP policy link from the IP configuration sheet. The panel shown in **Figure 8.7** will appear.

   NOTE: If IP filters are already defined on the router, then the IP filter summary panel will display and the user will need to select the add IP filter link.

2. Enter an **ID** for the filter.
3. Select either **permit** or **deny** or **QoS**.
4. Enter the **source address** and **mask** for the filter.

   NOTE: The user can specify the wildcard value ’any’ in the source and destination IP address and mask fields to allow all traffic. Entering 0.0.0.0 represents ’any’. Likewise, to allow all protocols to be accepted by a filter, the user can enter a single zero (0) in the protocol field.

5. Enter the **destination address** and **mask** for the filter.
6. Enter either TCP or UDP in the **protocol** field.
7. Select the **operator** for the filter.

8. Enter the port number in the **TCP/UDP** port field. For example, if the user wished to filter on HTTP traffic, the user would enter the value 80.
9. Select the **filter established TCP** option to filter out TCP SYN packets for the defined port range.
10. Select the **add** button to assign the IP Filter.

To modify or delete an IP Filter:

1. Select IP policy from the IP configuration sheet. This will display the IP filter summary panel as seen in **Figure 8.7**.
2. Select either the **modify** or **delete** button to the right of the IP filter you wish to change or delete.

NOTE: If modify is selected, an entry panel for that interface will appear. Make the desired changes and select **Add** to save the changes. If delete is selected, just select the button and no other steps are required

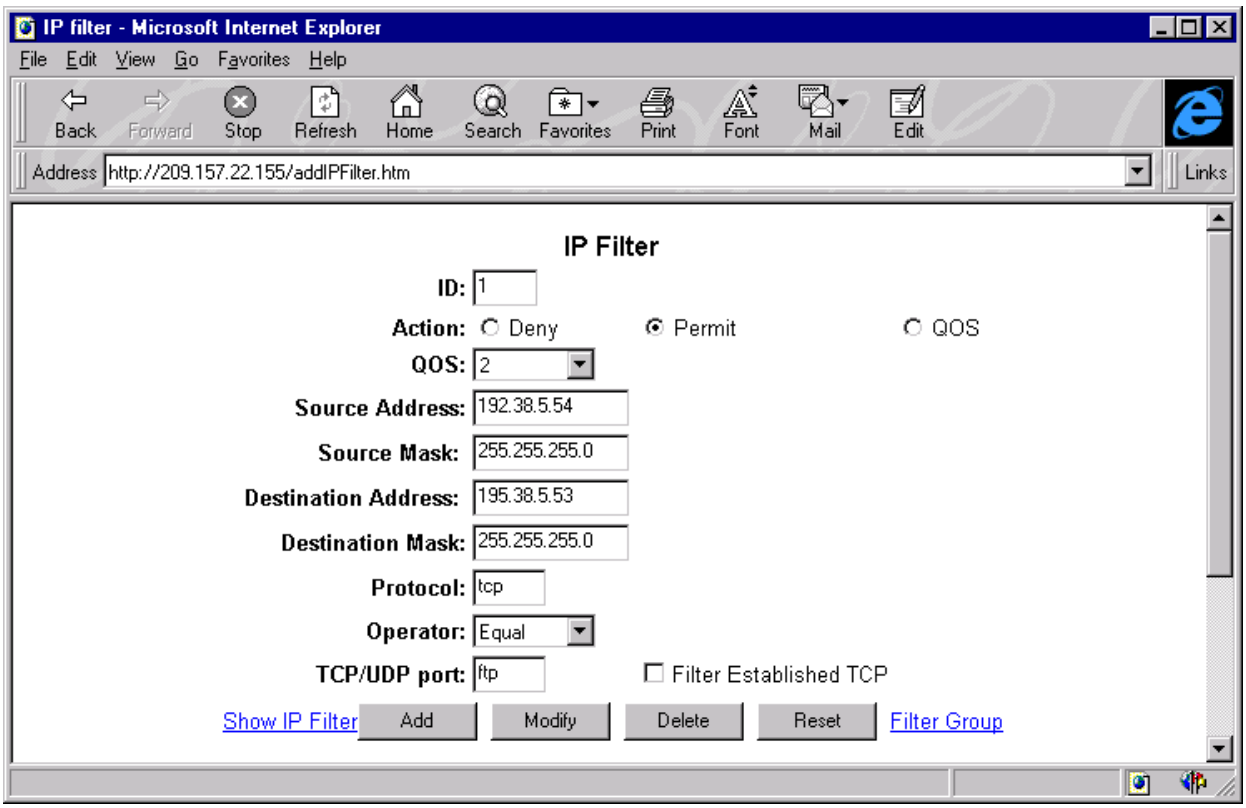

Figure 8.7 IP filter entry panel

Assigning IP filter groups (optional)

Once an IP filter is defined, it can be assigned to multiple interfaces using the IP filter group option.

USING THE CLI

To assign IP filters 2, 3 and 5 to port 1 on module 2 of a chassis, the user would enter the following:

```
HP9300(config)# interface e 2/1
HP9300(config-if-2/1)# ip filter-group in 2 3 5
```

syntax: ip filter-group <in | out> <filterID>

USING THE WEB MANAGEMENT INTERFACE

To assign IP filters 2, 3 and 5 to port 1 on module 2 of a chassis, the user would enter the following:

1. Select the filter group link from the IP filter configuration panel. The panel seen in **Figure 8.8** will appear.

NOTE: If at least one IP filter groups is already defined on the router, then the IP filter group summary panel will display first and the user will need to select the add IP filter group link.

---

2. Enter an **ID** for the filter.
3. Select the **slot/port** that the filters are to be assigned.
4. Select either or both the **in** and **out** options. Selecting 'in' will apply the filters to all incoming traffic on the port and selecting 'out' will apply the filters to all outgoing traffic on the port. Selecting both in and out options will apply filters to both incoming and outgoing traffic.
5. Enter the **filter ID** for all filters that are to be applied to the interface.

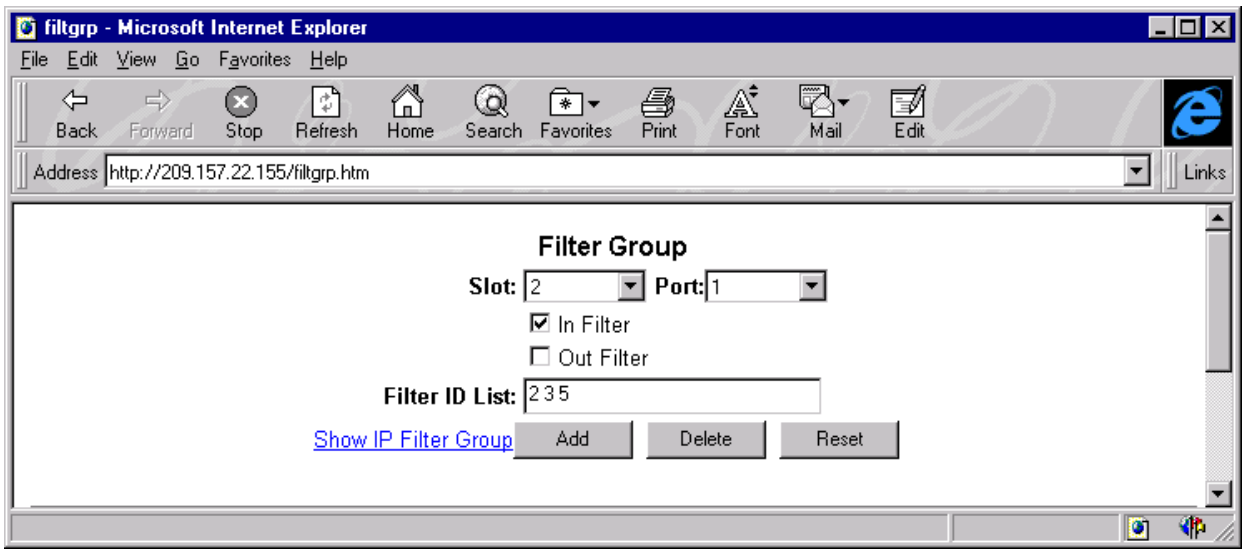

Figure 8.8 Assigning IP filters 1, 2 and 5 to incoming traffic on port 1 of module 2 of a chassis

Defining IP/RIP Filters

To define an IP/RIP filter, RIP must be enabled on the router. A filter will define what routes will be stored in the IP routing table for inbound routes. For outbound routes, the filter defines what routes will be advertised through a given interface. Up to 64 route filters can be defined for a router.

NOTE: A route is defined by its IP address and IP mask.

USING THE CLI

To enable RIP on the router and then define IP/RIP filters, the user would enter the following:

```
HP9300 (config)# router rip
HP9300 (config-rip-router)# filter 1 permit 192.53.4.1 255.255.255.0
HP9300 (config-rip-router)# filter 2 permit 192.53.5.1 255.255.255.0
HP9300 (config-rip-router)# filter 3 permit 192.53.6.1 255.255.255.0
HP9300HP9300 (config-rip-router)# filter 4 deny 192.53.7.1 255.255.255.0
```

syntax: filter <index> <permit | deny> <source ip address | any> <source mask | any>

NOTE: Instead of specifying a specific route, the user can also specify all routes versus a specific sub-net by using the value, 'any.'

USING THE WEB MANAGEMENT INTERFACE

To define a RIP route filter:

1. Select RIP route filter from the RIP configuration sheet and the entry panel shown in **Figure 8.9** will appear.

   NOTE: If RIP route filters already exist on the switching router, a summary panel will appear. The user will then need to select the add RIP route filter link to reach the entry panel.

2. Enter the filter ID.
3. Select either **permit** or **deny** as the action.
4. Enter an **IP address** and **mask** or the wildcard value, 0.0.0.0, to allow all routes.
5. Select the **add** button to save the filter.

To modify or delete a RIP route filter:

1. Select RIP route filter from the RIP configuration sheet and a summary panel of all defined RIP route filters will appear.
2. Select the **modify** or **delete** button next to the filter you wish to change or delete.

   NOTE: If the modify button is selected, enter the changes to either or both of the **action** or **IP address** fields and then select the **modify** button to apply the changes. If the **delete** button is selected, the filter is removed immediately.

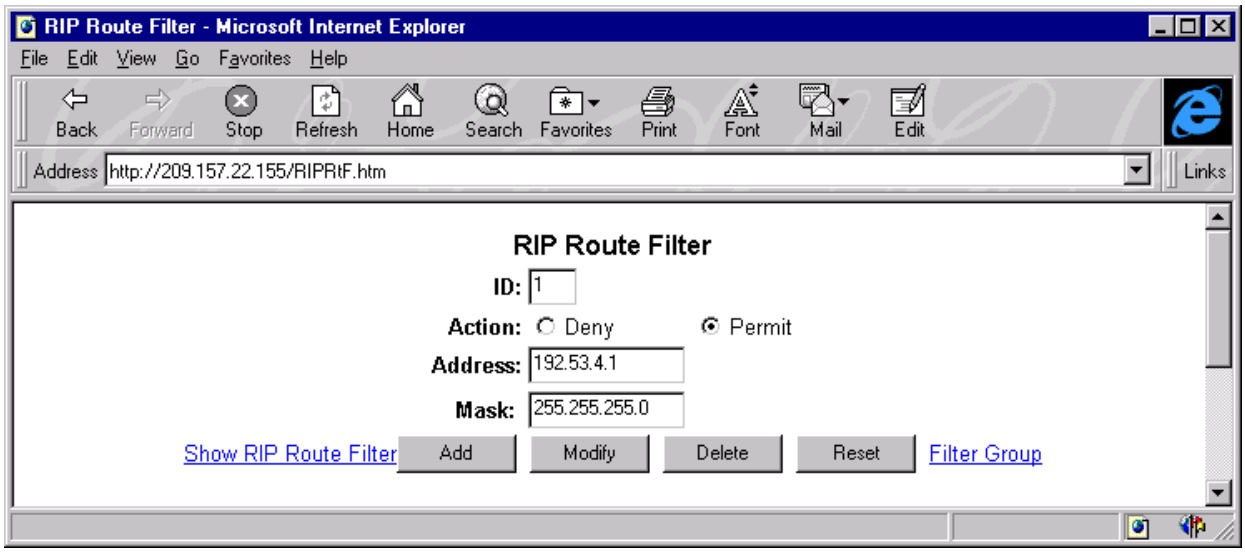

Figure 8.9 IP/RIP filter entry panel

Assigning IP/RIP Filter Groups Globally

Once IP/RIP filters are defined, the user can assign them to individual interfaces. The user can also specify if he or she only wants the filter applied to outgoing or incoming routes using the terms out and in respectively.

USING THE CLI

To assign filters 2, 3 and 4 to all incoming routes, the user would enter the following:

```
HP9300(config)# ip rip filter-group in 2 3 4
```

syntax: ip rip filter-group <in | out> <index>

NOTE: If the user where to specify **out** in the above example, filters 2, 3 and 4 would be applied to all RIP routes being advertised.

USING THE WEB MANAGEMENT INTERFACE

1. Select the filter group link from the RIP filter configuration panel.
2. Select the **slot/port** to which the filter(s) will be assigned.
3. Select either or both the **in filter** or **out filter** options. Selecting the 'in filter' option will apply filters to incoming traffic only. Selecting the 'out filter' option will apply filters to outgoing traffic only. Selecting both will apply the filters to both incoming and outgoing traffic
4. Enter the filters to be applied to the interface in the **filter ID list** field.
5. Select the **add** button to assign the changes.

Defining IP/RIP Neighbor Filters

This feature allows the user to specify the neighbor routers from which it will receive RIP routes. By default, RIP routes will be learned from all neighbors. Up to 64 neighbor filters can be defined.

This command is used to specify those routers from which a router will receive RIP routes.

In the example below, no RIP routes will be learned from any neighbor router. By default, RIP routes will be learned from all neighbors.

USING THE CLI

To configure a router so that no RIP routes are learned from neighbor routers, the user would enter:

```
HP9300 (config-rip-router)# neighbor 1 deny any
```

syntax: neighbor <index> <permit | deny> <source IP address | any>

USING THE WEB MANAGEMENT INTERFACE

To define a RIP neighbor filter, the user would do the following:

1. Select RIP neighbor filter from the RIP configuration sheet. The panel seen in **Figure 8.10** will appear.
2. Enter the filter **ID**.
3. Select either the permit or deny **action**.
4. Enter the **source IP** address that will be filtered or 0.0.0.0 to filter on all neighboring routers.
5. Select the **add** button to assign the filter.

To modify or delete a RIP neighbor filter, the user would do the following:

1. Select RIP neighbor filter from the RIP configuration sheet. A summary panel of all defined RIP neighbor filters will appear.
2. Select the **modify** or **delete** button next to the filter that is to be changed or deleted.

NOTE: If modify is selected, enter the changes to the **action** and/or **IP address** fields and then select the **modify** button apply the changes. If the delete button is selected, the filter is removed immediately.

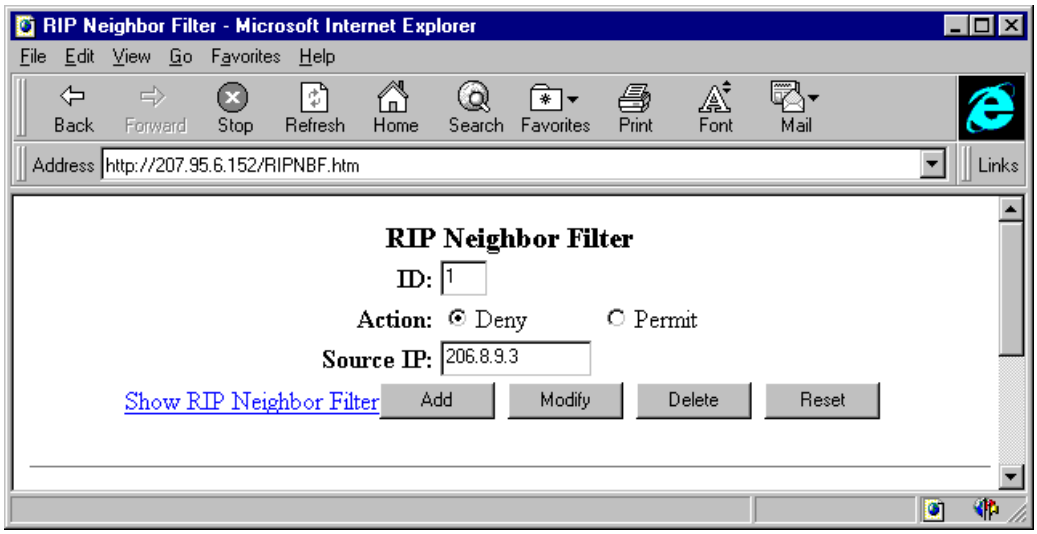

Figure 8.10 RIP neighbor filter entry panel

Assigning IP/RIP Filter Groups to Interfaces

Once RIP filters are defined, the user can assign them to individual interfaces. The user can also specify if he or she only wants the filter applied to outgoing or incoming routes using the terms out and in respectively.

USING THE CLI

To assign filters 2, 3 and 4 to all incoming routes on interface 1 of module 2, the user would enter the following:

```
HP9300(config)# interface e 2/1
HP9300(config-if-2/1)# ip rip filter-group in 2 3 4
```

syntax: ip rip filter-group <in | out> <index>

NOTE: If the user where to specify **out** in the above example, filters 2, 3 and 4 would be applied to all RIP routes being advertised.

Filter groups can also be assigned on a **global** basis.

USING THE WEB MANAGEMENT INTERFACE

1. Select the filter group link from the RIP filter configuration panel. The panel seen in **Figure 8.11** will appear.
2. Select the **slot/port** to which the filter(s) will be assigned.
3. Select either or both the **in filter** or **out filter** options. Selecting the 'in filter' option will apply filters to incoming traffic only. Selecting the 'out filter' option will apply filters to outgoing traffic only. Selecting both will apply the filters to both incoming and outgoing traffic
4. Enter the filters to be applied to the interface in the **filter ID list** field.
5. Select the **add** button to assign the changes.

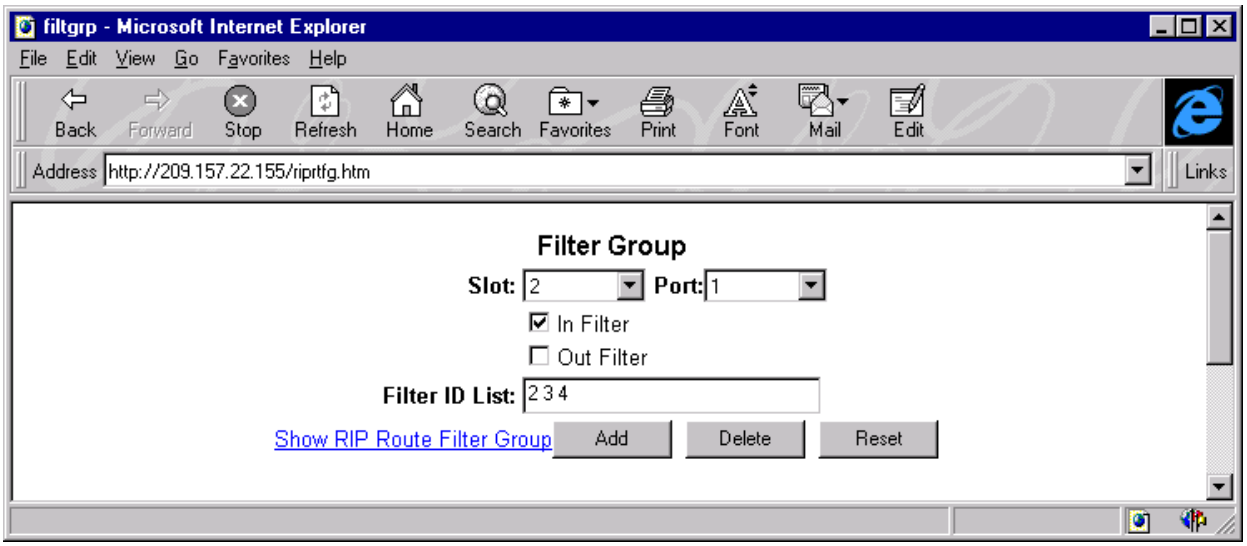

Figure 8.11 Assigning IP/RIP filters to an interface

Defining Redistribution Filters

Once redistribution is enabled for RIP, the should define routes to which redistribution will be applied (permit filter) or not applied (deny filter) by defining redistribution filters. Redistribution filters can be defined by interface protocol or metric.

USING THE CLI

EXAMPLE 1: To deny redistribution on all incoming routes received from the 207.92.0.0 network (by interface), the user would enter the following:

```
HP9300(config)# router rip
HP9300(config-rip-router)# deny redis 2 all 207.92.0.0 255.255.0.0
```

EXAMPLE 2: To deny redistribution on OSPF routes only, the user would enter the following:

```
HP9300(config-rip-router)# deny redis 3 ospf 207.92.0.0 255.255.0.0
```

EXAMPLE 3: To deny redistribution by metric, the user would enter the following:

```
HP9300(config-rip-router)# deny redis 3 ospf 207.92.0.0 255.255.0.0 match-metric 10
```

syntax: <permit|deny> redistribute <index> <all|ospf|static> <ip address> <ip mask> [match-metric<value>|set-metric <value>]

Possible values:

all	apply redistribution to all route types
ospf	apply redistribution to OSPF routes only
static	apply redistribution to the static route only
ip address	apply redistribution to a specific network and sub-net address
match-metric	apply redistribution to those routes with a specific metric value; possible *v*alues are between 1-15
set-metric	N/A to deny redistribution command

USING THE WEB MANAGEMENT INTERFACE

1. Select the redistribution filter link from the RIP configuration sheet. The panel shown in **Figure 8.12** will appear.
2. Enter an **IP address** and **mask** to filter on a specific network. Zeros (0.0.0.0) can be used instead of a specific interface, to allow all IP addresses or mask ranges.
3. Enter the **filter ID**.
4. Select either permit or deny as the **action**.
5. Select the types of routes you wish to filter on–**all, static** or **OSPF**.
6. Enable the **match metric** parameter, to limit the import of routes to only those that match a specific metric, as defined in the match metric field.
7. Enable the **set metric** parameter to define and assign a specific metric to an imported route. If enabled, the specified value will override the default metric defined on the RIP configuration sheet.
8. Select the **add** button to assign the redistribution filter.

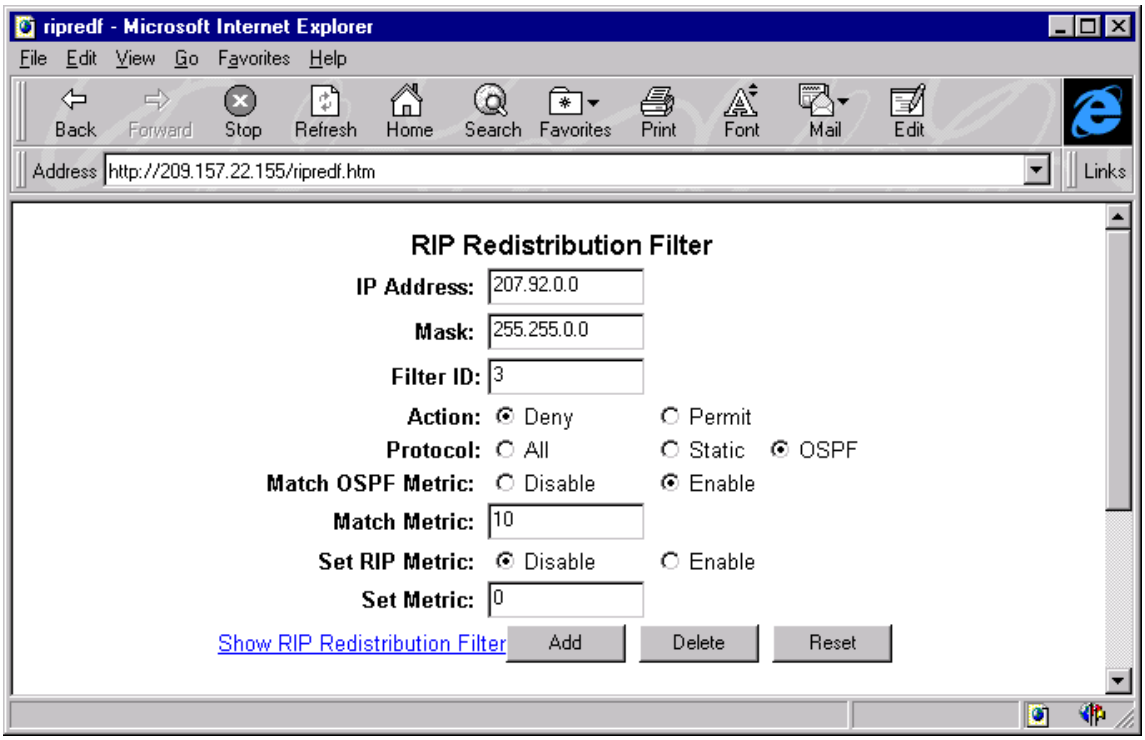

Figure 8.12 IP/RIP redistribution filter entry panel

Modify IP and IP/RIP Interface Parameters (optional)

IP and IP/RIP come with default settings for their interface parameters. The user need not modify any of these parameters unless required by network requirements.

IP interface parameters:

- Encapsulation format
- Maximum transmission unit (MTU)
- Metric

IP/RIP interface parameters:

- Enable RIP routing on individual router ports
  - Select RIP Version—version 1, version 2 or version 1 compatible
  - Enable or disable poison reverse
- Assign a filter group to a interface

A description of these parameters noting their possible values and their default value is summarized below.

NOTE: The user can also define IP filters, assign static IP routes and define static ARP and RARP entries for interfaces. For more details on these features, the user should refer to the specific sections on their configuration within this chapter.

IP interface Parameters

- Encapsulation format
- Maximum transmission unit (MTU)
- Metric

Modifying Encapsulation Format

This parameter allows the user to select the encapsulation format to be used on a port for MAC address encapsulation. This can vary by port. Options are—Ethernet II or SNAP. The default format is Ethernet II.

USING THE CLI

To change the encapsulation type on an interface (e.g. 5, slot 2) to Ethernet SNAP, the user would enter:

```
HP9300(config)# int e 2/5
HP9300(config-if-2/5)#ip encapsulation ethernet_snap
```

syntax: ip encapsulation <ethernet_snap | ethernet_ii>

USING THE WEB MANAGEMENT INTERFACE

1. Select the IP interface link from the main menu. The panel shown in **Figure 8.3** will appear.
2. Select the desired **encapsulation** type from the pull down menu.
3. Select the **apply** button to assign the changes.

Modifying the Size of the Maximum Transmission Unit (MTU)

The MTU field defines the maximum packet size to be accepted on a given port. The possible size for Ethernet II packets is 572 to 1500. Ethernet SNAP packets can be from 572 to 1492. The default value for Ethernet II packets is 1500 and 1492 for SNAP.

USING THE CLI

To change the MTU for an interface (e.g. 5, slot 2) to 1000, the user would enter:

```
HP9300(config)# int e 2/5
```

```
HP9300(config-if-2/5)#ip mtu 1000
```

syntax: ip mtu <572-1500> (Ethernet SNAP); ip mtu <572-1492> (Ethernet II)

USING THE WEB MANAGEMENT INTERFACE

1. Select the IP interface link from the IP configuration sheet and the panel shown in **Figure 8.13** will appear.

   NOTE: If at least one IP interface is defined on the router, then a summary panel will appear first. The user will then need to select the configure IP interface link to reach the IP interface panel shown in **Figure 8.13**.

2. Enter an **MTU** value between 572 and 1500 if the interface is operating with Ethernet SNAP encapsulation. If the interface is operating with Ethernet II enter a value between or 572 and 1492.
3. Select the **apply** button to assign the changes.

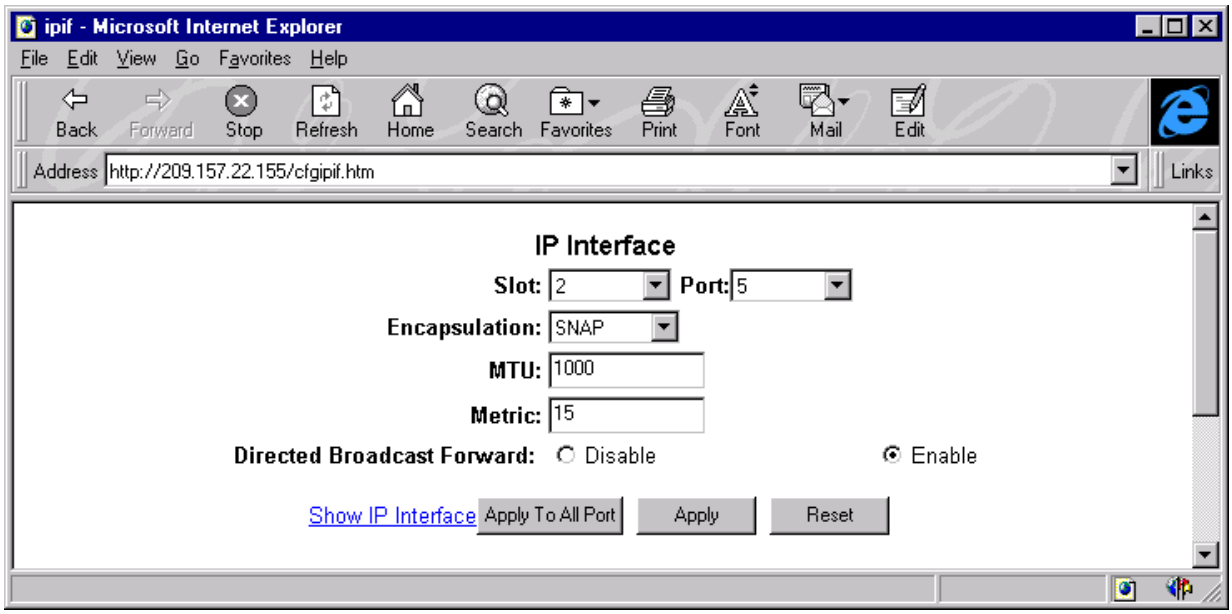

Figure 8.13 IP interface configuration panel

Modifying the Metric

Metric defines the cost that will be applied to all IP routes on an interface. A metric cost of between 1 and 16 can be assigned. The default value is 1.

USING THE CLI

To assign a route cost (metric) of 15 to an interface (e.g. 6, slot 2), the user would enter:

```
HP9300(config)# int e 2/6
HP9300(config-if-2/6)# ip metric 15
```

syntax: ip metric <1-16>

USING THE WEB MANAGEMENT INTERFACE

1. Select the IP interface link from the main menu. The panel shown in **Figure 8.13** will appear.
2. Enter a value between 1 and 16 for **metric**.
3. Select the **apply** button to assign the changes.

IP/RIP Interface Parameters (optional)

- Enable RIP routing on individual router ports
  - Select RIP Version—version 1, version 2 or version 1 compatible
  - Enable or disable poison reverse
- Assign a filter group to a interface

Enabling IP/RIP Routing on Interfaces and Modify Parameters (optional)

As autonomous systems, HP routing switches can support multiple protocols on the same system. RIP can be enabled on individual ports by simply selecting that port from the pull down menu, assigning a **version type** and either enabling or disabling the parameter **poison reverse**.

USING THE CLI

To enable RIP on an interface, define the type of RIP route and enable poison reverse for an interface (e.g. interface 1, slot 2), the user would enter:

```
HP9300(config)# int e 2/1
HP9300(config-if-2/1)# ip rip v1-only
HP9300(config-if-2/1)# ip rip poison-reverse
HP9300(config-if-2/1)# end
HP9300# write memory
HP9300# reload
```

syntax: ip rip <v1-only|v1-compatible-v2|v2-only>; ***syntax:*** ip rip poison-reverse

USING THE WEB MANAGEMENT INTERFACE

To enable RIP routing on individual interfaces, the user would do the following:

1. Select RIP interface from the RIP configuration sheet. The panel shown in **Figure 8.14** will appear.

   NOTE: If RIP is already defined on some interfaces, an interface configuration summary panel will appear and the user will need to select configure RIP interface to add an interface.

2. Select the **slot/port** to be configured from the pull down menus.
3. Assign the RIP type **version** from the pull down menu. Options are version 1, version 2, v1 compatible v2 or disabled. The default state is version 2.
4. Enable **poison reverse**, a loop prevention feature, if desired.
5. Select **apply** to assign the changes.

NOTE: To assign the configured interface parameters to all other RIP interfaces on the router, select the **apply all port** button.

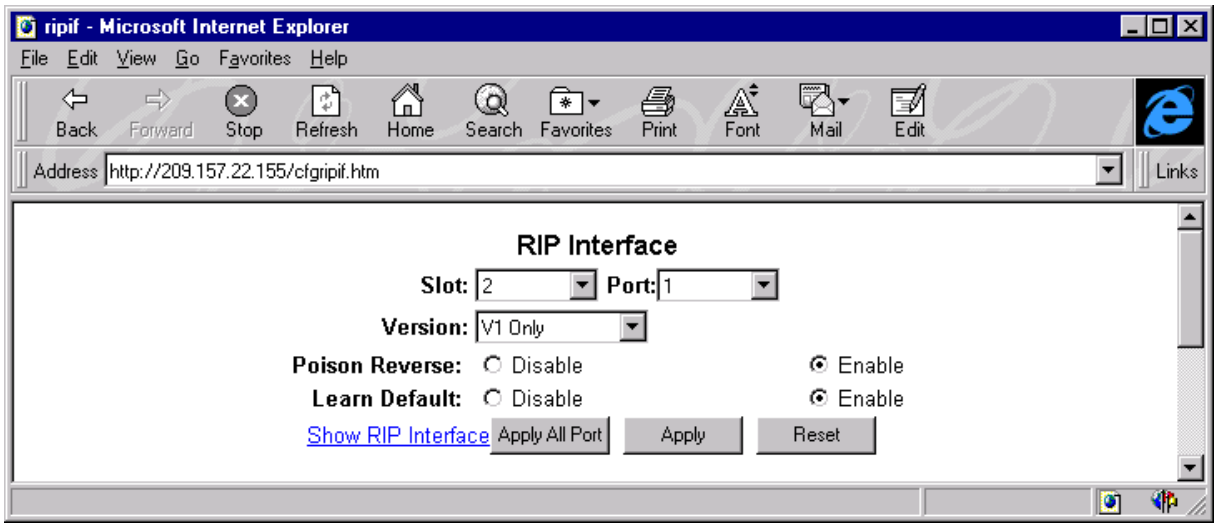

Figure 8.14 RIP interface display and entry panel

Modify Global IP/RIP Parameters

IP/RIP protocol comes with a number of global parameters with default settings. There is no need to modify these parameters unless the network requires it.

The following RIP parameters are modified at the RIP router level when using the CLI and at the RIP configuration sheet when using the Web management interface.

- Update time
- Enable or disable of redistribution
- Global default metric used for redistribution
- Enable IP/RIP Default Route Learning and Advertising

Modifying Update Time Value

Sets the time interval that will exist between the transmission of regular RIP response packets. Possible values are 1 to 1,000 seconds. The default value is 30 seconds.

USING THE CLI

To modify the interval (e.g. 120) in which RIP response packets are transmitted, the user would enter the following:

```
HP9300(config)# router rip
HP9300(config-rip-router)# update 120
```

syntax: update-time <1-1,000>

USING THE WEB MANAGEMENT INTERFACE

1. Select the RIP link from the main menu. The panel shown in **Figure 8.15** will appear.
2. Enter a value between 1 and 1,000 in the **update time** field.
3. Select the **apply** button to assign the changes.

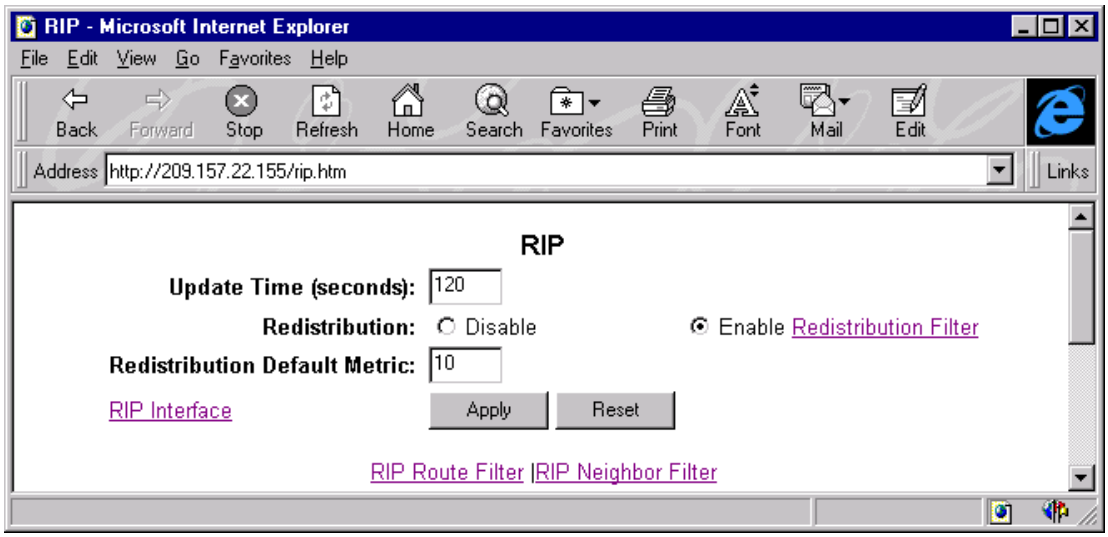

Figure 8.15 RIP configuration sheet

Enabling or Disabling Redistribution

When enabled, RIP will import external routes (OSPF or Static routes) into the RIP domain. Redistribution is by default disabled.

USING THE CLI

To enable redistribution for RIP, the user would enter the following:

```
HP9300(config)# router rip
HP9300(config-rip-router)# redistribution
```

syntax: redistribution

USING THE WEB MANAGEMENT INTERFACE

1. Select the RIP link from the main menu and the panel shown in **Figure 8.15** will appear.
2. **Enable** redistribution.
3. Select the **apply** button to assign the changes.

Modifying the Redistribution Global Default Metric

This feature allows the user to define the global default metric(cost) that will be assigned to all external routes imported into RIP for redistribution. Possible values are 1 to 15. The default value is 1.

USING THE CLI

To assign a global metric of 10 as the default cost, the user would enter the following:

```
HP9300(config)# router rip
HP9300(config-rip-router)# default 10
```

syntax: default-metric <1-15>

USING THE WEB MANAGEMENT INTERFACE

1. Select the RIP link from the main menu. The panel shown in **Figure 8.15** will appear.
2. Enter a value between 1 and 15 in the **redistribution default metric** field.
3. Select the **apply** button to assign the changes.

Enabling IP/RIP Default Route Learning and Advertising

Learning and advertising of IP/RIP routes can be enabled on a global or interface basis.

USING THE CLI

To enable learning of default IP/RIP routes on a global basis (all RIP interfaces), the user would enter:

```
HP9300(config)# router rip
HP9300(config-rip-router)# learn-default
```

To enable learning of default IP/RIP routes on an interface basis, the user would enter:

```
HP9300(config)# int e1
HP9300(config-if-1)# ip rip learn-default
```

syntax: learn-default

USING THE WEB MANAGEMENT INTERFACE

To enable learning of default IP/RIP routes, the user would:

1. Select the RIP interface link from the RIP configuration sheet. A summary panel of all RIP interfaces will appear.
2. Select the **modify** button next to the interface upon which learning of default routes is to be enabled. The RIP interface entry panel will appear.
3. Enable **learn default**.
4. Select the **apply** button to assign the changes.

NOTE: To globally enable learning of default routes across all interfaces, select the **apply to all ports** button instead of the **apply** button.

Configuring Domain Name Server (DNS) Resolver

The Domain Name Server (DNS) resolver feature allows a user to use a host name to perform Telnet, ping and trace route commands. The user can also define a DNS domain on a switching router and thereby recognize all hosts within that domain. The switching router will then automatically append the appropriate domain to the host and forward it to the domain name server.

For example, if a domain of newyork.com is defined on the routing switch and a user wishes to initiate a ping to a host, NYC01, on that domain, the user would only need to reference the host name in the command versus the host name and its domain name as shown below:

HP9300# ping nyc01 will yield the same result as HP9300# ping nyc01.newyork.com

Defining a DNS entry

Up to four DNS servers can be defined for each DNS entry with the first entry serving as the primary default address. Should a query to the primary address fail to be resolved after three attempts, the next gateway address will be queried for three times as well. This process will continue for each defined gateway address until a query is resolved. The order in which the default gateway addresses are polled is tied to the order in which they are entered when initially defined as shown in the example below:

USING THE CLI

A user wants to define the domain name of newyork.com on a routing switch and define four possible default DNS gateway addresses. To do so, the user would enter:

```
HP9300(config)#ip dns domain-name newyork.com
HP9300(config)# ip dns server-address 207.95.6.199 205.96.7.1
208.95.7.25 201.98.7.15
```

In this example, the first IP address entered in the ***ip dns server-address…***command will be recognized as the primary gateway address and all others will be secondary addresses with IP address 201.98.7.15, the last address that will be queried.

USING THE WEB MANAGEMENT INTERFACE

To map a domain name server to multiple IP addresses, the user would do the following:

1. Select the DNS link from the Ip configuration sheet. The panel seen in **Figure 8.16** will appear.
2. Enter the name of the domain name server in the **domain name** field.
3. Enter an IP address for each system that will serve as a gateway to the domain name server.

NOTE: The first address entered will be the primary DNS gateway address. The other addresses will be used in chronological order, left to right, should the primary address not be available.

4. Select the **apply** button when all gateway addresses are entered to assign the changes.
5. Select the save to flash link to save the configuration to flash.

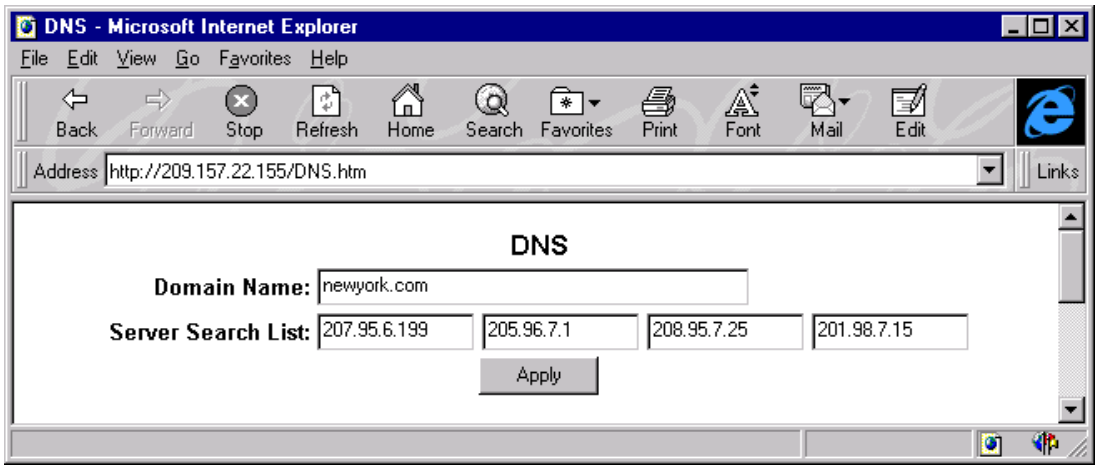

Figure 8.16 DNS resolver configuration panel

Initiating a Trace Route

EXAMPLE: A user wants to trace the route from a switching router to a remote server identified as NYC02 on domain newyork.com. Because the newyork.com domain is already defined on the switch, the user would only need to enter the host name, NYC02, as noted below:

```
HP9300# traceroute nyc02
```

Once the trace route command is entered, a message indicating that the DNS query is in process and the current gateway address (IP address of the domain name server) being queried will appear on the screen:

```
Type Control-c to abort

Sending DNS Query to 207.95.6.199

Tracing Route to IP node 207.95.6.30

To ABORT Trace Route, Please use stop-traceroute command.

 Traced route to target IP node 207.95.6.30:

   IP Address          Round Trip Time1    Round Trip Time2

  207.95.6.30         93 msec             121 msec
```

NOTE: In the above example, 207.95.6.199, is the IP address of the domain name server (default DNS gateway address) and 207.95.6.30 represents the IP address of the NYC02 host.

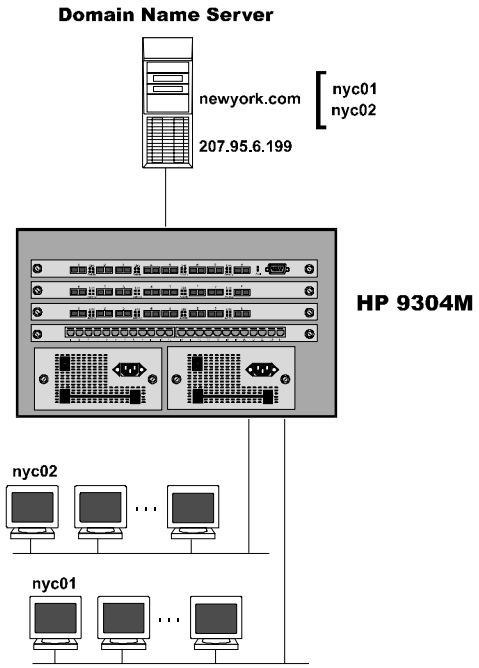

Figure 8.17 Querying a host on the newyork.com domain

Configuring UDP Helper (optional)

HP routing switches support relay of UDP/DHCP packets to their destinations for a specific application (e.g. bootps, domain, tftp) for cases when the destination server is not on the local LAN segment.

The following port sockets are defined for the UDP helper feature:

number	echo	snmp
bootpc	mobile-ip	snmp-trap
bootps	netbios-dgm	tacacs
discard	netbios-ns	talk
dnsix	ntp	tftp

NOTE: The user can also specify any UDP application by number.

NOTE: By default when an IP helper address is configured on an interface, UDP broadcast forwarding is enabled for the following UDP packets: bootps, domain, tftp, time, netbios-dgm, netbios-ns and tacacs.

USING THE CLI

To configure the UDP/DHCP helper feature on an interface (e.g. port 1 on module 2), the user would enter the following:

```
HP9300 (config)# interface e 2/1
HP9300 (config-if-2/1)# ip helper-address 1 207.95.7.6
```

syntax: ip helper-address < 1-4> <ip address>

USING THE WEB MANAGEMENT INTERFACE

To configure the UDP/DHCP helper feature on an interface, the user would do the following:

1. Select the UDP helper option on the IP configuration sheet and the panel seen in **Figure 8.18** will appear.
2. Select the **slot/port** to which the UDP helper packets will be forwarded, from the pull down menus.
3. Enter the **IP address** of the remote server for which the router will be relaying the packets.
4. Select the **add** button to apply the changes. The user is now ready to assign applications to be forwarded, highlighted in the next section.

To select an application to be forwarded to the server by the switching router, the user should do the following:

1. Select system broadcast forward from the UDP helper entry panel. The panel shown in **Figure 8.19** will appear.
2. From the pull down menu, select the application(s) to be forwarded to the server. The chosen broadcast forwards will be displayed in the display panel under the **selected forward ports** heading. By default, the following applications will already be selected: bootps, domain, tftp, time, netbios-dgm, netbios-ns and tacacs.
3. Select the **add** button to apply the changes.

A user can define his or her own protocol with the user define panel. To do so, the user would do the following:

1. Select the user broadcast forward link from the UDP helper configuration panel. The panel shown in **Figure 8.20** will appear.
2. Enter a value between 1 and 65535.
3. Select the **add** button to assign the change.

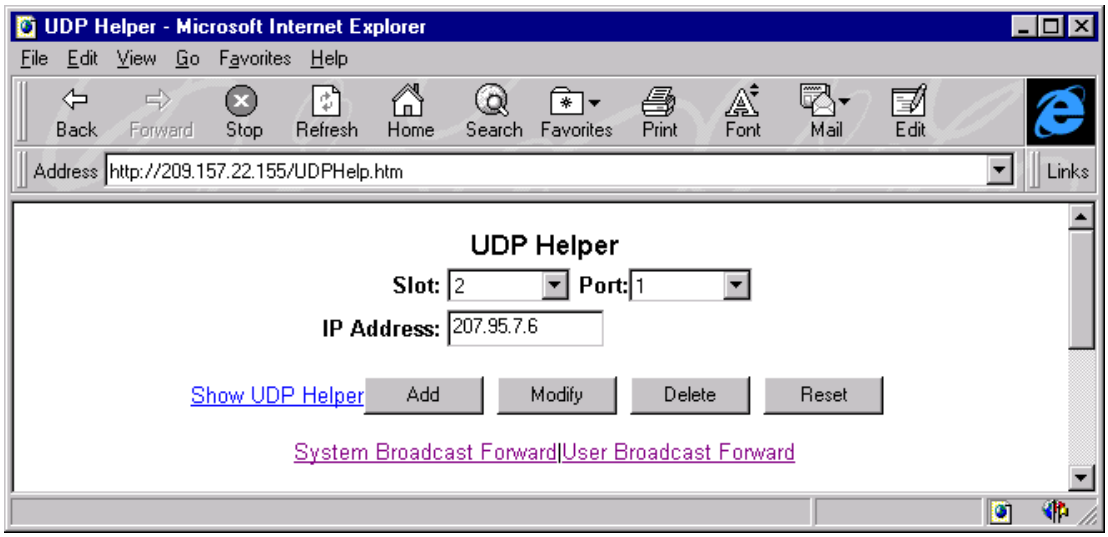

Figure 8.18 UDP helper configuration panel

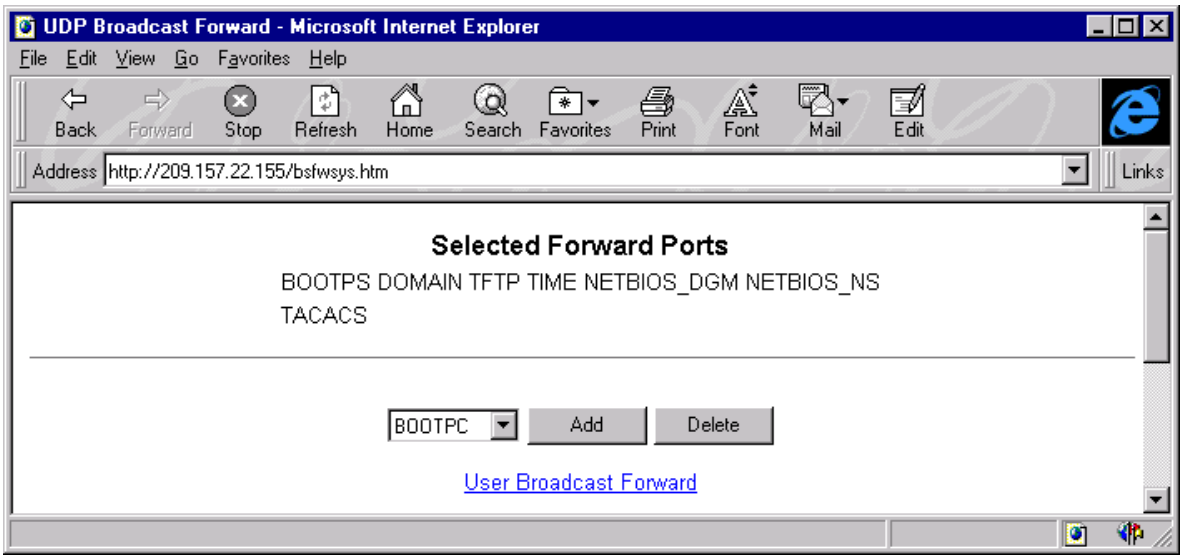

Figure 8.19 System broadcast forward entry panel

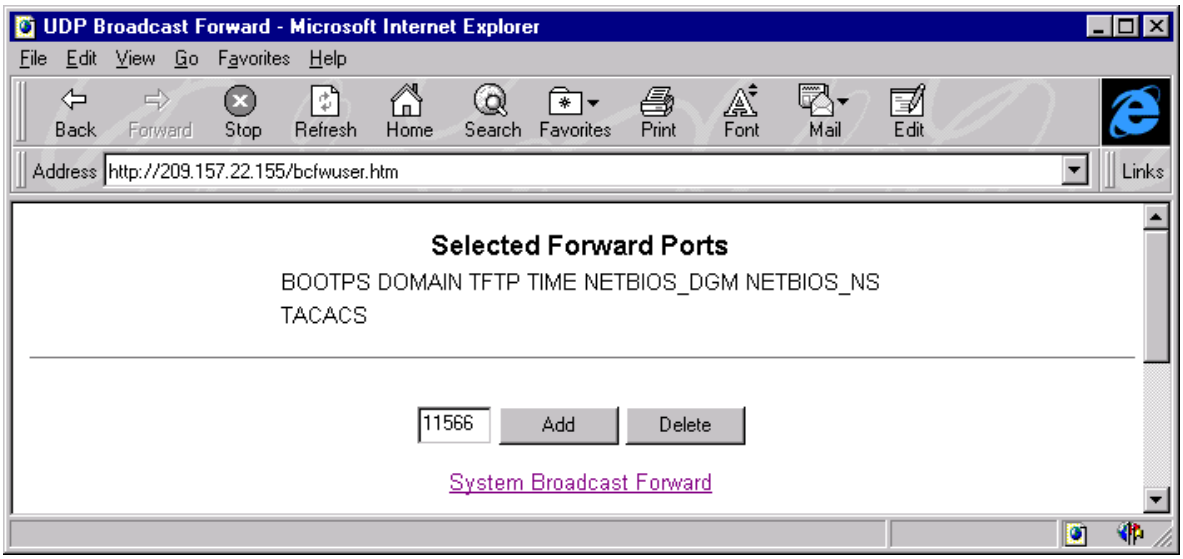

Figure 8.20 User-defined broadcast forward entry panel