Chapter 12
Configuring IPX

This chapter covers how to configure the IPX protocol on the HP routing switches using the CLI and Web management interface.

A summary of all CLI commands noting syntax along with possible values can be found in **Appendix B**.

Overview of IPX

The Internet Packet Exchange (IPX) protocol created by Novell™, is built upon a client-server networking architecture.

The Routing Information Protocol (RIP) and the Service Advertisement Protocol (SAP) are two key components of Novell NetWare and its IPX protocol suite. By default, Novell NetWare versions 3.x and 4.x broadcast RIP and SAP updates at 60 second intervals. NetWare uses these broadcasts to collect information for the routing and service tables that it uses to communicate.

Multiple IPX Frame Type Support per Interface

Up to four different IPX network numbers and frame encapsulation types can be defined for each IPX interface on an HP routing switch. This allows a user to define and receive traffic from four separate IPX networks on a single interface. Each of the networks must have a distinct network number and encapsulation type (Ethernet SNAP, Ethernet 802.2, Ethernet 802.3 and Ethernet II).

Configuring IPX

To begin using IPX on the router, the user should do the following:

1. Enable IPX on the router.
2. Enable NetBIOS on the system level.
3. Define network number, frame type and enable NetBIOS on IPX interfaces (optional).
4. Modify maximum number of RIP and SAP filters supported
5. Define RIP, SAP and forward filters (optional).
6. Assign RIP, SAP and Forward filter groups (optional).
7. Modify the maximum number of SAP and RIP Route entries supported (optional).
8. Modify the hop count increment for RIP and SAP broadcast packets (optional).

Dynamic IPX Configuration

The IPX Protocol is by default disabled at system startup. When first enabling the IPX protocol, the system must be reset but thereafter all changes to the following parameters will become effective immediately.

Global Parameters

- Enabling of NetBIOS Allow
- Defining IPX filters—Forward, RIP and SAP

Interface Parameters

- Adding, deleting or modifying IPX network numbers and frame types
- Adding, deleting or modifying filter groups assigned to interfaces

Enable IPX

The IPX Protocol is by default disabled at system startup. When first enabling the IPX protocol, the system must be reset but thereafter all changes as noted in the dynamic parameters section above will become effective immediately.

USING THE CLI

To enable IPX:

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

syntax: router ipx

USING THE WEB MANAGEMENT INTERFACE

To enable IPX:

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

Enable NetBIOS

The router can support routing of NetBIOS broadcasts (type 20) over IPX. IPX must be enabled on the router and the interface level for it to be operational. By default, this feature is disabled.

USING THE CLI

To enable NetBIOS on the router (system level), the user would enter:

```
HP9300(config)# ipx netbios-allow
```

syntax: ipx <netbios-allow | netbios-disallow>

USING THE WEB MANAGEMENT INTERFACE

To enable NetBios (type 20) on the router and an interface:

1. Select the allow NetBios (type 20) option from the IPX configuration sheet and the panel shown in **Figure 12.1** will appear.
2. Select the **enable** option.
3. Select the **apply** button to assign the changes.

NOTE: After enablimg NetBIOS at the global level the user then needs to enable it at the interface level.

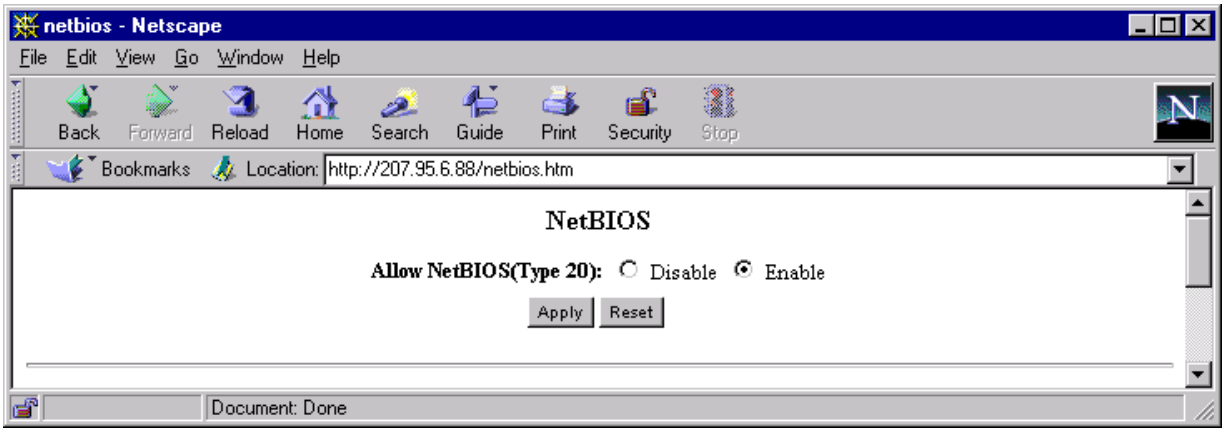

Figure 12.1 NetBIOS configuration panel

Assign IPX Network Number, Frame Type, Enable NetBios on an Interface

Once IPX is enabled on the router, IPX network numbers are assigned on an interface by interface basis. The user can also enable NetBIOS broadcasts on an interface.

USING THE CLI

EXAMPLE: To configure interfaces 1, 2 and 3 with their IPX network number and frame type as seen in **Figure 12.1**, the user would enter the following:

```
HP9300(config)# int e 2/1
HP9300(config-if-2/1)# ipx network 100 ethernet_802.2
HP9300(config-if-2/1)# int e 2/2
HP9300(config-if-2/2)# ipx network 200 ethernet_802.2
HP9300(config-if-2/2)# int e 2/3
HP9300(config-if-2/3)# ipx network 300 ethernet_802.2
```

syntax: ipx network <network number> <frame type> <net-bios-allow | netbios-disallow>

NOTE: Once an interface is configured with a network number and frame type, filters can be defined and assigned to the interface.

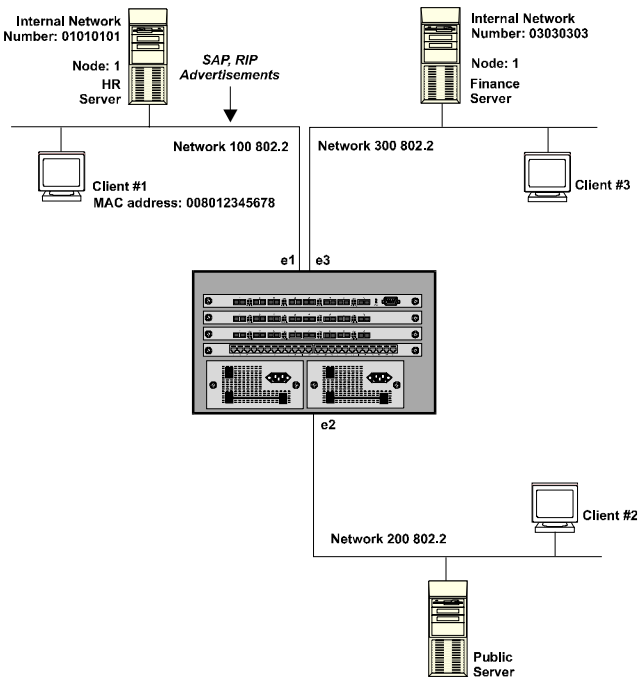

Figure 12.2 Defining and assigning IPX Forward, RIP and SAP filters

USING THE WEB MANAGEMENT INTERFACE

To assign IPX to an interfaces 1, 2 and 3 as seen in **Figure 12.2**:

1. Select the IPX link from the main menu and the panel shown in **Figure 12.3** will appear.
2. Select the **slot/port** numbers to be configured as an IPX interface from the pull down menu.
3. Enter the **network number**.
4. Select the **frame type** from the pull down menu.
5. Enable **NetBIOS** if desired.
6. Select the **add** button to assign the changes.

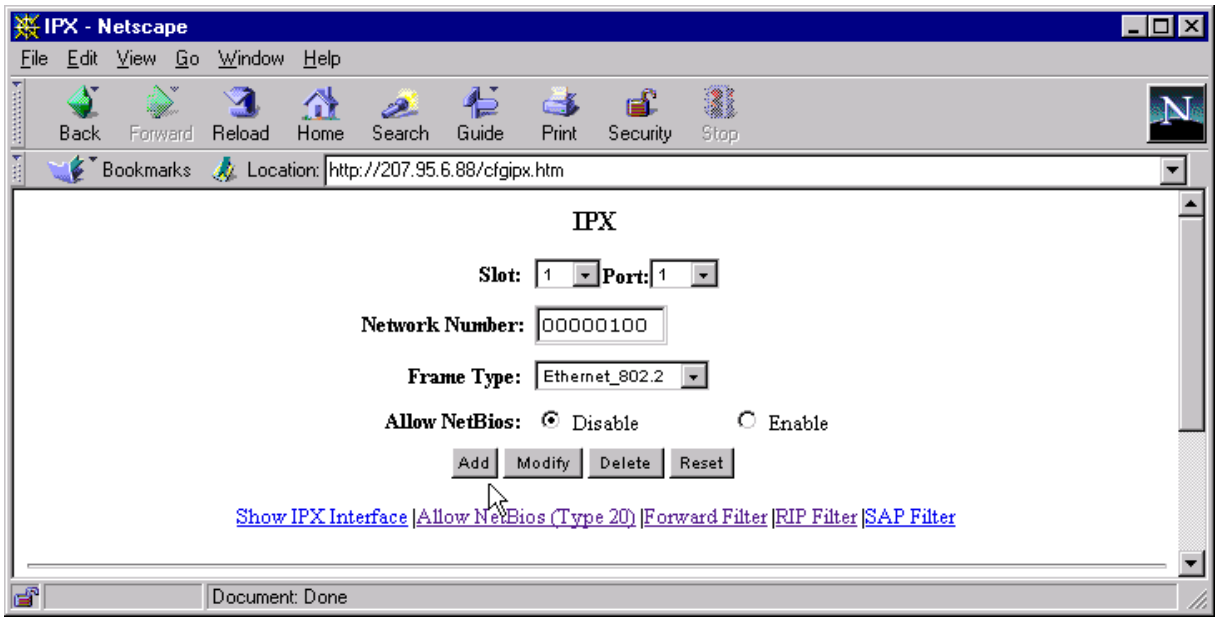

Figure 12.3 IPX configuration sheet

Define and Assign a Forward Filter and Group

A forward filter can be defined to allow a remote IPX client access to a restricted-access server.

A network number and frame type must be defined for the IPX interface before defining a forward filter. Up to 32 forward filters can be defined for each routing switch. Once a filter is defined it is assigned to an interface by using the forward filter group

EXAMPLE: To allow IPX Client 1 on network 100 access to the finance server in Network 300 (**Figure 12.2**) the user would define the following forward filter at the Global Level and then assign it to port 3 as a filter group.

NOTE: Forward filters can be assigned to either the input or output traffic on an interface.

USING THE CLI

```
HP9300(config)# ipx forward-filter 1 permit 100 008012345678 03030303 1 451

HP9300(config)# int e 2/3

HP9300(config-if-2/3)# ipx forward-filter-group in 1
```

***ipx-forward-filter syntax*:** ipx forward-filter <filterID> <permit|deny> <source network number|any> <source node number|any> <destination network number|any> <destination node number|any> <destination socket number | any>

***ipx-forward-filter-group syntax*:** ipx rip-filter-group <in|out> <filterID>

NOTE: When defining filters, the network number for a server, is its internal network number. The node number for a client will be its MAC address and the value of '1' is used to represent a server.

USING THE WEB MANAGEMENT INTERFACE

EXAMPLE: To allow IPX Client 1 on network 100 access to the finance server in Network 300 (**Figure 12.2**) the user would define the following forward filter at the Global Level and then assign it to port 3 as a filter group.

1. Select forward filter from the IPX configuration sheet, the IPX forward filter entry panel, shown in **Figure 12.3**, will appear.

   NOTE: If filters are defined on the router already, the show forward filter summary panel will appear first and the user will need to select add forward filter from that panel to assign filters.

2. Enter a filter ID value of between 1 and 32.
3. Select either **permit** or **deny**.
4. Enter the appropriate number for the destination socket of the application running in the **socket** field. Entry of all zeros in this field will allow any socket to be accepted.
5. Enter the **source network** Address on which you wish to filter traffic. Entry of all zeros in this field will allow any source network to be accepted.
6. Enter the address of the **source node** within the source network that you wish to filter traffic.
7. Enter the **destination** network number. Entry of all zeros in this field will allow any destination network number to be accepted.
8. Enter the **destination node** network number. Entry of all zeros in this field will allow any destination node network number to be accepted.
9. Select **add** to save the defined forward filter.
10. Select the forward filter group option from the Forward Filter panel. The panel shown in **Figure 12.4** will appear.

    NOTE: If forward filter group assignments already exist on the routing switch, then the show forward filter group display panel will appear first, and then the user will need to select the add filter forward group link.

11. Select the slot/port combination to which the filter(s) is to be assigned.
12. Check either or both of the **in filter** and **out filter** boxes. By checking the in box, all incoming traffic will be filtered as defined. Checking the out box will define the filter on outgoing traffic. By selecting both the in and the out boxes, the assigned filters will apply to both incoming and outgoing traffic.
13. Enter the filter ID(s) that you wish to assign to the port. Multiple filter entries can be entered and separated by commas or blanks.
14. Select the **add** button to assign the changes.

To modify or delete a forward filter:

1. Select show forward filter group from the IPX forward filter entry panel shown in **Figure 12.4**.
2. Select the **modify** or **delete** button next to the filter you wish to modify. A panel for that filter will appear.

   NOTE: If the **modify** button is selected, the configuration panel for that filter will appear. Make the desired changes, and then select the **add** button to apply the changes.

   If the **delete** button is selected, the filter will be removed immediately.

   NOTE: Any filter group assignment must first be deleted before the filter deletion will be allowed.

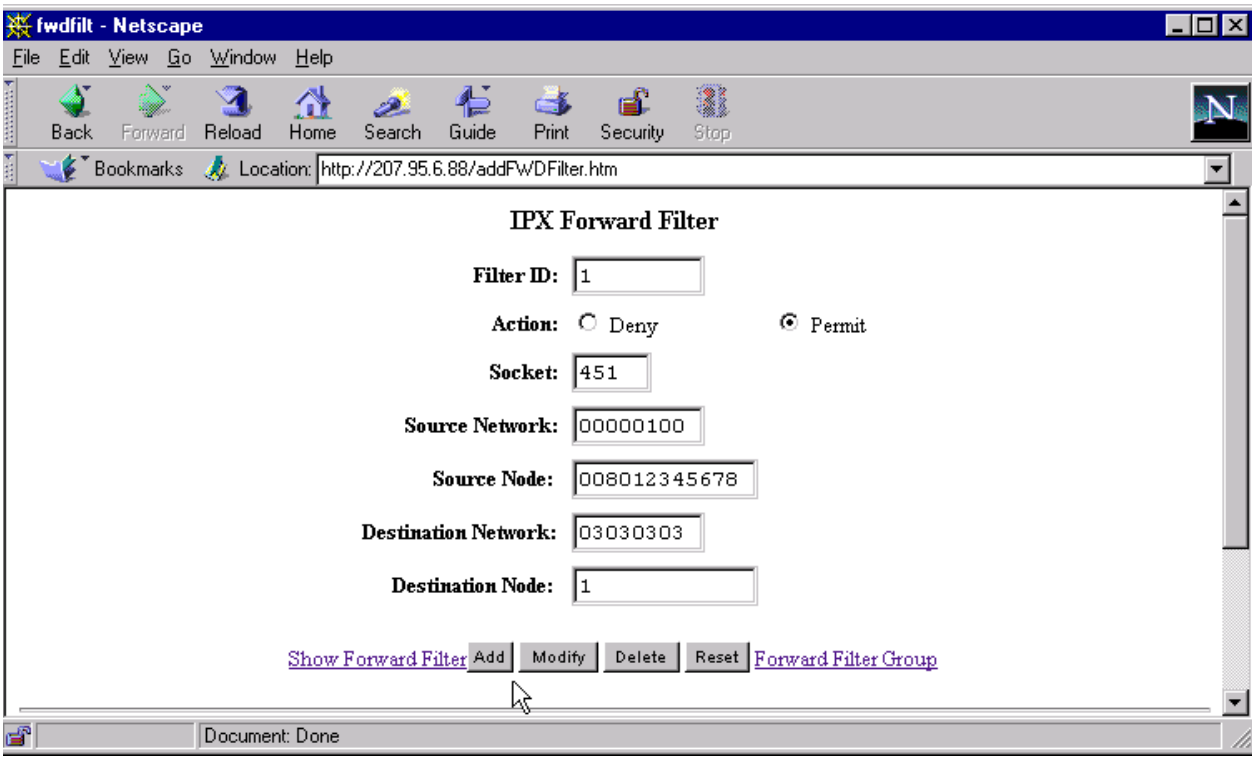

Figure 12.4 Defining a forward filter

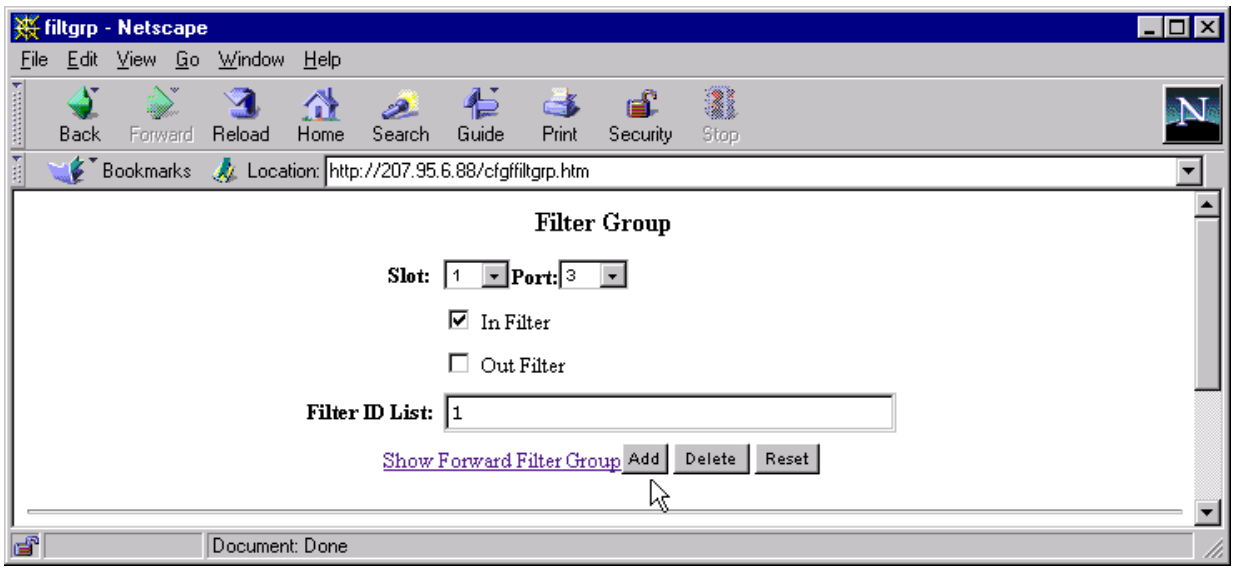

Figure 12.5 Assigning a forward filter group to an interface

Define and Assign a RIP Filter and Group

A client can define a filter for a router to block RIP routes being advertised to other parts of the network. RIP filters are defined at the global level and assigned on either a global or interface basis. Filters can be applied to either incoming or outgoing traffic.

IPX interfaces must be defined on the router before assigning a filter to an interface. Up to 128 RIP filters can be defined for a router.

EXAMPLE: To block RIP routes from being advertised outside of Network 100, shown in **Figure 12.2**, the user would define and assign the following RIP filter on interface 1:

USING THE CLI

```
HP9300(config)# ipx rip-filter 1 deny 100 01010101 any
HP9300(config-)# int e 1/1
HP9300(config-if-1/1)# ipx rip-filter-group in 1
```

***syntax*:** ipx rip-filter <filterID> <permit|deny> <network number|any> <network mask|any>

***syntax*:** ipx rip-filter-group <in|out> <filterID>

USING THE WEB MANAGEMENT INTERFACE

1. Select the RIP Filter option on the IPX configuration sheet.

   NOTE: If no RIP filters are currently defined on the system, the IPX RIP Filter entry panel will immediately appear as seen in **Figure 12.4**. If RIP filters are defined on the router, the IPX RIP Filter summary panel will appear and the user will need to select add IPX RIP filter from that panel to assign filters.

2. Enter a Filter ID value in the appropriate field as seen on **Figure 12.5**.
3. Select either **permit** or **deny**.
4. Enter the source network address on which you wish to filter traffic in the **network** field. The network field can also be assigned a wildcard value of all zeros (00000000) to allow all entries. It will appear as 'any' in the display.
5. Enter the source network address mask for the network address defined in the **mask** field. The mask field can also be assigned a wildcard value of all zeros (00000000) to allow all entries. It will appear as 'any' in the display.
6. Select the **add** button to save the filter entry.
7. Select RIP filter group from the IPX RIP Filter entry panel. The panel shown in **Figure 12.6** will appear.
8. Select the slot/port to which you want to assign the filter(s).
9. Check either or both of the **in filter** and **out filter** boxes. By checking the **in filter** box, all incoming traffic will be filtered as defined. Checking the **out filter** box will define the filter on outgoing traffic. By selecting both the in and out boxes, the assigned filters will apply to both incoming and outgoing traffic.
10. Enter the filter ID(s) you wish to assign to the port. Multiple filter entries can be entered and separated by commas or blanks. Defined RIP filters and their IDs can be seen by selecting show RIP filters from the RIP Filter panel. To reach that screen from the current one, go back one screen.
11. Select the **add** button to assign the filter group assignment.

To modify or delete a RIP Filter:

1. Select show RIP filter from the IPX RIP Filter entry panel shown in **Figure 12.6**.
2. Select the **modify** or **delete** button next to the filter you wish to modify. A panel for that filter will appear.

NOTE: If the **modify** button is selected, the configuration panel for that filter will appear. Make the desired changes, and then select the **add** button to apply the changes. If the **delete** button is selected, the filter will be removed immediately.

NOTE: Any filter group assignment must first be deleted before the filter deletion will be allowed.

To modify or delete a RIP filter group assignment:

1. Select the show RIP filter group link from the filter group panel shown in **Figure 12.7**.
2. Select the **modify** or **delete** button next to the filter group assignment to be modified or removed.

NOTE: If the **modify** button is selected, the configuration panel for that filter group will appear. Make the desired changes, and then select the **add** button links to apply the changes. If the **delete** button is selected, the entry will be removed immediately.

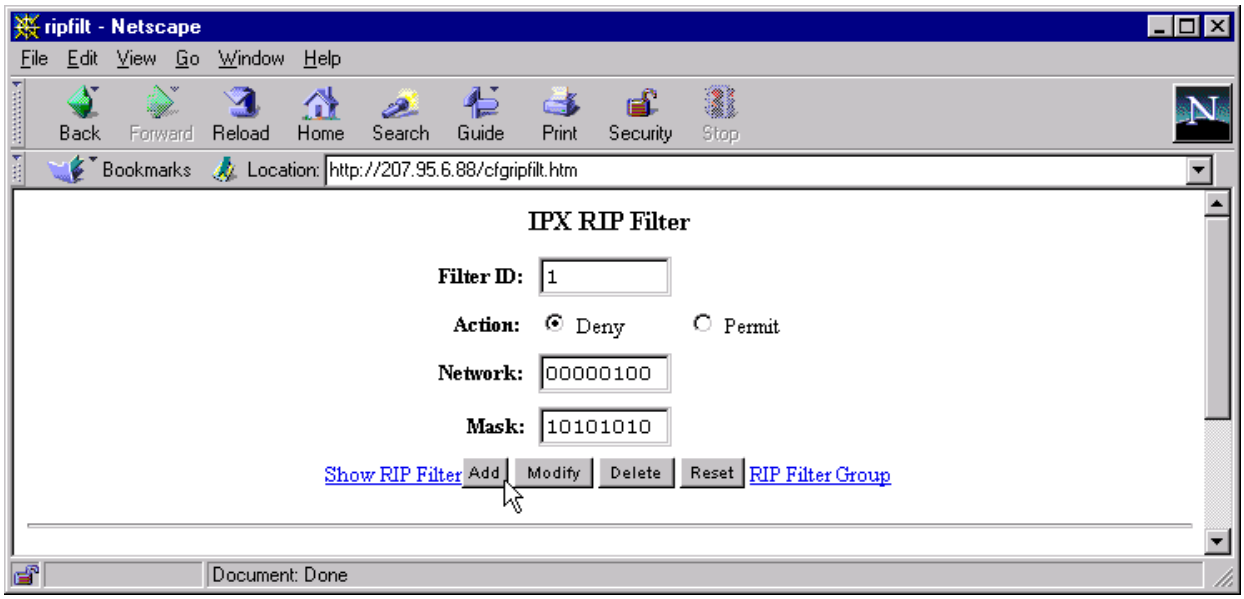

Figure 12.6 RIP filter entry panel

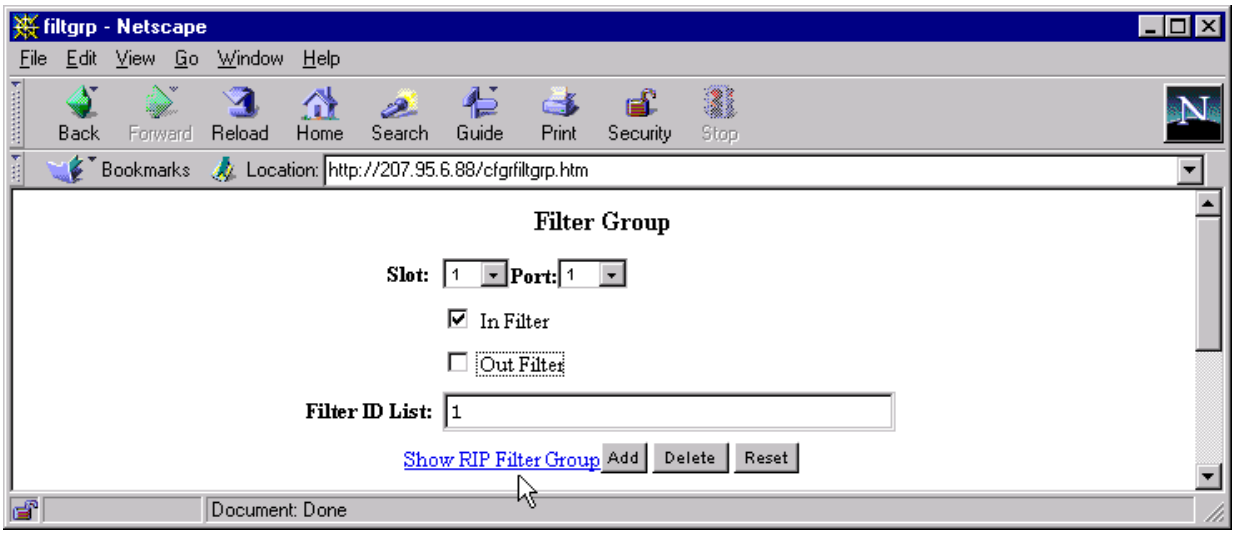

Figure 12.7 Assigning a RIP filter group to an interface

Define and Assign a SAP Filter and Group

A client can define a filter for a router to block SAP routes being advertised to other parts of the network.

IPX interfaces must be defined on the router before assigning a filter to an interface. Up to 128 SAP filters can be defined for a router.

EXAMPLE: To define a filter that will block SAP routes from the human resource server from being advertised outside of Network 100, the user would define the following SAP filter and assign it to Interface 1.

USING THE CLI

```
HP9300(config)# ipx sap-filter 5 deny 0004 hr_server
HP9300(config)# int e 1/1
HP9300 (config-if-1/1)# ipx sap-filter-group in 5
```

syntax: ipx sap-filter <filterID> <permit|deny> <server type | any> <server name | any>

syntax: ipx sap-filter-group <in|out> <filterID>

USING THE WEB MANAGEMENT INTERFACE

1. Select SAP Filter from the IPX configuration sheet. The SAP filter entry panel shown in **Figure 12.8** will appear.
2. Enter a **filter ID** value of between 1 and 32.
3. Select either **permit** or **deny**.
4. Enter the **service type**. The service type field can also be assigned a zero to allow all entries. It will appear as 'any' in the display.
5. Enter the **server name**. The server name field can also be assigned the wildcard, “any” to accept all server names.
6. Select the **add** button to add the filter.
7. Select add SAP filter group from the Show SAP Filters panel or SAP filter group from the IPX SAP Filter entry panel.
8. Select the slot/port combination to which you want to assign a filter or filters from the pull down menu.

9. Check either or both of the **in filter** and **out filter** boxes. By checking the in filter box, all incoming traffic will be filtered as defined. Checking the out filter box will define the filter on outgoing traffic. By selecting both the in and out boxes, the assigned filters will apply to both incoming and outgoing traffic.
10. Enter the filter(s) you wish to assign to the port. Commas or blanks should separate multiple filter entries.
11. Select the **add** button to assign the filter group.

To modify or delete a SAP Filter:

1. Select show SAP filter from the IPX SAP Filter entry panel.
2. Select the **modify** or **delete** button next to the filter entry you wish to change or remove.

NOTE: If the **modify** button is selected, the configuration panel for that filter group will appear. Make the desired changes, and then select the **add** button to apply the changes. If the **delete** button is selected, the filter entry will be removed immediately.

NOTE: Any filter group assignment must first be deleted before the filter deletion will be allowed.

To modify or delete a SAP filter group:

1. Select Show SAP Filter Group from the filter group assignment panel.
2. Select the **modify** or **delete** button next to the entry you wish to change or delete.

NOTE: If the **modify** button is selected, the configuration panel for that filter group will appear. Make the desired changes, and then select the **add** button to apply the changes.

NOTE: If the **delete** button is selected, the filter group assignment will be removed immediately.

NOTE: The user can view a summary of all defined filters group assignments, by selecting SAP filter group from the filter group entry panel.

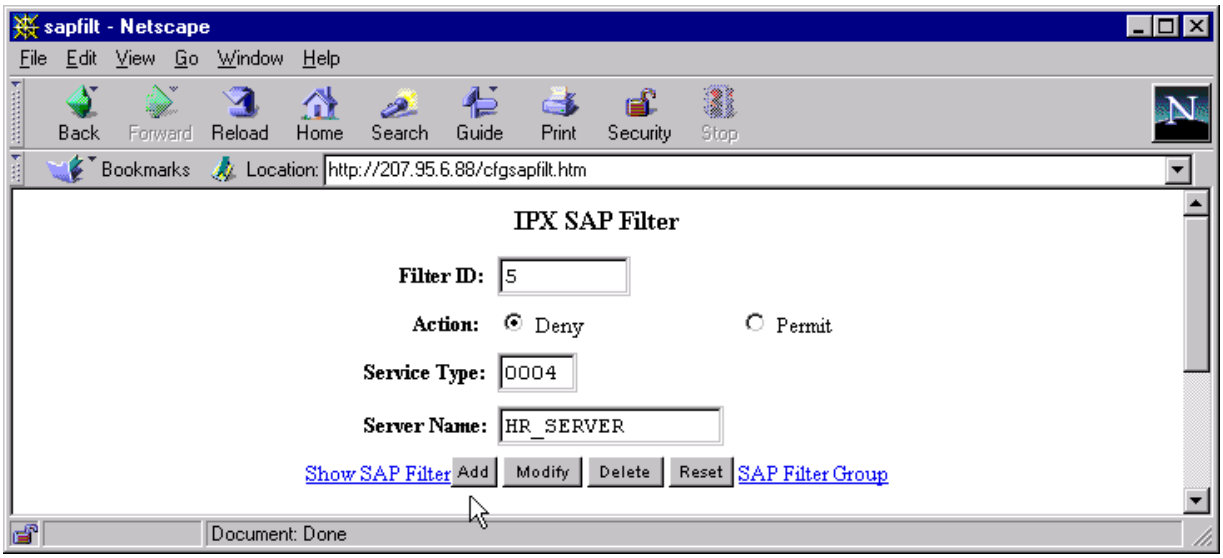

Figure 12.8 SAP filter entry panel

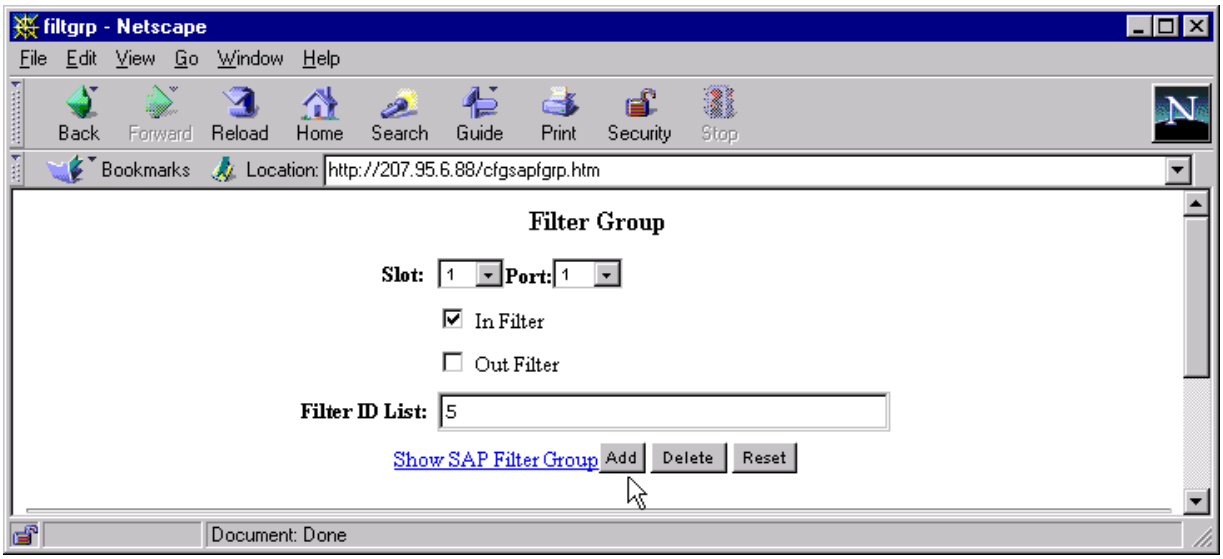

Figure 12.9 Assigning a SAP filter group to an interface

Modify Maximum SAP and RIP Route Entries

The user can define a maximum number of IPX/RIP and IPX/SAP routes that will be stored and forwarded. IPX must be enabled on the router for these items to be configurable.

Between 64 and 8,192 RIP entries can be defined. The default number of RIP entries supported is 2,048.

Between 64 and 8,192 SAP entries can be defined. The default number of SAP entries supported is 4,096.

USING THE CLI

To limit the number of RIP entries stored to 3000 from a default of 2048, the user would enter:

```
HP9300(config)# system-max-ipx-rip-entry 3500
```

***syntax*:** system-max-ipx-rip-entry <value>

To limit the number of SAP entries stored to 6000 from a default of 4096, the user would enter:

```
HP9300(config)# ipx max-sap-entries 6000
```

***syntax*:** system-max-ipx-sap-entry <value>

USING THE WEB MANAGEMENT INTERFACE

To modify the maximum number of RIP or SAP route entries supported on a router:

1. Select the Parameter link found on the System configuration sheet.
2. Select the **modify** button next to the parameter to be changed.
3. Enter the new value for the parameter within the prescribed range of values.
4. Select the **add** button to assign the changes.

Modify RIP and SAP Hop Count Increment

The user can modify the incremental value that is added to a RIP or SAP record before it is propogated to the next interface. By default, a value of one will be added to a record before it is broadcast to the next interface.

In a network of parallel routers, the router that receives a RIP or SAP record with the lowest hop count is seen as the router with the most optimal information and is seen as the primary router. As primary router, it is elected to forward the packet to the next interface.

A user can manage which router is selected as the primary router by a host by modifying the hop count assigned to an IPX interface. For example, in **Figure 12.10**, a user wants to ensure that all traffic between server1 and server2 is routed through router 1 and that it is seen as the primary router. To ensure that this occurs, the user can assign higher hop counts (e.g. 10) to the router interfaces on router 2.

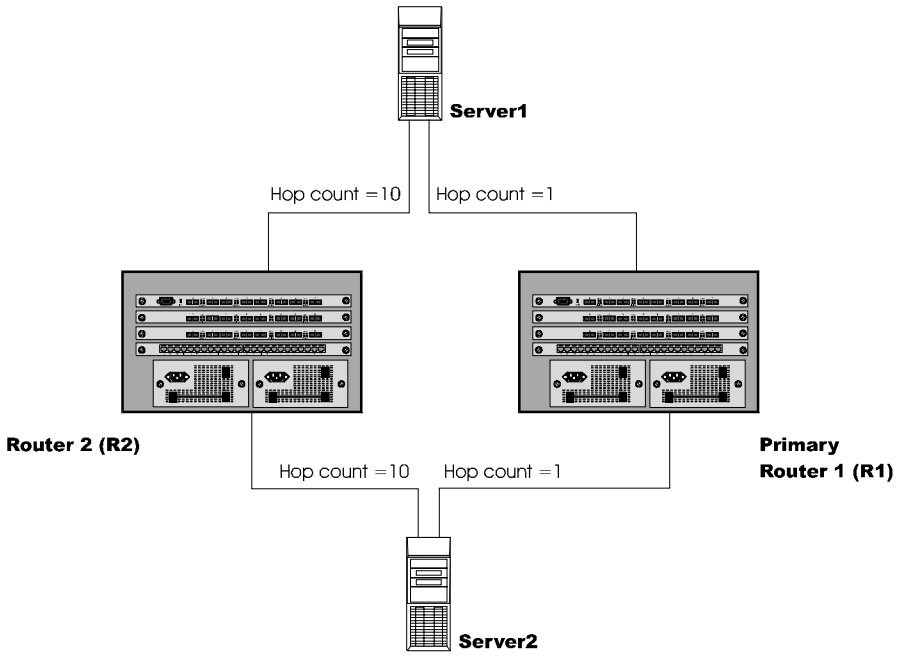

Figure 12.10 Using higher hop count assignments to bias traffic away from the router

USING THE CLI

To increase the hop count increment assessed to an interface (e.g. 5 on slot 1), the user would enter the following:

```
HP9300(config)# int e 1/5
HP9300(config-if-1/5)# ipx-rip-update-hop-count-increment <2-15>
HP9300(config-if-1/5)# ipx-sap-update-hop-count-increment <2-15>
```

***syntax*:**ipx-rip-update-hop-count-increment <2-15>, ipx-sap-update-hop-count-increment <2-15>

USING THE WEB MANAGEMENT INTERFACE

This parameter cannot be configured with the Web management interface.