Chapter 11
Configuring IPX

This chapter describes how to configure the Internet Packet Exchange (IPX) protocol on the HP 9304M, HP 9308M, and HP 6208M-SX routing switches using the CLI and Web management interface.

To display IPX configuration information and statistics, see “Displaying IPX Configuration Information and Statistics” on page 11-16.

For complete syntax information for the CLI commands shown in this chapter, see the *Command Line Interface Reference*.

Overview of IPX

The IPX protocol was created by Novell™. IPX 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 for communicating.

NOTE: IPX/RIP is different from IP/RIP. IP/RIP configuration parameters do not apply to IPX/RIP and IPX/RIP parameters do not apply to IP/RIP.

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 a routing switch. The multiple encapsulation support allows you to define and receive traffic from four separate IPX networks on a single interface. Each network must have a distinct network number and encapsulation type (Ethernet SNAP, Ethernet 802.2, Ethernet 802.3, or Ethernet II).

Configuring IPX

To use IPX on the routing switch, perform the following tasks:

1. Enable IPX on the routing switch.
2. Enable NetBIOS on the system level.
3. Define the network number and 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).
9. Modify the maximum advertisement packet size for RIP and SAP packets (optional).
10. Modify the advertisement interval for RIP and SAP updates (optional).
11. Modify the age timer for learned RIP and SAP entries (optional).

Dynamic IPX Configuration

The IPX Protocol is by default disabled at system startup. When you first enable IPX, you must reset the system. However, after you reset the system all changes to the following parameters 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
- Modifying the RIP advertisement packet size
- Modifying the SAP advertisement packet size
- Modifying the RIP advertisement interval
- Modifying the SAP advertisement interval
- Modifying the age timer for learned IPX routes
- Modifying the age timer for learned SAP entries

Enable IPX

The IPX Protocol is by default disabled at system startup.

NOTE: Make sure you restart the system after enabling IPX. After you restart, additional IPX parameter settings take effect immediately.

USING THE CLI

To enable IPX, enter the following commands:

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

Syntax: router ipx

USING THE WEB MANAGEMENT INTERFACE

To enable IPX:

1. Log on to the device using a valid user name and password for read-write access. The System configuration dialog is displayed.
2. Select the Enable radio button next to IPX.
3. Click the Apply button to apply the changes to the device's running-config file.

4. Select the Save link at the bottom of the dialog. Select Yes when prompted to save the configuration change to the startup-config file on the device's flash memory.
5. Click on the plus sign next to Command in the tree view to list the command options.
6. Select the Reload link and select Yes when prompted to reload the software. You must reload after enabling IPX to place the change into effect.

Enable NetBIOS

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

USING THE CLI

To enable NetBIOS on the routing switch (system level), enter the following command:

```
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. Log on to the device using a valid user name and password for read-write access. The System configuration dialog is displayed.
2. Click on the plus sign next to Configure in the tree view to expand the list of configuration options.
3. Click on the plus sign next to IPX in the tree view to expand the list of IPX option links.
4. Click on the Allow NetBIOS (Type 20) link to display the NetBIOS panel.
5. Select Enable.
6. Click the Apply button to apply the changes to the device's running-config file.
7. Select the Save link at the bottom of the dialog. Select Yes when prompted to save the configuration change to the startup-config file on the device's flash memory.

NOTE: After enabling NetBIOS at the global level, you need to enable NetBIOS at the interface level.

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

Once you enable IPX on the routing switch, you can assign IPX network numbers on an interface-by-interface basis. You also can enable NetBIOS broadcasts on an interface.

USING THE CLI

EXAMPLE:

To configure interfaces 1, 2, and 3 with the IPX network number and frame type shown in Figure 11.1, enter the following commands:

```
HP9300(config)# int e1/1
HP9300(config-if-1/1)# ipx network 100 ethernet_802.2
HP9300(config-if-1/1)# int e1/2
HP9300(config-if-1/2)# ipx network 200 ethernet_802.2
HP9300(config-if-1/2)# int e1/3
HP9300(config-if-1/3)# ipx network 300 ethernet_802.2
```

Syntax: ipx network <network-number> <frame-type> [netbios-allow | netbios-disallow]

NOTE: Once you configure an interface with a network number and frame type, you can define filters and assign them to the interface.

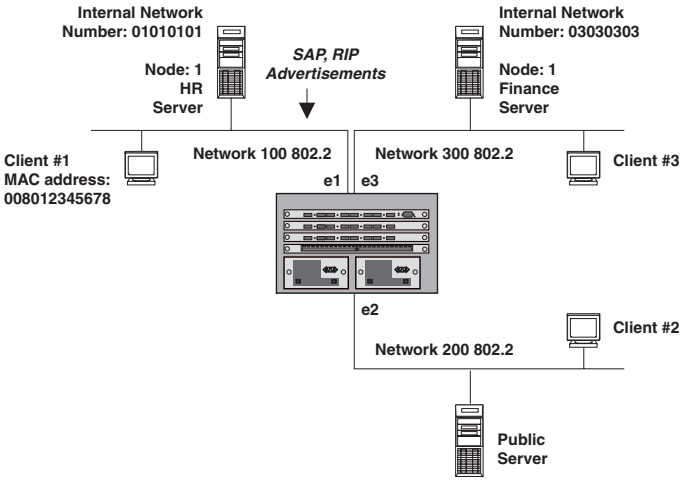
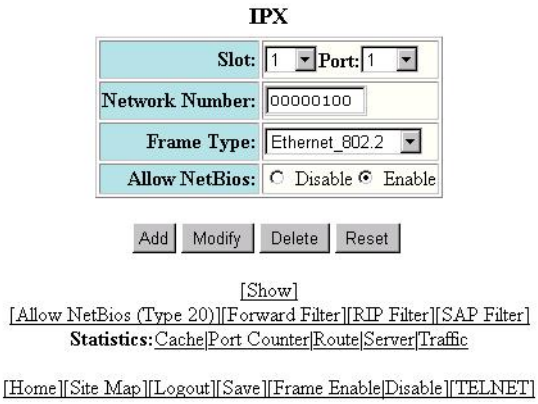


Figure 11.1 Defining and assigning IPX Forward, RIP and SAP filters

USING THE WEB MANAGEMENT INTERFACE

To assign IPX to interfaces 1, 2 and 3 as shown in Figure 11.1:

1. Log on to the device using a valid user name and password for read-write access. The System configuration dialog is displayed.
2. Click on the plus sign next to Configure in the tree view to expand the list of configuration options.
3. Click on the plus sign next to IPX in the tree view to expand the list of IPX option links.
4. Click on the Interface link.
   - If the device does not have an IPX interface configured, the IPX configuration panel is displayed, as shown in the following example.
   - If an IPX interface is already configured and you are adding a new one, click on the Configure IPX Interface link to display the IPX interface configuration panel, as shown in the following example.
   - If you are modifying an existing IPX interface, click on the Modify button to the right of the row describing the interface to display the IPX configuration panel, as shown in the following example.



5. Select the port or slot/port numbers to be configured as an IPX interface from the pull down menu.

6. Enter the network number.
7. Select the frame type from the pull down menu.
8. Enable NetBIOS if desired.
9. Click the Add button to apply the changes to the device's running-config file.
10. Select the Save link at the bottom of the dialog. Select Yes when prompted to save the configuration change to the startup-config file on the device's flash memory.

Define and Assign a Forward Filter and Group

You can define a forward filter to allow a remote IPX client access to a restricted-access server. You can define up to 32 forward filters on a routing switch. Once you define the filter, you assign the filter to an interface by placing the filter in a forward filter group.

NOTE: A network number and frame type must be defined for the IPX interface before defining a forward filter.

EXAMPLE:

To allow IPX Client 1 on network 100 access to the finance server in Network 300 (Figure 11.1), define the following forward filter at the Global Level and then assign the filter to port 1/3 as a filter group.

NOTE: You can assign forward filters 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 e1/3
HP9300(config-if-1/3)# ipx forward-filter-group in 1
```

Syntax: ipx forward-filter <filter-id> permit | deny <source-network-number> | any <source-node-number> | any <destination-network-number> | any <destination-node-number> | any <destination-socket-number> | any

Syntax: ipx forward-filter-group in | out <filter-id>

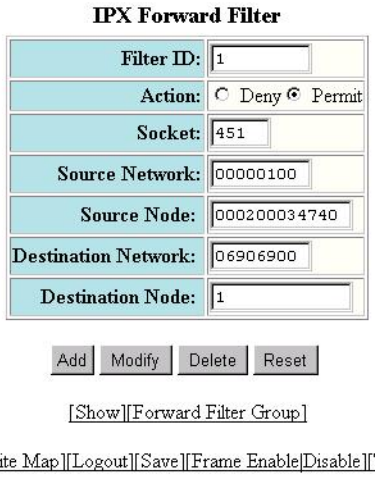
NOTE: When you define filters, the network number for a server is its internal network number. The node number for a client is the client's MAC address. The value 1 represents a server.

USING THE WEB MANAGEMENT INTERFACE

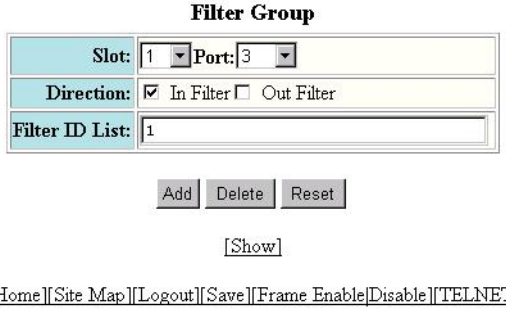
EXAMPLE:

To allow IPX Client 1 on network 100 access to the finance server in Network 300 (Figure 11.1), define the following forward filter at the Global Level and then assign it to port 1/3 as a filter group.

1. Log on to the device using a valid user name and password for read-write access. The System configuration dialog is displayed.
2. Click on the plus sign next to Configure in the tree view to expand the list of configuration options.
3. Click on the plus sign next to IPX in the tree view to expand the list of IPX option links.
4. Click on the Forward Filter link.
   - If the device does not have an IPX forward filter configured, the IPX Forward Filter configuration panel is displayed, as shown in the following example.
   - If an IPX forward filter is already configured and you are adding a new one, click on the Add Forward Filter link to display the IPX Forward Filter configuration panel, as shown in the following example.
   - If you are modifying an existing IPX forward filter, click on the Modify button to the right of the row describing the filter to display the IPX Forward Filter configuration panel, as shown in the following example.



5. Enter a filter ID value from 1 – 32.
6. Select either Permit or Deny.
7. Enter the appropriate number for the destination socket of the application running in the Socket field. If you enter all zeros in this field, the filter will accept any socket.
8. Enter the Source Network Address on which you want to filter traffic. If you enter all zeros in this field, the filter will accept any source network.
9. Enter the address of the Source Node within the source network on which you want to filter traffic.
10. Enter the Destination network number. If you enter all zeros in this field, the filter will accept any destination network number.
11. Enter the Destination Node network number. If you enter all zeros in this field, the filter will accept any destination node network number.
12. Click the Add button to apply the changes to the device's running-config file.
13. Select the Forward Filter Group link.
    - If the device does not have an IPX forward filter group configured, the Filter Group configuration panel is displayed, as shown in the following example.
    - If an IPX forward filter group is already configured and you are adding a new one, click on the Add Forward Filter Group link to display the IPX Filter Group configuration panel, as shown in the following example.
    - If you are modifying an existing IPX forward filter group, click on the Modify button to the right of the row describing the group to display the IPX Filter Group configuration panel, as shown in the following example.



14. Select the port or slot/port combination to which you are assigning the filter(s).
15. Check either or both of the In Filter and Out Filter boxes. If you check the In Filter box, all incoming traffic is filtered as defined. If you check the Out Filter box, all outgoing traffic is filtered. By selecting both the In Filter and Out Filter boxes, you can assign the filters to both incoming and outgoing traffic.
16. Enter the filter ID(s) that you want to assign to the port. You can enter multiple filters entries separated by commas or blanks.
17. Click the Add button to apply the changes to the device's running-config file.
18. Select the Save link at the bottom of the dialog. Select Yes when prompted to save the configuration change to the startup-config file on the device's flash memory.

Define and Assign an IPX/RIP Filter and Group

You can define a filter for a routing switch to block RIP routes being advertised to other parts of the network. You define RIP filters at the global level and assign them on either a global or interface basis. You can apply filters to either incoming or outgoing traffic. You can define up to 128 IPX/RIP filters on a routing switch.

NOTE: An IPX interface must be defined on the routing switch before you can assign a filter to that interface.

EXAMPLE:

To block RIP routes from being advertised outside of Network 100, shown in Figure 11.1, 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 e1/1
HP9300(config-if-1/1)# ipx rip-filter-group in 1
```

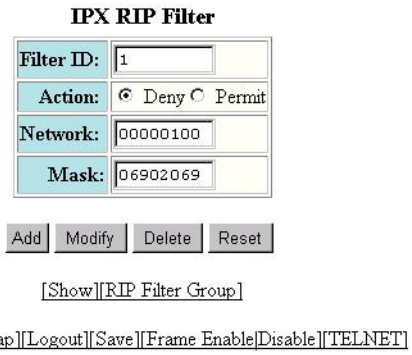
Syntax: ipx rip-filter <filter-id> permit | deny <network-number> | any <network-mask> | any

Syntax: ipx rip-filter-group in | out <filter-id>

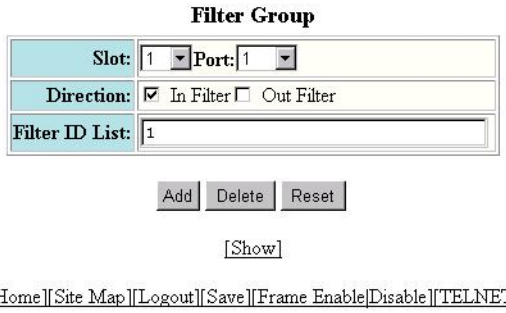
USING THE WEB MANAGEMENT INTERFACE

1. Log on to the device using a valid user name and password for read-write access. The System configuration dialog is displayed.
2. Click on the plus sign next to Configure in the tree view to expand the list of configuration options.
3. Click on the plus sign next to IPX in the tree view to expand the list of IPX option links.
4. Click on the RIP Filter link.
   - If the device does not have an IPX RIP filter configured, the IPX RIP Filter configuration panel is displayed, as shown in the following example.
   - If an IPX RIP filter is already configured and you are adding a new one, click on the Add RIP Filter link to display the IPX RIP Filter configuration panel, as shown in the following example.

- If you are modifying an existing IPX RIP filter, click on the Modify button to the right of the row describing the filter to display the IPX RIP Filter configuration panel, as shown in the following example.



5. Enter a Filter ID value in the Filter ID field.
6. Select either Permit or Deny.
7. Enter the source network address on which you want to filter traffic in the Network field. You also can assign a wildcard value of all zeros (00000000) to allow all entries. The zeroes appear as 'any' in the display.
8. Enter the source network address mask for the network address in the Mask field. You can assign a wildcard value of all zeros (00000000) to allow all entries. The zeroes appear as 'any' in the display.
9. Click the Add button to apply the changes to the device's running-config file.
10. Select the RIP Filter Group link.
    - If the device does not have an IPX RIP filter group configured, the Filter Group configuration panel is displayed, as shown in the following example.
    - If an IPX RIP filter group is already configured and you are adding a new one, click on the Add RIP Filter Group link to display the Filter Group configuration panel, as shown in the following example.
    - If you are modifying an existing IPX RIP filter group, click on the Modify button to the right of the row describing the group to display the Filter Group configuration panel, as shown in the following example.



11. Select the port to which you want to assign the filter(s).
12. Check either or both of the In Filter and Out Filter boxes. If you check the In Filter box, all incoming traffic is filtered. If you check the Out Filter box, all outgoing traffic is filtered. If you check both In Filter and Out Filter, the assigned filters apply to both incoming and outgoing traffic.
13. Enter the filter ID(s) you want to assign to the port. You can enter multiple filter entries separated by commas or blanks.
14. Click the Add button to apply the changes to the device's running-config file.
15. Select the Save link at the bottom of the dialog. Select Yes when prompted to save the configuration change to the startup-config file on the device's flash memory.

Configuring IPX SAP Access Control Lists (ACLs)

You can configure Access Control Lists (ACLs) for filtering Service Advertisement Protocol (SAP) replies sent on a routing switch's IPX interfaces. You configure IPX SAP access lists on a global basis, then apply them to the IPX inbound or outbound filter group on specific interfaces. You can configure up to 32 access lists. The same access list can be applied to multiple interfaces.

When you configure more than one access list on an IPX interface, the software applies the access lists in numerical order. For example, if you configure access lists 1, 10, and 32 and apply them to an interface, the software applies access list 1 first, then access list 10, then access list 32. This is true regardless of the order in which you configure the access lists. At the first match, the software takes the action specified by the access list (deny or permit) and stops comparing the update against the access lists.

IPX SAP access lists apply to SAP updates sent or received by the routing switch. You can apply them to a port's inbound or outbound IPX traffic.

NOTE: IPX access lists replace the IPX filter mechanism in software releases earlier than 06.x. The older commands are supported for backward compatibility but are not listed in the on-line help. If the devices' startup-config file contains IPX filter commands of the older format, they are replaced by equivalent IPX ACL commands when you save the device's configuration while running 06.x or later.

Before you configure an access list on an IPX interface, all SAP updates are sent and received by default. However, once you configure an access filter, the default action changes from permit to deny. Thus, SAP updates that are not explicitly permitted are denied. To change the default action to permit, configure SAP access list 32 to permit all updates on all networks.

NOTE: Each IPX SAP access list is a single filter. This is different from the system-wide ACLs, which each can contain multiple individual filters. See "Using Access Control Lists (ACLs)" on page 3-1.

To configure IPX access lists, use the following CLI method.

USING THE CLI

To configure three IPX access lists and apply them to IPX interfaces on port 1/1, enter the following commands:

```
HP9300(config)# router ipx
HP9300(config-ipx-router)# ipx sap-access-list 1 deny abcd
HP9300(config-ipx-router)# ipx sap-access-list 10 deny efef.1234.1234.1234
HP9300(config-ipx-router)# ipx sap-access-list 32 permit -1 0
HP9300(config-ipx-router)# exit
HP9300(config)# int e 1/1
HP9300(config-if-1/1)# ipx sap-filter-group out 10 20 32
HP9300(config-if-1/1)# write memory
```

In this example, access list 1 denies all SAP updates containing IPX network abcd. Access list 10 denies SAP updates for print server "Prt1" from network efef, node 1234.1234.1234. Access list 32 ensures that all updates that are not denied by the preceding access lists are permitted.

Syntax: [no] ipx sap-access-list <num> deny | permit <network>[.<node>] [<network-mask>.<node-mask>] [<service-type> [<server-name>]]

Syntax: [no] ipx sap-filter-group in | out <num> [<num>…]

The <num> parameter specifies the access list number and can be from 1 – 32.

The **deny | permit** parameter specifies whether the routing switch allows the SAP update or denies it.

The <network>[.<node>] parameter specifies the IPX network. Optionally, you also can specify a specific node (host) on the network. The <network> parameter can be an eight-digit hexadecimal number from 1 – FFFFFFFE. To specify all networks ("any"), enter –1 as the network number. If the network number has leading zeros, you do not need to specify them. For example, you can specify network 0000abab as "abab".

The node is a 48-bit value represented by three four-digit numbers joined by periods; for example, 1234.1234.1234.

The [<network-mask>.<node-mask>] parameter lets you specify a comparison mask for the network and node. The mask consists of zeros (0) and ones (f). Ones indicate significant bits. For example, to configure a mask that matches on network abcdef*xx*, where *xx* can be any value and the node address can be any value, specify the following mask: ffffff00.0000.0000.0000

NOTE: To apply an ACL for filtering GNS replies to an interface, you must use the **ipx output-gns-filter** command instead of the **ipx sap-filter-group** command. See "Filter GNS Replies" on page 11-10.

The **in** | **out** parameter of the **ipx sap-filter-group** command specifies whether the ACLs apply to incoming traffic or outgoing traffic.

USING THE WEB MANAGEMENT INTERFACE

You cannot configure a SAP access list using the Web management interface.

Enable Round-Robin GNS Replies

By default, the routing switch replies to a GNS request with the most recently learned server supporting the requested service. You configure the routing switch to instead use round-robin to rotate among servers of a given service type when responding to GNS requests. To do so, use one of the following methods.

USING THE CLI

To enable the routing switch to use round-robin to select servers for replies to GSN requests, enter the following commands:

```
HP9300(config)# ipx gns-round-robin
HP9300(config)# write memory
```

Syntax: [no] ipx gns-round-robin

USING THE WEB MANAGEMENT INTERFACE

You cannot enable round-robin for GNS replies using the Web management interface.

Filter GNS Replies

You can use IPX access lists to permit or deny specific services and servers in GNS replies to specific IPX nodes (hosts). To do so, use either of the following methods to configure IPX access lists that include service and server information, then apply them to specific ports.

USING THE CLI

To configure IPX ACLs and apply them to a port to control responses to GNS requests on that port, enter commands such as the following:

```
HP9300(config)# router ipx
HP9300(config-ipx-router)# ipx sap-access-list 2 deny efff 47 Prt0
HP9300(config-ipx-router)# ipx sap-access-list 20 deny aaaa.bbbb.cccc.dddd 47 Prt1
HP9300(config-ipx-router)# ipx sap-access-list 32 permit -1 0
HP9300(config-ipx-router)# exit
HP9300(config)# int e 1/1
HP9300(config-if-1/1)# ipx output-gns-filter 10 20 32
HP9300(config-if-1/1)# write memory
```

The commands in this example configure three ACLs. Two of the ACLs contain server network, service type, and server information and deny reporting these servers to the clients. For example, ACL 2 does not permit the routing switch from sending server "Prt0" with network efff in GNS replies to the client.

ACL 32 changes the default action from deny to permit. All GNS replies that are not explicitly denied by other ACLs are permitted by this one.

Syntax: [no] ipx sap-access-list <num> deny | permit <network>[.<node>] [<network-mask>.<node-mask>] [<service-type> [<server-name>]]

The <service-type> [<server-name>] parameter lets you specify a service type and, optionally, a specific server. Use these parameters when you are configuring an ACL for filtering Get Nearest Server (GNS) replies. The service type is a hexadecimal number. To specify all service types (“any”), enter 0. For a list of service types, see the software documentation for your IPX servers. If you also enter the sever name, the access list applies only to updates for that server, not to other serves of the same type.

For information about the other parameters, see “Configuring IPX SAP Access Control Lists (ACLs)” on page 11-9.

Syntax: [no] ipx output-gns-filter <num> [<num>…]

USING THE WEB MANAGEMENT INTERFACE

You cannot configure GNS reply filters using the Web management interface.

Disable GNS Replies

When IPX is enabled in the routing switch, the device responds to all GNS requests by default. You can disable GNS replies on individual routing switch ports. Use one of the following methods to do so.

USING THE CLI

To disable IPX GNS replies on port 1/1, enter the following commands. GNS replies are disabled for all IPX interfaces on the port.

```
HP9300(config)# int eth 1/1
HP9300(config-if-1/1)# ipx gns-reply-disable
HP9300(config-if-1/1)# write memory
```

Syntax: [no] ipx gns-reply-disable

USING THE WEB MANAGEMENT INTERFACE

You cannot disable IPX GNS replies using the Web management interface.

Modify Maximum SAP and RIP Route Entries

You can define the maximum number of IPX/RIP and IPX/SAP routes that the router can store and forward.

- From 64 – 8192 RIP entries can be defined. The default number of RIP entries supported is 2048.
- From 64 – 8192 SAP entries can be defined. The default number of SAP entries supported is 4096.

NOTE: IPX must be enabled on the router for these items to be configurable.

USING THE CLI

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

```
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, enter the following command:

```
HP9300(config)# system-max ipx-sap-entry 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. Log on to the device using a valid user name and password for read-write access. The System configuration panel is displayed.
2. Select the Max-Parameter link to display the Configure System Parameter Maximum Value table. This table lists the settings and valid ranges for all the configurable table sizes on the device.
3. Click the Modify button next to ipx-rip-entry or ipx-sap-entry.

4. Enter the new value for the table size. The value you enter specifies the maximum number of entries the table can hold.
5. Click Apply to save the changes to the device's running-config file.
6. Select the Save link at the bottom of the dialog. Select Yes when prompted to save the configuration change to the startup-config file on the device's flash memory.
7. Click on the plus sign next to Command in the tree view to list the command options.
8. Select the Reload link and select Yes when the Web management interface asks you whether you really want to reload the software. Changes to table sizes do not take effect until you reload the software.

Modify RIP and SAP Hop Count Increment

You can modify the incremental value (hop) that the routing switch adds to a RIP or SAP record before propagating the record to the next interface. By default, a value of one is 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.

You 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 11.2, an administrator wants to ensure that all traffic between server1 and server2 is routed through router 1 and that router 1 is seen as the primary router. To ensure that this occurs, the administrator can assign higher hop counts (for example, 10) to the router interfaces on router 2.

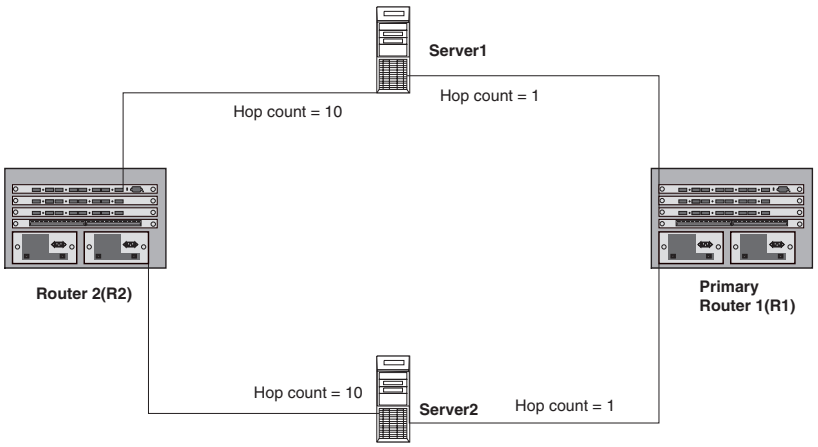


Figure 11.2 Using higher hop count assignments to bias traffic away from the router

USING THE CLI

To increase the hop count increment assessed to interface 1/5, enter the following commands:

```
HP9300(config)# int e 1/5
HP9300(config-if-1/5)# ipx-rip-update-hop-count-increment 10
HP9300(config-if-1/5)# ipx-sap-update-hop-count-increment 10
```

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

USING THE WEB MANAGEMENT INTERFACE

You cannot modify hop count increments using the Web management interface.

Modify the RIP Advertisement Packet Size

The default IPX RIP packet size is 432 bytes, which allows 50 routes plus 32 bytes of header in an IPX RIP update packet. Each route requires eight bytes. You can configure the packet size to be from 40 bytes (enough for one route) – 1488 bytes (enough for 182 routes).

NOTE: You can specify packet length that does not fall evenly on a route or server boundary. The device will use the packet size but will include only the number of routes or servers that fit entirely within the packet.

To change the RIP advertisement packet size, use the following CLI method.

USING THE CLI

EXAMPLE:

To change the maximum packet size of IPX RIP advertisements sent on interface 1/1 from the default 432 bytes to 832 bytes, enter the following command. This command increases the number of IPX RIP routes an advertisement packet holds from 50 to 100.

```
HP9300(config) int e 1/1
HP9300(config-if-1/1) ipx rip-max-packetsize 832
HP9300(config-if-1/1) write memory
```

Syntax: ipx rip-max-packetsize <bytes>

The number of bytes can be from 40 bytes (enough for one route) – 1488 bytes (enough for 182 routes). The default is 432 bytes.

USING THE WEB MANAGEMENT INTERFACE

You cannot modify the RIP advertisement packet size using the Web management interface.

Modify the SAP Advertisement Packet Size

The default IPX SAP packet size is 480 bytes, which allows seven servers plus 32 bytes of header in an IPX SAP update packet. Each server requires 64 bytes. You can configure the packet size to be from 96 bytes (enough for one server) – 1440 bytes (enough for 22 servers).

NOTE: You can specify packet length that does not fall evenly on a route or server boundary. The device will use the packet size but will include only the number of routes or servers that fit entirely within the packet.

To change the SAP advertisement packet size, use the following CLI method.

USING THE CLI

EXAMPLE:

To change the maximum number of bytes in IPX SAP advertisements sent on interface 5/1 from 480 to 672 (enough for 10 servers plus the 32 bytes of packet header), enter the following commands:

```
HP9300(config) int e 5/1
HP9300(config-if-5/1) ipx sap-max-packetsize 672
HP9300(config-if-5/1) write memory
```

Syntax: ipx sap-max-packetsize <bytes>

The number of bytes can be from 96 bytes (enough for one server) – 1440 bytes (enough for 22 servers). The default is 480 bytes.

USING THE WEB MANAGEMENT INTERFACE

You cannot modify the SAP advertisement packet size using the Web management interface.

Modify the RIP Advertisement Interval

The IPX RIP advertisement interval specifies how often the routing switch sends IPX RIP updates to neighboring IPX routers. The update intervals are separate for RIP and SAP and are configurable on an individual interface basis.

By default, the routing switch sends an IPX RIP update every 60 seconds. You can change the interval to be from 10 – 65535 seconds. You cannot disable the advertisements.

NOTE: If you change an advertisement interval, you do not need to change the age time. The software automatically calculates the age time by multiplying the advertisement interval times the age timer, which is 3 by default.

To change the RIP advertisement interval, use the following CLI method.

USING THE CLI

EXAMPLE:

To change the advertisement interval for IPX RIP advertisements sent on interface 1/1 from 60 seconds to 30 seconds, enter the following commands:

```
HP9300(config) int e 1/1
HP9300(config-if-1/1) ipx update-time 30
HP9300(config-if-1/1) write memory
```

Syntax: ipx update-time <interval>

The <interval> can be from 10 – 65535 seconds. The default is 60.

USING THE WEB MANAGEMENT INTERFACE

You cannot modify the RIP advertisement interval using the Web management interface.

Modify the SAP Advertisement Interval

The IPX SAP advertisement interval specifies how often the routing switch sends IPX SAP updates to neighboring IPX routers. The update intervals are separate for RIP and SAP and are configurable on an individual interface basis.

By default, the routing switch sends an IPX SAP update every 60 seconds. You can change the interval to be from 10 – 65535 seconds. You cannot disable the advertisements.

NOTE: If you change an advertisement interval, you do not need to change the age time. The software automatically calculates the age time by multiplying the advertisement interval times the age timer, which is 3 by default.

To change the SAP advertisement packet size, use the following CLI method.

USING THE CLI

EXAMPLE:

To change the advertisement interval for IPX SAP advertisements sent on interface 1/1 from 60 seconds to 120 seconds, enter the following commands:

```
HP9300(config) int e 1/1
HP9300(config-if-1/1) ipx sap-interval 120
HP9300(config-if-1/1) write memory
```

Syntax: ipx sap-interval <interval>

The <interval> can be from 10 – 65535 seconds. The default is 60.

USING THE WEB MANAGEMENT INTERFACE

You cannot modify the SAP advertisement interval using the Web management interface.

Modify the Age Timer for Learned IPX Routes

The age timer specifies how many seconds a learned IPX route can remain in the routing switch's IPX route table before aging out.

The software calculates the age time by multiplying the advertisement interval times the age timer. For example, the default age time for IPX routes is 180 seconds, which is 60 (the default advertisement interval) multiplied by 3 (the default age timer).

You can configure the age timer for RIP to a value from 1 – 65535. The default is 3. You cannot disable the age timer.

To change the age timer for learned IPX routes, use the following CLI method.

USING THE CLI

To change the age timer for IPX routes from 3 to 4 on interface 1/1, enter the following commands.

```
HP9300(config) int e 1/1
HP9300(config-if-1/1) ipx rip-multiplier 4
HP9300(config-if-1/1) write memory
```

Syntax: ipx rip-multiplier <num>

The <num> parameter specifies the age time and can be from 1 – 65535. The default is 3.

USING THE WEB MANAGEMENT INTERFACE

You cannot modify the route age timer using the Web management interface.

Modify the Age Timer for Learned SAP Entries

The age timer specifies how many seconds a learned IPX server can remain in the routing switch's IPX service table before aging out.

The software calculates the age time by multiplying the advertisement interval times the age timer. For example, the default age time for IPX service entries is 180 seconds, which is 60 (the default advertisement interval) multiplied by 3 (the default age timer).

You can configure the age timer for SAP to a value from 1 – 65535. The default is 3. You cannot disable the age timer.

To change the age timer for learned SAP entries, use the following CLI method.

USING THE CLI

To change the age timer for IPX servers from 3 to 2 on interface 5/1, enter the following commands.

```
HP9300(config) int e 5/1
HP9300(config-if-5/1) ipx sap-multiplier 2
HP9300(config-if-5/1) write memory
```

Syntax: ipx sap-multiplier <num>

The <num> parameter specifies the age time and can be from 1 – 65535. The default is 3.

USING THE WEB MANAGEMENT INTERFACE

You cannot modify the SAP age timer using the Web management interface.

Displaying IPX Configuration Information and Statistics

You can use CLI commands and Web management options to display the following IPX information:

- Global IPX parameter settings – see “Displaying Global IPX Configuration Information” on page 11-16.
- IPX interfaces – see “Displaying IPX Interface Information” on page 11-17.
- IPX forwarding cache – see “Displaying the IPX Forwarding Cache” on page 11-19.
- IPX route table – see “Displaying the IPX Route Table” on page 11-20.
- IPX server table – see “Displaying the IPX Server Table” on page 11-21.
- IPX traffic statistics – see “Displaying IPX Traffic Statistics” on page 11-22.

Displaying Global IPX Configuration Information

To display global IPX configuration information for the routing switch, use one of the following methods.

USING THE CLI

To display IPX configuration information, enter the following command at any CLI level:

```
HP9300> show ipx

IPX Enabled
NetBIOS (type 20): Disallowed

Maximum RIP entries: 2048
Maximum SAP entries: 4096

Maximum IPX RIP filters: 32
Maximum IPX SAP filters: 32
Maximum IPX forward filters: 32
```

Syntax: show ipx

This display shows the following information.

Table 11.1: CLI Display of Global IPX Configuration Information

This Field...	Displays...
IPX Enabled	Verifies that IPX is enabled. **Note**: If IPX is disabled, the following message is displayed in stead: “ipx not running”
IPX NetBIOS (type 20)	Indicates whether IPX is configured to allow NetBIOS type 20 packets. This field can have one of the following values: • Allowed • Disallowed To change this parameter, see “Enable NetBIOS” on page 11-3.
Maximum IPX RIP filters	How many IPX route filters you can configure in the routing switch. On some devices, you can change this value by changing the amount of memory allocated for the filters. See “Displaying and Modifying System Parameter Default Settings” in the “Configuring Basic Features” chapter of *Installation and Getting Started Guide*.

Table 11.1: CLI Display of Global IPX Configuration Information (Continued)

This Field...	Displays...
Maximum IPX SAP filters	How many IPX service filters you can configure in the routing switch. On some devices, you can change this value by changing the amount of memory allocated for the filters. See "Displaying and Modifying System Parameter Default Settings" in the "Configuring Basic Features" chapter of *Installation and Getting Started Guide*.
Maximum IPX forward filters	How many IPX forward filters you can configure in the routing switch. On some devices, you can change this value by changing the amount of memory allocated for the filters. See "Displaying and Modifying System Parameter Default Settings" in the "Configuring Basic Features" chapter of *Installation and Getting Started Guide*.

USING THE WEB MANAGEMENT INTERFACE

To determine whether IPX is enabled:

1. Log on to the device using a valid user name and password for read-only or read-write access. The System configuration dialog is displayed.
2. Verify that the Enable option is selected next to IPX. If the option is not selected and you want to enable IPX, see "Enable IPX" on page 11-2.

To determine whether NetBIOS is enabled or disabled:

1. Click on the plus sign next to Configure.
2. Click on the plus sign next to IPX in the tree view to expand the list of IPX option links.
3. Click on the Allow NetBIOS (Type 20) link. Verify that Enable is selected.

To view the maximum number of IPX filters you can configure:

1. Click the Home link from any panel to display the System configuration panel.
2. Select the Max-Parameter link to display the Configure System Parameter Maximum Value table. This table lists the settings and valid ranges for all the configurable table sizes on the device.
3. Scroll down to display the values in the Max Current Value field for the following parameters:
   - ipx-forward-filter – IPX forward filters
   - ipx-rip-filter – IPX RIP filters
   - ipx-sap-filter – IPX SAP filters

Displaying IPX Interface Information

To display IPX interface information for the routing switch, use one of the following methods.

USING THE CLI

To display IPX interface information, enter the following command at any CLI level:

```
HP9300# show ipx interface ethernet 3/5

Interface Ethernet 3/5
  MAC address: 00e0.5284.0b44  Port state: UP
  IPX network:       0000ABCD  Frame type: ethernet_snap   Allow NetBIOS: NO
  rip-interval: 60  rip-max-packet-size: 432  rip-multiplier: 3
  sap-interval: 60  sap-max-packet-size: 480  sap-multiplier: 3
```

Syntax: show ipx interface [ethernet <portnum> | ve <num>]

The **ethernet** <portnum> parameter lets you specify a routing switch port.

The **ve** <num> parameter lets you specify a virtual interface (VE).

This display shows the following information.

Table 11.2: CLI Display of IPX Interface Information

This Field...	Displays...
Interface	The port or virtual interface on which the IPX interface is configured.
MAC address	The MAC address of the interface.
Port state	The state of the interface. The state can be one of the following: • DOWN • UP
IPX network	The IPX network number.
Frame type	The frame type of the network. The frame type can be one of the following: • ethernet_802.2 • ethernet_802.3 • ethernet_ii • ethernet_snap
Allow NetBIOS	Indicates whether the interface allows NetBIOS traffic. This field can have the following values: • NO • YES
rip-interval	The RIP advertisement interval. The RIP advertisement interval specifies how often the routing switch sends IPX RIP updates to neighboring IPX routers. To modify this parameter, see “Modify the RIP Advertisement Interval” on page 11-14.
rip-max-packet-size	The maximum packet size for IPX RIP updates. The default IPX RIP packet size is 432 bytes, which allows 50 routes plus 32 bytes of header in an IPX RIP update packet. To modify this parameter, see “Modify the RIP Advertisement Packet Size” on page 11-13.
rip-multiplier	The age timer for learned IPX routes. The age timer specifies how many seconds a learned IPX route can remain in the routing switch's IPX route table before aging out. To modify this parameter, see “Modify the Age Timer for Learned IPX Routes” on page 11-15.

Table 11.2: CLI Display of IPX Interface Information (Continued)

This Field...	Displays...
sap-interval	The SAP advertisement interval. The IPX SAP advertisement interval specifies how often the routing switch sends IPX SAP updates to neighboring IPX routers. To modify this parameter, see “Modify the SAP Advertisement Interval” on page 11-14.
sap-max-packet-size	The maximum packet size for IPX SAP advertisements. The default IPX SAP packet size is 480 bytes, which allows seven servers plus 32 bytes of header in an IPX SAP update packet. To modify this parameter, see “Modify the SAP Advertisement Packet Size” on page 11-13.
sap-multiplier	The age timer for learned SAP entries. The age timer specifies how many seconds a learned IPX server can remain in the routing switch's IPX service table before aging out. To modify this parameter, see “Modify the Age Timer for Learned SAP Entries” on page 11-15.

USING THE WEB MANAGEMENT INTERFACE

To display IPX interface information:

1. Log on to the device using a valid user name and password for read-only or read-write access. The System configuration dialog is displayed.
2. Click on the plus sign next to Configure in the tree view.
3. Click on the plus sign next to IPX in the tree view to expand the list of IPX option links.
4. Click on the Interface link to display the IPX interface table.

Displaying the IPX Forwarding Cache

To display the IPX forwarding cache for the routing switch, use one of the following methods.

USING THE CLI

To display the IPX forwarding cache, enter the following command at any CLI level:

```
HP9300> show ipx cache
Total number of IPX cache entries 3

Forwarding

Index  Network   Router      Out-Filter  Frame-Type    Port
1      11110007  0000.0000.0000  off      ethernet_802.3    7
2      11110005  0000.0000.0000  off      ethernet_802.3    5
3      32D564FA  00a0.24bf.89ca  off      ethernet_802.3    5
```

Syntax: show ipx cache [<num(hex)>]

The <num(hex)> parameter lets you specify an IPX network number.

This display shows the following information.

Table 11.3: CLI Display of IPX Forwarding Cache

This Field...	Displays...
Total number of IPX cache entries	The number of entries in the forwarding cache.
Index	The row number of this entry in the cache.
Network	The network containing the destination node.
Router	The MAC address of the next-hop IPX router. If the destination is local, the address is shown as all zeros.
Out-Filter	Whether an outbound filter is configured for traffic to the destination network number or node. The value can be one of the following: • No • Yes
Frame-Type	The frame encapsulation type, which can be one of the following: • Ethernet SNAP • Ethernet 802.2 • Ethernet 802.3 • Ethernet II
Port	The port through which the routing switch sends traffic to the destination network and node.

USING THE WEB MANAGEMENT INTERFACE

To display the IPX forwarding cache:

1. Log on to the device using a valid user name and password for read-only or read-write access. The System configuration dialog is displayed.
2. Click on the plus sign next to Monitor in the tree view to display the list of monitoring options.
3. Click on the plus sign next to IPX in the tree view to expand the list of IPX option links.
4. Click on the Cache link.

Displaying the IPX Route Table

To display the IPX route table, use one of the following methods.

USING THE CLI

To display the IPX route table, enter the following command at any CLI level:

```
HP9300> show ipx route

Total number of IPX route entries 3

Forwarding

Index   Network   Router          Hops  Ticks Port
1       11110007  0000.0000.0000     0     1     7
2       32D564FA  00a0.24bf.89ca     1     2     5
3       11110005  0000.0000.0000     0     1     5
```

Syntax: show ipx route [<num(hex)>]

The <num(hex)> parameter lets you specify an IPX network number.

This display shows the following information.

Table 11.4: CLI Display of IPX Route Table

This Field...	Displays...
Total number of IPX route entries	The number of entries in the table.
Index	The index number of the table entry.
Network	The IPX network at the route's destination.
Router	The MAC address of the next-hop IPX router.
Hops	The number of hops (routers) separating the router from the network.
Ticks	The number of ticks.
Port	The port through which the routing switch sends traffic to the destination network.

USING THE WEB MANAGEMENT INTERFACE

To display the IPX route table:

1. Log on to the device using a valid user name and password for read-only or read-write access. The System configuration dialog is displayed.
2. Click on the plus sign next to Monitor in the tree view to display the list of monitoring options.
3. Click on the plus sign next to IPX in the tree view to expand the list of IPX option links.
4. Click on the Route link.

Displaying the IPX Server Table

To display the IPX server table, use one of the following methods.

USING THE CLI

To display the IPX server table, enter the following command at any CLI level:

```
HP9300> show ipx servers

Total number of IPX server entries 3

Index  Network   Node            Socket    Type      Hops
1      32D564FA  0000.0000.0001   0005     026B        1
         Server-name: HPD
2      32D564FA  0000.0000.0001   4006     0278        1
         Server-name: HPM
3      32D564FA  0000.0000.0001   0451     0004        1
         Server-name: HP-MPR2
```

Syntax: show ipx servers [<name>]

The <name> parameter lets you specify a server name.

This display shows the following information.

Table 11.5: CLI Display of IPX Server Table

This Field...	Displays...
Index	The index number of the table entry.
Network	The network in which the server is located.
Node	The six-byte node number. The node number can be a MAC address or, for some IPX server types, a “1”.
Socket	The two-byte socket number.
Type	The two-byte number for the server type.
Hops	The number of IPX router hops to the server’s network.
Server-name	The IPX server name.

USING THE WEB MANAGEMENT INTERFACE

To display the IPX server table:

1. Log on to the device using a valid user name and password for read-only or read-write access. The System configuration dialog is displayed.
2. Click on the plus sign next to Monitor in the tree view to display the list of monitoring options.
3. Click on the plus sign next to IPX in the tree view to expand the list of IPX option links.
4. Click on the Server link.

Displaying IPX Traffic Statistics

To display IPX traffic statistics, use one of the following methods.

USING THE CLI

To display IPX traffic statistics, enter the following command at any CLI level:

```
HP9300> show ipx traffic

                                              Dropped              Filtered
Port    Forward    Receive   Transmit    Receive   Transmit   Receive  Transmit
 1/5          46         36          8          2          0         0         0
 1/7           0          0          6          0          0         0         0
Tot           46         36         14          2          0         0         0
```

Syntax: show ipx traffic

This display shows the following information.

Table 11.6: CLI Display of IPX Traffic Statistics

This Field...	Displays...
Port	The port for which the statistics apply. Only the ports that have IPX interfaces configured on them are listed.
Forward	The number of IPX packets received by the routing switch from another device and then sent on the port.
Receive	The number of IPX packets received on the port.
Transmit	The number of IPX packets originated on the routing switch and sent on the port.
Dropped Receive	The number of packets received on this port by the routing switch that the routing switch dropped.
Dropped Transmit	The number of packets queued for sending on this port by the routing switch but then dropped.
Filtered Receive	The number of packets received by this port that matched an inbound IPX filter configured on the port.
Filtered Transmit	The number of packets queued for sending on this port that matched an outbound IPX filter configured on the port.

USING THE WEB MANAGEMENT INTERFACE

To display summary IPX traffic statistics:

1. Log on to the device using a valid user name and password for read-only or read-write access. The System configuration dialog is displayed.
2. Click on the plus sign next to Monitor in the tree view to display the list of monitoring options.
3. Click on the plus sign next to IPX in the tree view to expand the list of IPX option links.
4. Click on the Traffic link.

This display shows the following information.

Table 11.7: Web Display of IPX Traffic Statistics

This Field...	Displays...
In Packets	The number of IPX packets received on the routing switch.
Out Packets	The number of IPX packets originated on the routing switch and sent on the routing switch.
Forwarding Packets	The number of IPX packets received by the routing switch from another device and then sent on the routing switch.
Rcv Drop Packets	The number of packets received by the routing switch that the routing switch dropped.
Tx Drop Packets	The number of packets queued for sending by the routing switch but then dropped.

Table 11.7: Web Display of IPX Traffic Statistics (Continued)

This Field...	Displays...
Rcv Filter Packets	The number of packets received by the routing switch that matched an inbound IPX filter.
Tx Filter Packets	The number of packets queued for sending that matched an outbound IPX filter.

To display traffic statistics for each port or virtual interface on which an IPX interface is configured:

1. Log on to the device using a valid user name and password for read-only or read-write access. The System configuration dialog is displayed.
2. Click on the plus sign next to Monitor in the tree view to display the list of monitoring options.
3. Click on the plus sign next to IPX in the tree view to expand the list of IPX option links.
4. Click on the Port Counter link.

This display shows the following information.

Table 11.8: Web Display of IPX Port Statistics

This Field...	Displays...
Port	The port or virtual interface on which the IPX interface is configured.
Forward Packets	The number of IPX packets received by the routing switch from another device and then sent on the port.
Rcv Packets	The number of IPX packets received on the port.
Tx Packets	The number of IPX packets originated on the routing switch and sent on the port.
Rcv Drop Packets	The number of packets received on this port by the routing switch that the routing switch dropped.
Tx Drop Packets	The number of packets queued for sending on this port by the routing switch but then dropped.
Rcv Filter Packets	The number of packets received by this port that matched an inbound IPX filter configured on the port.
Tx Filter Packets	The number of packets queued for sending on this port that matched an outbound IPX filter configured on the port.