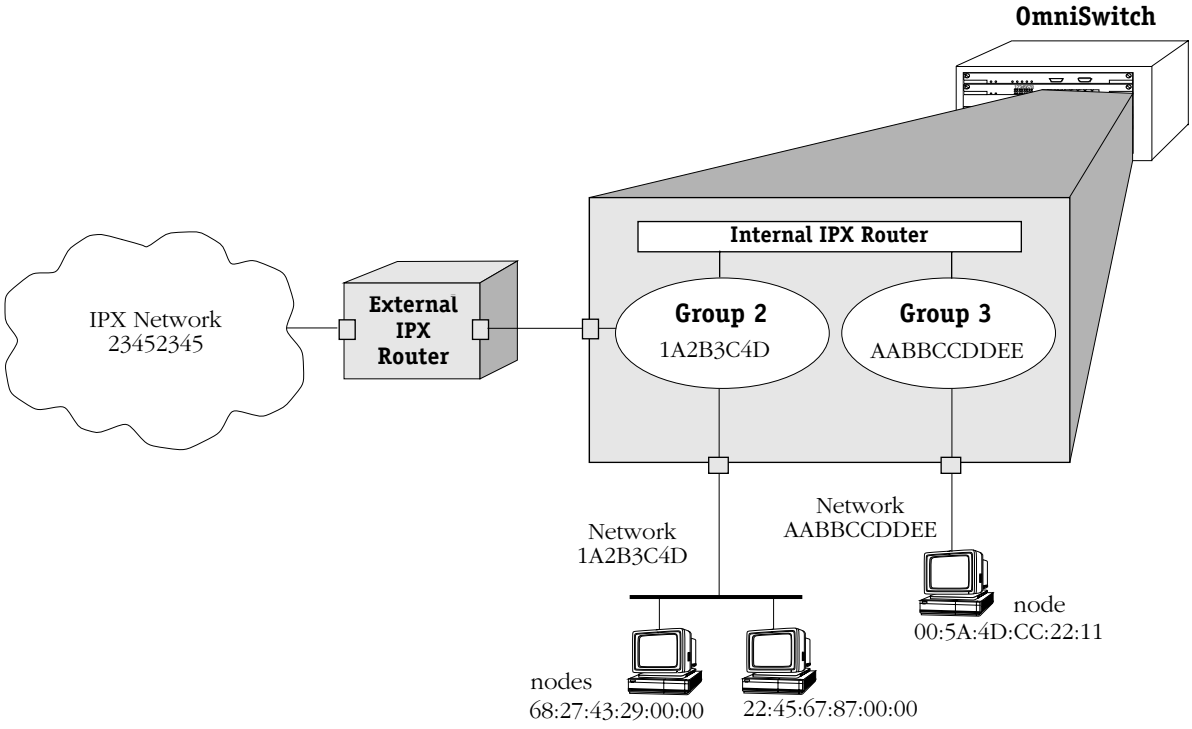
33 IPX Routing

Introduction

This chapter gives an overview of Internetwork Packet Exchange (IPX) routing and includes information about configuring static IPX routes as well as configuring Routing Information Protocol (RIP) and Service Advertising Protocol (SAP) filters and timers. IPX is a layer 3 protocol developed by Novell for interconnecting NetWare clients and servers. (NetWare is Novell's network server operating system.) IPX routing requires at least one IPX router port to be configured on the switch.

When IPX routing is enabled on the switch, the switch will be able to exchange routing information with IPX routers in the network, and stations connected to groups and VLANs with virtual IPX router ports will be able to communicate. Groups or VLANs that do not have IPX router ports with IPX routing enabled cannot communicate with each other.

In the example shown here, stations connected to each group will be able to communicate if a virtual IPX router port is created for each group and each router port on the switch has IP routing enabled. Stations in group 2 and group 3 will also be able to communicate with stations attached to the external IPX router if a static route to that router is configured on the switch or the switch learns about the external router through IPX RIP or SAP.



IPX Routing Overview

In IPX routing, the switch builds routing tables to keep track of optimal destinations for traffic it receives that is destined for remote IPX networks. The switch sends and receives routing messages, or advertisements, to/from other routers in the network. When the switch receives an IPX packet, it looks up the destination network number in its routing table. If the network is directly connected to the switch, the switch also checks the destination node address. The network number consists of eight hex digits, and the node address is typically the MAC address of the end station or server.

Creating routing tables is performed by switch software unless a Hardware Routing Engine (HRE) or HRE-X is installed. The HRE or HRE-X significantly improves routing performance. See Chapter 1, "Omni Switch/Router Chassis and Power Supplies," and Chapter 6, "The MPM," for information about the HRE-X and HRE respectively.

IPX is associated with additional protocols built into the switch software. These are described in the next section.

IPX Protocols

The switch supports the following IPX protocols:

- **SPX** (Sequenced Packet Exchange) is a Transport-layer protocol that provides a reliable end-to-end communications link by managing packet sequencing and delivery. SPX does not play a direct role in IPX routing; it simply guarantees the delivery of routed packets.
- **IPX RIP** (Routing Information Protocol) is a layer 3 protocol used by NetWare routers to exchange IPX routing information. IPX RIP functions similarly to IP RIP. IPX RIP uses two metrics to calculate the best route: hop count and ticks. An IPX router periodically transmits packets containing the information currently in its own routing table to neighboring IPX RIP routers in order to advertise the best route to an IPX destination.
- **SAP** (Service Advertising Protocol) is a layer 3 protocol used by NetWare routers to exchange IPX routing information. SAP is similar in concept to IPX RIP. Just as RIP enables NetWare routers to exchange information about routes, SAP enables NetWare devices to exchange information about available network services. NetWare workstations use SAP to obtain the network addresses of NetWare servers. IPX routers use SAP to gather service information and then share it with other IPX routers.

Setting Up IPX Routing on the Switch

IPX routing is enabled on a per-port basis by creating a virtual IPX router port for a group/VLAN. The switch does not do any routing unless the virtual IPX router port has IPX routing enabled (routing is enabled by default). The steps for setting up IPX routing on the switch are given here:

Step 1. Configuring a Virtual Router Port

A virtual IPX router port may be created when you set up or modify a group/VLAN through the **crgp** command or **modvl** command described in Chapter 25, "Managing Groups and Virtual Ports." To create a virtual router port, you enable IPX routing and specify a network address for the router port.

♦ Note ♦

IP and IPX routing may be enabled on the same port.

IPX router ports on the switch must also be configured with a particular encapsulation type for Ethernet: 802.3, 802.2 or LLC, SNAP, or Ethernet II.

Step 2. Configuring Optional IPX Routing Parameters

Optional configuration for IPX routing includes the following:

- Static routes. These are routes that are manually added to the routing table and may be used rather than dynamic routes that are learned through RIP or SAP.
- IPX RIP and SAP filters. IPX RIP and SAP filters may be configured and displayed. The default timers for RIP and SAP may also be modified. Extended RIP and SAP packets may also be configured.

In addition to optional routing configuration, there is an HRE-X filtering option that may be used for IPX routing, which filters IPX traffic at the router port if an HRE-X is installed. See Chapter 34, "HRE-X Filtering."

The IPX Submenu

The **ipx** command in the Networking menu is used to access a submenu containing all the IPX-related commands. For more information about the Networking menu, see Chapter 31, "IP Routing."

To display the IPX submenu, enter the following commands:

```
IPX

?
```

If you have enabled the verbose mode, you don't need to enter the question mark (**?**).

A screen similar to the following displays:

```
  Command          IPX Menu
-------------------- ------------------------------------------------------------
  ipxr               View IPX routes
  ipxs               View IPX stats and errors
  ipxsap             View IPX SAP bindery
  aipxsr             Add an IPX static route
  ripxsr             Remove an IPX static route
  ipxoff             Turn off the IPX router complex
  ipxon              Turn on the IPX router complex
  ipxflush           Flush IPX router RIP and/or SAP tables
  ipxping            IPX Ping a system
  ipxfilter          Add/delete an IPX RIP/SAP filter
  ipxf               Display IPX RIP/SAP filters
  ipxserialf         Enable/Disable IPX Serialization Packet Filtering
  ipxspoof           Enable/Disable IPX Watchdog Spoofing
  spxspoof           Enable/Disable SPX Keepalive Spoofing
  ipxtype20          Turn on/off forwarding of IPX Type 20 packets
  ipxtimer           Add/Delete SAP and RIP timers
  ipxt               Display SAP and RIP timers
  ipxdrt             Turn on/off a default route for IPX
  ipxext             Turn on/off extended IPX RIP and SAP packets

   Main      File      Summary   VLAN      Networking
   Interface Security  System    Services  Help
```

This chapter describes all of the above commands. The remaining sections of this chapter cover each of the above commands in the order in which they appear in the IPX submenu.

Viewing the IPX Routing Table

The **ipxr** command is used to display the IPX Routing Table. The entries in the table show the routes entered by the IPX RIP protocol and the static routes that you may have entered manually. All entries in the table are sorted by destination network. The IPX Routing Table can contain a maximum of 2,010 routes.

Displaying All Entries in the IPX Routing Table

To display all entries in the IPX Routing Table, enter the following command:

```
ipxr
```

A screen similar to the following displays:

```
Displaying all (4) routes:

Dest Net      Router              Hops  Delay  Static  Aged  Redir  Chg  Dir  GP:VL
    3333  e8024.0000c021a5b8     1     3      N       Y     N      N    N    7:1
    5555  5555.Direct            0     1      N       N     N      N    Y    4:1
    e8024 e8024.Direct           0     1      N       N     N      N    Y    7:1
 3041c204 e8024.0000c021a5b8     1     3      N       Y     N      N    N    7:1
```

The fields on this screen have the following meanings:

Dest Net

The destination network IPX address.

Router

The IPX address (network.node) of the next hop router to reach the destination network.

Hops

The number of routers between this node and the destination network.

Delay

The number of "ticks" between this node and the destination network. A "tick" is about 1/18th of a second.

Static

Whether this route was statically defined (see the **aipxsr** command).

Aged

Indicates if this route has timed out. Once a route times out it is kept in the routing table for 10 "ticks." Once the 10 "ticks" expire, the route is deleted.

Redir

Indicates that a route to an IPX network that was formerly reachable via a direct interface has been replaced by an alternate route.

Chg

The information in this route has recently been updated, but the new information has not yet been forwarded to neighbor routers.

Dir

Indicates that this is a local interface (direct route) as opposed to a route to a destination network.

GP:VL

The first number is the Group associated with this entry; the second number is the VLAN associated with this entry. This identifies the interface used when sending traffic to the destination network.

Using IPXR with Frame Relay or ISDN Boards

The following additional column heading appears in the **ipxr** display when a Frame Relay or ISDN board is installed in the switch:

s/p/vc or Peer ID

The Slot, Port and Virtual Connection (i.e., DLCI) identifiers or the PPP Peer ID of the interface on which the routing information was received.

Here is an example of a display generated by the **ipxr** command in this situation:

Displaying all (12) routes:

Dest Net	Router	Hops	Delay	Static	Aged	Redir	Chg	Dir	GP:VL	s/p/vc Peer ID
100	100.Direct	0	1	N	N	N	N	Y	3:1	
120	120.Direct	0	1	N	N	N	N	Y	4:1	
5000	120.0020da092ef5	1	2	N	N	N	N	N	4:1	5/3/100
5556	8484.0020da2200f4	1	2	N	N	N	N	N	6:1	P1
8484	8484.Direct	0	1	N	N	N	N	Y	6:1	
26dc012a	120.0020da092ef5	1	2	N	N	N	N	N	4:1	5/3/220
55555555	120.0020da092ef5	1	2	N	N	N	N	N	4:1	5/3/100
66666666	66666666.Direct	0	1	N	N	N	N	Y	5:1	
95000095	120.0020da092ef5	2	3	N	N	N	N	N	4:1	5/3/100

In this example, traffic destined for Network 5000 will go through Slot 5, Port 3, DLCI 100 which is associated with the interface on Group 4.

Displaying a List of Specific IPX Routes

You can limit the number of routes that are displayed by the **ipxr** command by using an extra argument along with the command. To find out if a route to a particular destination network is known, simply include the network number on the command line. (The examples shown below came from a switch that contained a Frame Relay board and an ISDN board.)

Here is an example for destination network 5000 (the command used is: **ipxr 5000**):

Dest Net	Router	Hops	Delay	Static	Aged	Redir	Chg	Dir	GP:VL	s/p/vc Peer ID
5000	120.0020da092ef5	1	2	N	N	N	N	N	4:1	5/3/100

To display only those routes learned from a particular interface, you can specify the interface number on the command line. You can also further specify the slot/port/vc or PPP Peer ID.

This is an example for Interface 3:1 (the command used was: **ipxr 3:1**):

Displaying routes for interface 3:1

Dest Net	Router	Hops	Delay	Static	Aged	Redir	Chg	Dir	GP:VL	s/p/vc Peer ID
100	100.Direct	0	1	N	N	N	N	Y	3:1	

This is an example for Interface 4:1 5/3/100 (the command used was: **ipxr 4:1 5/3/100**):

Displaying routes for interface 4:1

Dest Net	Router	Hops	Delay	Static	Aged	Redir	Chg	Dir	GP:VL	s/p/vc Peer ID
5000	120.0020da092ef5	1	2	N	N	N	N	N	4:1	5/3/100
55555555	120.0020da092ef5	1	2	N	N	N	N	N	4:1	5/3/100
95000095	120.0020da092ef5	2	3	N	N	N	N	N	4:1	5/3/100

This is an example for Interface 6:1 P1 (the command used was: **ipxr 6:1 P1**):

Displaying routes for interface 6:1

Dest Net	Router	Hops	Delay	Static	Aged	Redir	Chg	Dir	GP:VL	s/p/vc Peer ID
5556	8484.0020da2200f4	1	2	N	N	N	N	N	6:1	P1

Viewing IPX Statistics

The **ipxs** command is used to display data on IPX statistics and errors.

To display information about IPX statistics and errors, enter the following command:

```
ipxs
```

A screen similar to the following displays:

```
IPX Statistics and Errors:

IPX is ON

IPX Input Statistics:
 pkts rcvd                 =  3280
 pkts delivered locally    =  3161
 pkts discarded            =  0
 input header errors       =  0

IPX Output Statistics:
 pkts sent                 =  4731
 pkts generated locally    =  4681
 pkts discarded            =  0
 pkts with no route found  =  1
 HRE pkts sent             =  0

There are 2 IPX interfaces defined.

Stats for IPX Router Interface on (Group:VLAN) 3:1, Net address 3333
 Interface name is IPX Router 3333
   state              =  ON          status       =  UP
   state changes      =  1500        type         =  BROADCAST
   rtr encapsulation  =  FD

   RIP is ON: sent = 1527, rcvd = 1568, update interval = 60 secs.
   SAP is ON: sent = 1, rcvd = 1568, update interval = 60 secs.

Stats for IPX Router Interface on (Group:VLAN) 4:1, Net address 5555
 Interface name is  IPX Router 5555
   state              =  ON          status       =  UP
   state changes      =  1500        type         =  BROADCAST
   rtr encapsulation  =  EN

   RIP is ON: sent = 1571, rcvd = 1, update interval = 60 secs.
   SAP is ON: sent = 1533, rcvd = 1, update interval = 60 secs.
```

The fields (and the subfields) on this screen have the following meanings:

IPX

Indicates whether IPX routing is "ON" or "OFF."

IPX Input Statistics

pkts rcvd: The number of packets received.

pkts delivered locally: The number of received packets delivered to local IPX applications (RIP and SAP).

pkts discarded: The number of discarded packets.

input header errors: The number of packets discarded due to IPX packet header errors.

IPX Output Statistics

pkts sent: The number of packets forwarded (not including fast path routed packets).

pkts generated locally: The number of packets forwarded that were generated by local IPX applications (RIP and SAP).

pkts discarded: The number of discarded packets.

pkts with no route found: The number of packets that could not be forwarded because a route to the destination IPX network could not be found.

Stats for IPX Router Interface

state: State of the IPX router for this interface (ON or OFF).

status: Status of the interface (UP or DOWN).

type: The type of interface (BROADCAST or POINT-TO-POINT).

rtr encapsulation: Router port encapsulation used for this interface (EN=Ethernet, FD=FDDI, TR=Token Ring).

state changes: The number of state changes that have occurred on this interface (up to down, down to up).

RIP

sent: The number of RIP packets sent.

received: The number of RIP packets received.

update interval: The RIP update timer interval for this interface. If a WAN interface is configured as a Triggered RIP/SAP interface, this field will contain the word “triggered.” Triggered interfaces transmit information only once, when the change occurs.

SAP

sent: The number of SAP packets sent.

received: The number of SAP packets received.

update interval: The SAP update timer interval for this interface. If a WAN interface is configured as a Triggered RIP/SAP interface, this field will contain the word “triggered.” Triggered interfaces transmit information only once, when the change occurs.

Viewing the IPX SAP Bindery

The **ipxsap** command is used to display a listing of the servers in the SAP Bindery, sorted by server name.

To display a list of SAP servers, enter the following command:

```
ipxsap
```

A screen similar to the following displays:

```
Displaying all (3) entries in the SAP bindery:

    Server Name   Type   Address            Hp    Sckt    GP:VL
Develop           0004   67.000000000001    1     0451     3:1
Finance           026b   67.000000000001    1     0005     2:1
Marketing         0278   67.000000000001    1     4006     2:1
```

The fields on this screen have the following meanings:

Server Name

The name of the server offering this service.

Type

The service type being offered (as defined by Novell).

Address

The IPX address of this server (network.node).

Hp

The number of networks between this node and the server.

Sckt

The Novell socket number to which this service is attached.

GP:VL

The first number is the Group associated with this entry, and the second number is the VLAN associated with this entry.

Using IPXSAP with Frame Relay or ISDN Boards

The following additional column heading appears in the **ipxsap** display when a Frame Relay or ISDN board is installed in the switch.

s/p/vc or Peer ID

The Slot, Port and Virtual Connection (i.e., DLCI) identifiers or the PPP Peer ID of the interface on which the server information was received.

Here is an example of a display generated by the **ipxsap** command in this situation:

Displaying all (3) entries in the SAP bindery:

Server Name	Type	Address	Hp	Sckt	GP:VL	s/p/vc Peer ID
HR	0004	200.000000000022	1	0451	3:1	5/3/100
Sales	026b	200.000000000022	1	0005	2:1	5/3/220
Support	0278	200.000000000022	1	4006	2:1	5/3/220

Displaying a List of Specific SAP Servers

You can limit the number of SAP server names that is displayed by the **ipxsap** command by using an extra argument with the command.

To display only those servers from a specific interface, simply include the interface number on the command line. The following is an example for Interface 2:1 (the command used was **ipxsap 2:1**):

Displaying all SAPs for interface 2:1:

Server Name	Type	Address	Hp	Sckt	GP:VL
Finance	026b	67.000000000001	1	0005	2:1
Marketing	0278	67.000000000001	1	4006	2:1

To display a specific type of server, simply include a Server Type value (in hex) on the command line. The following is an example for 26b (the command used was **ipxsap 26b**):

Displaying SAP entries of type 0x26b:

Server Name	Type	Address	Hp	Sckt	GP:VL
Finance	026b	67.000000000001	1	0005	2:1

To find out if a particular server is known, simply include all, or just a portion of, the server name on the command line. The server name (or portion thereof) must be entered inside of quotation marks. The following is an example for an entry of “nance” (the command used was **ipxsap “nance”**):

Displaying SAP entries whose names contain the substring “nance”:

Server Name	Type	Address	Hp	Sckt	GP:VL
Finance	026b	67.000000000001	1	0005	2:1

Adding an IPX Static Route

The **aipxsr** command is used to add IPX static routes to the switch's IPX Routing Table. You might want to add a static route to send traffic from a node in an OmniSwitch VLAN to an external IPX network address (such as an address reached through an external network router attached to the switch).

In order to add a static route, you will need to know the host/net and the gateway which will be used to route traffic there.

Follow the steps below to add an IPX static route.

1. Enter **aipxsr.**

   A screen similar to the following displays:

   Do you want to see the current route table? (y or n) (y) :

2. Enter **y** at this prompt (or press **<Enter>**) to display the current routing table.

   A screen similar to the following displays:

   Displaying all (4) routes:

Dest Net	Router	Hops	Delay	Static	Aged	Redir	Chg	Dir	GP:VL
3333	e8024.0000c021a5b8	1	3	N	Y	N	N	N	7:1
5555	5555.Direct	0	1	N	N	N	N	Y	4:1
e8024	e8024.Direct	0	1	N	N	N	N	Y	7:1
3041c204	e8024.0000c021a5b8	1	3	N	Y	N	N	N	7:1

   Destination IPX network :

   Enter the IPX address of the network to which you are setting up a route.

3. The following prompt displays:

   IPX network of next hop :

   Enter the IPX network adress of the next hop. This is the number that appears before the dot under the "Router" heading in the IPX Route Table.

4. The following prompt displays:

   IPX node address of next hop (format - xx:xx:xx:xx:xx:xx)

   Enter the IPX node address of the next hop.

5. A message will confirm the addition of the static route:

   Route successfully added

Removing an IPX Static Route

The **ripxsr** command is used to remove IPX static routes from the switch's IPX Routing Table.

Follow the steps below to remove an IPX static route.

1. Enter **ripxsr.**

   A screen similar to the following displays:

   ```
   Do you want to see the current route table?
       (y or n) (y) : y
   ```

2. Enter **y** at this prompt (or press **<Enter>**) to display the current routing table.

   A screen similar to the following displays:

   ```
   Displaying all (4) routes:

   Dest Net        Router              Hops  Delay  Static  Aged  Redir  Chg  Dir  GP:VL
        3333   e8024.0000c021a5b8       1      3       N     Y      N     N    N    7:1
        5555     5555.Direct            0      1       N     N      N     N    Y    4:1
        e8024    e8024.Direct           0      1       N     N      N     N    Y    7:1
     3041c204   e8024.0000c021a5b8       1      3       N     Y      N     N    N    7:1
      aaaaaa      304.0020da05f694       1      1       Y     N      N     Y    N    7:1


   Destination IPX network :
   ```

3. Enter the name of the destination IPX network you want to remove.

   A message will confirm the deletion of the static route:

   ```
   Route successfully deleted.
   ```

Turning the IPX Router Complex On and Off

The **ipxoff** command is used to turn off the IPX Router Complex, which disables IPX routing on the switch.

To turn off IPX routing, enter the following command:

```
ipxoff
```

A screen similar to the following displays:

```
IPX turned off.
```

The **ipxon** command is used to turn on the IPX Router Complex, which enables IPX routing on the switch.

To turn on IPX routing, enter the following command:

```
ipxon
```

A screen similar to the following displays:

```
IPX turned on.
```

Flushing the IPX RIP/SAP Tables

The **ipxflush** command is used to flush the IPX RIP Routing and SAP Bindery Tables.

Follow the steps below to flush both the IPX tables.

1. Enter **ipxflush.**

   A screen similar to the following displays:

```
Flush tables (RIP routing and SAP bindery) in:
    { RIP and SAP(b),
     RIP only(r),
     SAP only(s)} (b) :
```

2. Enter **b** (or just press Enter) to flush both tables. Enter **r** to flush just the Routing Table. Enter **s** to flush just the SAP Bindery Table.

   You will be returned to the system prompt.

Using the IPXPING Command

The **ipxping** command is used to test the reachability of certain types of IPX nodes. The software supports two different types of IPX pings:

- Novell-defined, which can test the reachability of NetWare servers currently running the NetWare Loadable Module called IPXRTR.NLM. This type *cannot* be used to reach NetWare workstations running IPXODI. Novell uses a unique type of ping for this purpose (implemented by their IPXPNG.EXE program) which is not currently supported by the switch software. Other vendor's switches may respond to this type of ping.
- Alcatel-proprietary, which can test the reachability of OmniSwitches or Omni Switch/Routers on which IPX routing has been enabled.

Network devices that do not recognize the specific type of IPX ping request sent from the switch will not respond at all. The lack of a response does not necessarily mean that a specific network device is inactive or missing. Therefore, you might want to try using both types before concluding that the network device is "unreachable."

Follow the steps below to issue an IPX ping request.

1. Enter **ipxping**.

   A screen similar to the following displays:

   ```
   Dest Net () : 304
   ```

   Enter the Destination Network of the node that you want to ping.

2. The following prompt displays:

   ```
   Dest Node (format - xx:xx:xx:xx:xx:xx) () : 00:20:da:05:f6:94
   ```

   Enter the Destination Node that you want to ping.

   ♦ Note ♦

   If you are attempting to ping an interface that is specified with a noncanonical address, you must specify a noncanonical address for the ping.

3. The following prompt displays:

   ```
   Count (0 for infinite) (1) : 245
   ```

   Enter a number to indicate the number of packets to be sent out. An entry of 0 (zero) will create an infinite count (press **<Enter>** to cancel). The default count is 1 (one).

4. The following prompt displays:

   ```
   Size (64) :
   ```

   Enter a number to indicate the number of data bytes included in the packet. The default size is 64.

5. The following prompt displays:

   ```
   Timeout (1) :
   ```

   Enter the number of seconds to wait for a response. The default timeout is 1.

6. The following prompt displays:

```
Type (n for Novell, x for Xylan) (n) :
```

Enter the type of IPX ping to be issued. The default is the Novell type.

7. After answering the previous prompt, a message similar to the following displays:

```
IPX Ping starting, hit <RETURN> to stop
PING 304.00:20:da:05:f6:94: 64 data bytes

[0      ] ..... ..... ..... ..... ..... ..... ..... ..... ..... .....
[50     ] ..... ..... ..... ..... ..... ..... ..... ..... ..... .....
[100    ] ..... ..... ..... ..... ..... ..... ..... ..... ..... .....
[150    ] ..... ..... ..... ..... ..... ..... ..... ..... ..... .....
[200    ] ..... ..... ..... ..... ..... ..... ..... ..... .....

---304.00:20:da:05:f6:94 IPXPING Statistics---
245 packets transmitted, 245 packets received, 0% packet loss
```

You may also elect to bypass the above prompts. To do so, simply include the options on the command line in the exact order in which they appear in the prompts. You will be prompted for any options you leave out. Therefore, the syntax for the command is:

```
ipxping [destnet] [destnode] [count] [size] [timeout] [type]
```

For example, the following command string will send 100 Novell-type pings, using 64 data bytes per packet with a timeout of 1 second, to an IPX server with MAC address of 00:00:c0:21:a5:b8 on IPX network e8024:

```
ipxping e8024 00:00:c0:21:a5:b8 100 64 1 n
```

Configuring IPX RIP/SAP Filtering

The **ipxfilter** command is used to add or delete an IPX RIP or SAP Output or Input filter. The IPX RIP/SAP Filtering feature give you a means of controlling the operation of the IPX RIP/SAP protocols. By using IPX RIP/SAP filters, you can minimize the number of entries put in the IPX RIP Routing and SAP Bindery Tables, improve overall network performance by eliminating unnecessary traffic, and control users' access to NetWare services.

Five types of IPX RIP/SAP filters are available:

1. **RIP Input** filters control which networks are allowed into the routing table when IPX RIPs are received.
2. **RIP Output** filters control the list of networks included in routing updates sent out an interface. These filters control which networks the router advertises in its IPX RIP updates.
3. **SAP Input** filters control the SAPs received by the router prior to a router accepting information about a service. The router will filter all incoming service advertisements received before accepting information about a service.
4. **SAP Output** filters control which services are included in SAP updates sent by the router. The router applies the SAP output filters prior to sending SAP packets.
5. **GNS Output** filters control which servers are included in the GNS responses sent by the router.

Here are some example uses of IPX RIP/SAP filters:

- RIP Input and Output filters can be used to isolate entire network segments (and/or routers) in order to make the network appear differently to the different segments.
- RIP Input and Output filters can be used to reduce the amount of WAN traffic needed to advertise routes that shouldn't be used by a particular network segment.
- SAP Input and Output filters can be used to improve the performance of IPX in a WAN environment by limiting the amount of SAP traffic. For example, because printing is generally a local operation, there's no need to advertise print servers to remote networks. A SAP filter can be used in this case to restrict "Print Server Advertisement" SAPs.

♦ Important Note ♦

All types of IPX Filters can be configured either to *allow* or to *block* traffic. The default setting for all filters is to allow traffic. Therefore, you will typically only have to define a filter to block traffic. However, defining a filter to allow certain traffic may be useful in situations where a more generic filter has been defined to block the majority of the traffic. For example, you could use a filter to allow traffic from a specific host on a network where all other traffic has been blocked. A discussion of the precedence of "Allow" filters appears later in this section. Keep in mind that precedence applies only to "allow" filters, *not* to "block" filters.

You can apply filters to *all* router interfaces by defining a "global" filter, or you can limit the filter to *specific* interfaces. In addition, for WAN networks, you can apply filters to a specific Frame Relay virtual circuit (DLCI) or PPP Peer. Each of these options is described under individual heading in this section.

Adding a "Global" IPX RIP/SAP Filter

Follow the steps below to add a "global" IPX RIP or SAP filter.

1. Enter **ipxfilter**.

   A screen similar to the following displays:

   ```
   Selecting global IPX filter:

   Add or delete entry {add(a), delete(d)} (a) :
   ```

   Enter **a** (or just press **<Enter>**) to select to add a filter.

2. The following prompt displays:

   ```
   Filter type {SAP output(so),
                SAP input(si),
                RIP Output(ro),
                RIP Input(ri),
                GNS output(go)} (so) :
   ```

   Enter **so** (or just press **<Enter>**) to add a SAP Output filter. Enter **si** to add a SAP Input filter. Enter **ro** to add a RIP Output filter. Enter **ri** to add a RIP Input filter. Enter **go** to add a GNS Output filter.

3. The following prompt displays:

   ```
   Filter action {block(b), allow(a)} (a) :
   ```

   Enter **a** (or press **<Enter>**) to define the filter to allow traffic. Enter **b** to define the filter to block traffic.

4. The following prompt displays:

   ```
   IPX network (default: all networks):
   ```

   Enter the IPX network address (in hexadecimal format) that is to be used (or press **<Enter>** to use the default of "all networks").

5. The following prompt displays:

   ```
   IPX network mask (default: FFFFFFFF) :
   ```

   Enter the IPX network mask (in hexadecimal format) to be used (or press **<Enter>** to use the default mask of FFFFFFFF). *If you selected the default of "all networks" in the previous step, this step is skipped.*

6. The following prompt displays:

   ```
   IPX node address (default: all nodes):
   ```

   Enter the IPX node address (in hexadecimal format) to be used (or press **<Enter>** to use the default of "all nodes").

7. The following prompt displays:

   ```
   IPX node mask (default: all F's)  :
   ```

   Enter the IPX node mask (in hexadecimal format) to be used (or just press **<Enter>** to use the default mask of all F's). *If you selected the default of "all nodes" in the previous step, this step is skipped.*

8. The following prompt displays:

   SAP service type (default: all services) :

   Enter the SAP service type (in hexadecimal format) as defined by NetWare (or press **<Enter>** to use the default of all services).

9. A message will confirm the addition of the filter:

   ipxfilter successfully added

Adding an IPX RIP/SAP Filter for a Specific Group or VLAN

Follow the steps below to add an IPX RIP or SAP Output or Input filter for a specific Group or VLAN.

1. Enter the Group and VLAN numbers after the command like this: **ipxfilter 1:1**.

   A screen similar to the following displays:

   Selecting IPX filter for interface 1:1:

   Add or delete entry {add(a), delete(d)} (a) :

   Enter **a** (or press **<Enter>**) to select to add a filter.

2. The following prompt displays:

   Filter type {SAP output(so),
   SAP input(si),
   RIP Output(ro),
   RIP Input(ri),
   GNS output(go)} (so) :

   Enter **so** (or press **<Enter>**) to add a SAP Output filter. Enter **si** to add a SAP Input filter. Enter **ro** to add a RIP Output filter. Enter **ri** to add a RIP Input filter. Enter **go** to add a GNS Output filter.

3. The following prompt displays:

   Filter action {block(b), allow(a)} (a) :

   Enter **a** (or press **<Enter>**) to define the filter to allow traffic. Enter **b** to define the filter to block traffic.

4. The following prompt displays:

   IPX network (default: all networks):

   Enter the IPX network address (in hexadecimal format) that is to be used (or press **<Enter>** to use the default of "all networks").

5. The following prompt displays:

   IPX network mask (default: FFFFFFFF) :

   Enter the IPX network mask (in hexadecimal format) to be used (or just press **<Enter>** to use the default mask of FFFFFFFF). *If you selected the default of "all networks" in the previous step, this step is skipped.*

6. The following prompt displays:

   IPX node address (default: all nodes):

   Enter the IPX node address (in hexadecimal format) to be used (or just press **<Enter>** to use the default of "all nodes").

7. The following prompt displays:

IPX node mask (default: all F's) :

Enter the IPX node mask (in hexadecimal format) to be used (or just press **<Enter>** to use the default mask of all F's). *If you selected the default of "all nodes" in the previous step, this step is skipped.*

8. The following prompt displays:

SAP service type (default: all services) :

Enter the SAP service type (in hexadecimal format) as defined by NetWare (or just press **<Enter>** to use the default of all services).

9. A message will confirm the addition of the filter:

ipxfilter successfully added

Using Filters with Frame Relay or ISDN Boards

If the Group or VLAN you enter (such as 1:1 used in the above example) refers to a WAN interface like Frame Relay or PPP, you'll be asked if you want the filter applied to a specific WAN endpoint.

10. This prompt appears after the previous prompt for "SAP Service Type":

Do you wish to apply this filter to a specific WAN endpoint? (n):

Enter **y** to select to apply this filter to a specific WAN endpoint.

11. The following prompt displays:

Frame Relay VC or PPP Peer {vc(v), peer(p)} (v):

Enter **v** (or just press **<Enter>**) to apply this filter to a Frame Relay Virtual Circuit. Proceed to the next step.

Enter **p** if you want to apply this filter to a PPP Peer. Skip to the last step.

12. If you chose to apply a filter to a Frame Relay VC, this prompt displays:

Slot/port:

Enter the slot and port to which you want to apply this filter (for example, **3/1**).

Enter the VC to which you want to apply this filter.

13. If you chose to apply a filter to a PPP Peer, this prompt displays:

Peer ID:1

Enter the Peer ID to which you want to apply this filter (for example, **1**).

Deleting an IPX RIP/SAP Filter

Follow the steps below to delete an existing IPX RIP or SAP filter.

1. Enter **ipxfilter**.

   A screen similar to the following displays:

   ```
   Selecting global IPX filter:

     Add or delete entry {add(a), delete(d)} (a) :
   ```

   Enter **d** to select to delete a filter.

2. A screen similar to the following displays:

   ```
   Displaying all filters:

                                                                          GP:VL  (s/p/vc)
    #    Type          Net/Mask        Node/Mask                  Svc   Md        (Peer ID)
   ------ ------------ ---------------------- ---------------------------------- ------ ---- --------------------
     1   SAP OUT       67/ffffffff     000000000001/ffffffffffff   ALL    B   global
     2   SAP IN        67/ffffffff     000000000001/ffffffffffff   0278   B   1:1
     3   RIP IN        67/ffffffff                                        B   global

     Entry number to delete? (default: none) : 1
   ```

   This screen contains a list of the existing IPX RIP/SAP filters. The fields on this screen are described in the next section (see *Displaying IPX RIP/SAP Filters* on page 33-23).

3. Enter the index number of the filter you want to delete. If you decide at this point that you want to abort out of the deletion process, simply press **<Enter>** to accept the default of "none."

4. A message will confirm the deletion of the filter:

   ```
   ipxfilter successfully deleted.
   ```

Displaying IPX RIP/SAP Filters

The **ipxf** command is used to display a list of all existing IPX RIP and SAP filters. See *Adding a "Global" IPX RIP/SAP Filter* on page 33-19 for complete information on creating these filters. You can enter optional parameters with the **ipxf** command to display specific filters.

Displaying a List of All IPX Filters

To display a listing of all existing IPX RIP and SAP filters, enter the following command:

```
ipxf
```

A screen similar to the following displays:

```
Displaying all filters:

                                                                    GP:VL  (s/p/vc)
 #    Type         Net/Mask        Node/Mask                 Svc   Md        (Peer ID)
------ ------------ ---------------------- ---------------------------------- ------ ---- --------------------
   1  SAP OUT      67/ffffffff     000000000001/ffffffffffff  ALL    B   global
   2  SAP IN       67/ffffffff     000000000001/ffffffffffff  0278   B   1:1
   3  RIP IN       67/ffffffff                                       B   global
   4  SAP IN       All Networks                  All Nodes    ALL    B   3:1 (P1)
```

This screen contains a list of the existing IPX RIP and SAP filters. The fields on this screen have the following meanings.

#

The index number assigned to identify each filter.

Type

The type of filter. The five types are: RIP IN, RIP OUT, SAP IN, SAP OUT, and GNS OUT.

Net/Mask

The IPX network address to be filtered ("All networks" means all networks are filtered).

Node/Mask

The IPX node address to be filtered ("All nodes" means all nodes are filtered). This field does not apply to RIP IN or RIP OUT filters.

Svc

The SAP service type (shown as a hexadecimal number) on which the filter is applied, as defined by Novell. By default, all services will be filtered. (Note: This field does not apply to RIP IN or RIP OUT filters.)

Md

The Mode of operation for the filter: A to Allow, B to Block.

GP:VL (s/p/vc) or (Peer ID)

The first number (**GP**) is the Group associated with this entry. The second number (**VL**) is the VLAN associated with this entry. When a filter applies to all interfaces, this field will say "global." If an entry refers to a Frame Relay interface, column headings for slot, port, and virtual circuit (**s/p/vc**) may be displayed when the filter is applied to a particular virtual circuit rather than to the entire VLAN. If an entry refers to a PPP interface, the Peer ID (**Peer ID**) may be displayed when the filter is applied to a particular PPP Peer.

Displaying a List of "Global" IPX Filters

To display a listing of just the global IPX filters, enter the following command:

```
ipxf global
```

A screen similar to the following displays:

```
Displaying global filters:
                                                                    GP:VL  (s/p/vc)
 #    Type         Net/Mask        Node/Mask                  Svc   Md        (Peer ID)
------ ------------ ---------------------- ------------------------------------ ------ ---- --------------------
   1  SAP OUT      67/ffffffff     000000000001/ffffffffffff   ALL    B   global
   3  RIP IN       67/ffffffff                                       B   global
```

Displaying a List of Specific IPX Filters

To display a listing of IPX RIP or SAP filters for a specific interface, you can specify other parameters along with the **ipxf** command. The format for the command in this case is:

```
ipxf <type> <GP:VL>
```

The type is one of these codes:

ri	for RIP INput
ro	for RIP OUTput
si	for SAP INput
so	for SAP OUTput
go	for GNS OUTput

For example, to display a list of the filters defined for Group 1, VLAN 1, you would enter:

```
ipxf 1:1
```

A screen similar to the following displays:

```
Displaying filters for interface 1:1:
                                                                    GP:VL  (s/p/vc)
 #    Type         Net/Mask        Node/Mask                  Svc   Md        (Peer ID)
------ ------------ ---------------------- ------------------------------------ ------ ---- --------------------
   2  SAP IN       67/ffffffff     000000000001/ffffffffffff  0278    B   1:1
```

As another example, to display a list of all global RIP Input filters, you would enter:

```
ipxf ri global
```

A screen similar to the following displays:

```
Displaying all global RIP INPUT filters:

                                                                    GP:VL  (s/p/vc)
 #     Type          Net/Mask        Node/Mask                Svc  Md        (Peer ID)
------ ------------ ---------------------- ---------------------------------- ------ ---- --------------------
  3   RIP IN        67/ffffffff                                        B   global
```

IPX RIP/SAP Filter Precedence

Whenever you use multiple "allow" filters you must first define a filter to block all RIPs or SAPs. Then, all of the seceding "allow" filters of the same type must be *at least* as specific in all areas in order for the filters to work. Note that filtering precedence is related only to "allow" filters. Multiple "block" filters can be defined with varying specificity in each of the areas of the filter. The filtering done by the configurable parameters (Net/Mask, Node/Mask, Service/Mode) in the "allow" filter must be at least as specific as the filtering defined in the "block" filter.

As an example, consider a switch that knows of multiple Type 4 SAPs on various networks, including a network with an address of "40." The switch also knows of various types of SAPs on Network 40. For this example, you want to block all SAPs coming from Network 40, but you want to allow all Type 4 SAPs, including the ones that come from Network 40.

To meet these objectives, you must configure the filters like this:

```
 #     Type          Net/Mask        Node/Mask                Svc  Md  GP:VL
------ ------------ ---------------------- ---------------------------------- ------ ---- ----------
  1   SAP IN        40/ffffffff                                        B   global
  2   SAP IN        40/ffffffff                                        A   global
```

The filters shown below will *not* work for our example because in Filter 2 the type of service is *less* specific than the type defined in Filter 1. All Type 4 SAPs will be blocked by the filter.

```
 #     Type          Net/Mask        Node/Mask                Svc  Md  GP:VL
------ ------------ ---------------------- ---------------------------------- ------ ---- ----------
  1   SAP IN        All networks                                       B   global
  2   SAP IN        40/ffffffff                                        A   global
```

The following filters will also *not* work because in Filter 2 the network and netmask are *less* specific than the network and netmask defined in Filter 1. All SAPs from Network 40 will be blocked by the filter.

```
 #     Type          Net/Mask        Node/Mask                Svc  Md  GP:VL
------ ------------ ---------------------- ---------------------------------- ------ ---- ----------
  1   SAP IN        40/ffffffff                                        B   global
  2   SAP IN        All networks                                       A   global
```

Configuring IPX Serialization Packet Filtering

The **ipxserialf** command is used to enable and disable IPX Serialization Packet filtering on any or all WAN routing services. This feature can be used to reduce traffic on WAN links by preventing the transmission of NetWare serialization packets.

Novell uses a serialization mechanism to make sure that licensed copies of NetWare are not improperly copied to multiple servers. NetWare's built-in copy protection scheme transmits serialization packets between file servers which contain unique serialization numbers. These packets are sent out at about 66-second intervals. If a server detects duplicate serialization identifiers, it broadcasts a copyright violation message to all users and to the console log. The major problem with this protection scheme for dial-on-demand links, such as ISDN, is the generation of traffic that continuously reactivates the WAN link.

Enabling IPX Serialization Filtering

Follow the steps below to enable IPX Serialization Packet Filtering.

1. Enter **ipxserialf**.

   A screen similar to the following displays:

   View the current status of all WAN routing services? (y or n) (n) :

   Enter **y** if you do want to see the current filtering status. Enter **n** (or press **<Enter>**) if you entered this command by mistake or if you don't need to see the current status.

2. A screen similar to the following displays:

Group	IPX Serialization Filtering
3	Disabled
4	Disabled

   Enter Group (default: all WAN) :

   This screen shows the WAN routing Groups that exist in the switch and the current status of the IPX Serialization packet filtering for these groups.

   Enter a Group number to proceed to enable IPX Serialization filtering for that Group.

   Or, press **<Enter>** to select to enable filtering for *all* WAN routing services.

3. The following prompt displays:

   Enable IPX Serialization Filtering? (y or n) (n) :

   Enter **y** to select to enable IPX Serialization Filtering.

   Enter **n** (or press **<Enter>**) if you do *not* want to enable Serialization Filtering.

4. The following prompt displays:

   Enable IPX Serialization Filtering on all WAN routing services? (y or n) (n) :

   This prompt requires you to verify that you want to enable filtering in order to avoid the situation of accidental filtering of IPX Serialization packets. This example prompt asks if you want to disable filtering on all WAN routing services. If you had entered a specific Group number, the prompt would refer to that particular Group.

   Enter **y** to enable IPX Serialization Filtering.

5. Filtering will then become active. A message will appear indicating that IPX Serialization Filtering is enabled, either on all WAN routing services or for a specific Group:

```
IPX Serialization Filtering is now enabled on all WAN routing services
```

Disabling IPX Serialization Filtering

Follow the steps below to disable IPX Serialization Packet Filtering.

1. Enter **ipxserialf**.

   A screen similar to the following displays:

```
View the current status of all WAN routing services? (y or n) (n) :
```

   Enter **y** if you do want to see the current filtering status. Enter **n** (or press **<Enter>**) if you entered this command by mistake or if you don't need to see the current status.

2. A screen similar to the following displays:

```
Group      IPX Serialization Filtering
---------- ---------------------------------------
3                    Enabled
4                    Enabled

Enter Group (default: all WAN) :
```

   This screen shows the WAN routing Groups that exist in the switch and the current status of the IPX Serialization packet filtering for these groups.

   Enter a Group number to proceed to disable IPX Serialization filtering for that Group.

   Or, just press **Enter** to select to proceed to disable filtering for *all* WAN routing services.

3. The following prompt displays:

```
Enable IPX Serialization Filtering? (y or n) (n) :
```

   Enter **n** (or press **<Enter>**) to select to disable Serialization Filtering.

4. The following prompt displays:

```
Disable IPX Serialization Filtering on all WAN routing services? (y or n) (n) :
```

   This prompt requires you to verify that you want to disable filtering. This example prompt asks if you want to disable filtering on all WAN routing services. If you had entered a specific Group number, the prompt would refer to that particular Group.

   Enter **y** to disable IPX Serialization Filtering.

5. A message will appear indicating that IPX Serialization Filtering is disabled, either on all WAN routing services or for a specific Group:

```
IPX Serialization Filtering is now disabled on all WAN routing services
```

Configuring IPX Watchdog Spoofing

The **ipxspoof** command is used to enable and disable IPX Watchdog Spoofing on any or all WAN routing services. The use of this feature is explained below:

Novell's IPX Watchdog Protocol, which is used by NetWare to maintain network node and server connections, can consume significant network bandwidth and thereby incur costs on expensive dial-on-demand, pay-per-packet WAN links. The OmniSwitch provides an IPX Watchdog Spoofing feature to prevent Watchdog packets from initiating connections on WAN links in situations where no other data is ready to be transferred.

The IPX Watchdog Spoofing feature enables the switch to respond to a NetWare server's Watchdog "Query" requests on behalf of a remote client, thus spoofing the requests. The spoofing action occurs when the switch "sees" an incoming Watchdog packet destined for an interface on which spoofing has been enabled. The switch responds to the server by sending out a valid Watchdog response. Spoofing thus maintains the required Watchdog function while avoiding the cost of making and maintaining a WAN link.

In some situations, the use of the IPX Watchdog Spoofing feature can make a NetWare server "believe" that an inactive session is still active. This occurrence can cause connectivity problems by denying login rights to legitimate users. Therefore, if you use the spoofing feature on networks that also limit the number of IPX or SPX sessions, you should utilize NetWare's "auto-logoff" function to minimize inappropriate denials of legitimate logins.

Enabling IPX Watchdog Spoofing

Follow the steps below to enable IPX Watchdog Spoofing.

1. Enter **ipxspoof**.

   A screen similar to the following displays:

   ```
   View the current spoofing status of all WAN routing services? (y or n) (n) :
   ```

   Enter **y** if you do want to see the current IPX spoofing status. Enter **n** (or just press **Enter**) if you entered this command by mistake or if you don't need to see the current status.

2. A screen similar to the following displays:

   ```
   Group       IPX Spoofing
   ----------  ----------------------------
   3                 Disabled
   4                 Disabled

   Enter Group (default: all WAN) :
   ```

   Enter a Group number to proceed to enable IPX spoofing for that particular Group.

   Or, just press **Enter** to proceed to enable IPX spoofing for *all* WAN routing services.

3. The following prompt displays:

   ```
   Enable Spoofing? (y or n) (n) :
   ```

   Enter **y** to proceed to enable IPX spoofing.

4. The following prompt displays:

   ```
   Enable IPX Spoofing on all WAN routing services? (y or n) (n) : y
   ```

   This prompt requires you to verify that you want to enable spoofing in order to avoid the situation of accidental spoofing of IPX packets.

This example prompt asks if you want to enable spoofing on all WAN routing services. If you had entered a specific Group number, the prompt would refer to that particular Group.

Enter **y** to enable IPX Watchdog Spoofing.

5. IPX Spoofing will then become active. A message will appear indicating that IPX Watchdog Spoofing is enabled, either on all WAN routing services, or for a specific Group:

```
IPX Spoofing is now enabled on all WAN routing services
```

Disabling IPX Watchdog Spoofing

Follow the steps below to disable IPX Watchdog Spoofing.

1. Enter **ipxspoof**.

   A screen similar to the following displays:

```
View the current spoofing status of all WAN routing services? (y or n) (n) :
```

   Enter **y** if you do want to see the current IPX spoofing status. Enter **n** (or just press **<Enter>**) if you entered this command by mistake or if you don't need to see the current status.

2. A screen similar to the following displays:

```
Group      IPX Spoofing
---------- ----------------------------
3                Enabled
4                Enabled

Enter Group (default: all WAN) :
```

   Enter a Group number if you want to disable IPX spoofing for that particular Group.

   Or, press **<Enter>** to disable IPX spoofing for *all* WAN routing services.

3. The following prompt displays:

```
Enable Spoofing? (y or n) (n) :
```

   Enter **n** (or just press **<Enter>**) to proceed to disable IPX spoofing.

4. The following prompt displays:

```
Disable IPX Spoofing on all WAN routing services? (y or n) (n) : y
```

   This prompt requires you to verify that you want to disable spoofing. This example prompt asks if you want to disable spoofing on all WAN routing services. If you had entered a specific Group number, the prompt would refer to that particular Group.

   Enter **y** to disable IPX Watchdog Spoofing.

5. IPX Spoofing will then become inactive. A message will appear indicating that IPX Watchdog Spoofing is disabled, either on all WAN routing services, or for a specific Group:

```
IPX Spoofing is now disabled on all WAN routing services
```

Configuring SPX Keepalive Spoofing

The **spxspoof** command is used to enable and disable SPX Keepalive Spoofing on any or all WAN routing services. The use of this feature is explained below:

Novell's SPX Keepalive Protocol, which is used by NetWare to maintain SPX connections between end nodes, can also consume significant network bandwidth and thereby incur unnecessary costs on expensive dial-on-demand, pay-per-packet WAN links. The OmniSwitch provides a SPX Keepalive Spoofing feature to prevent keepalive packets from keeping WAN links active when they are not otherwise needed for data transmissions.

The SPX Spoofing feature enables the switch to respond to client/server keepalive packets on the behalf of the remote clients/servers. SPX spoofing thereby effectively stops keepalive packets from crossing a WAN link while maintaining existing SPX connections.

SPX-Packet Tolerance Counting

NetWare's SPX and SPXII watchdog and keepalive packets unfortunately are not labeled with a unique packet type. Therefore, valid acknowledge packets or window-update packets could be mistaken for keepalive packets. To prevent blocking of critical packets, a packet tolerance counting mechanism is employed by the Spoofing feature to count SPX packets.

When active, the Spoofing feature observes all watchdog and keepalive packets as they go between network endpoints. If successive packets are found to have the same sequence number, acknowledge number, and "alloc" number, spoofing will not begin until the specified SPX-packet tolerance count has been reached. Only watchdog packets which have the ACK_REQUSTED bit set will have an effect on the SPX-packet tolerance counter.

Once the specified tolerance count has been reached, spoofing of watchdog packets will begin and all keepalive packets will be dropped. Refer to *Controlling IPX Type 20 Packet Forwarding* on page 33-32 for help on using NetWare's configurable parameters to change the frequency and number of keepalive/watchdog packets sent.

Enabling SPX Keepalive Spoofing

Follow the steps below to enable SPX Keepalive Spoofing.

1. Enter **spxspoof**.

   A screen similar to the following displays:

   ```
   View the current spoofing status of all WAN routing services? (y or n) (n) :
   ```

   Enter **y** if you do want to see the current SPX spoofing status. Enter **n** (or press **<Enter>**) if you entered this command by mistake or if you don't need to see the current status.

2. A screen similar to the following displays:

   ```
   Group       SPX Spoofing
   ----------  ----------------------------
   3                 Disabled
   4                 Disabled

   Enter Group (default: all WAN) :
   ```

   Enter a Group number to proceed to enable SPX spoofing for that particular Group.

   Or, press **<Enter>** to proceed to enable SPX spoofing for *all* WAN routing services.

3. The following prompt displays:

   ```
   Enable Spoofing? (y or n) (n) :
   ```

Enter **y** to proceed to enable spoofing.

4. The following prompt displays:

```
Enable SPX Spoofing on all WAN routing services? (y or n) (n) : y
```

This prompt requires you to verify that you want to enable spoofing in order to avoid the situation of accidental spoofing of SPX packets. This example prompt asks if you want to enable SPX spoofing on all WAN routing services. If you had entered a specific Group number, the prompt would refer to that particular Group.

Enter **y** to enable spoofing.

5. SPX Spoofing will then become active. A message will appear indicating that SPX Spoofing is enabled, either on all WAN routing services, or for a specific Group:

```
SPX Spoofing is now enabled on all WAN routing services
```

Disabling SPX Keepalive Spoofing

Follow the steps below to disable SPX Keepalive Spoofing.

1. Enter **spxspoof**.

A screen similar to the following displays:

```
View the current spoofing status of all WAN routing services? (y or n) (n) :
```

Enter **y** if you do want to see the current SPX spoofing status. Enter **n** (or press **<Enter>**) if you entered this command by mistake or if you don't need to see the current status.

2. A screen similar to the following displays:

```
Group       SPX Spoofing
----------  ----------------------------
3                 Enabled
4                 Enabled

Enter Group (default: all WAN) :
```

Enter a Group number to proceed to disable SPX spoofing for that particular Group.

Or, just press **<Enter>** to proceed to disable SPX spoofing for *all* WAN routing services.

3. The following prompt displays:

```
Enable Spoofing? (y or n) (n) :
```

Enter **n** to proceed to disable spoofing.

4. The following prompt displays:

```
Disable SPX Spoofing on all WAN routing services? (y or n) (n) : y
```

This prompt requires you to verify that you want to disable spoofing in order to avoid the situation of accidental spoofing of SPX packets. This example prompt asks if you want to disable SPX spoofing on all WAN routing services. If you had entered a specific Group number, the prompt would refer to that particular Group.

Enter **y** to disable spoofing.

5. SPX Spoofing will then become inactive. A message will appear indicating that SPX Spoofing is disabled, either on all WAN routing services, or for a specific Group:

```
SPX Spoofing is now disabled on all WAN routing services
```

Controlling IPX Type 20 Packet Forwarding

The **ipxtype20** command is used to control the forwarding of IPX Type 20 packets. The default setting is to *not* forward IPX Type 20 packets. You can use the **ipxtype20** command to explicitly enable the forwarding of Type 20 packets for individual interfaces routing IPX traffic.

Type 20 packets contain the value 20 (14 hex) in the "packet type" field of the IPX header. Novell has defined the use of these packets to support certain protocol implementations, such as NetBIOS. As these packets are broadcasted and propagated across networks, the addresses of those networks (up to 8) are stored in the packet's data area.

The reason why forwarding of Type 20 packets is normally "off" is that they can cause problems in highly redundant IPX networks by causing what appears to be a broadcast storm. This problem is aggravated whenever misconfigured PCs are added to a network.

Follow the steps below to enable IPX Type 20 packet forwarding on a given interface.

1. Enter **ipxtype20**.

   A screen similar to the following displays:

   ```
   Do you want to see the status of IPX Type 20 packet forwarding?
                                                    (y or n) (y) :
   ```

2. Enter a **y** at this prompt (or press **<Enter>**) to display the current handling of IPX Type 20 packets on all configured IPX interfaces.

   A screen similar to the following displays:

   ```
   GP:VL     Type20 Packet Forwarding
    -------  ---------------------------------------
     3:1      off
     4:1      off

   group:vlan () :
   ```

3. Enter the Group and VLAN numbers associated with the IPX interface for which you wish to enable Type 20 packet forwarding. For example, you could enter **3:1**.

   A screen similar to the following displays:

   ```
   Currently, Group 3:Vlan 1 has IPX Type 20 packet forwarding off.
     "on" or "off" (off) :
   ```

4. Enter **on** to turn IPX Type 20 packet forwarding "on" for this interface. The default is "off".

   A screen similar to the following displays:

   ```
   IPX Type 20 packet forwarding on 3:1 has been changed to on.
   ```

You may also elect to bypass the above prompts. To do so, simply include the Group and/or VLAN number and the word "on" (or "off") as part of the command line.

For example, to turn forwarding "on" for Group 4, VLAN 1, enter **ipxtype20 4 on.**

A screen similar to the following displays:

```
IPX Type 20 packet forwarding on 4:1 has been changed to on.
```

If you enter the **ipxtype20** command with options for an interface that is not configured for IPX, a message similar to the following will appear:

```
Group 1:Vlan 1 isn't configured for IPX.

Usage: ipxtype20 [group:vlan] [on | off]
```

Configuring NetWare to Minimize WAN Connections

If you have access to NetWare's control parameters, you can "fine-tune" your network to minimize traffic on WAN links such as ISDN connections or Frame Relay lines. Doing so will reduce the costs associated with each connection that is made. Some suggested approaches are described below.

1. NetWare Directory Services (NDS), included in NetWare 4.x, includes a time synchronization protocol. By default, NetWare servers send time synchronization packets every 10 minutes. To help cut down on unnecessary connections that result from the time synchronization protocol, you could load the NLM (NetWare Loadable Module) named TIMESYNC.NLM onto your NetWare time servers. This NLM will allow you to modify the update interval of the time synchronization packets.

2. NDS also introduces more traffic in order to maintain replicas of NDS partitions. The NLMs named DSFILTER.NLM and PINGFILT.NLM can be used to modify NDS synchronization updates.

3. NetWare's IPX Watchdog protocol monitors the connection status of NetWare clients and transmits reports when a connection fails to respond. You could modify the following three Watchdog parameters on your NetWare file servers to help cut down the costs associated with the IPX protocol:

   - SET NUMBER OF WATCHDOG PACKETS (the default is 10, range is 5 to 100 packets).
   - SET DELAY BETWEEN WATCHDOG PACKETS (the default is 59.3 seconds, range is 9.9 seconds to 10 minutes and 26.2 seconds).
   - SET DELAY BEFORE FIRST WATCHDOG PACKET (the default is 4 minutes 56.6 seconds, range is 15.7 seconds to 20 minutes and 52.3 seconds).

4. There are two basic categories of timeouts which can cause extra network traffic and/or loss of SPX connections:

   - If a data packet goes unacknowledged, it is re-transmitted a certain number of times before the connection is aborted.
   - When a connection is idle and the SPX Watchdog is enabled, system packets are sent periodically, and if not eventually acknowledged, the connection is aborted.

5. The following parameters can be modified in the NET.CFG file to determine when packets should be resent or when connections should be aborted:

   - MINIMUM SPX RETRIES determines how many unacknowledged transmit requests are allowed before assuming the connection has failed.
   - SPX VERIFY TIMEOUT determines how often (in ticks) the SPX protocol sends a packet to the other side of a connection to indicate that it is still alive.
   - SPX LISTEN TIMEOUT specifies how long (in ticks) the SPX protocol waits without receiving a packet from the other side of the connection before it requests the other side to send a packet to ascertain whether the connection is still valid.
   - SPX ABORT TIMEOUT specifies how long (in ticks) the SPX protocol waits without receiving any response from the other side of the connection before it terminates the session.

6. Novell has developed a workaround that can be used to disable the SPX Watchdog mechanism. This workaround could be used instead of enabling the SPX Spoofing feature on your switch. SPWXDOG.NLM is a patch that is used to disable NetWare's SPX Watchdog mechanism on 3.x and 4.x servers. The patch adds the following file server set parameter:

"set spx watchdogs=ON/OFF" (The default is ON.)

To fully disable SPX Watchdog packets, the remote client/server should also disable Watchdogs. IPXODI v3.02 and IPX.NLM support a NET.CFG parameter to disable SPX Watchdogs ("spx watchdog=off").

Configuring RIP and SAP Timers

The standard time between broadcasts of RIP and SAP messages is 60 seconds. This default may be modified in order to alleviate network congestion or facilitate the discovery of network resources.

Adding a RIP and SAP Timer

1. To adjust the time between RIP and SAP messages, enter the following command at the system prompt:

   ipxtimer

   The following prompt displays:

   Add or delete entry {add(a), delete(d)} (a) :

2. Enter **a** and the following prompt displays:

   Group: (global) : 1

3. Enter the group number or leave the field blank and press Enter. If you do not enter a group number, the SAP and RIP timers will be adjusted for all groups on the switch.

   The following prompt displays:

   RIP timer (1..180 secs): (60) :

4. Enter the desired value or press **<Enter>** to configure the default value, which is 60 seconds. The following prompt displays:

   SAP timer (1..180 secs): (60) :

5. Enter the desired value or press **<Enter>** to configure the default value, which is 60 seconds. The following message displays:

   ipxtimer successfully added

Viewing RIP and SAP Timers

To view the RIP and SAP timers that have been configured through the **ipxtimer** command, enter the following command:

```
ipxt
```

A screen similar to the following displays:

```
 #     Group    RIP Timer (secs)   SAP Timer (secs)
===   =======   ================   ================
  1       1            30                 15
  2    global          45                 45
```

The fields are defined as follows:

Group

Displays the group number or **global** to indicate all groups.

RIP Timer (secs)

Displays the RIP timer configured for the group using the **ipxtimer** command.

SAP Timer (secs)

Displays the SAP timer configured for the group using the **ipxtimer** command.

Configuring Extended RIP and SAP Packets

Larger RIP and SAP packets may be transmitted so that congestion in the network is reduced. Other switches and routers in the network must support larger packet size if this feature is configured on the switch.

Use the **ipxext** command to enable or disable extended packets or to view the current status of extended packet transmission.

Enabling or Disabling Extended RIP and SAP Packets

To enable larger RIP and SAP packets, enter the following command:

```
ipxext on
```

To disable larger RIP and SAP packets, enter the following command:

```
ipxext off
```

Viewing the Current Status of Extended Packets

To display the current status of this feature, enter the following command:

```
ipxext
```

When the feature is disabled (the default), the following message displays:

```
IPX extended RIPs and SAPs off
```

When the feature is enabled, the following message displays:

```
IPX extended RIPs and SAPs on
```

Configuring an IPX Default Route

A default IPX route may be configured for packets destined for networks unknown to the switch. If RIP messages are disabled, packets can still be forwarded to a router that knows where to send them. Use the **ipxdrt** command to add a default route, view the status of a default route, or disable the default route.

Adding an IPX Default Route

To configure a default route, use the **ipxdrt** command with the relevant network ID. For example:

```
ipxdrt 222
```

If the network ID indicates a direct network on the switch, the MAC address must also be specified, and the following prompt will display:

```
IPX node address of next hop (format - xx:xx:xx:xx:xx:xx) :
```

Enter the relevant address.

Viewing the Status of an IPX Default Route

To view the status of the default route, enter the **ipxdrt** command. A message similar to the following displays:

```
IPX default route:   00000222   00:20:da:99:88:77
```

Disabling an IPX Default Route

To disable the default route, enter the following:

```
ipxdrt off
```

If you enter the **ipxdrt** command again, the following message displays:

```
IPX default route is disabled
```