CHAPTER 3

IPX Routing & Bridging

IPX Routing: Ethernet Configuration Dialog Box

To access this dialog box (Figure 3-1), select Ethernet/IPX Routing in the Device View.

Figure 3-1 IPX Routing: Ethernet Configuration Dialog Box

IPX Ethernet Frame Types

These devices support all four defined IPX frame types, and will perform routing between frame types as necessary. Whether each or all of these frame types are used on an individual Ethernet interface is determined by the settings for each type.

- **Ethernet Type II** is commonly used by TCP/IP and DECnet. The default seeding value is Non-Seed.
- **Ethernet 802.3 (Raw)** is the default frame type for earlier versions of Novell Netware. The default seeding value is Auto-Seed.
- **Ethernet 802.2** is a modified version of Ethernet_II and is the default frame type for Novell Netware 4. The default seeding value is Auto-Seed.
- **Ethernet 802.2 SNAP** is used by the AppleTalk protocol. The default seeding value is Non-Seed.

IPX Routing/Bridging/Off

This set of radio buttons controls how IPX packets are handled for this interface.

- If set to **IPX Routing**, then IPX packets received on this interface are routed to the correct interface on the device.
- If set to **IPX Bridging**, then any IPX packets received on this interface are forwarded to the device's internal bridge. This setting makes this Ethernet interface a member of the "IPX Bridge Group" for this device.

The IPX Bridging radio button will be grayed out unless bridging has been turned on globally for the device using the Main Bridging Configuration dialog box (under Global/Bridging) and locally on this interface using the Ethernet-Bridging dialog box (under Ethernet/Bridging).

- If it is set to **IPX Off**, then any IPX packets received on this interface are discarded.

Seed Status (per Frame Type)

One of the functions which routers perform in IPX internetworking is setting the IPX network number for each network segment. A router which sets the network number for a segment is said to have "seeded" the network.

- **Seed** means the device will listen for an IPX network number being set by another router (including Novell software routers residing on servers) on the segment connected to this interface and use this number if it exists. If it doesn't discover a number in use, the device will use the configured IPX Network Number to set the network number for the segment.
- **Non-Seed** means the device will listen for an IPX network number being set by another router (including Novell software routers residing on servers) on the segment connected to this interface and use this number if it exists. If it doesn't discover a number in use, the device will wait indefinitely until a number is set by another router on the segment.
- **Auto-Seed** means the device will listen for an IPX network number being set by another router (including Novell software routers residing on servers) on the segment connected to this interface and use this number if it exists. If it doesn't discover a number in use, the device will auto-generate a valid number using its routing tables.
- **Off** means the device will neither listen for, nor send packets with this frame type on this interface.

Network Number (per Frame Type)

This is an eight-digit hexadecimal number that uniquely identifies the network segment connected to this interface. Values range from 1 to FFFFFFFE.

Accidental selection of an IPX network number which is already in use on another network segment may cause hard-to-diagnose problems. You should carefully track which IPX network numbers are in use, and where they are used.

RIP Update Timer

This value dictates how often the device sends out IPX RIP (Routing Information Protocol) packets on the network segment attached to this interface. The RIP packets sent out on this interface contain information about networks for which this device is responsible. RIP packets received tell the device about other networks and routers. The default is 60 seconds.

SAP Update Timer

This value dictates how often the device sends out IPX SAP (Service Access Protocol) packets on the network segment attached to this interface. The SAP packets sent out on this interface contain information about services (such as servers, printers, etc.) for which this device is responsible. SAP packets received tell this device about services available on other network segments. The default is 60 seconds.

Block IPX Type 20 Output Packets

In order for some protocols, notably NetBIOS, to function in the NetWare environment, routers must propagate a certain type of broadcast packet throughout an IPX internetwork. IPX packet type 20 is designated to perform broadcast propagation for these protocols.

When an IPX device receives a type 20 packet, it rebroadcasts it out all interfaces, except the one on which it was received. The IPX network number of the originating interface is included in the rebroadcast packets.

This checkbox allows you to control the rebroadcasting of IPX type 20 packets on this interface. This is useful for on-demand WAN links where the link may be brought up as a result of propagating this type of packet.

- If **checked**, then type 20 packets will not be propagated on this interface. The default is unchecked.

IPX Routing: WAN Configuration Dialog Box

To access this dialog box (Figure 3-2), select WAN/IPX Routing in the Device View.

Figure 3-2 IPX Routing: WAN Configuration Dialog Box

IPX Routing/Bridging/Off

This set of radio buttons controls how IPX packets are handled for this interface.

- If set to **IPX Routing**, then IPX packets received on this interface are routed to the correct interface on the device.
- If set to **IPX Bridging**, then any IPX packets received on this interface are forwarded to the device's internal bridge. This setting makes this interface a member of the "IPX Bridge Group" for this device.

The IPX Bridging radio button will be grayed out unless bridging has been turned on globally for the device using the Main Bridging Configuration dialog box (under Global/Bridging) and locally on this interface using the WAN-Bridging dialog box (under WAN/Bridging).

- If it is set to **IPX Off**, then any IPX packets received on this interface are discarded.

Numbered Interface

This checkbox determines whether the Wide Area Network connected to this interface will have an IPX network number associated with it.

Many WAN connections are simple point-to-point links. These links do not generally require a network number because there are only two devices on the link. All traffic sent from one end is, by definition, destined for the other end. You generally do not need a numbered WAN interface if you are using the PPP transport protocol.

In contrast, Frame Relay networks may have a number of participating devices connected through a single physical interface. Because of this, use of the Frame Relay transport protocol requires a numbered WAN interface.

- If **checked**, then you must set an IPX Network Number for this WAN interface. The default is unchecked.

Network Number

This is an eight-digit hexadecimal number that uniquely identifies the network segment connected to this interface. Values range from 1 to FFFFFFFE.

Accidental selection of an IPX network number which is already in use on another network segment may cause hard-to-diagnose problems. You should carefully track which IPX network numbers are in use, and where they are used.

Update Method

WAN interfaces which are configured to provide “dial-on-demand” service will bring a connection up (i.e. dial the other end) when there are network packets which must be transferred over the link. Once a dial-on-demand connection is up, network traffic passing across the link causes the inactivity timer for the link to be reset, keeping the connection up.

The IPX RIP protocol periodically sends out update information across a link. These periodic update packets will cause a WAN interface set for dial-on-demand operation to either stay up indefinitely, or to continuously dial, connect, and then drop the connection.

- If **Triggered** is selected with this pull-down menu, the device will modify the standard IPX RIP behavior for this interface to send IPX RIP packets only when there has been an update to its routing table information, or when it has detected a change in the accessibility of the next hop router.
- If **Periodic** is selected with this pull-down menu, the device will use the standard IPX RIP protocol, which sends RIP packets over the link based on the RIP Update Timer value set.

RIP Update Timer

This value dictates how often the device sends out IPX RIP (Routing Information Protocol) packets on the WAN link attached to this interface. The RIP packets sent out on this interface contain information about networks for which this device is responsible. RIP packets received tell the device about other networks and routers. The default is 60 seconds.

SAP Update Timer

This value dictates how often the device sends out IPX SAP (Service Access Protocol) packets on the WAN link attached to this interface. The SAP packets sent out on this interface contain information about services (such as servers, printers, etc.) for which this device is responsible. SAP packets received tell this device about services available on other network segments. The default is 60 seconds.

Optional Remote Node Network Number

Besides defining a method for router-to-router communication, the PPP protocol defines a method for individual client machines to dial in to a router interface. Once a client machine has connected to a router interface in this fashion, the router provides proxy services which allow the client machine to participate as a node on one of the router's local networks.

If remote node operation is desired, the WAN interface would usually be set up as an unnumbered interface, and the Remote Node Network Number would then be set to an IPX network number from the router's Ethernet interface(s).

Alternatively, if the interface is set to be numbered, an unused IPX network number may be used.

Use Ethernet Port as End-Node Proxy

The router can be set to dynamically reserve an IPX address for this WAN interface on an Ethernet segment. This proxy address will then be used if the remote PPP IPX implementation requests address negotiation (generally used by end-node clients).

Since the reserved address will be assigned to this interface, this checkbox can only be checked on an interface set to be unnumbered.

- If **checked**, then an IPX address will be reserved for this WAN interface on an Ethernet segment. The default is unchecked.

Block IPX Type 20 Output Packets

In order for some protocols, notably NetBIOS, to function in the NetWare environment, routers must propagate a certain type of broadcast packet throughout an IPX internetwork. IPX packet type 20 is designated to perform broadcast propagation for these protocols.

When an IPX router receives a type 20 packet, it rebroadcasts it out all interfaces, except the one on which it was received. The IPX network number of the originating interface is included in the rebroadcast packets.

This checkbox allows you to control the rebroadcasting of IPX type 20 packets on this interface. This is useful for on-demand WAN links where the link may be brought up as a result of propagating this type of packet.

- If **checked**, then type 20 packets will not be propagated on this interface. The default is unchecked.

Novell's router specification recommends that type 20 packets not be propagated across links with bandwidths of less than 1 megabit per second (such as asynchronous dial-up links and 56K leased lines).

IPX Routing: VPN Configuration Dialog Box

VPN (Virtual Private Network) ports must first be added to the edit area of a device before they can be configured. For more information about adding and deleting VPN ports, see Chapter 6, "VPN Ports and LAN-to-LAN Tunnels."

A VPN port is a virtual port which handles tunneled traffic. Tunnels are virtual point-to-point connections through a public network such as the Internet. All packets sent through a VPN tunnel are IP-encapsulated packets, including AppleTalk, IPX and even IP packets. This encapsulation is added or removed, depending on the direction, by "Tunnel Partner" devices.

Once a packet reaches the remote Tunnel Partner, the TCP/IP encapsulation is stripped off, leaving the original protocol. The unencapsulated packet is then handled according to the VPN port's protocol configuration settings. Networks connected via a tunnel will communicate as if they are on the same network, even though they are separated by the Internet.

You must set up both ends of every tunnel. Therefore, you must repeat this setup with the remote device.

To access this dialog box (Figure 3-3), select VPN/IPX Routing in the Device View under the VPN port's icon.

Figure 3-3 IPX Routing: VPN Configuration Dialog Box

IPX Routing/Bridging/Off

This set of radio buttons controls how IPX packets are handled for this interface.

- If set to **IPX Routing**, then IPX packets received on this interface are routed to the correct interface on the device.
- If set to **IPX Bridging**, then any IPX packets received on this interface are forwarded to the device's internal bridge. This setting makes this interface a member of the "IPX Bridge Group" for this device.

The IPX Bridging radio button will be grayed out unless bridging has been turned on globally for the device using the Main Bridging Configuration dialog box (under Global/Bridging) and locally on this interface using the VPN-Bridging dialog box (under VPN/Bridging).

- If it is set to **IPX Off**, then any IPX packets received on this interface are discarded.

Numbered Interface

This checkbox determines whether the VPN port will have an IPX network number associated with it.

VPN tunnels are essentially point-to-point links. These links do not generally require a network number because all traffic sent from one end is, by definition, destined for the other end. However, you may wish to assign an address for network tracking purposes.

Network Number

This IPX Network Number is an eight-digit hexadecimal number that uniquely identifies the network segment(s) connected to this interface. Values range from 1 to FFFFFFFE.

Accidental selection of an IPX network number which is already in use on another network segment may cause hard-to-diagnose problems. You should carefully track which IPX network numbers are in use, and where they are used.

Update Method

VPN links which are configured to provide “dial-on-demand” service will bring a connection up (i.e. dial the other end) when there are network packets which must be transferred over the link. Once a dial-on-demand connection is up, network traffic passing across the link causes the inactivity timer for the link to be reset, keeping the connection up.

The IPX RIP protocol periodically sends out update information across a link. These periodic update packets will cause a VPN link set for dial-on-demand operation to either stay up indefinitely, or to continuously dial, connect, and then drop the connection.

- If **Triggered** is selected with this pull-down menu, the device will modify the standard IPX RIP behavior for this link to send IPX RIP packets only when there has been an update to its routing table information, or when it has detected a change in the accessibility of the next hop router.
- If **Periodic** is selected with this pull-down menu, the device will use the standard IPX RIP protocol, which sends RIP packets over the link based on the RIP Update Timer value set.

RIP Update Timer

This value dictates how often the device sends out IPX RIP (Routing Information Protocol) packets on the network segments attached to this interface. The RIP packets sent out on this interface contain information about networks for which this device is responsible. RIP packets received tell the device about other networks and routers. The default is 60 seconds.

SAP Update Timer

This value dictates how often the device sends out IPX SAP (Service Access Protocol) packets on the network segments attached to this interface. The SAP packets sent out on this interface contain information about services (such as servers, printers, etc.) for which this device is responsible. SAP packets received tell this device about services available on other network segments. The default is 60 seconds.

Block IPX Type 20 Output Packets

In order for some protocols, notably NetBIOS, to function in the NetWare environment, devices must propagate a certain type of broadcast packet throughout an IPX internetwork. IPX packet type 20 is designated to perform broadcast propagation for these protocols.

When an IPX device receives a type 20 packet, it rebroadcasts it out all interfaces, except the one on which it was received. The IPX network number of the originating interface is included in the rebroadcast packets.

This checkbox allows you to control the rebroadcasting of IPX type 20 packets on this interface. This is useful for on-demand links where the link may be brought up as a result of propagating this type of packet.

- If **checked**, then type 20 packets will not be propagated on this interface. The default is unchecked.

Novell's router specification recommends that type 20 packets not be propagated across links with bandwidths of less than 1 megabit per second (such as asynchronous dial-up links and 56K leased lines).

IPX Routing: Bridge Configuration Dialog Box

Bridging operates on physical network addresses (such as Ethernet addresses), rather than logical addresses (such as IPX addresses). From the standpoint of IPX networking, interfaces which are set to bridge IPX between themselves appear as a single logical entity.

Thus, a device's "IPX Bridge Group" is made up of all of the physical network interfaces in a device which have been set to bridge IPX. This setting can be found in the IPX Configuration dialog box for each individual physical interface. For example, see the IPX Routing/Bridging/Off radio buttons in the IPX Routing: Ethernet Configuration dialog box.

Logically, the IPX Bridge Group is treated by the device as an interface (Bridge 0). The settings in the IPX Routing: Bridge 0 Configuration dialog box determine the IPX parameters for all of the physical network interfaces which make up the IPX Bridge Group. This is shown schematically in Figure 3-4.

Figure 3-4 Bridge Logical Diagram

To access the IPX Routing: Bridge dialog box (Figure 3-5), select Bridge 0/IPX Routing in the Device View.

Figure 3-5 IPX Routing: Bridge 0 Configuration Dialog Box

IPX Frame Types

These devices support all four defined IPX frame types, and will perform routing between frame types as necessary. Whether each or all of these frame types are used on an individual Bridge interface is determined by the settings for each type.

- **Ethernet Type II** is commonly used by TCP/IP and DECnet. The default seeding value is Non-Seed.
- **Ethernet 802.3 (Raw)** is the default frame type for earlier versions of Novell Netware. The default seeding value is Auto-Seed.
- **Ethernet 802.2** is a modified version of Ethernet_II and is the default frame type for Novell Netware 4. The default seeding value is Auto-Seed.
- **Ethernet 802.2 SNAP** is used by the AppleTalk protocol. The default seeding value is Non-Seed.

IPX Routing/Off

These radio buttons control whether IPX packets received by a member interface of the IPX Bridge Group are passed on for IPX routing.

- If set to **Routing**, then IPX packets received on a member interface of the IPX Bridge Group which cannot simply be bridged to another member interface of the group are passed on for IPX routing.
- If set to **Off**, then IPX packets received on a member interface of the IPX Bridge Group which cannot be bridged to another member interface of the group are dropped. This setting means that further IPX configuration information is not required for the IPX Bridge Group.

Seed Status (per Frame Type)

One of the functions which routers perform in IPX internetworking is setting the IPX network number for each network segment. A device which sets the network number for a segment is said to have "seeded" the network. Remember that all segments connected to interfaces which are members of an IPX Bridge Group will appear as the same logical segment.

- **Seed** means the device will listen for an IPX network number being set by another device (including Novell software routers residing on servers) on the segment(s) connected to this interface and use this number if it exists. If it doesn't discover a number in use, the device will use the configured IPX Network Number to set the network number for the segment(s)
- **Non-Seed** means the device will listen for an IPX network number being set by another router (including Novell software routers residing on servers) on the segment(s) connected to this interface and use this number if it exists. If it doesn't discover a number in use, the device will wait indefinitely until a number is set by another router on the segment(s).
- **Auto-Seed** means the device will listen for an IPX network number being set by another router (including Novell software routers residing on servers) on the segment(s) connected to this interface and use this number if it exists. If it doesn't discover a number in use, the device will auto-generate a valid number using its routing tables.
- **Off** means the device will neither listen for, nor send packets with this frame type on this interface.

Network Number (per Frame Type)

This is an eight-digit hexadecimal number that uniquely identifies the network segment(s) connected to this interface. Values range from 1 to FFFFFFFE.

Accidental selection of an IPX network number which is already in use on another network segment may cause hard-to-diagnose problems. You should carefully track which IPX network numbers are in use, and where they are used.

RIP Update Timer

This value dictates how often the device sends out IPX RIP (Routing Information Protocol) packets on the network segment(s) attached to this interface. The RIP packets sent out on this interface contain information about networks for which this device is responsible. RIP packets received tell the device about other networks and routers. The default is 60 seconds.

SAP Update Timer

This value dictates how often the device sends out IPX SAP (Service Access Protocol) packets on the network segment(s) attached to this interface. The SAP packets sent out on this interface contain information about services (such as servers, printers, etc.) for which this device is responsible. SAP packets received tell this device about services available on other network segments. The default is 60 seconds.

Block IPX Type 20 Output Packets

In order for some protocols, notably NetBIOS, to function in the NetWare environment, routers must propagate a certain type of broadcast packet throughout an IPX internetwork. IPX packet type 20 is designated to perform broadcast propagation for these protocols.

When an IPX device receives a type 20 packet, it rebroadcasts it out all interfaces, except the one on which it was received. The IPX network number of the originating interface is included in the rebroadcast packets.

This checkbox allows you to control the rebroadcasting of IPX type 20 packets on this interface. This is useful for on-demand WAN links where the link may be brought up as a result of propagating this type of packet.

- If **checked**, then type 20 packets will not be propagated on this interface. The default is unchecked.