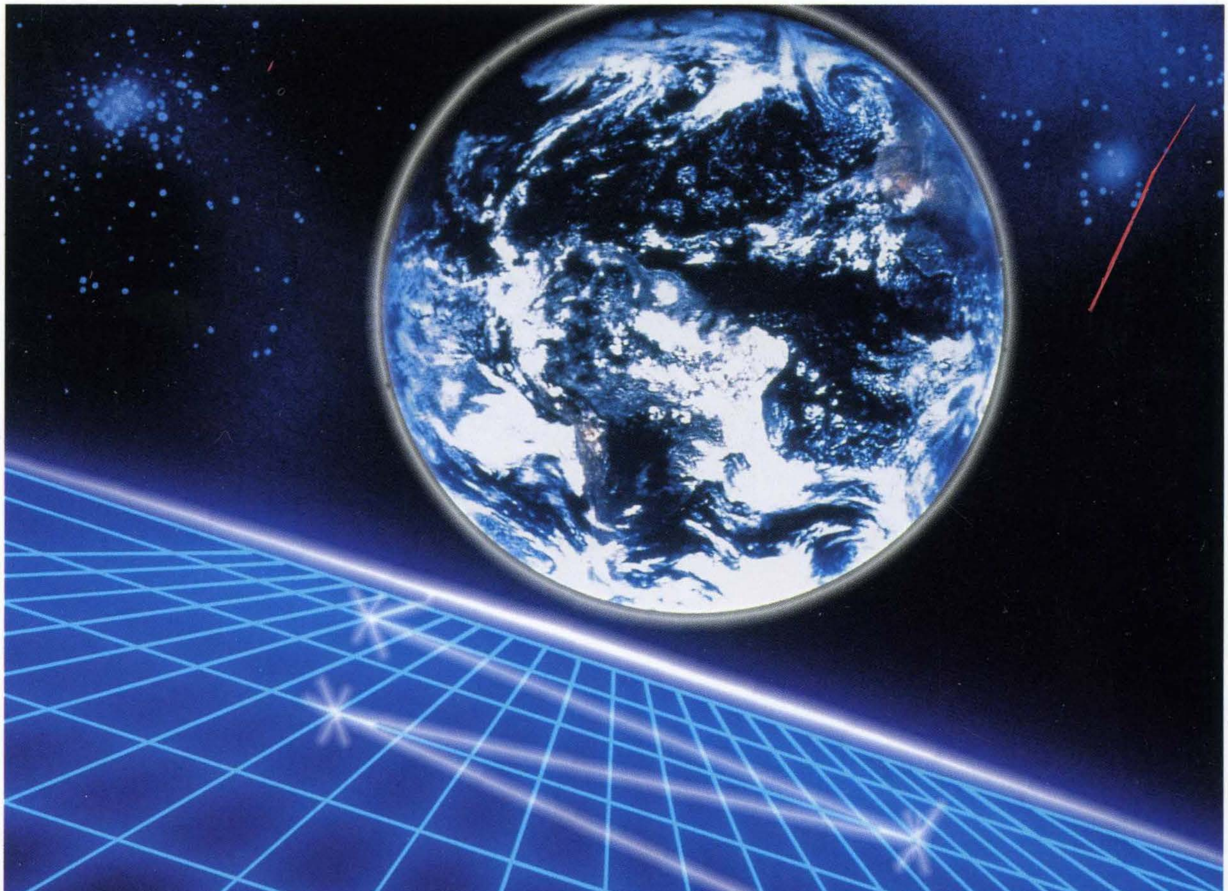


Bay Networks

The Merged Company of SynOptics and Wellfleet

Customizing IPX Services

Part No. 110050 A

Customizing IPX Services

Router Software Version 8.10
Site Manager Software Version 2.10

Part No. 110050 Rev. A
February 1995

Bay Networks
The Merged Company of SynOptics and Wellfleet

Copyright © 1995 Bay Networks, Inc.

All rights reserved. Printed in USA. February 1995.

The information in this document is subject to change without notice. This information is proprietary to Bay Networks, Inc.

The software described in this document is furnished under a license agreement or nondisclosure agreement and may only be used in accordance with the terms of that license. The terms of the Software License are provided with the documentation.

Restricted Rights Legend

Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013.

Notice for All Other Executive Agencies

Notwithstanding any other license agreement that may pertain to, or accompany the delivery of, this computer software, the rights of the Government regarding its use, reproduction, and disclosure are as set forth in the Commercial Computer Software-Restricted Rights clause at FAR 52.227-19.

Trademarks of Bay Networks, Inc.

ACE, BLN, BN, and Wellfleet are registered trademarks and AFN, AN, ASN, BCN, BCNX, BLNX, BNX, CN, FN, FRE, LN, PPX, Bay Networks, and the Bay Networks logo are trademarks of Bay Networks, Inc.

Third-Party Trademarks

3Com is a registered trademark of 3Com Corporation.

AIX, NetView, and IBM are registered trademarks of International Business Machines Corporation.

AppleTalk and EtherTalk are registered trademarks of Apple Computer, Inc.

AT&T and ST are registered trademarks of American Telephone and Telegraph Company.

DEC, DECnet, VAX, and VT100 are trademarks of Digital Equipment Corporation.

Distinct is a registered trademark and Distinct TCP/IP is a trademark of Distinct Corporation.

Fastmac and MADGE are trademarks of Madge Networks, Ltd.

Hayes is a registered trademark of Hayes Microcomputer Products, Inc.

HP is a registered trademark of Hewlett-Packard Company.

Intel is a registered trademark of Intel Corporation.

IPX, NetWare, and Novell are registered trademarks of Novell, Inc.

MCI is a registered trademark of MCI Communications Corporation.

Microsoft, MS, and MS-DOS are registered trademarks and Windows is a trademark of Microsoft Corporation.

Motif and OSF/Motif are registered trademarks of Open Software Foundation, Inc.

Motorola is a registered trademark of Motorola, Inc.

NetBIOS is a trademark of Micro Computer Systems, Inc.

Open Look and UNIX are registered trademarks of UNIX System Laboratories, Inc.

Sun and Solaris are registered trademarks and SPARCstation is a trademark of Sun Microsystems, Inc.

VINES is a registered trademark of Banyan Systems Incorporated.

X Window System is a trademark of the Massachusetts Institute of Technology.

Xerox is a registered trademark and XNS is a trademark of Xerox Corporation.

All other trademarks and registered trademarks are the property of their respective owners.

Bay Networks, Inc., 8 Federal Street, Billerica, MA 01821

Bay Networks Software License

This Software License shall govern the licensing of all software provided to licensee by Bay Networks ("Software"). Bay Networks will provide licensee with Software in machine-readable form and related documentation ("Documentation"). The Software provided under this license is proprietary to Bay Networks and to third parties from whom Bay Networks has acquired license rights. Bay Networks will not grant any Software license whatsoever, either explicitly or implicitly, except by acceptance of an order for either Software or for a Bay Networks product ("Equipment") that is packaged with Software. Each such license is subject to the following restrictions:

1. Upon delivery of the Software, Bay Networks grants to licensee a personal, nontransferable, nonexclusive license to use the Software with the Equipment with which or for which it was originally acquired, including use at any of licensee's facilities to which the Equipment may be transferred, for the useful life of the Equipment unless earlier terminated by default or cancellation. Use of the Software shall be limited to such Equipment and to such facility. Software which is licensed for use on hardware not offered by Bay Networks is not subject to restricted use on any Equipment, however, unless otherwise specified on the Documentation, each licensed copy of such Software may only be installed on one hardware item at any time.
2. Licensee may use the Software with backup Equipment only if the Equipment with which or for which it was acquired is inoperative.
3. Licensee may make a single copy of the Software (but not firmware) for safekeeping (archives) or backup purposes.
4. Licensee may modify Software (but not firmware), or combine it with other software, subject to the provision that those portions of the resulting software which incorporate Software are subject to the restrictions of this license. Licensee shall not make the resulting software available for use by any third party.
5. Neither title nor ownership to Software passes to licensee.
6. Licensee shall not provide, or otherwise make available, any Software, in whole or in part, in any form, to any third party. Third parties do not include consultants, subcontractors, or agents of licensee who have licensee's permission to use the Software at licensee's facility, and who have agreed in writing to use the Software only in accordance with the restrictions of this license.

7. Third-party owners from whom Bay Networks has acquired license rights to software that is incorporated into Bay Networks products shall have the right to enforce the provisions of this license against licensee.

8. Licensee shall not remove or obscure any copyright, patent, trademark, trade secret, or similar intellectual property or restricted rights notice within or affixed to any Software and shall reproduce and affix such notice on any backup copy of Software or copies of software resulting from modification or combination performed by licensee as permitted by this license.

9. Licensee shall not reverse assemble, reverse compile, or in any way reverse engineer the Software. [Note: For licensees in the European Community, the Software Directive dated 14 May 1991 (as may be amended from time to time) shall apply for interoperability purposes. Licensee must notify Bay Networks in writing of any such intended examination of the Software and Bay Networks may provide review and assistance.]

10. Notwithstanding any foregoing terms to the contrary, if licensee licenses the Bay Networks product "Site Manager," licensee may duplicate and install the Site Manager product as specified in the Documentation. This right is granted solely as necessary for use of Site Manager on hardware installed with licensee's network.

11. This license will automatically terminate upon improper handling of Software, such as by disclosure, or Bay Networks may terminate this license by written notice to licensee if licensee fails to comply with any of the material provisions of this license and fails to cure such failure within thirty (30) days after the receipt of written notice from Bay Networks. Upon termination of this license, licensee shall discontinue all use of the Software and return the Software and Documentation, including all copies, to Bay Networks.

12. Licensee's obligations under this license shall survive expiration or termination of this license.

Contents

Chapter 1
IPX Overview

Chapter 2
IPX Implementation Notes

Chapter 3
Editing IPX Parameters

Figures

Tables

About This Guide

If you are responsible for customizing Wellfleet® router software for IPX services, refer to this guide for

- An overview of the IPX routing protocol and a description of how Wellfleet routing services work (see Chapter 1, "IPX Overview")
- Implementation notes that may affect how you configure IPX routing services (see Chapter 2, "IPX Implementation Notes")
- Instructions on editing IPX global and interface parameters and configuring IPX services (see Chapter 3, "Editing IPX Parameters")

For information and instructions about the following topics, see *Configuring Wellfleet Routers*.

- Initially configuring and saving an IPX interface
- Retrieving a configuration file
- Rebooting the router with a configuration file

Before You Begin

Before using this guide, you must complete the following procedures:

- ❒ Create and save a configuration file that contains at least one IPX interface.
- ❒ Retrieve the configuration file in local, remote, or dynamic mode.

Refer to *Configuring Wellfleet Routers* for instructions.

How to Get Help

For additional information or advice, contact the Bay Networks Help Desk in your area:

United States	1-800-2LAN-WAN
Valbonne, France	(33) 92-966-968
Sydney, Australia	(61) 2-903-5800
Tokyo, Japan	(81) 3-328-0052

Conventions

arrow character (➔)	Separates menu and option names in instructions. Example: Protocols➔IPX identifies the IPX option in the Protocols menu.
command text	Denotes command names in text. Example: Use the **set** command.
italic text	Indicates variable values in command syntax descriptions, new terms, file and directory names, and book titles.
quotation marks (“ ”)	Indicate the title of a chapter or section within a book.

Acronyms

ATM	Asynchronous Transfer Mode
AUI	attachment unit interface
CNN	Common Network Number
DLCI	Data Link Connection Identifier
FDDI	Fiber Distributed Data Interface
HSSI	high-speed serial interface
IDP	Internet Data Packet
IPX	Internet Packet Exchange
ISO	International Standards Organization
LSAP	Layer Service Access Point
MAC	media access control
MIC	medium interface connector
NetBIOS	Network Basic Input-Output System
NIC	network interface card
PNN	Primary Network Number
PPP	Point-to-Point Protocol
PROM	Programmable Read Only Memory
RIP	Routing Information Protocol
SAP	Service Advertising Protocol
SMDS	Switched Multimegabit Data Services
SNAP	Subnetwork Access Protocol
WAN	wide area network
XNS	Xerox Network System

Chapter 1
IPX Overview

The Internet Packet Exchange (IPX®) Protocol is the Novell®, Inc. adaptation of the Xerox® Network System (XNS™). IPX has the following characteristics:

- It is a *connectionless datagram* delivery protocol. *Connectionless* means that it does not need a channel established for packet delivery. *Datagram* means that each packet is treated as an individual entity, having no logical or sequential relation to any other packet.
- It does not guarantee the delivery of packets. Higher-level protocols assume the responsibility for reliability. The higher-level protocols used by IPX are described in the section "Upper-Layer Services."
- It uses the Internet Data Packet (IDP) format.

IPX is the network-layer routing protocol used in the NetWare® environment. The primary tasks of IPX are addressing, routing, and switching of information packets from one location to another on a network. The network interface card (NIC) in a client provides network node addressing. IPX defines the *internetwork* and *intranode* addressing as follows:

- Network numbers form the basis of the IPX *internetwork* addressing scheme. Every network segment of an internetwork is assigned a unique network address by which routers forward packets to their final destination network. A network number in the NetWare environment consists of eight hexadecimal characters (four 8-bit bytes). In the following example, *n* is a hexadecimal character.

0x*nnnnnnnn*

- Socket numbers are the basis for an IPX intranode address. They allow a process (for example, RIP or SAP) to distinguish itself to IPX. To be able to communicate on the network, the process must request a socket number. Any packets IPX receives addressed to that socket are then passed on to the process within the node. Therefore, socket numbers provide a fast method of routing packets within a node.

The remainder of this chapter describes the lower-layer, network-layer, and higher-layer internetworking services supported by the Wellfleet router running IPX.

Lower-Layer Services

Table 1-1 shows the types of LAN circuits and frame formats supported by the Wellfleet router running IPX. Table 1-2 shows the types of WAN circuits, the WAN protocols, and the frame formats supported by the Wellfleet router running IPX. You can choose a combination of physical circuits and data link layer frame formats that are appropriate for the types of clients and applications on your network.

Refer to Chapter 2 in *Configuring Wellfleet Routers* for instructions on

- Configuring a physical LAN or WAN circuit (see “Configuring the Circuit”)
- Enabling a WAN protocol (see the appropriate section)
- Selecting the appropriate frame format (see “Enabling IPX Services”)

Table 1-1. LAN Circuit and Frame Support for IPX Interfaces

Circuit Type	Frame Type – Novell Terminology	Frame Type – Wellfleet Terminology
Ethernet attachment unit interface (AUI)	ETHERNET_II	ETHERNET
	ETHERNET_802.2	LSAP
	ETHERNET_802.3	NOVELL
	ETHERNET_SNAP	SNAP
Token Ring medium interface connector (MIC)	TOKEN-RING	LSAP
	TOKEN-RING_SNAP	SNAP
Fiber Distributed Data Interface (FDDI)	N/A	LSAP
		SNAP

Table 1-2. WAN Circuit and Frame Support for IPX Interfaces

Circuit Type	WAN Protocol	Frame Type – Wellfleet Terminology
Synchronous – V.35 – RS-232/V.24 – RS-422/423 – X.21 – T1 – E1	ATM	SNAP
	Frame Relay	SNAP
	PPP	PPP
	SMDS	SNAP
	X.25 Point-to-Point	ETHERNET
	Wellfleet Point-to-Point	ETHERNET
High-Speed Synchronous Interface (HSSI)	ATM	SNAP
	Frame Relay	SNAP
	PPP	PPP
	SMDS	SNAP
	Wellfleet Point-to-Point	ETHERNET

Network-Layer Services

A Wellfleet router running IPX provides the following network-layer support:

❐ Dynamic routing of IPX packets

❐ Multiple IPX interfaces per circuit

❐ Static route support

❐ Adjacent host support

- IPX over WAN media
- IPXWAN and IPXCP

Dynamic routing occurs normally on any IPX interface; brief descriptions of the other support capabilities follow.

Multiple IPX Interfaces per Circuit

You can use the multiple host addressing feature of IPX to configure one or more IPX interfaces per physical circuit. The number of IPX logical interfaces you can configure on a circuit is equal to the number of unique frame formats available for that circuit type. (See Table 1-1 or Table 1-2 for details on circuit types and frame formats.)

For example, you can configure up to four IPX interfaces on a single Ethernet attachment unit interface (AUI) circuit, because the Wellfleet router supports four unique frame formats that are suitable for communication over an Ethernet LAN segment. To differentiate between IPX interfaces configured on the same physical circuit, the Wellfleet router uses the unique network address and frame format you assign to each interface.

By supporting multiple IPX interfaces on a single physical circuit, a Wellfleet router can service clients on independent *logical* LANs that coexist on the same *physical* LAN segment.

In Figure 1-1, each client on the right side of the router has a different logical network address and uses a different encapsulation method. If all clients need to access Server 1, then only Interface 1 of the router needs to support all the different encapsulation methods and multiple logical network addresses for the workstations. Interface 2 of the router needs to support only the SNAP encapsulation method supported by Server 1.

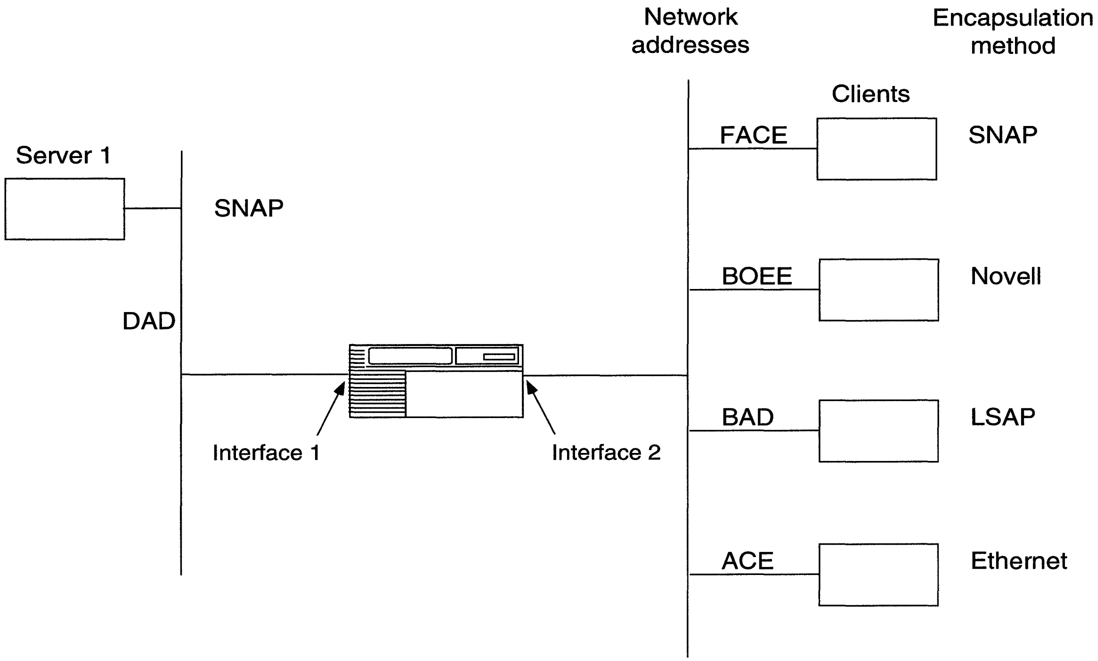


Figure 1-1. Multiple IPX Interfaces per Physical Circuit

The multiple host addressing feature also enables you to configure multiple circuits for each locally attached segment. More information on these topics follows in Chapters 2 and 3.

Note: *NetWare Users:* If you are upgrading client and server stations on your network to Novell NetWare Version 4.*x*, you can use the multiple-interface-per-circuit capability to gradually migrate stations on the same network segment to NetWare Version 4.*x* (that is, from one logical network to another, independent logical network). For example, you can upgrade and migrate NetWare clients from a logical network that supports only Novell encapsulated frames to a logical network that supports a more versatile LSAP (802.2/802.3) frame type.

Static Route Support

A static route specifies a transmission path to another network. Static routes specify the next hop in the transmission path a datagram must follow, based on the datagram's destination address. You configure a static route when you want to restrict the paths that packets can follow or you want to provide more security on your network.

A Wellfleet router running IPX allows you to configure static routes on each logical IPX interface.

Static route support for IPX allows you to

- Direct all IPX traffic destined for a given network to an adjacent host. See the following section for more information about adjacent hosts.
- Reduce routing traffic by disabling the Routing Information Protocol (RIP) supply function on all or on a subset of attached interfaces that are configured with static routes.
- Provide security by eliminating all dynamic routing capabilities and all RIP supply and listen activities over an IPX interface.

You should configure static routes and disable IPX RIP and SAP advertisements when implementing the dial-on-demand feature over a wide area link. IPX RIP and SAP advertisements force dial-on-demand connections to be continuously established, which prevents user-defined dial-on-demand expiration time limits from being reached.

Unlike routes learned through RIP, static routes remain in the route tables until you delete them.

If you have the RIP listen and supply functions enabled, the router may learn a better path, based on either the number of router hops or RIP timer ticks. If this is the case, the router will use the better path, not the static route you have configured.

If you do not have the RIP functions enabled, the local network will not learn about new routes entering the network, route changes, or deleted routes exiting the network.

Figure 1-2 shows the use of a static route in a Frame Relay network.

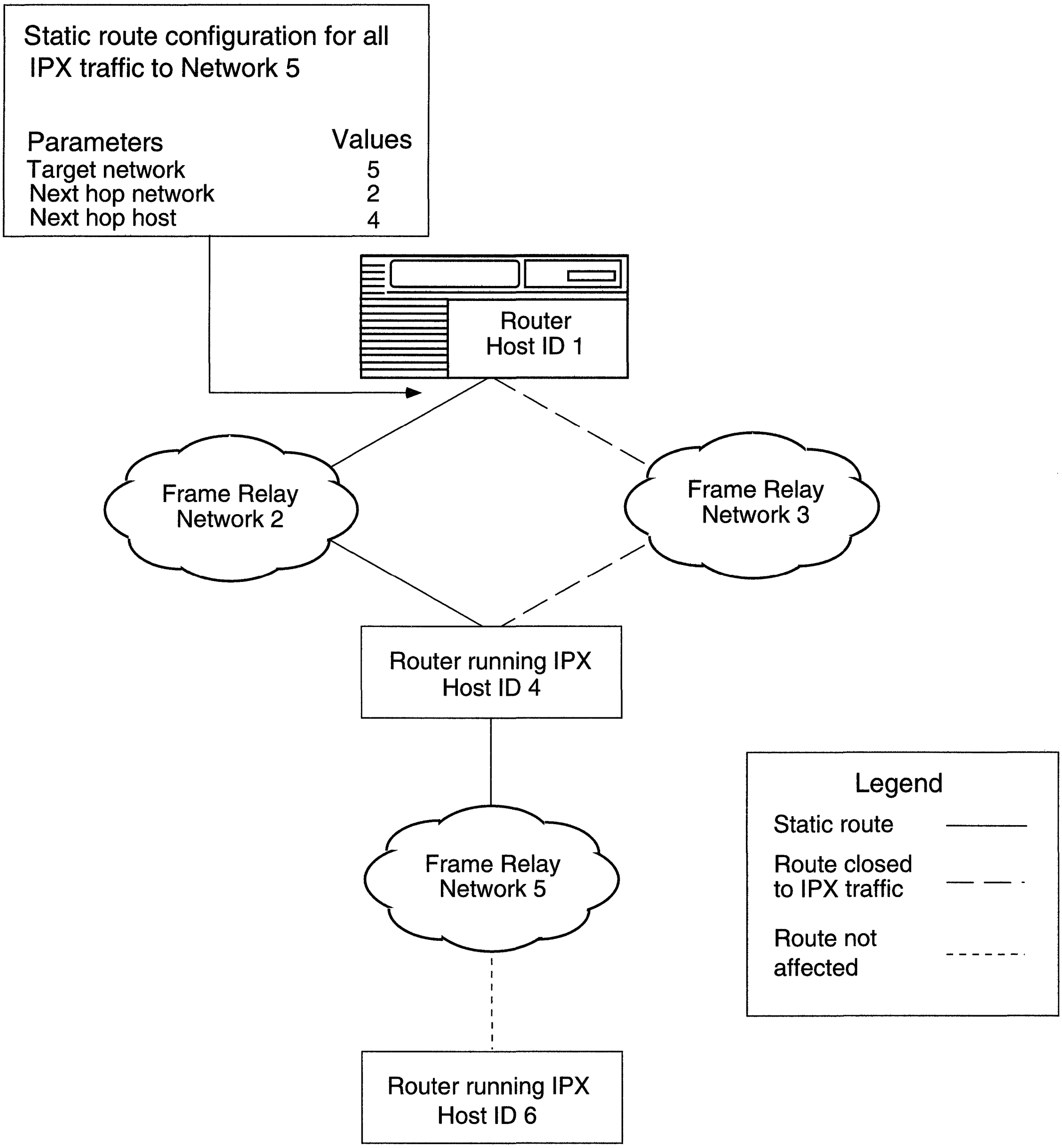


Figure 1-2. Static Route in a Frame Relay Network

In a Frame Relay, Asynchronous Transfer Mode (ATM), or Switched Multimegabit Data Services (SMDS) network, you must establish a data link layer connection for the router to send packets over a static route. To do this, you must configure an adjacent host (see "Adjacent Host Support"), then edit the Data Link Connection Identifier (DLCI) parameter in the IPX Adjacent Hosts window. Refer to "Editing Adjacent Host Parameters" in Chapter 3 for detailed instructions and parameter definitions.

Adjacent Host Support

Under normal IPX operation, routers connected to Frame Relay, SMDS, or ATM networks learn DLCI (Frame Relay and ATM) and SMDS address information from IPX RIP packets. This information is used to build DLCI or SMDS address-to-IPX address mappings. However, IPX RIP overhead may cause excessive congestion over these networks. Adjacent hosts eliminate the need for periodic RIP advertisements by supporting the static configuration of DLCI or SMDS address-to-IPX mappings.

An adjacent host is a network device that is local to a directly connected network. An adjacent host may or may not be a router.

A Wellfleet router running IPX allows you to configure a static route to an adjacent host. You can then disable RIP, which reduces the amount of RIP overhead on your network and increases the amount of bandwidth available for user data. A static transmission path to an adjacent host establishes the data link connection necessary for packet transmission along a static route in a Frame Relay, SMDS, or ATM network when RIP is not enabled.

Note: IPX adjacent hosts should only be configured when you are running IPX over Frame Relay, ATM, or SMDS and you do not have RIP configured on the IPX interface.

Adjacent hosts allow you to reduce the manual configuration requirements associated with static routing. For example, to transport

IPX packets between Network 1 and Network 2, you can configure a static route between Host 1 on Network 1 and Host 2 on Network 2, and configure Host 2 as an adjacent host. When Host 2 receives an IPX packet, it consults its RIP table and dynamically routes the packet to its destination on Network 2.

If you did not have an adjacent host on the end of your static route, you would have to configure a separate static route to each device on Network 2 that you wanted to receive packets.

When you set up an adjacent host, you must configure the adjacent host's network address and host ID, the network address of the next-hop interface, and a DLCI. You use the DLCI parameter to identify a virtual circuit when you configure a static adjacent host in a Frame Relay, ATM, or SMDS network. You display this parameter from the Adjacent Host Configuration window in Site Manager. (Refer to Chapter 3 for more information on how to access adjacent host parameters.)

In Figure 1-3, Host 4 is configured as a statically adjacent host to the IPX interface on Wellfleet router Host 1. This provides a data link connection for static routing between Host 1 and Network 5.

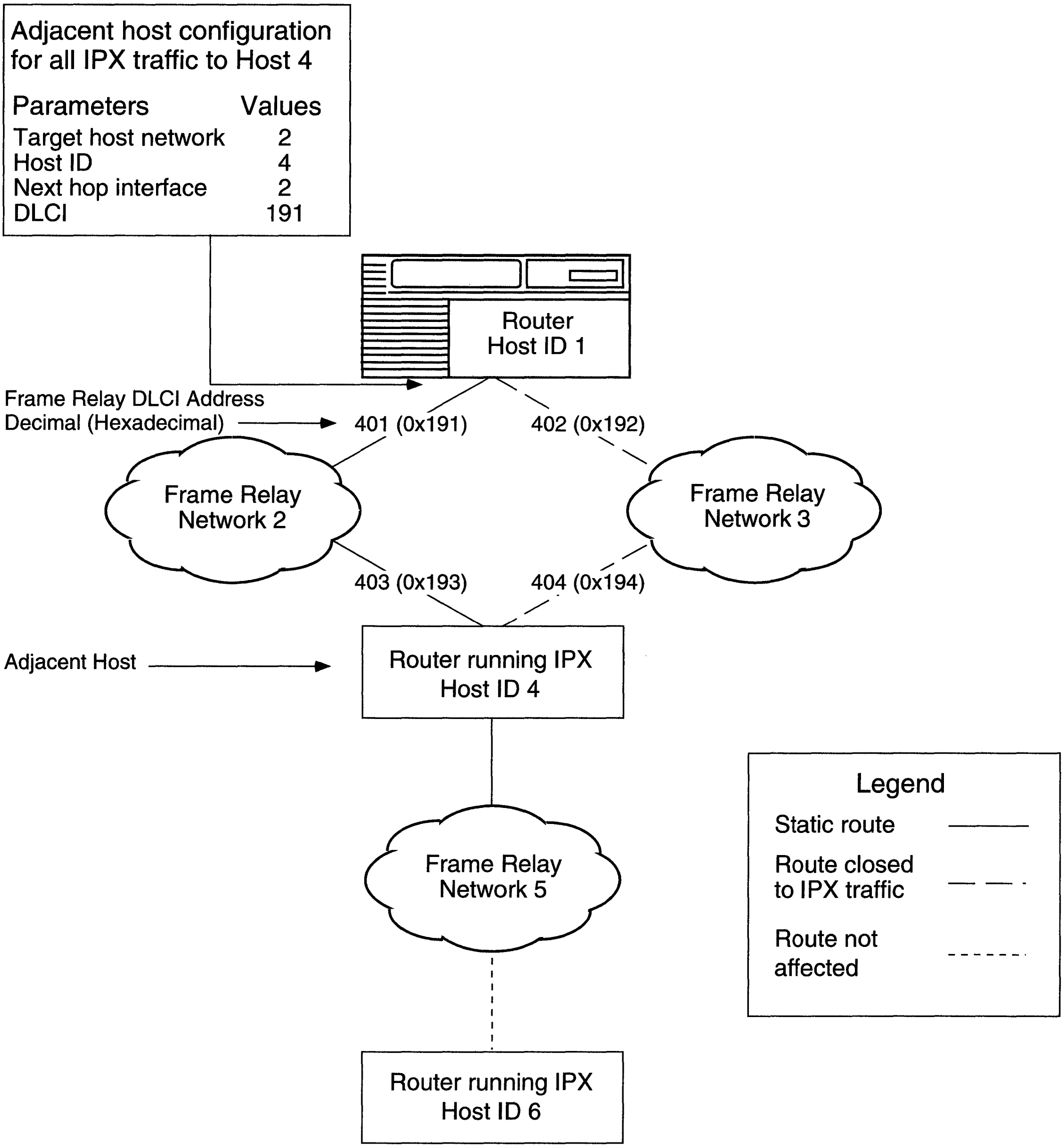


Figure 1-3. Static Adjacent Host in a Frame Relay Network

IPX over WAN Media

You can implement an IPX connection over any of these types of WAN media:

- ❐ Dial circuit
- ❐ Leased-line circuit
- ❐ T1/E1 circuit

The Wellfleet router software allows you to configure the IPXCP protocol and the IPXWAN protocol over point-to-point WAN interfaces. The following sections describe these protocols.

IPXCP

IPXCP (RFC 1552) supports the routing of IPX packets over wide area links that only support the Point-to-Point Protocol (PPP). It is a data link protocol running on top of PPP.

To enable IPXCP, you must first configure the interface to support PPP. Within the PPP Interface Lists window, you enable IPX support for this interface and enter a unique IPX network address. You do not need to enter an IPX remote node number for router to router connections. For instructions on performing these tasks, refer to *Customizing PPP Services*.

IPXWAN

The Bay Networks implementation of IPXWAN (RFC 1362) supports IPX using PPP or Frame Relay frame encapsulation over a wide-area, point-to-point connection. IPXWAN is more versatile than IPXCP because of the various wide area links it supports and its ability to calculate ticks over a WAN link. IPXWAN is a network layer protocol. For instructions on enabling IPXWAN for an IPX interface, refer to Chapter 2 in *Configuring Wellfleet Routers*.

Using IPXCP and IPXWAN

Incorporating IPXCP and IPXWAN in the Wellfleet router provides the following benefits:

- Adherence to RFC 1362 IPXWAN protocol developed by Novell
- A common link negotiation method for WAN media (Frame Relay, PPP, and Wellfleet Point-to-Point)
- Interoperability with other routing vendors (for example, Novell)
- A standardized means for tick-based routing over WAN media

Because both protocols support a PPP data link layer, a Wellfleet IPX router can initialize either type of interface on a PPP circuit. If a local and a remote node are each configured to support both IPXCP and IPXWAN, the routers determine whether to run IPXWAN or IPXCP during WAN link negotiation. IPXCP attempts to establish the link first. If it fails, IPXWAN negotiates the connection.

If you configure IPXWAN interfaces to run point-to-point between two Wellfleet nodes (both using the same encapsulation type), both routers initialize IPXWAN interfaces if they can negotiate the link configuration options required at each end satisfactorily.

If the local and remote nodes fail to negotiate interface configuration options satisfactorily, the IPX router retries the negotiation. You can configure the number and duration of retries with the IPXWAN Link Retry and IPXWAN Time Out parameters. See "Editing IPX Interface Parameters" in Chapter 3 for instructions.

If the wide area link loses connectivity, the IPX router immediately removes from its forwarding tables any information learned while opening that connection.

IPX Network Numbers

The range of valid network numbers is 0x00000000 to 0xFFFFFFFE. You reserve the 0x00000000 value for IPX interfaces configured with an IPXWAN or PPP/IPXCP lower layer for link negotiation. The router recognizes a network number of 0 on an interface as an indication that a lower protocol layer (IPXWAN or IPXCP) on the same circuit must negotiate with the remote IPX host for the network number of the intervening WAN segment.

The next two sections apply only to IPXWAN interfaces.

Primary Network Number

Like Novell routers and servers, a Wellfleet router running IPX implements a global "internal network," to which you must assign a network number called the Primary Network Number (PNN). The Wellfleet router running IPX applies the PNN to all slots configured with IPXWAN interfaces. Only IPXWAN interfaces require the PNN to determine whether the local or the remote interface in a wide area data link must serve as the primary or secondary link. (The router with the higher PNN serves as the primary link.)

You enter the Primary Network Number in the IPX Global Parameters window of the Wellfleet Configuration Manager tool. (Refer to Chapter 3 for more information on how to access the IPX Global Parameters window.)

Common Network Number

You specify a Common Network Number (CNN) that the local interface can assign to the locally attached IPXWAN link. To assign its CNN, the local IPXWAN link must serve as a primary in a WAN link. To specify a CNN, use the IPXWAN Common Network Net parameter in the IPX Interfaces window. Refer to Chapter 3 for more information on how to access this window.

All values between 1 and FFFFFFFE (hex) are valid CNN values. Never use the CNN values 0 and FFFFFFFF (hex); these values are reserved.

Sample IPXCP and IPXWAN Configurations

Figure 1-4 shows a local router communicating with a remote router using IPXCP over PPP, and the same local router communicating with a remote router using IPXWAN over Frame Relay.

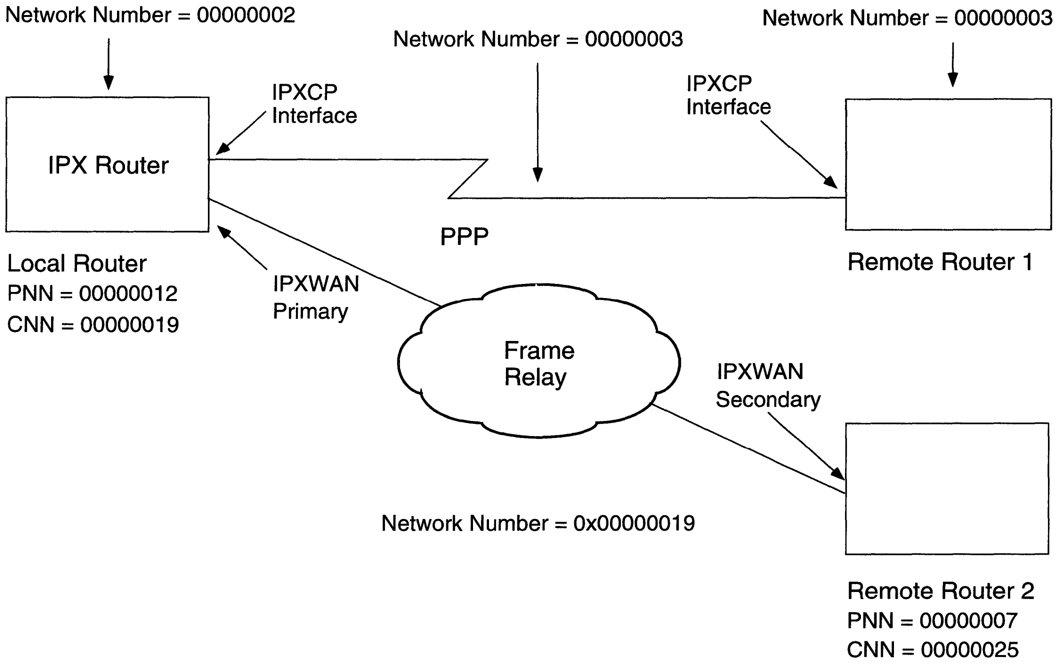


Figure 1-4. IPXCP and IPXWAN Configurations

IPXCP Link Negotiation

The local router and Remote Router 1, both configured for IPXCP, negotiate a connection at the data link layer. Once the options are successfully negotiated, the IPXCP interfaces in both the local router and remote router 1 must agree on a unique network number. (When you initially configure an IPXCP interface, you assign an IPX network number to that interface. The routers select the higher of the two IPX network numbers. See *Customizing PPP Services* for instructions on configuring the IPX network number for an IPXCP interface.)

Note: For PPP communication between a Wellfleet Version 7 or 8 IPX router and a Wellfleet Version 5 IPX router (or any other vendor's IPX router that does not support IPXCP negotiations), you must statically configure the network number of the IPX interface on both routers.

IPXWAN Link Negotiation

The local router and Remote Router 2 are both configured for IPXWAN. When you initially configure an IPXWAN interface, you assign a PNN to that interface. The interface with the highest PNN becomes the link master. In Figure 1-4, the IPXWAN interface on the local router is the link master and the IPXWAN interface on remote router 2 is the link slave. The IPXWAN interfaces in both routers negotiate their link options. If successful, the CNN configured for the link master becomes the IPX network number for the segment.

IPXWAN and IPXCP Link Negotiations

Table 1-3 shows the various WAN protocol configurations likely to exist within local and remote IPX router interfaces. Go to the configuration that applies to you, as indicated in the table.

Table 1-3. Configuration Table for IPX over WAN Media

Local IPX Interface	Remote IPX Interface			
	IPXWAN with IPXCP	IPXWAN but not IPXCP	PPP with IPXCP; no IPXWAN	PPP without IPXCP; no IPXWAN
IPXWAN with IPXCP	Go to Configuration 1	Go to Configuration 2	Go to Configuration 3	Go to Configuration 4*
IPXWAN but not IPXCP	Go to Configuration 2	Go to Configuration 2	Go to Configuration 4	Go to Configuration 4
PPP with IPXCP; no IPXWAN	Go to Configuration 3	Go to Configuration 4	Go to Configuration 3	Go to Configuration 4
PPP without IPXCP; no IPXWAN	Go to Configuration 4 *	Go to Configuration 4	Go to Configuration 4	Go to Configuration 4

*Wellfleet 8.10 to Wellfleet Series 5*x* IPX router compatibility.

Configuration 1

In this configuration, IPXWAN defers to IPXCP for link negotiation.

- If IPXCP successfully negotiates an IPX network number for the link, IPXWAN does not run, and the IPX interface becomes active on the link.
- If IPXCP fails to negotiate an IPX network number for the link, IPXWAN begins link negotiation.
- If IPXWAN negotiates successfully, the IPX interface becomes active. If IPXWAN negotiation fails, the IPX interface cannot become active.

Configuration Guidelines

- IPXCP – Use a nonzero value for the IPX network number when configuring the local or remote Point-to-Point Protocol interface.

- IPXWAN – Use a unique router name and Primary Network Number (PNN) in the IPX Global Parameters window when configuring each local and remote router.

  You must also configure the IPX network number of the local and remote IPX interfaces to a value of 0 (zero). (The router recognizes an IPX network number of 0 on an interface as an indication that a lower protocol layer — IPXWAN or IPXCP — on the same circuit must negotiate with the remote IPX host for the IPX network number of the intervening WAN segment.)

  Finally, you must enter a unique Common Network Number (CNN) for the IPX interface you configured.

Configuration 2

In this configuration, IPXWAN exclusively negotiates an IPX network number for the link.

- If IPXWAN negotiates successfully, the IPX interface becomes active.
- If IPXWAN negotiation fails, the IPX interface cannot become active.

Configuration Guidelines

- IPXCP – No configuration requirements.
- IPXWAN – Use a unique router name and Primary Network Number (PNN) in the IPX Global Parameters window when configuring each local and remote router.

  You must also configure the IPX network number of the local and remote IPX interfaces to a value of 0 (zero). (The router recognizes an IPX network number of 0 on an interface as an indication that a lower protocol layer — IPXWAN or IPXCP — on the same circuit must negotiate with the remote IPX host for the IPX Network Number of the intervening WAN segment.)

  Finally, you must enter a unique CNN for the IPX interface you just configured.

Configuration 3

In this configuration, IPXCP exclusively negotiates an IPX network number for the link.

- If IPXCP successfully negotiates the number, the IPX interface becomes active on the link.
- If IPXCP fails to negotiate the number, the IPX interface cannot become active.

Configuration Guidelines

- IPXCP – Use a nonzero value for the IPX network number when configuring the local or remote PPP interface.
- IPXWAN – No configuration requirements.

Configuration 4

In this configuration, the lower layer has no means of negotiating an IPX network number for the link. For this reason, you must manually configure the network number of the local and remote IPX interfaces to the same nonzero value.

Upper-Layer Services

The router encapsulates, within the data field of an IPX packet, any packets associated with Novell's upper-layer protocols. The structure of a packet, as well as the source and destination socket numbers contained in that packet, identify the protocol type associated with that packet (for example, Routing Information Protocol [RIP] or Service Advertising Protocol [SAP]). The upper-layer services are

- The Novell Service Advertising Protocol (SAP), which provides a means for servers to advertise their services to routers and other servers.
- The Novell implementation of the Routing Information Protocol (RIP), which provides workstations and routers with a means for exchanging information dynamically. This information enables

routers in the network to establish a best or minimum-delay route to each destination network.

Wellfleet router software enables you to select the basis on which an IPX router makes its routing decisions (on the number of *ticks* or on the number of *hops* required to reach a given destination network). Wellfleet IPX routing software also supports multipath routing and loadsharing over LAN and WAN media.

- Split Horizon capability.
- NetBIOS (Network Basic Input-Output System) all-networks-broadcast packets (Type 20 packets).
- Source routing and endstation support.
- IPX ping capability.

The following sections describe how Bay Networks supports these services.

Service Advertising Protocol (SAP)

SAP enables NetWare network services to inform clients of their presence. NetWare services use the SAP identification broadcasting services to tell clients their name, type, and IPX address. The IPX address in a broadcast identifies a server's location in terms of network, host, and socket.

Novell IPX routers maintain a database called a *bindery.* The bindery includes information such as type, IPX address, hop count, the interface to the server, a timer value to table entries, and a list of clients. If an entry in a bindery reaches its configured maximum age without being refreshed (timer resets to 0), the router deletes the entry from that bindery.

Wellfleet routers implement a similar structure (a global services table). Each time an IPX router receives a SAP packet, it compares the packet's contents to the contents of its SAP services table. If the SAP services table already contains information about a specific service, the router simply refreshes the age timer for that entry. If the SAP services table does *not* contain information about the service, and the routing table has no information on routes associated with the service, the router adds a new entry to the services table and advertises the new service to all connected networks.

Clients use SAP to request information about network services. Client information requests are nearest-service queries, which seek information on the closest service of a specified type.

Every IPX server and IPX router on the internetwork learns about all other IPX servers and services through the propagation of bindery information or services table information.

Each SAP packet contains 7 Service Advertising updates.

For a complete list of all known service types, see Table 3-1 in Chapter 3 of this manual.

NetWare Directory Services (NDS) and SAP

NDS is a globally distributed network database that replaces the bindery used in NetWare versions earlier than 4.0. Workstations locate services by querying an NDS server. The NDS server distributes the service information using direct unicast-based protocols instead of using broadcast-based SAP. Therefore, the use of SAP in an NDS network is greatly reduced. SAP is still used to locate the nearest NDS server at startup.

SAP Filters

You may want to create SAP filters on Wellfleet routers in your network, to control the size of resident SAP services tables and reduce bandwidth waste on your network due to SAP broadcast overhead. You may also want to create SAP filters to limit a user's view of services located elsewhere on the network.

The SAP filter mechanism determines whether the IPX router advertises a particular service in its SAP broadcasts or responds to client requests. SAP filters are *outbound* filters; that is, they affect only outgoing SAP advertisements. The effect is either to prevent the router from advertising service information or allow the router to advertise service information.

The IPX router does, however, update its own SAP services table according to *inbound* SAP data, regardless of the status of its SAP filters.

You can configure SAP filters using the following levels:

- You can filter SAP service information pertaining to individual servers by editing server-level SAP filters.

  At the service level, the filter matches a pattern (consisting of a target server name and a server type) in the SAP services table. The filter's Action parameter determines the action (advertise or suppress).

- You can filter service information pertaining to entire networks by editing network-level SAP filters.

  At the network level, the filter matches a pattern (consisting of a target network number and a server type) in the SAP services table. The filter's Action parameter determines the action (advertise or suppress).

Each interface supports up to 150 server-level and 50 network-level SAP filters, for a total of up to 200 filters.

The IPX router includes information about a service in a SAP packet if either of the following is true:

- The router finds a match between a filter's contents and the contents of its SAP services table and the filter action is Advertise.
- The router does not find a filter that matches the contents of its SAP services table.

The IPX router excludes information about a service from a SAP packet only if it finds a match between a filter's contents and the contents of its SAP services table and the filter action is Suppress.

You can use wildcards to advertise or suppress all service types, all service types in a specified network, or a specific service type in all networks.

The IPX router compares SAP filters to each pattern in the following order of precedence:

1. Server-level filters with specific service types
2. Server-level filters with wildcard service types configured as FFFF (hexadecimal)
3. Network-level filters with specific service types and specific network numbers
4. Network-level filters with wildcard service types and specific network numbers
5. Network-level filters with wildcard network numbers (FFFFFFFF hexadecimal)

Also, the order of precedence allows you to use wildcards to advertise or suppress all service types except those you configure to do the opposite.

For example, you may want to advertise from an IPX interface only one type of service (Type 4) belonging to a particular server (Server 1). You can configure

1. A server-level SAP filter with a target server name of Server 1, a service type of 4, and an action to advertise.
2. A network-level SAP filter with a target network of 0xFFFFFFFF, a type of 0xFFFF, and an action to suppress. (This network-level filter prevents all other services from being advertised from the interface.)

According to SAP filter precedence rules, the server-level filter takes precedence over the network-level filter.

Note: The order in which you create SAP filters does not affect filter precedence.

Using SAP Filters

The following example describes a situation in which you might want to configure SAP filters. An office complex contains three buildings. The staff in each building only use the print services within their own building and have no need to send files to printers outside their building. To free up wasted bandwidth, a SAP filter that suppresses print server advertisements should be configured on the interfaces of the routers that connect the three buildings.

To suppress print server advertisements, configure a network-level filter on the interfaces of the routers that connect the three buildings and suppress the advertisement of Server Type 0x0047 for all networks (0xFFFFFFFF). You use a network-level filter because it allows you to specify a server type or network number.

Static Services

When you statically configure NetWare services, the router learns about a NetWare service by means of the SAP information you enter using Site Manager. You can manually configure static services for each interface.

When you configure static services on an interface, you can then use SAP filters to eliminate the SAP announcements. This reduces traffic and bandwidth use on the WAN.

For network topologies that include slower-speed WAN links, reducing the amount of WAN bandwidth otherwise needed for SAP announcements can be helpful. You can also reduce traffic by setting the WAN SAP Period parameter to zero, which indicates no periodic SAP updates and no aging of SAP information resulting from periodic updates. SAP immediate updates still propagate through the network. A service sends an immediate update under one of the following three conditions: a service first comes up, a service changes, or a service is no longer available. For more information about the WAN SAP Period parameter, see "Configuring RIP and SAP Broadcast Timers," later in this chapter. For instructions on setting the WAN SAP Period parameter, see "IPX Interface Parameter Descriptions" in Chapter 3.

Figure 1-5 shows a sample network configured to use static SAP services. If you want Client 1 to have access only to File Server 3, you configure File Server 3 in the static SAP table on Router 2's interface. Then, to suppress any SAP broadcasts from Router 1 and thus reduce bandwidth use, you configure a SAP network-level filter with all Fs (hex) on Router 1's interface and set the action of the filter to Suppress.

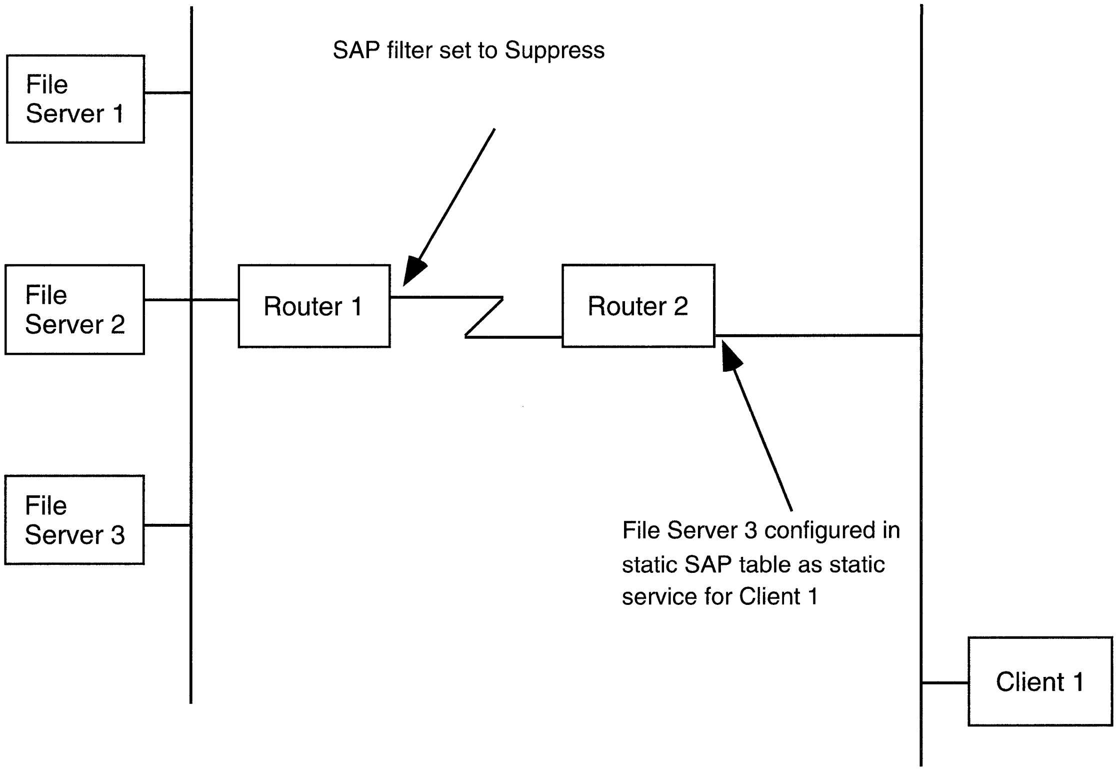

SAP filter set to Suppress
File Server 1
File Server 2
File Server 3
Router 1
Router 2
File Server 3 configured in static SAP table as static service for Client 1
Client 1

Figure 1-5. Static SAP Service Network Configuration

You add, edit, or delete static services through the IPX Static Services window. For instructions, see "Editing Static Service Parameters" in Chapter 3. You can configure only services that have valid network addresses. Valid network addresses are provided either by RIP or by statically configured routes. If you try to enter any services that have illegal network addresses in the router configuration, the router accepts the information but the services are unreachable.

Routing Information Protocol (RIP)

The Routing Information Protocol (RIP) enables workstations and routers to exchange route information and to establish the route to each network with the fewest hops and shortest delay.

Each IPX router maintains a route table. The route table contains the following information about every network in the IPX network topology:

- The network address.
- The number of ticks (units of delay time) to that network. (A tick is equal to about 1/18th of a second. The number of ticks to a network is the tick cost for that route. More information on this topic follows in the section, "Routing Methods," and in Chapter 3.)
- The number of hops to that network.
- The address of the next-hop node to which the local router forwards packets on their way to another destination network.

Routers maintain route tables by exchanging RIP request and response packets. A RIP request packet specifies the destination network. It can be

- A general request broadcast by a router to retrieve the fastest route to all known networks on an internetwork. The value FFFFFFFF in the network address field indicates that the packet is a general request.
- A specific request broadcast by a workstation or router to determine the fastest route to a particular network. One or more network addresses (excluding an address of all Fs) in the network address field indicates that the packet is a specific request.

Routers at the destination network issue RIP response packets. RIP response packets contain the network number and the number of hops and ticks required to get to the network. A RIP response can be one of the following types:

- A response to a request.

- An informational broadcast from a router issued at regular intervals (every 60 seconds).
- An informational broadcast when a change occurs in the routing table. Examples of changes in the routing table are tick or hop changes, timing out of routes, and the addition of routes to networks to the table.
- An informational broadcast when an interface initializes or performs an orderly shutdown procedure.

Each RIP packet contains 50 route updates.

To reduce traffic, RIP broadcasts are limited to a router's immediate segments and are not forwarded by receiving routers.

Note: The IPX router learns WAN addresses from RIP and SAP broadcasts received over WANs (Frame Relay, SMDS, ATM). The router stores IPX address/WAN address pairs for future use as next-hop destinations.

If RIP is not configured for a WAN interface, you must configure adjacent hosts for all transmission paths to nodes adjacent to Frame Relay, ATM, or SMDS circuits when you configure an IPX interface. You must then configure static routes that use the adjacent hosts to reach next-hop routers.

The IPX router allows you to enable the RIP listen and supply functions for each IPX interface. When you enable the listen function, the IPX router learns routes received in RIP updates from neighboring routers. When you enable the supply function, the IPX router transmits RIP periodic updates to routers in adjacent networks.

Caution: If you modify one or more RIP parameters for an IPXWAN interface or a PPP interface with an IPX network number of 0, the changes are made for all IPXWAN interfaces or PPP interfaces with IPX network numbers of 0 configured on the router.

Configuring RIP and SAP Broadcast Timers

A Wellfleet router running IPX allows you to control the frequency of RIP and SAP update packet transmissions. RIP and SAP transmissions provide the following benefits:

- You spend less time manually configuring changes to static services and service routes across your network.
- You reduce the cost of administering Wellfleet routers installed across your network compared to the cost of building static routes or static services tables.
- You allow a router to respond to changes in services and routes offered on the network.
- You enable users to have more accurate, up-to-date information on services and service routes offered on the network.

However, periodic RIP and SAP transmissions mean

- Less bandwidth is available for user data. Consequently, user data transmissions take longer, thereby increasing WAN line costs.
- You sacrifice some level of manual control over services and routes made available to network users. Your particular networking environment may require a higher degree of manual control over information on services and service routes offered to users on your network.

You can adjust the frequency of RIP and SAP update packet transmissions by means of the WAN RIP Period and WAN SAP Period parameters on the IPX Interfaces window. See Chapter 3 for instructions on configuring these parameters. The higher the number you enter, the less frequent the transmissions. If you enter 0, no periodic RIP or SAP updates are sent out the IPX interface of the router. However, RIP and SAP immediate (one-time) update packets still propagate through the network (adheres to Novell standards). You can eliminate all SAP broadcasts using SAP filters.

Eliminating periodic RIP and SAP updates provides the following benefits:

- Reduces the amount of RIP and SAP overhead on your network
- Increases the amount of bandwidth available for user data
- Reduces WAN line costs for packet transmission
- Increases manual control over network services and routes

However, no periodic RIP and SAP transmissions mean

- A slower response time of the network to changes in network services and routes.
- An increase in the time and cost of administering changes to services and service routes made available through Wellfleet routers on your network.

RIP and SAP timer settings should be the same on both sides of the WAN.

Routing Methods

To specify a method for making IPX "best-route" decisions for all slots, based on time delays (ticks) incurred or hops encountered for packet delivery, use the RIP Method parameter on the Edit IPX Global Parameters window. See Chapter 3 for instructions on using this parameter. The router can assess the time delay in one of two ways:

- *Number of RIP timer ticks* is the amount of time, expressed in *ticks*, that a packet requires to reach another network segment. (Each RIP timer tick = 1/18th of a second. The maximum configurable number of ticks is 65,534 ticks multiplied by 1/18th second = 3600 sec, or 60 min.)
- *Number of hops* is the number of router hops a packet must traverse to reach a network segment. (The maximum number of hops allowed in an IPX internetwork is 15.)

We recommend using the default (tick-based) method.

Configuring Interface Costs

You can set the cost (number of ticks or hops) for an interface using the Cost parameter on the IPX Interfaces window. The value you enter depends on the option (Metric or Tick) you selected for the RIP Method parameter. For more information about the Cost parameter, see Chapter 3.

The ability to configure an interface cost enables you to select the route you want to use rather than allowing the network to select the route. For example, two routes go to the same destination. Route A has a tick cost of 2; route B has a tick cost of 3. Because route A has the lower tick cost, the network selects it as the "best route" to the destination. If you want traffic to go over route B, you can set the tick cost of route A to 4, which then forces traffic to go over route B.

Multipath and Loadsharing

You can include multiple next-hop destinations as active routes to a destination network. The IPX router can find out about multiple paths by either RIP packets or statically configured routes.

The router can forward packets to the multiple next-hop nodes concurrently by multiplexing frame transmissions over the multiple equal-cost paths in a cyclic sequence. This is commonly referred to as *IPX multipath* or *IPX loadsharing*.

Multipath

Multipath is a "round-robin" or cyclic multiplexing mechanism. The IPX router uses this mechanism to divert individual, consecutive frames destined for the same target network to separate IPX interfaces and their associated physical circuits (see Figure 1-6).

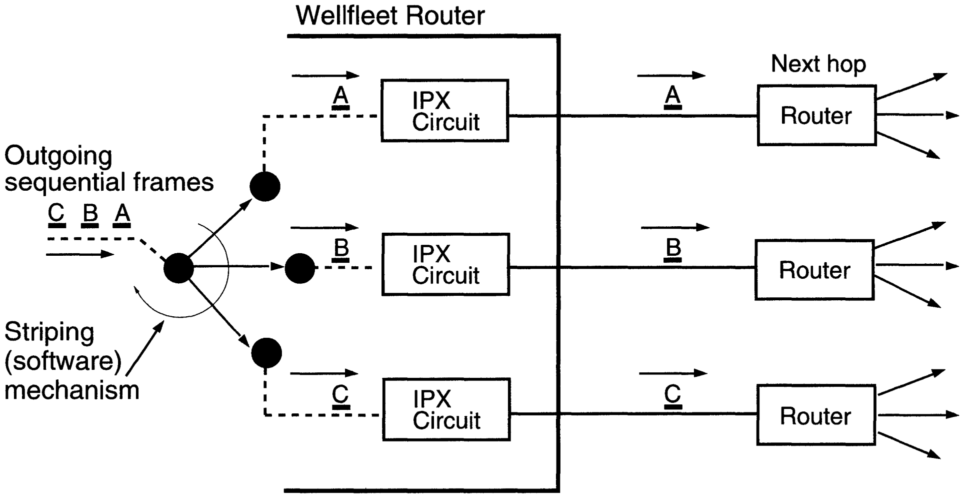


Figure 1-6. IPX Multipath

Because the IPX interfaces have duplex functionality, the router can also use multipath to collect frames received from separate IPX interfaces. The router operates this cyclic mechanism at a bandwidth significantly greater than a single IPX interface and its supporting physical circuit can support. The result is that IPX frames flow over multiple parallel LAN or WAN routes concurrently, in effect aggregating the bandwidth supported by the parallel routes. Each line shares $1/n^{th}$ of the total load (where n = the number of equal-cost parallel routes or paths to the destination network).

You set the maximum number of paths by means of the Maximum Path parameter on the Edit IPX Global Parameters window. See Chapter 3 for instructions on setting this parameter. Any setting greater than 1 engages the multipath mechanism.

Frames that belong to the same data stream may require resequencing at their ultimate destination. To derive maximum benefit from this feature, the source and destination nodes should support burst-mode operation.

Load Redistribution and Rerouting

If the router detects a failure, the multipath allows it to temporarily redistribute the round-robin loading among the remaining active multipath routes.

Multipath Route Precedence/Priority

The multipath mechanism generally uses the best path first. However, when two equal-cost paths exist, multipath uses the following priority scheme for route selection:

- Routes learned via RIP
- Statically configured routes
- Direct routes (paths to other routers on a segment directly attached to the local router)

Multipath Configurations

You can establish equal-cost multipath routes over LAN or WAN segments to support IPX traffic between routers, and between routers and servers. The slower the interconnecting LAN or WAN links, the more difference using multipath will make in client-server throughput.

Configurable Split Horizon

The Split Horizon algorithm is part of the Novell specification for IPX. Its purpose is to prevent circular routes and reduce network traffic. The Bay Networks implementation of Split Horizon excludes RIPs and SAPs learned from a neighbor when forwarding RIP and SAP updates to that neighbor. Split Horizon is enabled by default for each interface.

Caution: We advise you not to disable Split Horizon unless it is absolutely necessary.

In a star or non-fully meshed Frame Relay topology, you may need to disable Split Horizon on certain interfaces for the routers to learn about the other networks.

A fully meshed network is a WAN in which all nodes have a logically direct connection to each other. Figure 1-7 shows a sample fully meshed network with Split Horizon enabled.

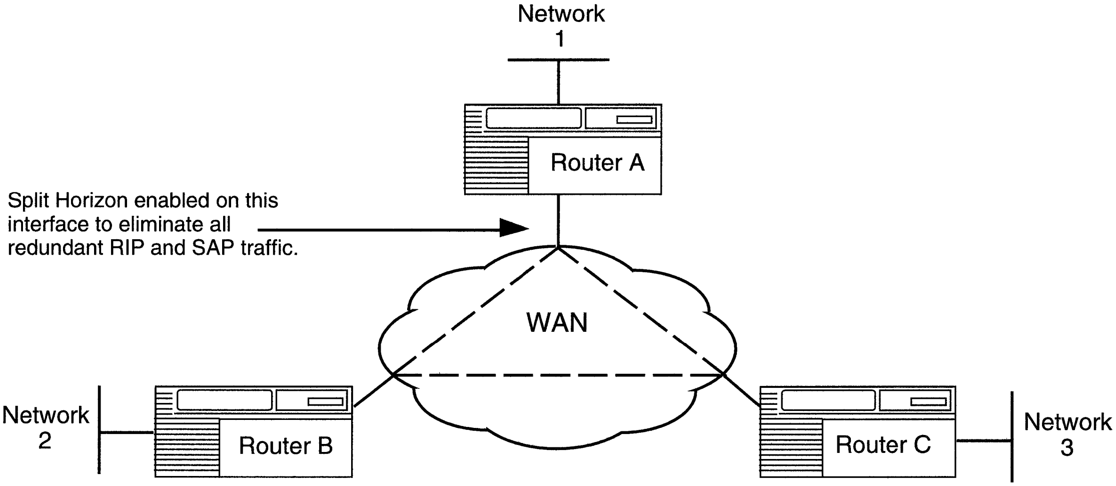

Network 1
Router A
Split Horizon enabled on this interface to eliminate all redundant RIP and SAP traffic.
WAN
Network 2
Router B
Router C
Network 3

Figure 1-7. Split Horizon Enabled in a Fully Meshed Network

A non-fully meshed network is a WAN in which one or more nodes do not have logically direct connections to all other nodes.
Figure 1-8 shows a sample non-fully meshed network with Split Horizon disabled.

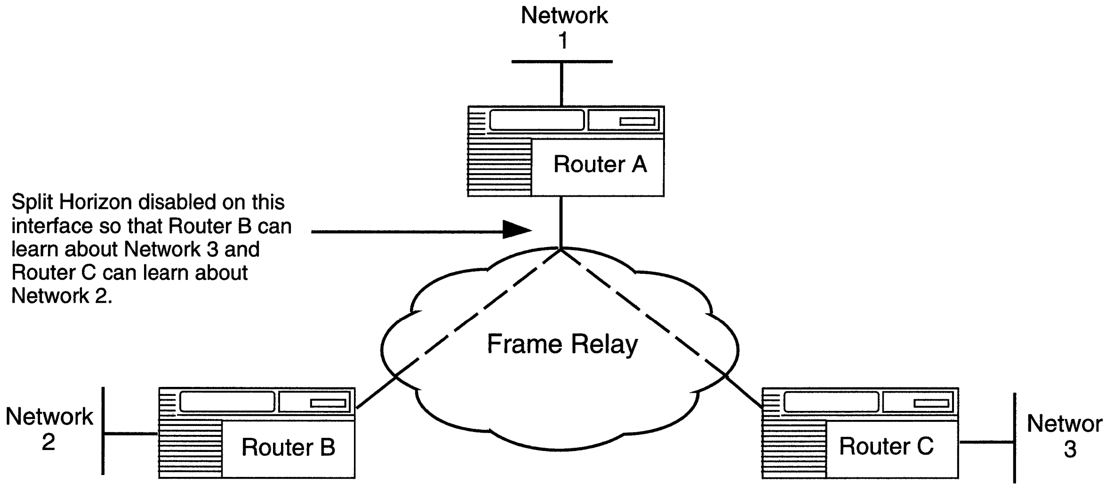

Network
1
Router A
Split Horizon disabled on this interface so that Router B can learn about Network 3 and Router C can learn about Network 2.
Frame Relay
Network
2
Router B
Router C
Network
3

Figure 1-8. Split Horizon Disabled in a Non-Fully Meshed Network

NetBIOS Static Routing

NetBIOS™ establishes sessions (logical connections) and allows for communication between PCs. The Wellfleet NetBIOS static route function allows you to reduce NetBIOS network traffic by configuring a NetBIOS static route to a server name and type. The IPX router then restricts broadcast NetBIOS packets, which are usually forwarded to all network interfaces on a single network.

Each IPX router interface supports up to 50 NetBIOS static routes. Each NetBIOS static route specifies a NetBIOS resource name and a destination network (where the resource resides).

Version 7.80 and greater of the Wellfleet IPX router software allows you to determine if

- You want to direct a NetBIOS broadcast (type 20) packet through a network by configuring a static route at the first router only. Before the packet is directed out an interface, the router software adds the IPX destination address to the packet so that it can be routed to its destination. Because the IPX specification states that the network address of broadcast packets must be left unchanged, this option does not conform to Novell standards.

- You want the router to propagate a packet out all of its interfaces (conforms to Novell standards).
- You want to direct a packet to its destination by configuring a static route for each hop in the network (conforms to Novell standards).

Directing a NetBIOS Packet Using Nonstandard Static Routing

To direct a NetBIOS packet through a network by configuring a NetBIOS static route in the first Wellfleet router to receive a NetBIOS broadcast packet, you must set the Novell Certification Conformance parameter on the Edit IPX Global Parameters window to Disable. You must set this parameter to Disable for all routers in the network. All NetBIOS packets sent from a client to the router must have a destination network value of 0, unless the packet passes a static route in the router. The router tests a packet against the static route table before it checks the packet's destination, thus allowing the router to accept packets that may not have a destination network of zero.

Caution: This method of defining IPX NetBIOS static routes is a nonstandard Wellfleet feature that may not interoperate with routers other than Wellfleet. This method converts a NetBIOS broadcast packet to a NetBIOS directed broadcast packet, thereby eliminating the loop checking and path tracing that is usually done for NetBIOS broadcast packets. This may cause problems with applications that rely on those mechanisms.

You configure a NetBIOS static route to a server name and type. After you specify the server name and type, the IPX router converts standard NetBIOS broadcast packets to NetBIOS directed broadcast packets. NetBIOS broadcast packets are sent to all accessible host IDs on all accessible IPX networks. NetBIOS directed broadcast packets are sent to all host IDs on a single IPX network.

When you configure a NetBIOS static route, the IPX router inserts the target network number in the network number field of each NetBIOS broadcast packet. Refer to Chapter 3 for instructions on how to add a NetBIOS static route to an IPX interface.

When you configure NetBIOS static routes on an interface, the IPX router compares all IPX NetBIOS broadcast packets received on the interface with interface-specific NetBIOS static routes. If the NetBIOS destination name found in the packet matches an entry in the routing table, the NetBIOS packet is routed to the associated destination network. If no match is found, the IPX router treats the packet as specified by the NetBIOS Accept and NetBIOS Deliver parameters. See "NetBIOS Accept and Deliver Parameters," in a later section.

Forwarding Packets Out All Interfaces

To configure a router to propagate a packet out all of its interfaces, which conforms to Novell standards, you set the Novell Certification Conformance parameter on the Edit IPX Global Parameters window to Enable. You must set this parameter to Enable for all routers in the network.

To control the flow of NetBIOS traffic, you can use the NetBIOS Accept and Deliver parameters to determine whether you want an interface to accept NetBIOS broadcasts from an attached network, and to deliver NetBIOS broadcasts to a network. See "NetBIOS Accept and Deliver Parameters," in a later section.

Directing a NetBIOS Packet Using Standard Static Routing

If you want to configure NetBIOS static routes in conformance to Novell standards, you must configure a static route for each hop in the network. Refer to Chapter 3 for instructions on how to add a NetBIOS static route to an IPX interface.

NetBIOS Accept and Deliver Parameters

The NetBIOS Accept and NetBIOS Deliver parameters on the IPX Interfaces window allow you to configure each interface to accept and forward NetBIOS broadcasts. The default setting for both of these parameters is Enabled.

Note: The description that follows assumes that the NetBIOS destination name found in the packet does not match an entry in the NetBIOS Static Routing table.

With Accept enabled on an interface, the IPX router accepts NetBIOS broadcast packets received on that interface. For example, in Figure 1-9 the IPX router accepts only NetBIOS broadcast packets received on Interfaces 1 and 2, because the Accept parameter for those interfaces is set to Enabled.

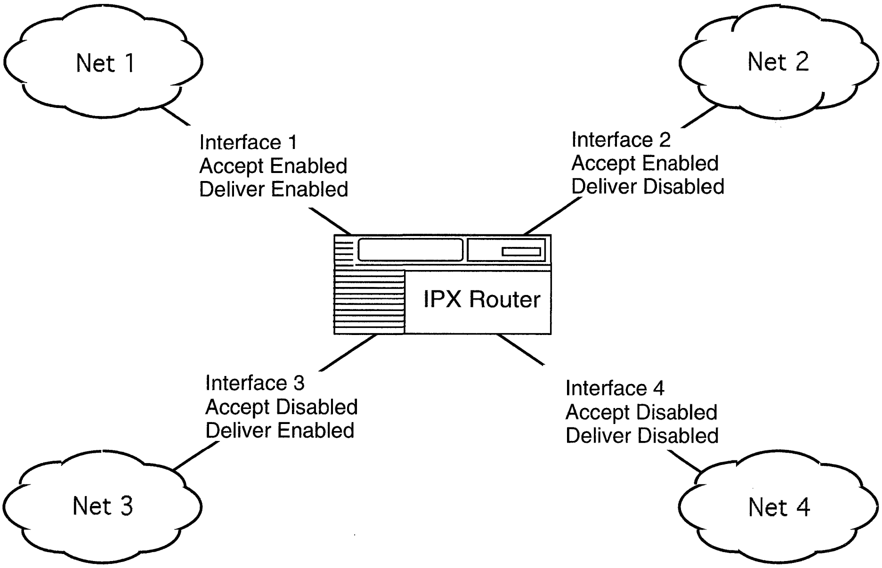


Figure 1-9. NetBIOS Directed Broadcast Packets in a Sample Network

With Deliver enabled on an interface, the IPX router delivers NetBIOS broadcast packets that are routed to that interface. For example, in Figure 1-9 the IPX router delivers only NetBIOS broadcast packets to Interfaces 1 and 3, because the Deliver parameter for those interfaces is set to Enabled.

The Accept parameter of the interface receiving NetBIOS broadcast packets and the Deliver parameter of the other interface must both be set to Enabled for delivery of such packets to occur. For example, Interface 1 can deliver only packets from Interface 2 to Net 1 because Interface 2 is the only other interface whose Accept parameter is set to Enabled.

Thus, NetBIOS client applications on Network 1 can initiate and establish sessions with NetBIOS server applications only on Network 3. NetBIOS client applications on Network 2 can initiate and establish sessions with NetBIOS server applications only on Networks 1 and 3. Client applications on Networks 3 and 4 cannot initiate any sessions with NetBIOS server applications via the IPX router.

Refer to “Editing IPX Interface Parameters” in Chapter 3 for instructions on how to disable the NetBIOS Accept and NetBIOS Deliver parameters.

Source Route Endstation Support

The Wellfleet router running IPX allows you to configure source route endstation support for Token Ring networks on each interface. This allows bridging and routing to coexist in the same IBM source route bridging environment. With endstation support enabled, endstations that support both source route bridging and IPX can use source routing to traverse bridged networks.

In a source routing network, every endstation supplies each frame it sends out with route descriptors, so that it can be source routed across the network. Thus, in order for routers running IPX to route packets across a source routing network, they must act like end stations, supplying route descriptors within each packet before they send it onto the network.

With endstation support enabled, the Wellfleet router running IPX does the following whenever it receives a packet and determines that the packet’s next hop is across a source routing network:

- ❐ Sends out an Explorer frame to discover a path to the next hop network
- ❐ Adds the necessary Routing Information Field (RIF) information to the packet's MAC header
- ❐ Sends the packet to the network, where it is source routed toward the next hop

After the peer router receives the packet from the Token Ring network, it strips off the RIF field and continues to route the packet toward the destination network address (see Figure 1-10).

You configure source route endstation support on each interface by setting the TR End Station parameter to Enable. See the section "Editing IPX Interface Parameters" in Chapter 3 for instructions on enabling this parameter.

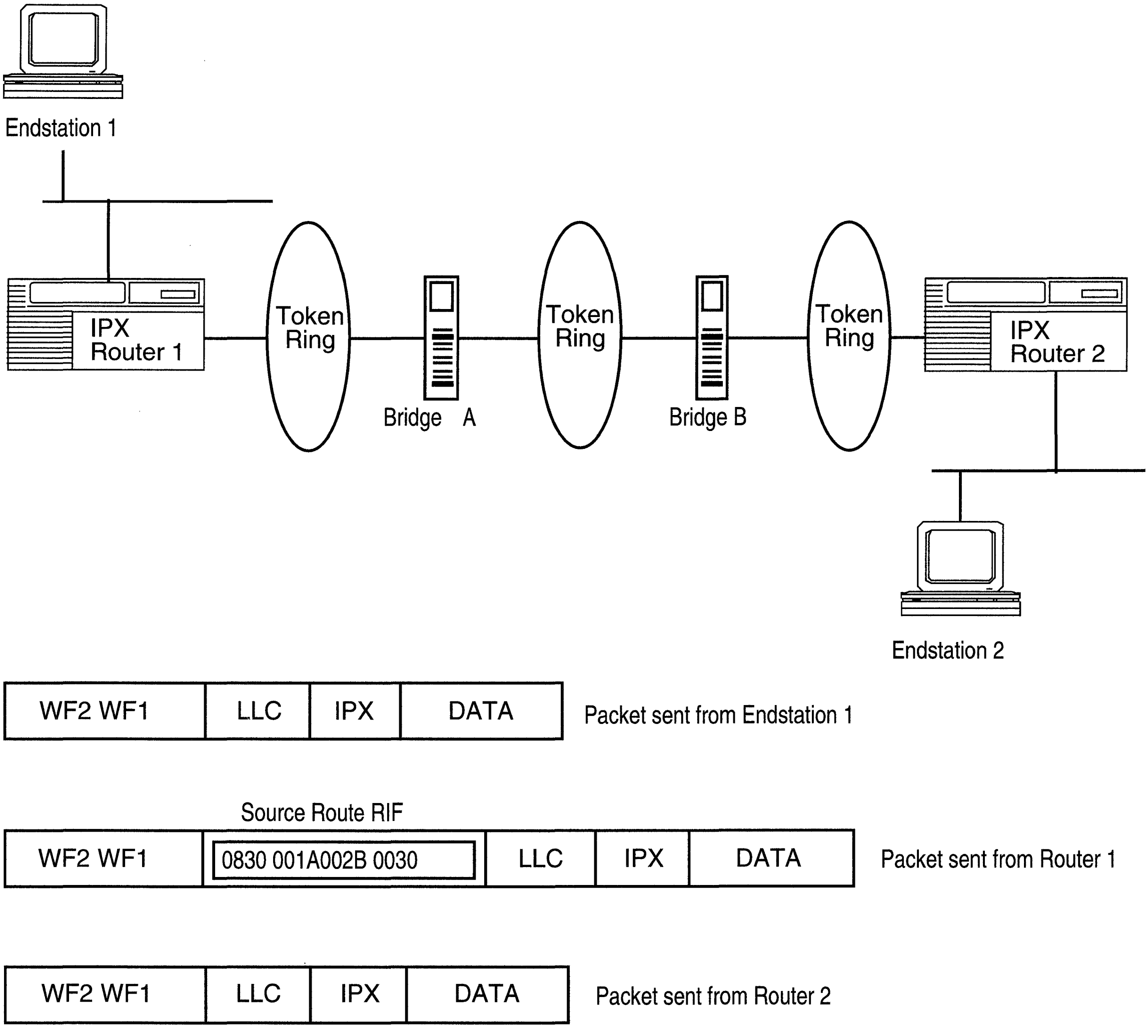

Endstation 1
IPX Router 1
Token Ring
Bridge A
Token Ring
Bridge B
Token Ring
IPX Router 2
Endstation 2
WF2 WF1 | LLC | IPX | DATA
Packet sent from Endstation 1
Source Route RIF
WF2 WF1 | 0830 001A002B 0030 | LLC | IPX | DATA
Packet sent from Router 1
WF2 WF1 | LLC | IPX | DATA
Packet sent from Router 2

Figure 1-10. IPX Routers Source Routing across a Token Ring Network

IPX Ping Support

The Wellfleet Site Manager supports IPX *ping* functionality, which allows you to determine the status not only of another Wellfleet router (alive or not responding), but the status of a Novell IPX server, a Novell multiprotocol router, or a NetWare client.

By means of the IPX **ping** command, the router attempts to communicate with another router running IPX, a server, or an IPX client, and determines whether the destination node is functioning and reachable from the source node. The "pinging" Wellfleet router sends an IPX diagnostic packet, called Configuration Request, and either the "pinged" router running IPX, the server, or the IPX client responds with a Configure Response packet.

You can access the IPX ping capability by choosing the Administration→Ping from Router→IPX menu path from the Wellfleet Site Manager window. Site Manager prompts you to supply the address of the router you want to ping, the length of time you want to ping the router, server, or client, and the number of ping retries at the specified address. See *Managing Wellfleet Routers* for instructions.

Role of the Wellfleet Router in a Client-Server Connection

This section describes how Wellfleet routers running IPX provide clients access to servers on an IPX internetwork.

Router Builds SAP and RIP Tables. The Wellfleet router builds its routing and services tables by listening to regularly scheduled SAP and RIP broadcasts from file servers. The broadcasts include the services a server has to offer and routes to a server. If regular SAP or RIP broadcasts from a file server stop, the local router times the entry out from its services or route table.

Client Sends get_nearest_service SAP Request. A client sends a *get_nearest_service* SAP request to locate a file server.

Router Decisions. If the server resides on the same network as the client, the server receives the request and responds. The local router does not respond because its services table indicates that the service is available on the client's network. In this case, client-router communications stop until the client sends the next *get_nearest_service* SAP request.

If the server does not reside on the same network, the router responds, because its services table indicates that the service is not available on the client's network. The SAP response sent by the router contains the server name, the internal address (if applicable), the service type, the socket number, and the intervening network count of the nearest device offering the service. Continue to *Client's RIP Request.*

If the server does not reside on the same network, and multiple servers of the same server type are available, the router picks the server that is the lowest number of ticks away. If two servers are the same number of ticks away, then the router chooses the server that is the lowest number of hops away. If two servers are the same number of ticks and hops away, then the router chooses based on the alphanumeric order of the server names listed in the services table. Continue to *Client's RIP Request.*

Client's RIP Request. The client then broadcasts a RIP request packet to the local segment. This packet requests the best path to the server's network.

Router's RIP Response. The router on the same network as the client refers to its route table and sends a RIP response to the client. The RIP response identifies the network on which the client resides. The RIP response also contains the server's internal network address, and the intervening hop and tick count.

Client's NCP Request. The client sends an Network Core Protocol (NCP) create connection request to the server. The request includes the router's MAC address as the destination address at the data link layer. Within the IPX header, the destination network address is the internal address and the destination node address of the file server. The client forwards the packet to the router.

Router Forwards Packet. The router running IPX forwards the packet to the network identified by the destination network address.

Example of Client-Server Connection via Wellfleet Router

In the example shown in Figure 1-11, Client A sends a SAP request to locate a file server. Because the server does not reside on LAN A (the same LAN as Client A), Wellfleet IPX Router, Host 2 sends a SAP response to Client A, informing it that File Server, Host 3 on Token-Ring 6 is the nearest device offering the requested service. Client A then sends a RIP request to determine the best path to Host 3. Wellfleet IPX Router, Host 2 sends a RIP response to Client A that includes the server's internal network address and the intervening hop and tick count from Host 3 to Client A. Client A sends an NCP request packet to the Wellfleet IPX Router, Host 2. The router then forwards the packet to Host 3.

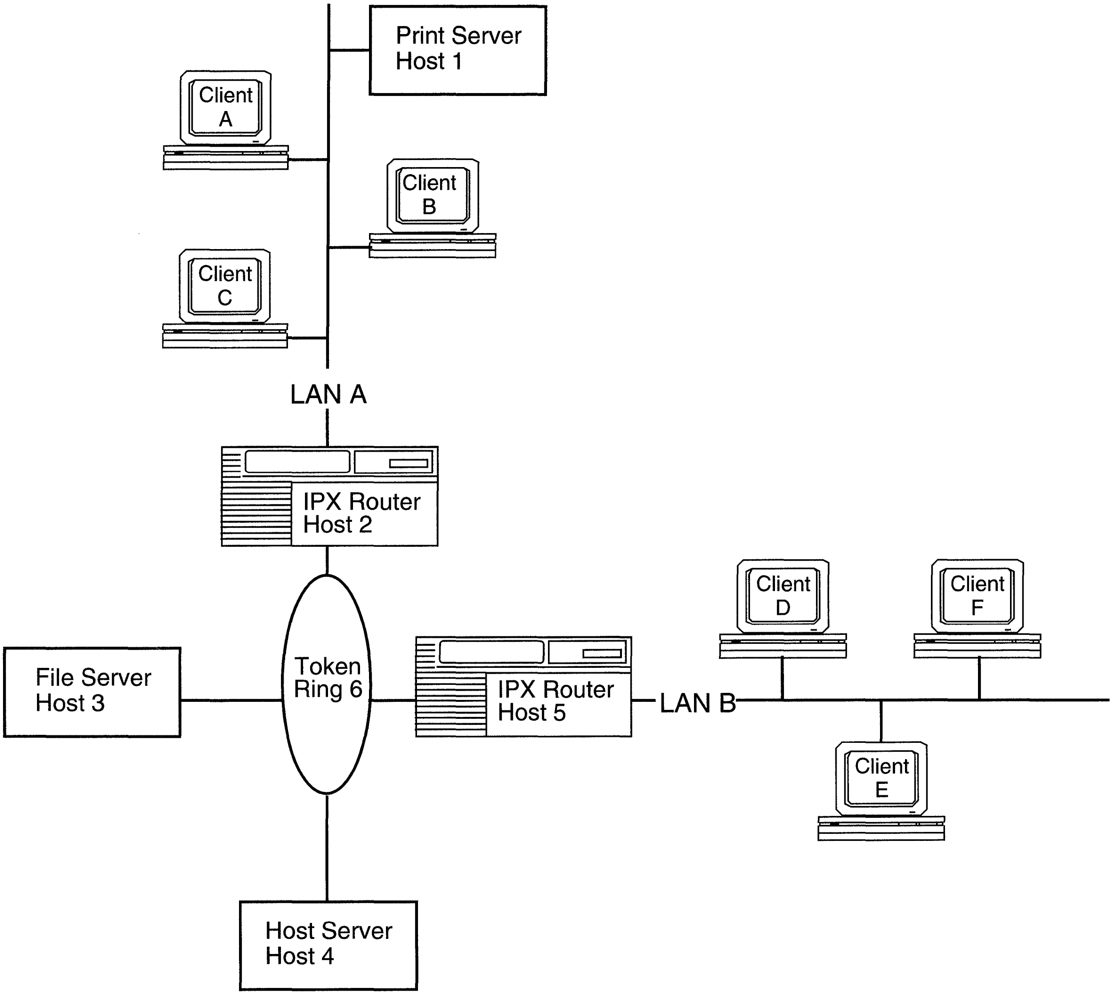


Figure 1-11. Sample IPX Network

For More Information about IPX

The following documents provide technical detail on IPX protocol implementation.

Novell, Inc. *Advanced NetWare, V2.0 Internet Packet Exchange Protocol (IPX) with Asynchronous Event Scheduler.* March 19, 1986.

Novell, Inc. *IPX Router Specification.* October 1993.

RFC 1362: *Novell IPX over Various WAN Media (IPXWAN).*

RFC 1552: *The PPP Internetwork Packet Exchange Control Protocol (IPXCP).*

Chapter 2
IPX Implementation Notes

To prepare your router for the IPX services environment, you need information on IPX configurations as well as additional information about

- IPX Configurations
- IPX Host ID Numbers
- Circuit MAC address assignments
- Configuring IPX without RIP

IPX Configurations and Parameter Requirements

There are two basic types of IPX configurations:

- Standard, with two configurations possible:
  - *Multiple-Host Router.* This common configuration supports one IPX interface per circuit; each interface has a unique IPX host number.
  - *Single-Host Router.* This configuration supports one IPX interface per circuit; every interface shares the same global (boxwide) IPX host number.
- Special, also with two possible configurations:
  - *Multiple Interfaces per Circuit.* This special configuration supports as many IPX interfaces per circuit as there are frame encapsulation types for the given circuit type.

- *Multiple Circuits per Segment.* This special configuration supports either concurrent bridging and IPX routing or IPX multipath and loadsharing.

Standard IPX Configurations

You can configure your Wellfleet router to serve as either a multiple-host or single-host router.

Multiple-Host Router

For this configuration, leave the Multiple Host Address Enable parameter at its default setting, Enable; the host number of each IPX interface is based on the MAC address of the underlying circuit. For more information about the Multiple Host Address Enable parameter, see Chapter 3 of this manual. The only decision you need to make is whether the source of the MAC address is a PROM on the circuit or a MAC Address Override entry that you specify for the circuit.

You specify the source for the MAC address by means of the MAC Address Select parameter. For more information about the MAC Address Override and MAC Address Select Token Ring line detail parameters, see Chapter 3 in *Configuring Wellfleet Routers*. For more information about setting the MAC Address Select parameter for IPX, refer to “MAC Address Selection,” later in this chapter.

Single-Host Router

For this configuration, you need to set the Multiple Host Address parameter to Disabled. Every IPX interface in the router configuration uses the same global host number, which is one of the following:

- An internal serial number retrieved automatically from the router backplane
- A number that you enter into the Host Number parameter field

You specify the source for the host number by entering a host number in the Host Number field of the IPX Global Parameters window. (If you do not enter a number, the router retrieves the internal serial number from the router backplane, and uses this number for the global host number.) For more information on how to access and edit IPX global parameters, refer to Chapter 3.

Special IPX Configurations

You can also configure your router to support multiple interfaces per circuit or multiple circuits per segment.

Multiple Interfaces per Circuit

IPX configurations with multiple interfaces per router circuit typically support migration from an existing release of Novell IPX to a later release. For this type of configuration, you must set the following parameters according to the guidelines that follow:

- Multiple Host Address Enable
- Host Number
- MAC Address Select
- MAC Address Override
- Network Number
- Configured Encapsulation type

Multiple Host Addressing, Host Numbers, and MAC Addresses

If you have multiple IPX interfaces per circuit, leave the Multiple Host Address Enable parameter at its default setting of Enabled. The source for the host number of each IPX interface depends on the circuit type.

If the circuit type is Token Ring or any other circuit type that supports only nonselective operation, each IPX interface adopts as its host number the MAC address value established for the circuit. The only choice you need to make is whether the source of the MAC address that an interface uses for a host number is

- A PROM on the circuit
- A MAC Address Override value that you enter for the circuit
- The global internal serial number retrieved automatically from the router backplane

You select a source for the MAC address by means of the MAC Address Select parameter. (For more information on this parameter, refer to "MAC Address Selection," later in this chapter.)

If the circuit type is Ethernet or any other circuit type that supports selective operation, then you select a source for the host number by entering a host number in the Host Number field of the IPX Interface Parameters window. (If you do not enter a number, the router uses the value you specified for the MAC address.) For more information on how to access and edit IPX interface parameters, refer to Chapter 3.

Network Numbers

When you initially add an IPX interface to the router configuration, the Configuration Manager tool requires you to enter the network number of the IPX network segment associated with that interface. The network number has a nonzero value for all IPX interfaces except

- Interfaces with IPXWAN enabled
- Interfaces with a lower protocol layer; these interfaces negotiate the IPX network number (via PPP, for example)

The network number must be unique among all other network numbers assigned throughout the IPX internetwork.

If you plan to enable IPXWAN for an IPX interface, when you first configure IPX, you must specify a network number of 0 (zero). See *Configuring Wellfleet Routers* for instructions. The router recognizes a network number of 0 on an interface as an indication that a lower protocol layer (IPXWAN or IPXCP) on the same circuit must negotiate with the remote IPX host for the network number of the intervening

WAN segment. Next, you must enter a primary network number and a unique router name in the IPX Global Parameters window. In addition, you must specify a unique common network number in the IPX Interface Parameters window for that interface.

Frame Encapsulation Types and the Number of IPX Interfaces per Circuit

When you add an IPX interface to the router configuration, you must set the Configured Encaps parameter according to the type of frame encapsulation required for communication between all clients on the same IPX logical network within the overall IPX internetwork.

You can configure as many logical interfaces on a circuit as there are encapsulation types available for that type of circuit. For example, you can configure four *different* encapsulations for four independent IPX interfaces on a single Ethernet circuit (Ethernet, Novell, LSAP, and SNAP). Each interface and encapsulation configured on a circuit supports a different logical network.

The Wellfleet Site Manager software allows you to choose for an IPX interface only those encapsulations that are appropriate for the type of physical circuit, as follows:

- Ethernet circuits support Ethernet, LSAP, Novell, and SNAP frames.
- Token Ring circuits support LSAP and SNAP frames.
- Synchronous circuits (V.35, RS-232/V.24, RS-422/423, X.21) support ATM SNAP, Frame Relay SNAP, PPP, SMDS SNAP, X.25 Point-to-Point (Ethernet), and Wellfleet Point-to-Point (Ethernet) frames.
- T1/E1 circuits support Ethernet, LSAP, Novell, and SNAP frames.
- FDDI circuits support LSAP and SNAP frames.
- HSSI circuits support ATM SNAP, Frame Relay SNAP, PPP, SMDS SNAP, and Wellfleet Point-to-Point (Ethernet) frames.

Multiple Circuits per Segment

This special configuration supports either

- Concurrent bridging and IPX routing
- IPX multipath and loadsharing

Refer to Chapter 1 for information on IPX multipath configurations. You can configure bridging as described in *Customizing Bridging Services*.

IPX Host ID Numbers

On Wellfleet routers, the IPX host ID number indicates a physical data link layer address (on a specific circuit or physical interface). An IPX logical interface can listen at this address and capture frames transmitted by nodes compatible with IPX on the local data link.

Figure 2-1 illustrates this concept in a Wellfleet router that has two IPX logical interfaces, each one configured on a different physical circuit.

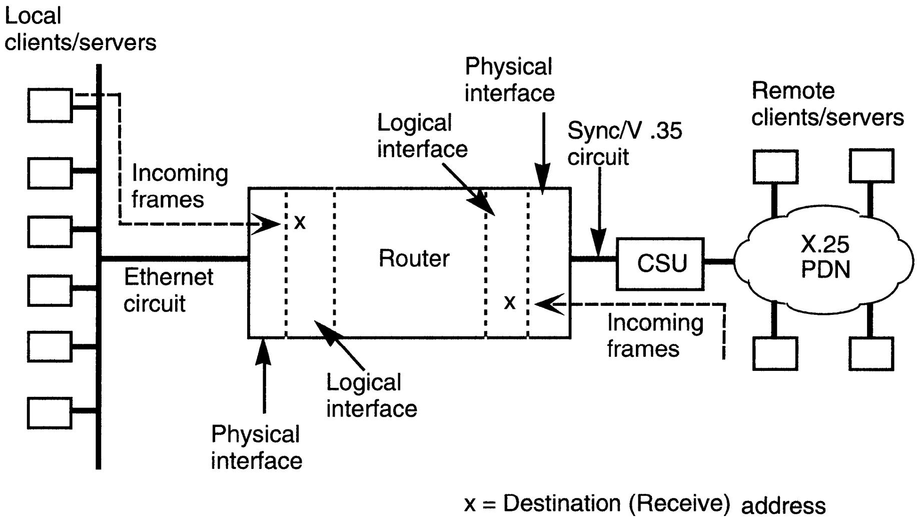


Figure 2-1. Frames Received at a Logical Interface

IPX compatible nodes on the same logical network and locally attached physical segment must use the host ID number of the IPX logical interface as a data link layer destination address, through which any transmitted frames can ultimately reach their target client or server applications.

Because an IPX logical interface can receive and send data, the host ID also identifies a source data link layer address from which the interface can send frames to nodes compatible with IPX anywhere else in the same IPX internetwork.

Figure 2-2 illustrates this concept in a Wellfleet router configured with two IPX logical interfaces, each one on a different physical circuit type.

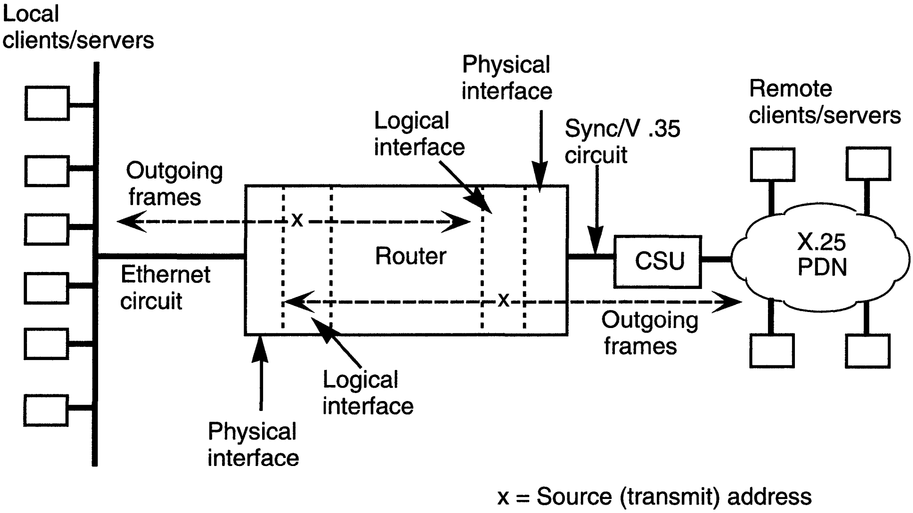


Figure 2-2. Frames Issued from a Logical Interface

Host ID Number for IPX on a Token Ring Circuit

In a configuration with IPX logical interfaces on a Token Ring circuit, the data link layer address is a MAC-layer address.

In Wellfleet routers, you set the MAC-layer address for the circuit and the host ID number for the IPX interface independently. However, the host ID number for every IPX logical interface on a given Token Ring circuit must be identical to the MAC address set for that circuit. Otherwise, the logical interface would send frames that contained an incorrect source MAC address, or the interface would listen for frames at the wrong MAC address.

MAC Address Selection

For Token Ring circuits, you can select the means by which the router determines the MAC address for a circuit by setting the MAC Address Select parameter for that circuit to one of the following choices:

- PROM. (This is the default setting.) The circuit retrieves the MAC address that is stored in a PROM on the supporting link module.
- BOXWIDE. The circuit generates a MAC address based on the serial number of the backplane of the router.
- CNFG. You can configure a MAC address.

For instructions on how to set the MAC Address Select parameter, see Chapter 3 in *Configuring Wellfleet Routers*.

Caution: Changing the setting of the MAC Address Select parameter to accommodate IPX configuration requirements may have secondary effects on other protocol interfaces (for example, LNM Servers or IP) configured on the same circuit(s) with IPX. If necessary, make adjustments to the parameter settings of any such (non-IPX) interfaces configured on the router.

If you choose the CNFG option of the MAC Address Select parameter, you must subsequently enter a valid MAC address in the MAC Address Override parameter. For instructions on how to set the MAC Address Override parameter, see Chapter 3 in *Configuring Wellfleet Routers*. You must repeat this procedure on any Token Ring circuit for which you choose CNFG (user configured) as the source for the MAC address assigned to the individual physical circuit.

Host ID Number for IPX over ATM

To establish an IPX connection over an ATM network, you must assign a unique host ID number to the ATM interface that is running IPX. To assign a number, you can either

- ❒ Enter a value using the Host Number parameter, which is located on the IPX Interface Parameters window
- ❒ Specify that the global MAC address be used for the host ID by disabling the Multiple Host Address Enable parameter, which is located on the Edit IPX Global Parameter window

For instructions on configuring the Host Number and the Multiple Host Address Enable parameters, see Chapter 3.

Configuring IPX without RIP

The IPX router learns WAN addresses from RIP and SAP broadcasts received over wide area networks. The router stores the IPX address/WAN address pairs in its route table for future determination of next-hop destinations.

Every IPX router on the internetwork learns about all of the other IPX routers through the propagation of route tables. These tables can grow very large in large internetworks. To control the size of these tables and reduce bandwidth, you may want to configure IPX without RIP. However, you must perform the following steps when you configure a WAN IPX interface without RIP:

1. Configure an adjacent host, and edit the DLCI parameter in the IPX Adjacent Hosts window for each host on an adjacent Frame Relay, ATM, or SMDS network.

Note: The only time you configure adjacent hosts is when you do not have RIP configured on the interface, and you are running IPX over Frame Relay, ATM, or SMDS.

Refer to the section “Editing Adjacent Host Parameters” in Chapter 3 for detailed instructions.

2. Configure a static route to the next-hop router for each remote network.

   Refer to the section “Editing Static Route Parameters” in Chapter 3 for detailed instructions.

Chapter 3
Editing IPX Parameters

Once you have enabled an IPX interface, you can use Site Manager to edit IPX parameters and customize IPX services. Use Site Manager to perform the following tasks:

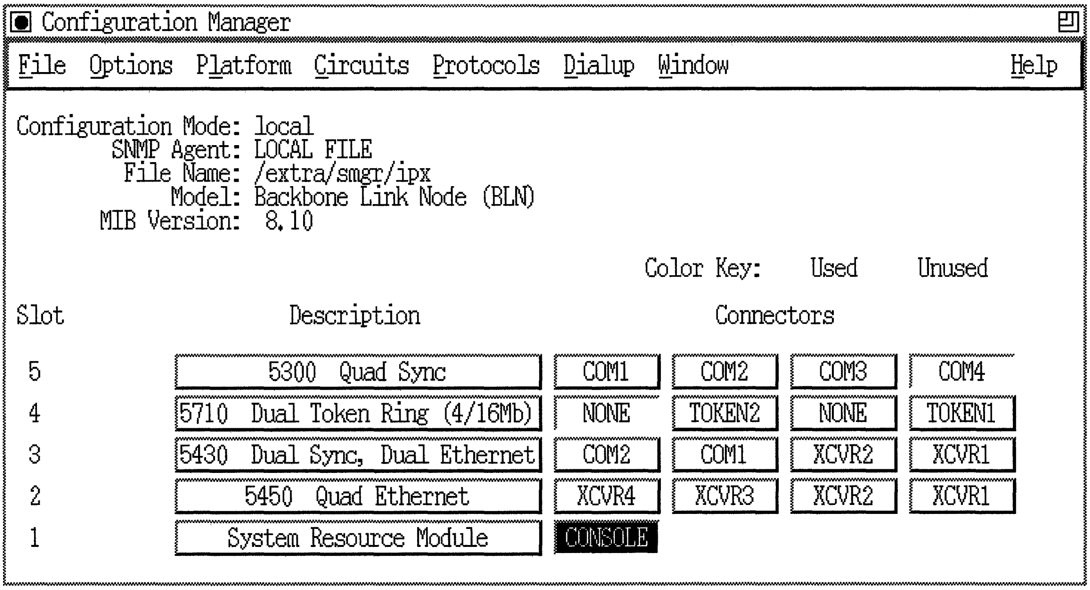
- Access IPX parameters
- Edit IPX global parameters
- Edit IPX interface parameters
- Edit IPX RIP interface parameters
- Add, edit, or delete adjacent hosts
- Add, edit, or delete static routes
- Add, edit, or delete NetBIOS static routes
- Add, edit, or delete static services
- Add, edit, or delete SAP network-level filters
- Add, edit, or delete SAP server-level filters
- Delete IPX from the router

Note: The instructions in this chapter assume that you have already configured at least one IPX interface on the router. If you have *not* yet configured an IPX interface, or want to add additional IPX interfaces, and the configure IPX filters, see *Configuring Wellfleet Routers* for instructions.

Accessing IPX Parameters

You access all IPX parameters from the Wellfleet Configuration Manager window shown in Figure 3-1. For each IPX parameter, this chapter provides information about default settings, valid parameter options, the parameter function, instructions for setting the parameter, and the Management Information Base (MIB) object ID.

The Technician Interface allows you to modify parameters by issuing **set** and **commit** commands with the MIB object ID. This process is equivalent to modifying parameters using Site Manager. For more information about using the Technician Interface to access the MIB, refer to *Using Technician Interface Software*.



```
Configuration Mode: local
        SNMP Agent: LOCAL FILE
         File Name: /extra/smgr/ipx
             Model: Backbone Link Node (BLN)
       MIB Version: 8.10
```

Slot	Description	Connectors			
5	5300 Quad Sync	COM1	COM2	COM3	COM4
4	5710 Dual Token Ring (4/16Mb)	NONE	TOKEN2	NONE	TOKEN1
3	5430 Dual Sync, Dual Ethernet	COM2	COM1	XCVR2	XCVR1
2	5450 Quad Ethernet	XCVR4	XCVR3	XCVR2	XCVR1
1	System Resource Module	CONSOLE			

Figure 3-1. Configuration Manager Window

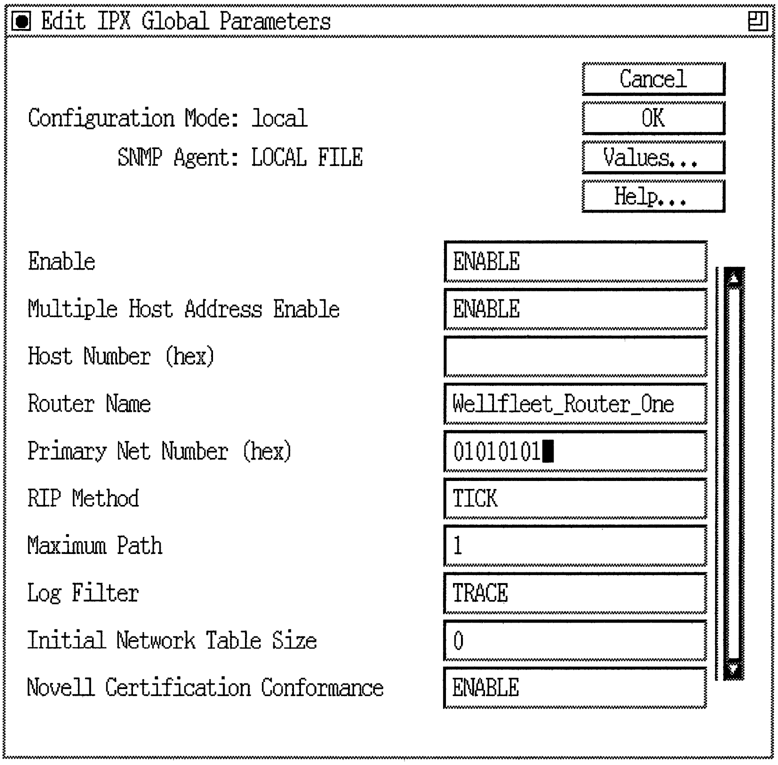
Editing IPX Global Parameters

To edit IPX global parameters, begin at the Configuration Manager window (Figure 3-1) and proceed as follows:

1. Select the Protocols→IPX→Global option.

   The Edit IPX Global Parameters window appears (see Figure 3-2).

2. Edit those parameters you want to change.
3. Click on the OK button to exit the window and save your changes when you are finished.



Configuration Mode: local
SNMP Agent: LOCAL FILE

Enable	ENABLE
Multiple Host Address Enable	ENABLE
Host Number (hex)	
Router Name	Wellfleet_Router_One
Primary Net Number (hex)	01010101
RIP Method	TICK
Maximum Path	1
Log Filter	TRACE
Initial Network Table Size	0
Novell Certification Conformance	ENABLE

Figure 3-2. Edit IPX Global Parameters Window

IPX Global Parameter Descriptions

This section describes all parameters shown on the Edit IPX Global Parameters window (Figure 3-2).

Parameter: **Enable**

Default: Enable

Options: Enable | Disable

Function: Globally enables or disables the system software mechanisms that allow users to add IPX interfaces to the node configuration. Also:

- *Disable* — Shuts down all IPX routing for the entire node.
- *Enable* — Initializes IPX routing for the entire node. Associated IPX interfaces become active, depending on their respective Enable | Disable parameters and on the state of each underlying circuit.

Instructions: Select Disable to disable every IPX interface on the node.

Select Enable to globally reinitialize all IPX interfaces on the node; each interface maintains the most recent setting of its own interface Enable | Disable parameter.

MIB Object ID: 1.3.6.1.4.1.18.3.5.5.1.2

Parameter: **Multiple Host Address Enable**

Default: Enable

Options: Enable | Disable

Function: If you enable this parameter, an IPX interface can

- Use the MAC address located in the PROM on the circuit associated with that interface
- Use a MAC address that you enter in the Host Number parameter field for that interface

Interfaces on a Token Ring circuit adopt a host ID number based only on the MAC address of the associated circuit.

Disabling this parameter causes all IPX interfaces to adopt a single boxwide host ID number, based either on the serial number of the router backplane or on a number that you enter in the Host Number parameter field.

Instructions: Choose Enable or Disable, as appropriate for the type of configuration (standard, multiple interfaces per circuit, or multiple circuits per physical segment). See Chapter 2 for a description of each type of configuration.

MIB Object ID: 1.3.6.1.4.1.18.3.5.5.1.15

Parameter: **Host Number (hex)**

Default: If you disable the Multiple Host Address Enable parameter and enter a unique host number, the Configuration Manager assigns this number to all IPX interfaces you configure on the router.

If you disable the Multiple Host Address Enable parameter and do not enter a boxwide host ID number for this parameter, the Configuration Manager automatically generates a unique 6-byte host ID number for all IPX interfaces. The generated host ID is based on the serial number of the router's backplane.

Options: Any valid host number

Function: Sets an IPX host ID number for IPX interfaces on all slots, or sets unique numbers for IPX interfaces on each slot, depending on your selection for this parameter.

Instructions: Enter a value for Host Number only if an IPX interface in the Wellfleet router resides on a Token Ring circuit, and both of the following are true:

- You are setting the Token Ring MAC Address Select parameter for that circuit to CNFG.
- You are setting a MAC Address Override value for that circuit.

Do not enter a value for IPX Host Number if either of the following is true:

- You want the Configuration Manager to generate a host number automatically.
- The interface is on a Token Ring circuit, and the Token Ring MAC Address Select parameter is set to BOXWIDE or PROM.

MIB Object ID: 1.3.6.1.4.1.18.3.5.5.1.4

Parameter: **Router Name**

Default: None

Options: Any valid NetWare router or server name.

Function: Specifies a symbolic name for the router. Any IPXWAN (RFC1362-compliant) interface in the node uses the name to identify itself to the IPX router or server at the opposite end of the WAN data link.

The symbolic name for the router must be unique among those assigned to IPX file servers and routers anywhere in the IPX internetwork.

Instructions: See the documentation that came with your NetWare operating system for guidelines on specifying a router or server name.

MIB Object ID: 1.3.6.1.4.1.18.3.5.5.1.10

Parameter: **Primary Net Number (hex)**

Default: None

Options: The Primary Network Number (PNN) is a string of up to 8 hexadecimal characters. (See the instructions that follow.)

Function: Specifies an IPX network number for IPXWAN (RFC1362-compliant) link negotiation on all slots. The value of the PNN determines whether the local or remote WAN interface serves as IPX Link Master. The node with the highest PNN value becomes the IPX Link Master.

The PNN should be unique among network numbers currently assigned.

Instructions: Enter a unique network number for each Wellfleet node requiring one or more IPXWAN (RFC1362-compliant) interfaces. (This network number must be unique across the IPX network. That is, do not enter a number that a server is using as an internal network number, or a number that has been assigned on any segment in the network.)

All unused values between 1 and FFFFFFFE (hex) are valid values.

MIB Object ID: 1.3.6.1.4.1.18.3.5.5.1.11

Parameter: **RIP Method**

Default: Tick

Options: Metric | Tick

Function: Specifies for all slots the method of making IPX "best-route" decisions by

- *Ticks* —The amount of time, expressed in ticks, that a packet requires to reach a server on another network segment.
  (Each tick = 1/18 second.)
- *Hops* —The number of router hops a packet must traverse to reach a server on another network segment.

If you accept the default, Tick, and the router knows about two paths to a network, and both paths have equal tick values, the router chooses the path with the smallest number of hops.

If you select Metric, and the best route results in the same number of hops, the router makes its decision based on hops only.

Instructions: Choose the method that results in the best routing performance. Usually, the best route is the one with

- The lowest number of ticks for a packet to reach a node on the destination network
- The lowest number of hops (if multiple routes exist with equal numbers of ticks for a packet to reach a node on the destination network)

If routes exist with equal numbers of ticks and hops, choose either method. We recommend using the default (tick-based) method.

MIB Object ID: 1.3.6.1.4.1.18.3.5.5.1.12

Parameter: **Maximum Path**

Default: 1 (path)

Range: 1 to 5 (paths)

Function: Specifies the maximum number of equal-cost paths allowed for a given network destination and routing method.

Instructions: Accept the default, 1.

MIB Object ID: 1.3.6.1.4.1.18.3.5.5.1.13

Parameter: **Log Filter**

Default: Trace

Options: None, Debug, Info, Trace, Debug Info, Debug Trace, Info Trace, Debug Info Trace

Function: Filters out the specified type of log message. For example, the default setting (Trace) filters out trace messages.

Instructions: Do not change the default value of this parameter unless you are an expert IPX user. Changing the value of this parameter produces significant boxwide effects on memory allocation within the router, which can significantly affect router performance. If you are qualified as an expert user, enter a filtering mode that yields a level of performance most appropriate for network applications supported by this router.

MIB Object ID: 1.3.6.1.4.1.18.3.5.5.1.8

Parameter: **Initial Network Table Size**

Default: 0 (table entries)

Range: 0 to 5000 (table entries)

Function: Specifies how much memory to set aside when creating the router's IPX forwarding and network tables.

Instructions: Do not change the default value of this parameter unless you are an expert IPX user (for example, a Bay Networks Customer Support engineer). Changing the value of this parameter produces significant boxwide effects on memory allocation within the router, which can significantly affect router performance. If you are qualified as an expert user, enter a table size that yields a level of performance most appropriate for network applications supported by this router.

MIB Object ID: 1.3.6.1.4.1.18.3.5.5.1.9

Parameter: **Novell Certification Conformance**

Default: Enabled

Options: Enabled | Disabled

Function: Indicates whether IPX NetBIOS static routes are used to direct a NetBIOS propagation packet through a network.

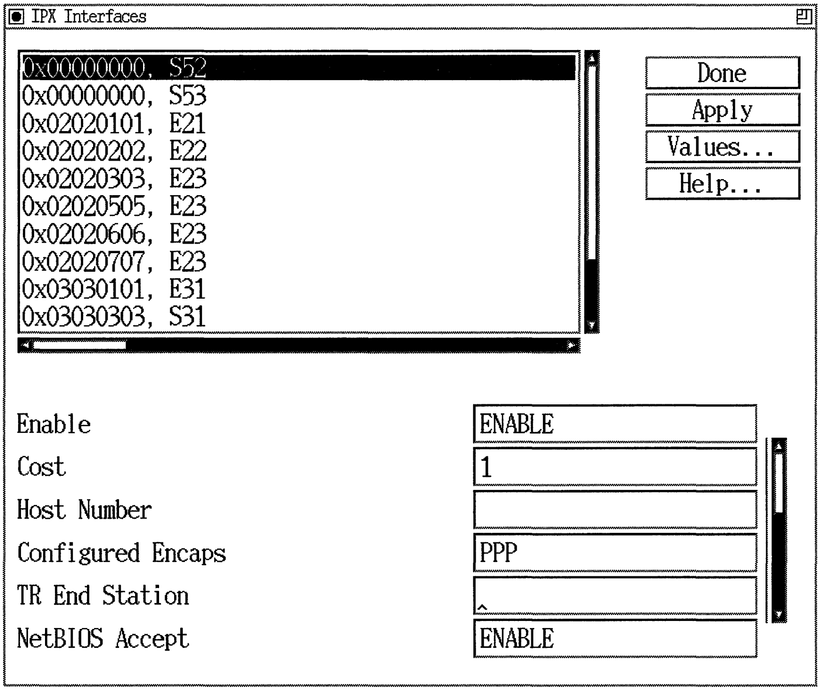
Instructions: Accept the default, Enabled, if you want the router to propagate a packet out all of its interfaces (conforms to Novell standards). Select Disabled if you have static routes configured and you want the router to direct a packet to its destination network. You must set the same option (Enabled or Disabled) for all routers in the network.

MIB Object ID: 1.3.6.1.4.1.18.3.5.5.1.16

Editing IPX Interface Parameters

Any IPX interface you add to a physical circuit inherits a default set of IPX parameter values from the global/slotwide IPX process. You can use the Configuration Manager to access and further modify or customize parameters belonging to a specific interface. To do so, begin at the Configuration Manager window (Figure 3-1) and proceed as follows:

1. Select the Protocols➔IPX➔Interfaces option to display the IPX Interfaces window (see Figure 3-3).



```
0x00000000, S52
0x00000000, S53
0x02020101, E21
0x02020202, E22
0x02020303, E23
0x02020505, E23
0x02020606, E23
0x02020707, E23
0x03030101, E31
0x03030303, S31
```

Enable	ENABLE
Cost	1
Host Number	
Configured Encaps	PPP
TR End Station	
NetBIOS Accept	ENABLE

Figure 3-3. IPX Interfaces Window

The IPX Interfaces window lists each IPX interface entry in the router configuration as follows:

<network_number>, <circuit_name>

2. Select the interface you want to modify. The parameters associated with that interface appear in the parameter value windows.
3. Edit those parameters you want to change. Click on the Apply button to implement your changes.
4. Click on the Done button to save your changes and exit the window.

IPX Interface Parameter Descriptions

This section describes how to set all parameters shown on the IPX Interfaces window (Figure 3-3).

Parameter: Enable

Default: Enable

Options: Enable | Disable

Function: Enables or disables IPX routing on this interface.

Enable — Initializes the IPX interface you added to a circuit. You can also use the Enable setting to reinitialize an existing disabled IPX interface. The actual operating state of an interface, once enabled, depends on

- The current state of the associated circuit
- The current state of the IPX global/slotwide protocol process

Disable — Forces an IPX interface into the down (inoperative) state.

Instructions: Select Enable if you previously set this parameter to Disable and now want to re-enable IPX routing on this interface.

Select Disable only if you want to disable IPX routing on this interface.

MIB Object ID: 1.3.6.1.4.1.18.3.5.5.4.1.3

Parameter:	**Cost**
Default:	1 (for hop- or tick-based routing)
Range:	0 to FFFF (if tick-based routing is enabled) 0 to 15 (if hop-based routing is enabled)
Function:	Sets the cost (number of ticks or hops) for this interface. The cost is added to route information learned on this interface through RIP and is included in subsequent RIP packets sent to other interfaces. IPX disposes of the packet when its hop count passes 15.
Instructions:	Enter the interface cost value. The standard RIP implementation assigns a cost of 1 tick or 1 hop. Increasing the cost causes the upper boundary cost value (FFFF for tick-based routing; 15 for hop-based routing) to be attained more rapidly.
MIB Object ID:	1.3.6.1.4.1.18.3.5.5.4.1.7

Parameter:	**Host Number**
Default:	None
Options:	Any valid IPX host ID number
Function:	If you enable Multiple Host Address Enable and want to accept the PROM-based default setting for the MAC Address Select circuit parameter, this IPX interface adopts a host number based on the MAC address of the underlying circuit. In this case, a PROM on the circuit supplies the number for the MAC address of the circuit and the host number of the interface. (Site Manager does not allow you to enter any value in the Host Number field.) Chapter 2 describes under what circumstances you enter a host number. You can enter a host number for this interface when

- Multiple Host Addressing is enabled
- You do not want to accept the PROM-based (default) setting for MAC Address Select
- The circuit type supports only selective mode of operation (such as with Ethernet circuits)

If you enter a host number, the circuit adopts that value as the MAC address at which this interface can receive frames. (The MAC address configured at the circuit/line level remains effective for all other interfaces configured on the same circuit.)

You can enter a host number for this interface when the underlying circuit is Token Ring; see the instructions that follow.

Site Manager does not allow you to enter an IPX host number for any IPX interface if you first disable Multiple Host Address Enable in the IPX Global Parameters window.

Instructions: Enter a value only if the circuit is not Token Ring and you want to assign a host number that is unique within the IPX internetwork to this IPX interface.

To set the host number of an IPX interface on a Token Ring circuit, you must change the MAC Address Select parameter for that circuit to CNFG (user-configured) and enter a MAC Address Override value for the circuit. The interface uses that value as its host number. This changes the circuit MAC address for all protocols configured on that Token Ring circuit.

MIB Object ID: 1.3.6.1.4.1.18.3.5.5.4.1.37

Parameter:	**Configured Encaps**
Default:	Circuit medium dependent
Options:	Circuit medium dependent
Function:	Specifies the encapsulation methods (such as Ethernet, Novell, LSAP, or SNAP) available for each circuit type (such as Ethernet, Token Ring, or sync). The encapsulation method supports communication on a specific logical network.
Instructions:	Select an encapsulation method that matches the one the clients and servers on the same logical network use and is appropriate for the physical circuit, as follows: – Ethernet circuits support Ethernet, LSAP, Novell, and SNAP frames. – Token ring circuits support LSAP and SNAP frames. – Synchronous circuits (V.35, RS-232/V.24, RS-422/423, X.21) support ATM SNAP, Frame Relay SNAP, PPP, SMDS SNAP, X.25 Point-to-Point (Ethernet), and Wellfleet Point-to-Point (Ethernet) frames. – T1/E1 circuits support Ethernet, LSAP, Novell, and SNAP frames. – FDDI circuits support LSAP and SNAP frames. – HSSI circuits support ATM SNAP, Frame Relay SNAP, PPP, SMDS SNAP, and Wellfleet Point-to-Point (Ethernet) frames.
MIB Object ID:	1.3.6.1.4.1.18.3.5.5.4.1.9

Parameter: **TR End Station**

Default: Disable

Options: Enable | Disable

Function: Enables or disables source routing on this interface. This parameter appears only when you add an IPX interface on a Token Ring circuit.

Instructions: Select Enable if this interface connects to a bridged Token Ring network. Select Disable only if you want to disable source routing over this interface.

MIB Object ID: 1.3.6.1.4.1.18.3.5.5.4.1.23

Parameter: **NetBIOS Accept**

Default: Enable

Options: Enable | Disable

Function: Enables or disables acceptance of all NetBIOS Type 20 (broadcast) packets received by this interface from an external source.

Instructions: Select Enable if you want this interface to accept all NetBIOS broadcast packets from an external source. Select Disable only if you want this interface to reject all NetBIOS broadcast packets from an external source.

MIB Object ID: 1.3.6.1.4.1.18.3.5.5.4.1.24

Parameter: **NetBIOS Deliver**

Default: Enable

Options: Enable | Disable

Function: Enables or disables outbound delivery of all NetBIOS Type 20 (broadcast) packets received by this interface from another interface in the same node.

Instructions: Select Enable if you want to reenable outbound delivery of NetBIOS broadcast packets received internally. Select Disable only to drop NetBIOS broadcast packets received internally.

MIB Object ID: 1.3.6.1.4.1.18.3.5.5.4.1.25

Parameter: **WAN RIP Period**

Default: 2 (two 30-sec intervals)

Range: 0 to 99 (number of 30-sec intervals)

Function: Specifies how often a given IPX interface transmits periodic (not immediate) RIP update information to other IPX nodes in the same wide area network. Both the local and remote ends of the data link associated with this interface must be configured with the same WAN RIP Period value. A value of 0 indicates no periodic RIP updates and no timing out of RIP information resulting from periodic updates. (Immediate updates still propagate through the network when WAN RIP Period = 0.)

Instructions: Enter any valid value, from 0 to 99. Ensure that both the local and remote ends of the data link associated with this interface are configured with the same WAN RIP Period value.

MIB Object ID: 1.3.6.1.4.1.18.3.5.5.4.1.36

Parameter: **WAN SAP Period**

Default: 2 (two 30-sec intervals)

Range: 0 to 99 (number of 30-sec intervals)

Function: Specifies the interval at which an IPX interface transmits periodic SAP advertisements. This parameter has no effect on SAP advertisements generated in response to bindery/SAP table changes or client requests. A value of 0 indicates no periodic SAP updates and no timing out of SAP information resulting from periodic updates. (Immediate updates still propagate through the network when WAN SAP Period = 0.) You can eliminate all SAP broadcasts by means of SAP filters.

Instructions: If the interface is configured on a LAN circuit, use the default interval of two 30-sec intervals. If the interface is connected to a WAN, enter a higher value to decrease the frequency of advertisements.

MIB Object ID: 1.3.6.1.4.1.18.3.5.5.4.1.26

Parameter:	**FR Broadcast (hex)**
Default:	0xFFFFFF (not displayed)
Options:	Default value or a user-specified Frame Relay broadcast address.
Function:	Specifies a Frame Relay broadcast address for this IPX interface. (This parameter appears only when you configure an IPX interface on a Frame Relay, SMDS, or ATM circuit.) The default value (0xFFFFFF) causes the data link layer to issue a Frame Relay broadcast packet on all active virtual circuits. The value is not actually included in the MAC field of the packet on the WAN. The packet instead contains a value that is appropriate for the type of data link protocol.
Instructions:	Leave blank to accept the default value or enter a Frame Relay broadcast address to send all broadcast traffic through the IPX interface you are configuring. With the default value, the IPX router sends all broadcast traffic through all logical connections associated with the IPX interface you are configuring. Broadcast traffic includes RIP and SAP broadcasts.
MIB Object ID:	1.3.6.1.4.1.18.3.5.5.4.1.27

Parameter: FR Multicast (hex)

Default: 0xFFFFFF (not displayed)

Options: Default value or a user-specified Frame Relay multicast address.

Function: Specifies a Frame Relay multicast address for this IPX interface. (This parameter appears only when you configure an IPX interface on a Frame Relay, SMDS, or ATM circuit.)

The default value (0xFFFFFF) causes the data link layer to issue a Frame Relay multicast packet on all active virtual circuits. The value is not actually included in the MAC field of the packet on the WAN. The packet instead contains a value that is appropriate for the type of data link protocol.

Instructions: Leave blank to accept the default value or enter a Frame Relay multicast address to send all multicast traffic through the IPX interface you are configuring. With the default value, the IPX router sends all multicast traffic through all logical connections associated with the IPX interface you are configuring.

MIB Object ID: 1.3.6.1.4.1.18.3.5.5.4.1.28

Parameter: **Split Horizon**

Default: Enable

Options: Enable | Disable

Function: When forwarding RIP and SAP updates from an interface, the interface can exclude RIP and SAP broadcast updates learned on that interface.

Instructions: Select Enable if you previously set this parameter to Disable and now do not want the router to transmit RIP and SAP updates received from the interface over that same interface.

Select Disable only if you want the router to transmit RIP and SAP updates received from the interface over that same interface.

MIB Object ID: 1.3.6.1.4.1.18.3.5.5.4.1.30

Parameter:	**IPXWAN Common Net (hex)**
Default:	None
Options:	Any valid, unique, and nonreserved network number (a string of up to 8 hexadecimal characters).
Function:	Specifies a Common Network Number (CNN) that the local interface can assign to the locally attached IPXWAN (RFC155-compliant) link. To assign its CNN, the local IPXWAN interface must serve as master in a WAN link with a remote IPXWAN link slave interface. (The link master and slave interfaces adopt the CNN of the link master upon successful completion of link negotiation.) The CNN should be unique among network numbers currently assigned. This parameter appears only when you configure an IPXWAN interface. (The IPXWAN Enable parameter must be set to Enable. See *Configuring Wellfleet Routers* for instructions on setting this parameter.)
Instructions:	Enter a valid, unique, and nonreserved network number for each IPXWAN (RFC1362-compliant) interface you add to the node. All values between 1 and FFFFFFFE (hex) are valid values. Do not enter any leading zeros in the configuration screen, and never enter a value of 0 or FFFFFFFF (hex); these are reserved values.
MIB Object ID:	1.3.6.1.4.1.18.3.5.5.4.1.33

Parameter: **IPXWAN Time Out**

Default: 60 (seconds)

Options: None

Function: Sets the amount of time an IPXWAN (RFC1362-compliant) interface allows to negotiate a data link across an associated WAN circuit.

This parameter appears only when you configure an IPXWAN interface. (The IPXWAN Enable parameter must be set to Enable. See *Configuring Wellfleet Routers* for instructions on setting this parameter.)

Instructions: No other settings for the WAN data link negotiation interval are supported in this release.

MIB Object ID: 1.3.6.1.4.1.18.3.5.5.4.1.34

Parameter: **IPXWAN Link Retry**

Default: 5 (retries)

Options: None

Function: Specifies the total number of times the calling IPXWAN interface can attempt to negotiate (establish) a WAN connection.

Each failed attempt causes the information message "IPXWAN negotiation failed on intf <network address>" to be recorded in the local event log (that is, in the event log of the calling node). If all attempts fail, the system software disables the calling IPXWAN interface. Disabling an IPXWAN interface also causes the information message "IPXWAN down on intf <IPX network address>" to be recorded in the local event log.

This parameter appears only when you configure an IPXWAN interface. (The IPXWAN Enable/Disable interface parameter must be set to Enable. See *Configuring Wellfleet Routers* for instructions on setting this parameter.)

Instructions: Accept the default, 5.

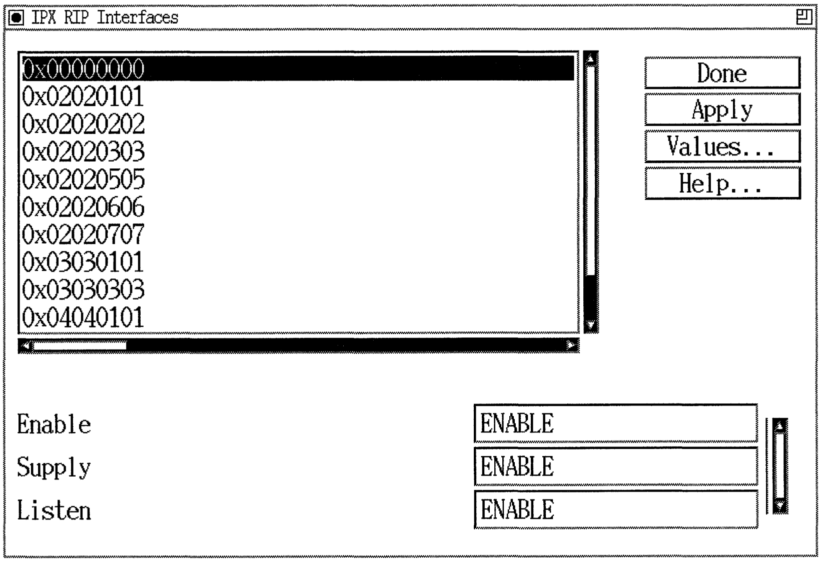
MIB Object ID: 1.3.6.1.4.1.18.3.5.5.4.1.35

Editing IPX RIP Interface Parameters

If RIP is enabled on an IPX interface, you can edit the RIP parameters of that interface by accessing the IPX RIP Interfaces window. For instructions on how to add an IPX RIP interface to a circuit, refer to *Configuring Wellfleet Routers*.

To edit the configurable RIP parameters of an IPX interface, begin at the Configuration Manager window (Figure 3-1) and proceed as follows:

1. Select the Protocols→IPX→RIP Interfaces option. The IPX RIP Interfaces window appears (see Figure 3-4). The window displays each RIP interface entry by its associated Network Number (in hexadecimal notation).
2. Select the RIP interface you want to edit by clicking on the appropriate entry in the list of RIP interfaces.
3. Click on any parameter value you want to change; then enter a new value.
4. Click on the Apply button to implement your changes.
5. Click on the Done button to save and exit the IPX RIP Interfaces window.



0x00000000
0x02020101
0x02020202
0x02020303
0x02020505
0x02020606
0x02020707
0x03030101
0x03030303
0x04040101

Enable ENABLE
Supply ENABLE
Listen ENABLE

Figure 3-4. IPX RIP Interfaces Window

IPX RIP Interface Parameter Descriptions

This section describes how to set all parameters shown on the IPX RIP Interfaces window (Figure 3-4).

Parameter: Enable

Default: Enable

Options: Enable | Disable

Function: Specifies whether RIP is enabled on this IPX interface.

Instructions: Select Enable to enable RIP on this interface. Select Disable to disable RIP on this interface.

MIB Object ID: 1.3.6.1.4.1.18.3.5.5.5.1.2

Parameter: Supply

Default: Enable

Options: Enable | Disable

Function: Specifies whether the interface transmits RIP Periodic and Triggered updates to routers in neighboring networks.

Instructions: Select Enable to configure the interface to transmit all RIP updates.

Select Disable to prohibit the interface from transmitting any RIP updates.

MIB Object ID: 1.3.6.1.4.1.18.3.5.5.5.1.5

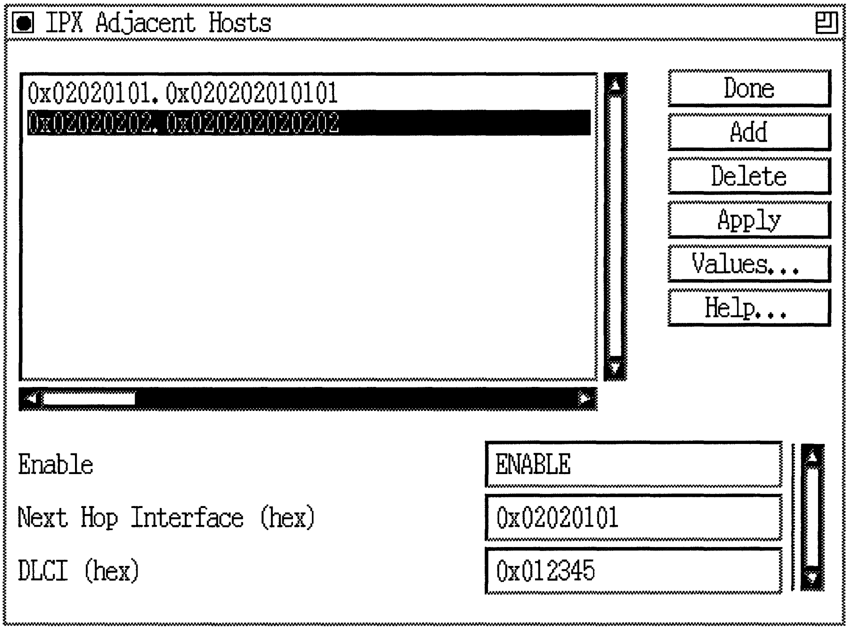
Parameter:	**Listen**
Default:	Enable
Options:	Enable | Disable
Function:	Specifies whether this interface listens to RIP Periodic and Triggered updates from neighboring networks.
Instructions:	Select Enable to configure this IPX interface to listen to RIP updates, and to convey received routing information to its internal routing table. Select Disable to configure this IPX interface to ignore RIP updates from neighboring routers. Disabling Listen also prevents this interface from conveying any received routing information to its internal routing table.
MIB Object ID:	1.3.6.1.4.1.18.3.5.5.5.1.6

Note: If this parameter is set to Enable, a route filter can still prohibit the interface from updating its internal routing tables.

Editing Adjacent Host Parameters

The following sections show you how to add, edit, and delete adjacent hosts in a Wellfleet router configuration. You perform these actions by means of the IPX Adjacent Hosts window.

To access the Adjacent Hosts window, begin at the Configuration Manager window (Figure 3-1) and select the Protocols→IPX→Adjacent Hosts option. The IPX Adjacent Hosts window appears (Figure 3-5), showing a list of all adjacent hosts currently defined in the router configuration.



0x02020101.0x020202010101
0x02020202.0x020202020202

Enable: ENABLE
Next Hop Interface (hex): 0x02020101
DLCI (hex): 0x012345

Figure 3-5. IPX Adjacent Hosts Window

The IPX Adjacent Hosts window displays each Adjacent Host entry in the router configuration in hexadecimal notation, as follows:

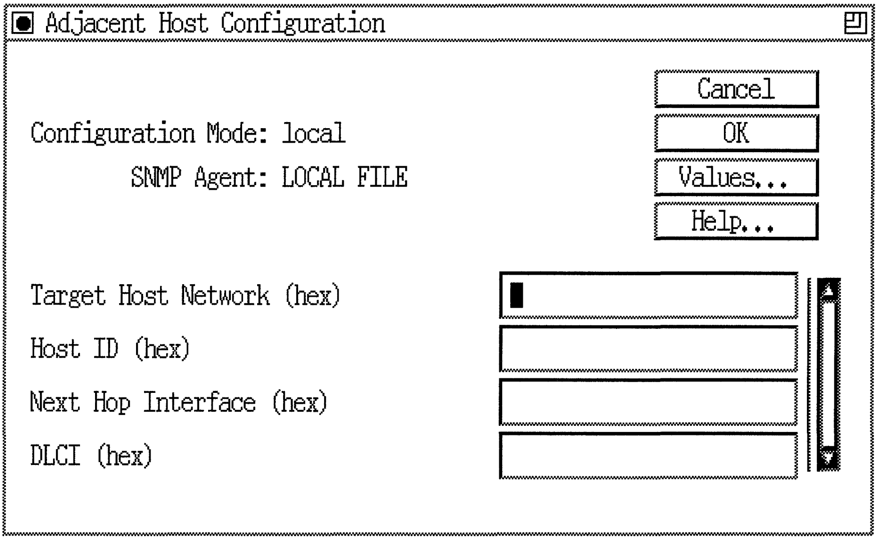
<adjacent_host_network>. <adjacent_host_ID>

Adding an Adjacent Host

To add an adjacent host, begin at the IPX Adjacent Hosts window (see Figure 3-5) and proceed as follows:

1. Click on the Add button.

   The Adjacent Host Configuration window appears (Figure 3-6).



Adjacent Host Configuration

Configuration Mode: local

SNMP Agent: LOCAL FILE

Target Host Network (hex)

Host ID (hex)

Next Hop Interface (hex)

DLCI (hex)

Figure 3-6. Adjacent Host Configuration Window

2. Enter values for the Target Host Network, Host ID, Next Hop Interface, and DLCI (WAN address) parameters.
3. Click on the OK button to save your entries to the configuration file.

The IPX Adjacent Hosts window (Figure 3-5) reappears immediately after you press the OK button.

Adjacent Host Configuration Parameter Descriptions

This section describes all parameters shown on the Adjacent Host Configuration window (Figure 3-6).

Parameter: **Target Host Network (hex)**

Default: None

Options: Valid network address of the adjacent host

Function: Specifies the network address of the adjacent host.

Instructions: Enter a network address of up to 8 hexadecimal characters.

MIB Object ID: 1.3.6.1.4.1.18.3.5.5.6.1.3

Parameter: **Host ID (hex)**

Default: None

Options: Valid host ID of the adjacent host

Function: Specifies the host ID of the adjacent host.

Instructions: Enter a host ID of up to 12 hexadecimal characters.

MIB Object ID: 1.3.6.1.4.1.18.3.5.5.6.1.4

Parameter: **Next Hop Interface (hex)**

Default: None

Options: The configured network address of the next-hop interface

Function: Specifies the network address of the next-hop interface.

Instructions: Enter a network address of up to 8 hexadecimal characters.

MIB Object ID: 1.3.6.1.4.1.18.3.5.5.6.1.5

Parameter: **DLCI (hex)**

Default: None

Options: Data Link Connection Identifier

Function: Allows you to enter a WAN address, whose format depends on the underlying data link protocol type.

Instructions: Enter a DLCI of up to 16 hexadecimal characters if the interface is on a Frame Relay network.

Leave blank if the interface is *not* on a Frame Relay network.

MIB Object ID: 1.3.6.1.4.1.18.3.5.5.6.1.6

Caution: The router cannot pass traffic through an interface to an adjacent host on a Frame Relay network if the adjacent host is not configured with the correct DLCI.

Editing an Adjacent Host

You can edit the configurable parameters of an Adjacent Host entry in the node configuration.

Note: The Configuration Manager does not allow you to change the Target Host Network and Host ID parameters you set in any Adjacent Host Configuration window. To establish new values for these parameters for a particular adjacent host, you must delete that host and configure a new host. You can, however, reconfigure all other parameters associated with an adjacent host.

To edit the configurable parameters associated with an existing adjacent host, begin at the Configuration Manager window (Figure 3-1) and select the Protocols→IPX→Adjacent Hosts option. The IPX Adjacent Hosts window appears, as shown in Figure 3-5. From this window, proceed as follows:

1. Select the adjacent host you want to edit by clicking on the appropriate entry in the list of adjacent hosts.
2. Click on any parameter value you want to change; then enter a new value.
3. Click on the Apply button to implement your changes.
4. Click on the Done button to save and exit the IPX Adjacent Hosts window.

IPX Adjacent Hosts Parameter Descriptions

This section describes the parameters listed in the IPX Adjacent Hosts window (Figure 3-5).

Parameter:	**Enable**
Default:	Enable
Options:	Enable | Disable
Function:	Sets the state (active or inactive) of the adjacent host record in the IPX routing tables.
Instructions:	Select Disable to make the adjacent host record inactive in the IPX routing table. Select Enable to make the adjacent host record active in the IPX routing table.
MIB Object ID:	1.3.6.1.4.1.18.3.5.5.6.1.2

Parameter: **Next Hop Interface (hex)**

Default: None

Options: Configured network address of the next hop

Function: Specifies the network address of the next-hop interface.

Instructions: Enter a network address of up to 8 hexadecimal characters.

MIB Object ID: 1.3.6.1.4.1.18.3.5.5.6.1.5

Parameter: **DLCI (hex)**

Default: None

Options: Data Link Connection Identifier

Function: Allows you to enter a WAN address, whose format depends on the underlying data link protocol type.

Instructions: Enter a DLCI of up to 16 hexadecimal characters if the interface is on a Frame Relay network.

Leave blank if the interface is *not* on a Frame Relay network.

MIB Object ID: 1.3.6.1.4.1.18.3.5.5.6.1.6

Caution: The router cannot pass traffic through an interface to an adjacent host on a Frame Relay network if the adjacent host is not configured with the correct DLCI.

Deleting an Adjacent Host

To delete an adjacent host:

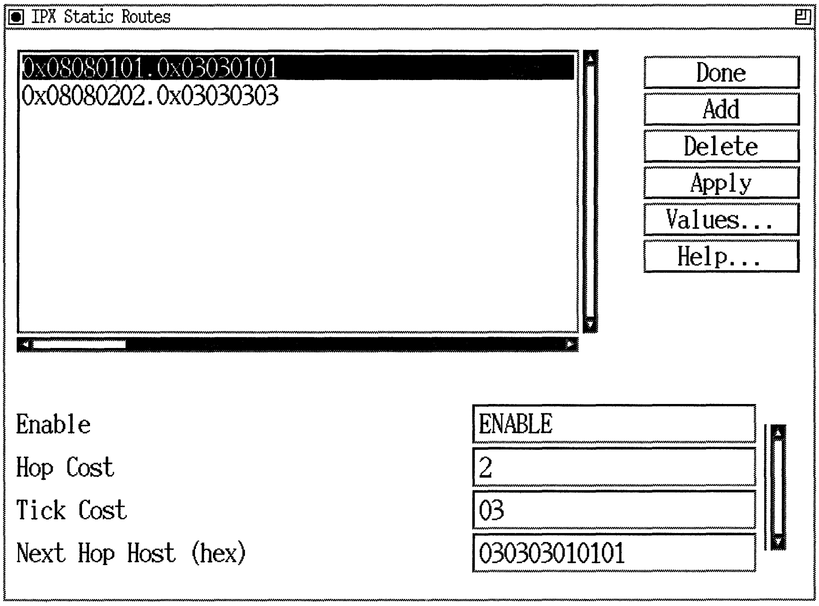
1. Select from the IPX Adjacent Hosts window (see Figure 3-5) the adjacent host you want to delete from the node configuration.
2. Click on the Delete button in the Adjacent Hosts window.

The system software deletes the Adjacent Host entry you selected, and the entry disappears from the list of adjacent hosts in the Adjacent Hosts window.

Editing Static Route Parameters

IPX static routes are user-specified transmission paths that IPX internet packets follow. You configure static routes when you want to restrict the paths that packets can follow. Static routes, like routes learned through RIP, are maintained in the IPX routing table. Unlike routes learned through RIP, however, static routes do not expire. Static routes remain in the IPX routing table until they are reconfigured manually.

The following sections show you how to add, edit, and delete IPX static routes in a Wellfleet router configuration. You perform these functions from the IPX Static Routes window. Begin at the Configuration Manager window (Figure 3-1) and select the Protocols→IPX→Static Routes option. The IPX Static Routes window appears (see Figure 3-7).



0x08080101.0x03030101
0x08080202.0x03030303

Enable ENABLE
Hop Cost 2
Tick Cost 03
Next Hop Host (hex) 030303010101

Figure 3-7. IPX Static Routes Window

Refer to the following sections to add, edit, and delete static routes.

Note: The following rule applies in the event that RIP is disabled over the WAN: to establish a data link layer connection in a Frame Relay, SMDS, or ATM network, which allows the router to send packets over a static route, you must first configure an adjacent host and edit the DLCI parameter in the IPX Adjacent Hosts window before you configure a static route to that adjacent host.

The IPX Static Routes window displays each Static Route entry in the router configuration in hexadecimal notation, as follows:

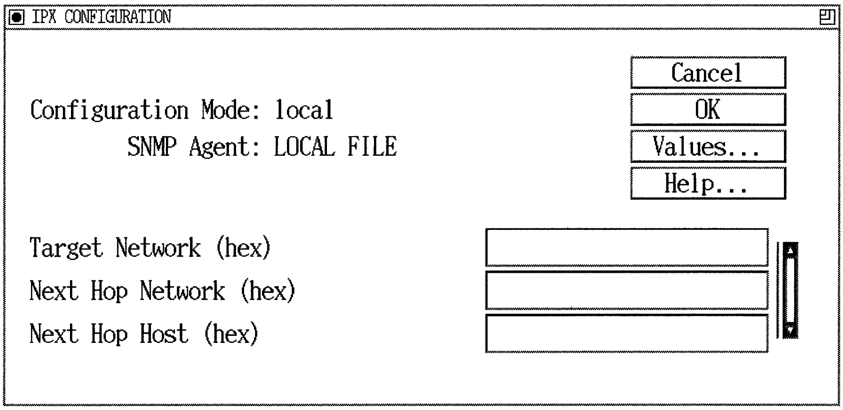
<target_network>.<next_hop_network>

Adding a Static Route

To add a static route, begin at the IPX Static Routes window (see Figure 3-7) and proceed as follows:

1. Click on the Add button.

   The IPX Configuration window appears (see Figure 3-8).



Configuration Mode: local
SNMP Agent: LOCAL FILE

Target Network (hex)
Next Hop Network (hex)
Next Hop Host (hex)

Figure 3-8. IPX Configuration Window

2. Edit the parameters, using the parameter descriptions that follow as guidelines.
3. Click on the OK button to save your entries.

The IPX Static Routes window (Figure 3-7) reappears immediately after you click on the OK button.

IPX Static Route Configuration Parameter Descriptions

This section describes all parameters shown in the IPX Configuration window.

Parameter: **Target Network (hex)**

Default: None

Options: Any valid network address in hexadecimal notation

Function: Specifies the address of the network to which you want to configure the static route.

Instructions: Enter a network address of up to 8 hexadecimal characters.

MIB Object ID: 1.3.6.1.4.1.18.3.5.5.7.1.3

Parameter: **Next Hop Network (hex)**

Default: None

Options: Any valid network address in hexadecimal notation

Function: Specifies the network address of the next-hop interface.

Instructions: Enter a network address of up to 8 hexadecimal characters.

MIB Object ID: 1.3.6.1.4.1.18.3.5.5.7.1.5

Parameter: **Next Hop Host (hex)**

Default: None

Options: Any valid host address in hexadecimal notation

Function: Specifies the address of the next-hop host in the static routing path.

Instructions: Enter a host address of up to 12 hexadecimal characters.

MIB Object ID: 1.3.6.1.4.1.18.3.5.5.7.1.6

Editing a Static Route

You can edit the configurable parameters of a static route in the node configuration.

Note: The Configuration Manager does not allow you to reconfigure the Target Network and Next Hop Network parameters for a static route. If you want to change these parameters, you must delete the static route and add a new route with the proper information. However, you can reconfigure all other parameters associated with a static route.

To edit the configurable parameters associated with an existing static route, begin at the Configuration Manager window (Figure 3-1) and select the Protocols➔IPX➔Static Routes option. The IPX Static Routes window appears (Figure 3-7). From this window, proceed as follows:

1. Select the static route you want to edit by clicking on the appropriate entry in the list of static routes.
2. Click on any parameter value you want to change; then enter a new value.
3. Click on the Apply button to save your changes.
4. Click on the Done button to exit the IPX Static Routes window.

IPX Static Route Parameter Descriptions

This section describes how to set all parameters shown on the IPX Static Routes window.

Parameter:	**Enable**
Default:	Enable
Options:	Enable | Disable
Function:	Specifies the state (active or inactive) of the static route record in the IPX routing tables.
Instructions:	Select Disable to make the static route record inactive in the IPX routing table. Select Enable to make the static route record active in the IPX routing table.
MIB Object ID:	1.3.6.1.4.1.18.3.5.5.7.1.2

Parameter:	**Hop Cost**
Default:	0
Range:	0 to 15
Function:	The IPX router uses Hop Cost when determining the best route for a datagram to follow. The hop cost is also propagated through RIP. The default setting of 0 for static routes gives them priority over RIP-learned routes.
Instructions:	Accept the default, 0, or enter a value between 1 and 15, inclusive.
MIB Object ID:	1.3.6.1.4.1.18.3.5.5.7.1.4

Parameter: **Tick Cost**

Default: 0

Range: 0 to FFFF (hexadecimal)

Function: Specifies the number of 1/18th-sec timer ticks required for an IPX datagram to traverse this static route. The IPX router uses Tick Cost when determining the best route for a datagram to follow. The tick cost is also propagated through RIP. The default setting of 0 for the tick cost of static routes gives them priority over RIP-learned routes.

Instructions: Enter the number of 1/18th-second ticks required for an IPX datagram to traverse this static route.

MIB Object ID: 1.3.6.1.4.1.18.3.5.5.7.1.8

Parameter: **Next Hop Host (hex)**

Default: None

Options: Any valid host address in hexadecimal notation

Function: Specifies the address of the next-hop host in the static routing path.

Instructions: Enter a host address of up to 12 hexadecimal characters.

MIB Object ID: 1.3.6.1.4.1.18.3.5.5.7.1.6

Deleting a Static Route

To delete an IPX static route:

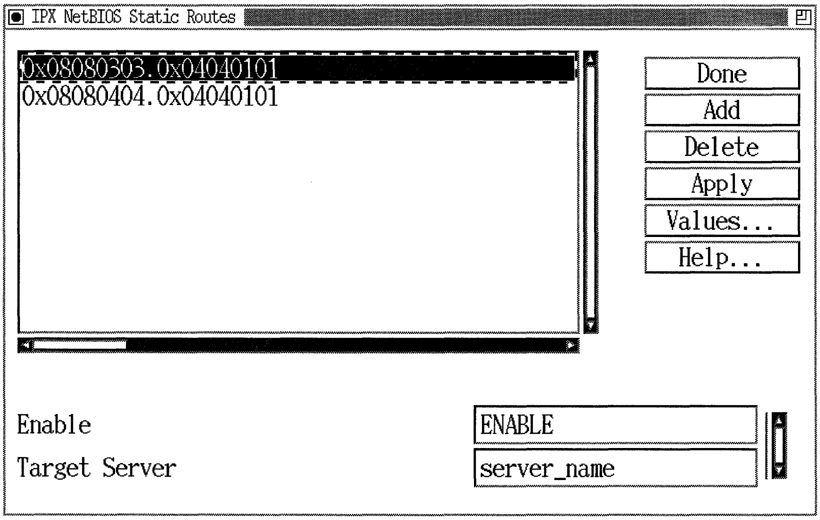
1. Select from the IPX Static Routes window the static route you want to delete from the node configuration.
2. Click on the Delete button in the IPX Static Routes window (see Figure 3-7).

The system software deletes the Static Route entry you selected, and the entry disappears from the list of static routes in the IPX Static Routes window.

Editing NetBIOS Static Route Parameters

The NetBIOS Static Route function allows you to reduce NetBIOS network traffic by configuring a NetBIOS static route to a server name and type. The IPX router then restricts broadcast NetBIOS packets, which are usually forwarded to all network interfaces on a single network.

You can add, edit, and delete NetBIOS static routes to other networks, regardless of the routers used in those networks. You perform these functions from the IPX NetBIOS Static Routes window. Begin at the Configuration Manager window (Figure 3-1) and select the Protocols➔IPX➔NetBIOS Static Routes option. The IPX NetBIOS Static Routes window appears (see Figure 3-9):



IPX NetBIOS Static Routes

0x08080303.0x04040101
0x08080404.0x04040101

Enable ENABLE
Target Server server_name

Figure 3-9. IPX NetBIOS Static Routes Window

The IPX NetBIOS Static Routes window displays each NetBIOS Static Route entry in the router configuration in hexadecimal notation, as follows:

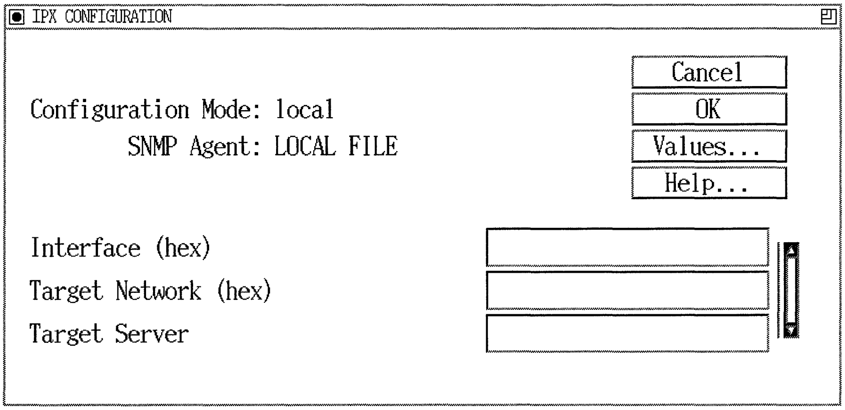
<target_network>.<interface / network_number>

Refer to the following sections to add, edit, and delete NetBIOS static routes.

Adding a NetBIOS Static Route

To add a NetBIOS static route, begin at the IPX NetBIOS Static Routes window (see Figure 3-9) and proceed as follows:

1. Click on the Add button.
2. The IPX Configuration window appears (see Figure 3-10).



Configuration Mode: local
SNMP Agent: LOCAL FILE

Figure 3-10. IPX Configuration Window

3. Enter values for the Interface, Target Network, and Target Server parameters, using the parameter descriptions that follow as guidelines.
4. Click on the OK button to save your entries.

The IPX NetBIOS Static Routes window (Figure 3-9) reappears immediately after you click on the OK button.

IPX NetBIOS Static Route Configuration Parameter Descriptions

This section describes all parameters shown in the IPX Configuration window.

Parameter: **Interface (hex)**

Default: None

Options: Any valid interface address in hexadecimal notation

Function: Specifies the address of the interface on which you want to configure the NetBIOS static route.

Instructions: Enter an interface address of up to 8 hexadecimal characters.

MIB Object ID: 1.3.6.1.4.1.18.3.5.5.8.1.5

Parameter: **Target Network (hex)**

Default: None

Options: Any valid network address in hexadecimal notation

Function: Specifies the address of a destination network that you want to receive NetBIOS broadcast packets destined for the specified target server.

Instructions: Enter a network address of up to 8 hexadecimal characters.

MIB Object ID: 1.3.6.1.4.1.18.3.5.5.8.1.3

Parameter:	**Target Server**
Default:	None
Options:	The name of a NetBIOS target server, specified as a string of up to 16 alphanumeric characters. You can include any printable character, including $, #, and so on. To specify a backslash, enter two backslashes (\ \). You can also use the hexadecimal equivalent (*xx*) of any valid ASCII character. For example, you can specify \20 for space or \21 for ! Note that *xx* is counted as one character.
Function:	Specifies the name of the NetBIOS target server.
Instructions:	Enter the name or part of the name of the NetBIOS target server. The name can be up to 16 alphanumeric characters. Also, you can leave the field blank.
MIB Object ID:	1.3.6.1.4.1.18.3.5.5.8.1.4

Editing a NetBIOS Static Route

You can edit the configurable parameters of a NetBIOS static route in the node configuration.

Note: The Configuration Manager does not allow you to reconfigure the Interface or Target Network parameters for a static route. If you want to change these parameters, you must delete the static route and add a new route. However, you can reconfigure all other parameters associated with a static route.

To edit the configurable parameters associated with an existing NetBIOS static route, begin at the Configuration Manager window (Figure 3-1) and select the Protocols→IPX→NetBIOS Static Routes option. The IPX NetBIOS Static Routes window appears as shown in Figure 3-9. From this window, proceed as follows:

1. Select the NetBIOS static route you want to edit by clicking on the appropriate entry in the list of static routes.
2. Click on any parameter value you want to change; then enter a new value.
3. Click on the Apply button to save your changes.
4. Click on the Done button to exit the IPX NetBIOS Static Routes window.

IPX NetBIOS Static Route Parameters Descriptions

This section describes how to set all parameters shown on the IPX NetBIOS Static Routes window (Figure 3-9).

Parameter:	**Enable**
Default:	Enable
Options:	Enable | Disable
Function:	Specifies the state (active or inactive) of the static route record in the NetBIOS routing table.
Instructions:	Select Disable to make the static route record inactive in the NetBIOS routing table. Select Enable to make the static route record active in the NetBIOS routing table.
MIB Object ID:	1.3.6.1.4.1.18.3.5.5.8.1.2

Parameter: Target Server

Default: None

Options: The name of a NetBIOS target server, specified as a string of up to 16 alphanumeric characters. You can include any printable character, including $, #, and so on. To specify a backslash, enter two backslashes (\\). You can also use the hexadecimal equivalent (*xx*) of any valid ASCII character. For example, you can specify \20 for space or \21 for ! Note that *xx* is counted as one character.

Function: Specifies the name of the NetBIOS target server.

Instructions: Enter the name or part of the name of the NetBIOS target server. The name can be up to 16 alphanumeric characters. Also, you can leave the field blank.

MIB Object ID: 1.3.6.1.4.1.18.3.5.5.8.1.4

Deleting a NetBIOS Static Route

To delete an IPX NetBIOS static route:

1. Select from the IPX NetBIOS Static Routes window the static route you want to delete from the node configuration.
2. Click on the Delete button in the NetBIOS Static Routes window (see Figure 3-9).

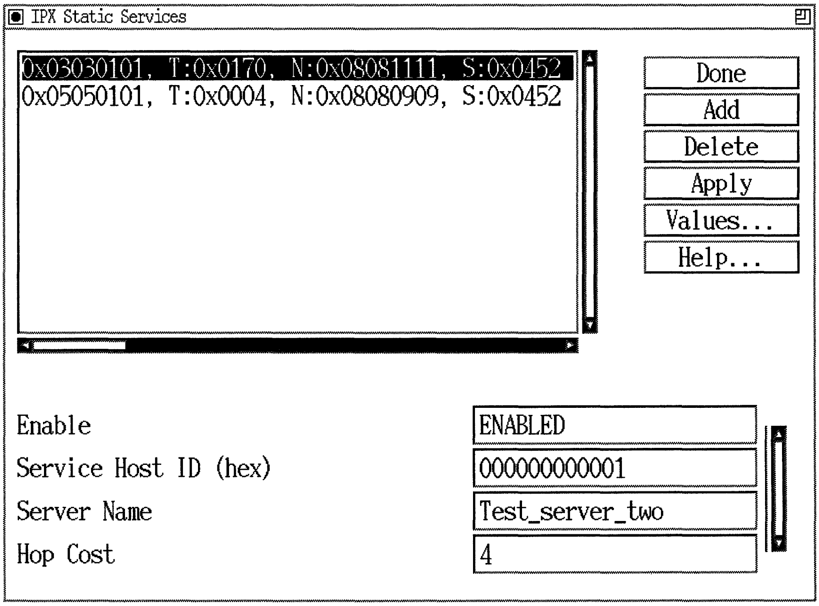
The system software deletes the NetBIOS static route entry you selected, and the entry disappears from the list of static routes in the IPX NetBIOS Static Routes window.

Editing Static Service Parameters

Once you add an IPX interface to a LAN circuit, you can use the Configuration Manager to add, edit, or delete static services on that interface. (For more information on static services, refer to Chapter 1.)

The static service provides an alternative to broadcasting Service Advertisement Protocol (SAP) announcements across a WAN. A static service instead advertises only to clients having access to the IPX interface you are configuring with this capability. The static service eliminates WAN traffic (and hence, the use of WAN bandwidth) associated with WAN SAP announcements.

You can add, edit, or delete static services through the IPX Static Services window. To access the window, begin at the Configuration Manager window (Figure 3-1) and select the Protocols→IPX→Static Services option. The IPX Static Services window shown in Figure 3-11 appears:



0x03030101, T:0x0170, N:0x08081111, S:0x0452
0x05050101, T:0x0004, N:0x08080909, S:0x0452

Enable ENABLED
Service Host ID (hex) 000000000001
Server Name Test_server_two
Hop Cost 4

Figure 3-11. IPX Static Services Window

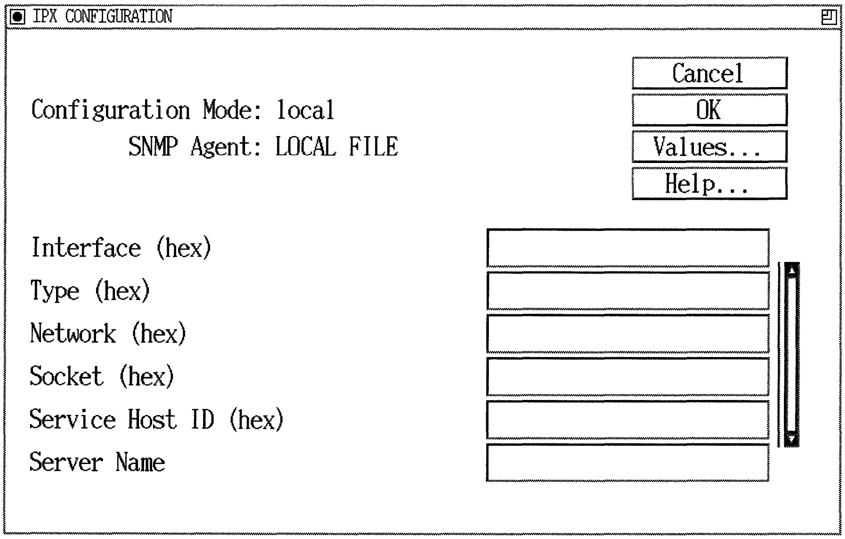
The IPX Static Services window displays each Server entry in the router configuration in hexadecimal notation, as follows:

<interface / network_number>,<type_of_service>, <network_address_of_service>,<socket_number_of_service>

Adding a Static Service

To add a static service, begin at the IPX Static Services window (see Figure 3-11) and proceed as follows:

1. Click on the Add button. The IPX Configuration window appears (see Figure 3-12):



IPX CONFIGURATION

Configuration Mode: local
SNMP Agent: LOCAL FILE

Figure 3-12. IPX Configuration Window

2. Edit the parameters, using the parameter descriptions that follow as guidelines.
3. Click on the OK button to save your entries to the configuration file.

The IPX Static Services window (Figure 3-11) reappears immediately after you click on the OK button.

IPX Static Service Configuration Parameter Descriptions

This section describes all parameters shown in the IPX Configuration window.

Parameter: Interface (hex)

Default: None

Options: Any valid IPX network number

Function: Specifies the network address of the next-hop IPX interface used to reach this static service.

Instructions: Enter an IPX network address of up to 8 hexadecimal characters.

MIB Object ID: 1.3.6.1.4.1.18.3.5.5.12.1.10

Parameter: Type (hex)

Default: None

Options: Any valid Novell server type number in 4-digit hexadecimal format. (The number must be a value between 0x0001 and 0xFFFE, inclusive.)

Function: Specifies the type of service to advertise from the associated IPX (LAN) interface.

Instructions: Enter the server type number in 4-digit hexadecimal format. Include leading zeros.

MIB Object ID: 1.3.6.1.4.1.18.3.5.5.12.1.3

Note: Refer to Table 3-1 for a current list of service types.

Table 3-1. Service Types and Identifiers

Service Type	Hexadecimal Identifier
Wild	FFFF
Unknown	0000
User	0001
User Group	0002
Print Queue	0003
NetWare File Server v3.x	0004
Job Server	0005
Gateway	0006
Print Server	0007
Archive Queue	0008
Archive Server	0009
Job Queue	000A
Administration	000B
Diagnostics	0017
NetBIOS	0020
NAS SNA Gateway	0021
NACS	0023
Remote Bridge Server	0024
Bridge Server	0026
TCP/IP Gateway (Racal-Datacom)	0027
Eicon X.25 Point-to-Point GW	0028

Table 3-1. Service Types and Identifiers *(continued)*

Service Type	Hexadecimal Identifier
Eicon 3270 Gateway	0029
(CHI) Corp	002A
Unknown	002C
Time Synchronization Server	002D
Archive Srvr Dynamic SAP/SMS TSA	002E
DI3270 Gateway	0045
Advertising Print Server	0047
TCP/IP Gateway (Racal-Datacom)	0048
Unknown	004A
Btrieve VAP 5.x	004B
NetWare SQL VAP/NLM	004C
Xtree Network Version	004D
Btrieve VAP 4.x	0050
QuickLink (Cubix)	0052
Print Queue User	0053
ARCserve VAP	0055
Eicon X.25 Multi-Point Gateway	0058
ARCserv	0064
ARCserve 3.0	0066
WANcopy Utility	0072
Cheyenne ARCserv 5.0 Intel	0077
TES-NetWare for VMS	007A

Table 3-1. **Service Types and Identifiers** *(continued)*

Service Type	Hexadecimal Identifier
Emerald Backup/WATCOM Debugger	0092
TES-NetWare for VMS	0095
NetWare Access Server (NAS)	0098
SQL Server (Named Pipes)	009A
NetWare Access Server	009B
Portable NetWare/SunLink NVT	009E
Progress Database Server	009F
PowerChute APC UPS NLM	00A1
Compaq IDA Status Monitor	00AC
Unknown	0100
Intel LAN Protect Bindery	0102
Oracle Database Server	0103
NetWare 386, Remote Console	0107
Novell SNA Gateway	010F
HP Print Server	0112
CSA MUX	0114
CSA LCA	0115
CSA CM	0116
CSA SMA	0117
CSA DBA	0118
CSA NMA	0119
CSA SSA	011A

Table 3-1. Service Types and Identifiers *(continued)*

Service Type	Hexadecimal Identifier
CSA STATUS	011B
CSA APPC	011E
SNA TEST (SAA profile)	0126
CSA TRACE	012A
Unknown	012E
Communications Executive	0130
NFS Domain Server	0133
NetWare Naming Service (NNS) Profile	0135
NNS Queue/NW Print Queue	0137
NNS Domain Scheme Descriptor	0138
Intel LANSpool VAP	0141
Aladdin Knowledge	0142
Optical drives	0143
IrmaLAN Gateway	0152
Named Pipe Server	0154
Intel PICKIT/CAS Talk Server	0168
Unknown (User)	0173
Compaq SNMP Agent	0174
Xtree Server	0180
Xtree	0189
NetWare Access Server	018A
GARP Gateway (Net Research)	01B0

Table 3-1. Service Types and Identifiers *(continued)*

Service Type	Hexadecimal Identifier
BindView (LAN Support Group)	01B1
Intel LanDesk Manager	01BF
Unknown	01CA
Shiva Netmodem	01CB
LanRover	01CC
Castelle FAXPress Server	01D8
Castelle LANPress Print Server	01DA
Unknown	01E4
Legato	01F0
Legato	01F1
SQL Server	0200
NMA Agent (NMS; socket 0x2F90)	0233
LANZ Agent (socket 0x401F; NetExp)	0237
LANZ Agent (socket 0x4800)	0238
NMS Hub Management	0239
LANZ Agent (socket 0x401F)	023A
NetWare SMS (Storage Management System)	023F
NetWare Connect	024E
NMS Console (name-stnMAC+IPX#)	026A
NW4 Time Sync Server (socket 0x040)	026B
NW4 NDS Server	0278
NetWare for SAA Gateway	0304

Table 3-1. Service Types and Identifiers *(continued)*

Service Type	Hexadecimal Identifier
Gallacticom BBS	030A
HP LaserJet (Quick Silver)	030C
Attachmate 3270 Gateway	0320
Multi Server Director	0327
Intel NetPort II	0361
ECS Cheyenne ARCserv 5.0 Intel	0375
Cheyenne ARC Serv 5.0 Intel SE	0376
PowerChute v3.0 (new)	037E
ViruSafe Notify	037F
HP Bridge	0386
HP Hub	0387
NetWare SAA Gateway	0394
Lotus Notes (OS/2 version)	039B
Central Point Anti Virus NLM	03B7
ARCserve 4.0 (socket 0x 8600)	03C4
Intel LANSpool 3.5	03C7
Lexmark 4033 Print Server	03D5
NetWare SQL/Gupta NLM	03DE
UnixWare	03E1
Unix Ware	03E4
NetWare File Server v4.x	0400
NetSprint print server	0414

Table 3-1. Service Types and Identifiers *(continued)*

Service Type	Hexadecimal Identifier
SiteLock Virus	0429
ARCserve 5.0	044C
Dell SCSI Array (SDA) Monitor	045B
SyBase	0474
SyBase	0475
Novix TCP/IP support NLM	04DC
SiteLock Checks	0520
Certus Anti Virus NLM (master)	0523
SiteLock Checks	0529
Delrina WinFax Pro network	0553
McAfee's NetShield anti-virus	0580
SiteLock	0B29
SiteLock Applications	0C29
SofTrack for NW v3.x	0C2C
LAI SiteLock	2380
Meeting Maker	238C
SofTrack for NW v4.x	2C0C
SiteLock Server (Brightworks)	4808
SiteLock User	5555
Tapeware	6312
Rabbit 3270 Gateway	6F00
Intel NetPort (Print Server)	8002

Table 3-1. Service Types and Identifiers *(continued)*

Service Type	Hexadecimal Identifier
WordPerfect Network Version	8008
Unknown	8069
Unknown	8746
McAfee's NetShield anti-virus	9000
SQL Monitor (IPX)	9604
Unknown	9892
Unknown	C00C
SiteLock Metering VAP/NLM	F11F
SiteLock	F1FF
SQL Server (IPX)	F503

Parameter:	**Network (hex)**
Default:	None
Options:	Any valid IPX network address in hexadecimal notation. Use a value of 0 only if the interface is IPXWAN (RFC1362-compliant).
Function:	Specifies the network address of this service.
Instructions:	Enter a network address of up to 8 hexadecimal characters. The path to the network you specify for this service must exist as an entry in the IPX routing tables. The entry can be learned dynamically by the router, or you can configure the entry as a static service.
MIB Object ID:	1.3.6.1.4.1.18.3.5.5.12.1.4

Parameter:	**Socket (hex)**
Default:	None
Options:	Any valid socket address. (The number must have a value between 0x0001 and 0xFFFE, inclusive.)
Function:	Specifies the socket address of this service.
Instructions:	Enter any valid socket address consisting of up to 4 hexadecimal characters.
MIB Object ID:	1.3.6.1.4.1.18.3.5.5.12.1.6

Parameter: **Service Host ID (hex)**

Default: None

Options: The address (host ID) of the service you want to advertise from the IPX interface you are configuring with this capability.

Function: Specifies the address of a remote IPX host (a NetWare server) that can provide local clients with specific NetWare services, such as file, print, gateway, or terminal server services.

Instructions: Enter a string of up to 12 hexadecimal characters (6 bytes) as the address (host ID) of the remote IPX host/server.

MIB Object ID: 1.3.6.1.4.1.18.3.5.5.12.1.5

Parameter:	**Server Name**
Default:	None
Options:	Any valid Novell NetWare server name
Function:	Specifies a name for the service you want to advertise.
Instructions:	Enter a name that is unique among all names assigned to IPX servers of the same type on the IPX internetwork. See the documentation that came with your NetWare operating system for guidelines on specifying a server name.
MIB Object ID:	1.3.6.1.4.1.18.3.5.5.12.1.7

Editing Static Service Parameters

You can customize or edit the configurable parameters of a static service entry for a particular IPX interface.

Note: The Configuration Manager does not allow you to change the Interface, Type, Network, and Socket parameters you set when you added the static service you now want to further customize or edit. To establish new values for these parameters for a particular static service, you must delete that service and configure a new service. You can, however, reconfigure all other parameters associated with a static service.

To edit the configurable parameters associated with an existing static service, begin at the Configuration Manager window (Figure 3-1) and select the Protocols→IPX→Static Service option. The IPX Static Services window appears, as shown in Figure 3-11. From this window, proceed as follows:

1. Select the static service you want to edit by clicking on the appropriate entry in the list of static services.

2. Click on any parameter value you want to change; then enter a new value.
3. Click on the Apply button to save your changes.
4. Click on the Done button to exit the IPX Static Services window.

IPX Static Service Parameter Descriptions

This section describes how to set all parameters shown on the IPX Static Services window.

Parameter: **Enable**

Default: Enable

Options: Enable | Disable

Function: Enables or disables a static service previously added to a specific IPX interface.

Instructions: Select Enable to re-enable a static service previously disabled. This restores client access to NetWare services configured earlier on the IPX interface.

Disable a static service to make NetWare services configured earlier unavailable to clients.

MIB Object ID: 1.3.6.1.4.1.18.3.5.5.12.1.2

Parameter: **Service Host ID (hex)**

Default: None

Options: The address (host ID) of the server or service you want to advertise from the IPX (LAN) interface you are configuring with this capability.

Function: Specifies the address of a remote IPX host (a NetWare server) that can provide local clients with specific NetWare services, such as file, print, gateway, or terminal server services.

Instructions: Enter a string of up to 12 hexadecimal characters (6 bytes) as the address (host ID) of the remote IPX host/server.

MIB Object ID: 1.3.6.1.4.1.18.3.5.5.12.1.5

Parameter: **Server Name**

Default: None

Options: Any valid Novell NetWare server name

Function: Specifies a name for the service you want to advertise.

Instructions: Enter a name that is unique among all names assigned to IPX servers of the same type on the IPX internetwork.

See the documentation that came with your NetWare operating system for guidelines on specifying a server name.

MIB Object ID: 1.3.6.1.4.1.18.3.5.5.12.1.7

Parameter: **Hop Cost**

Default: None

Range: Any valid number of hops, from 1 to 15.

Function: Specifies the number of subsequent router hops required from this router to reach a specific remote Novell server or service.

Instructions: Enter the number of router hops that exist between the service you want to advertise and the clients that require that service.

MIB Object ID: 1.3.6.1.4.1.18.3.5.5.12.1.8

Deleting a Static Service

To delete a static service:

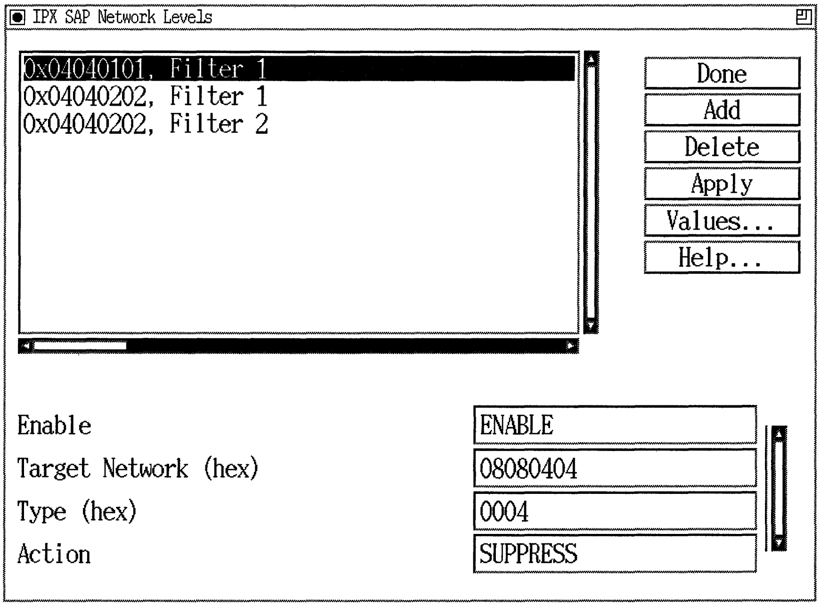
1. Select from the IPX Static Services window the static service you want to delete from the node configuration.
2. Click on the Delete button in the IPX Static Services window (see Figure 3-11).

The system software deletes the static service entry you selected, and the entry disappears from the list of static services in the IPX Static Services window.

Editing SAP Network-Level Filter Parameters

SAP network-level filters allow you to reduce IPX SAP network traffic by configuring network-level SAP filters.

You can add, edit, and delete up to 150 network-level SAP filters for each interface. You perform these functions from the IPX SAP Network Levels window. Begin at the Configuration Manager window (Figure 3-1) and select the Protocols→IPX→SAP Net Levels option. The IPX SAP Network Levels window appears (see Figure 3-13).



0x04040101, Filter 1
0x04040202, Filter 1
0x04040202, Filter 2

Enable ENABLE
Target Network (hex) 08080404
Type (hex) 0004
Action SUPPRESS

Figure 3-13. IPX SAP Network Levels Window

The IPX SAP Network Levels window displays each network-level SAP filter entry in the router configuration, as follows:

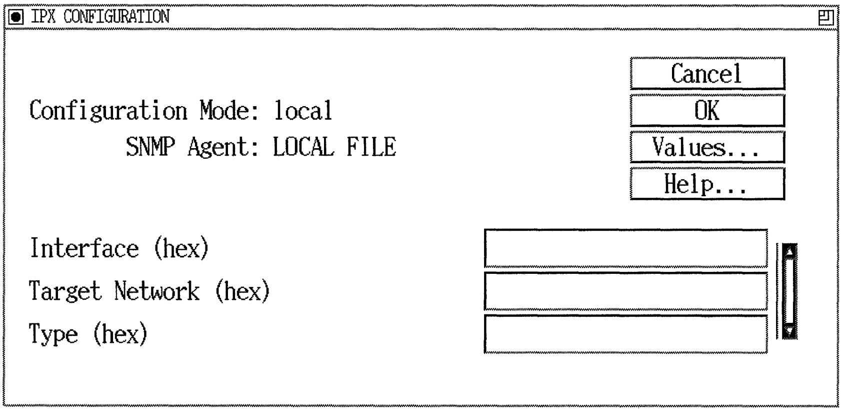
<interface / network_number>,<filter_no.>

Adding a SAP Network-Level Filter

To add a network-level SAP filter, first obtain the hexadecimal address of an interface that requires a new filter from the IPX Interfaces window (Figure 3-3). Then, begin at the IPX SAP Network Levels window (see Figure 3-13) and proceed as follows:

1. Click on the Add button.

   The IPX Configuration window appears (see Figure 3-14).



Configuration Mode: local
SNMP Agent: LOCAL FILE

Interface (hex)
Target Network (hex)
Type (hex)

Figure 3-14. IPX Configuration Window

2. Enter the hexadecimal address of the target IPX interface.
3. Enter the network address of a service that the SAP network-level filter should recognize.

4. Enter the type of network service that the SAP network-level filter should recognize. (The filter should allow any frames that contain the target network address and service type information you specified in Steps 3 and 4 onto the segment associated with the interface specified in Step 2.)
5. Click on the OK button to save your entry and exit the window.

SAP Network-Level Filter Configuration Parameters

This section describes all parameters shown in the IPX Configuration window.

Parameter: **Interface (hex)**

Default: None

Options: Any valid interface address in hexadecimal notation

Function: Specifies the address of the interface to which you are adding a network-level SAP filter. (You can obtain the address from the IPX Interfaces window, as illustrated in Figure 3-3.)

Instructions: Enter an interface address of up to 8 hexadecimal characters.

MIB Object ID: 1.3.6.1.4.1.18.3.5.5.9.1.6

Parameter: **Target Network (hex)**

Default: None

Options: Any valid IPX network address in hexadecimal notation

Function: Specifies the network address of the service that the SAP filter should recognize in its criteria for allowing certain SAP broadcasts to pass to the locally attached network segment.

Instructions: Enter a network address of up to 8 hexadecimal characters. You can specify all networks by entering FFFFFFFF. A hexadecimal value of 0 is invalid.

MIB Object ID: 1.3.6.1.4.1.18.3.5.5.9.1.3

Parameter:	**Type (hex)**
Default:	None
Options:	Any valid Novell server type number in 4-digit hexadecimal format
Function:	Specifies the type of server that the filter should recognize in its criteria for allowing certain SAP broadcasts to pass to the locally attached network segment.
Instructions:	Enter the server type number in 4-digit hexadecimal format. Include leading 0s. For all types, enter a value of FFFF. See Table 3-1 for a list of valid server types.
MIB Object ID:	1.3.6.1.4.1.18.3.5.5.9.1.4

Editing a SAP Network-Level Filter

You can customize or edit the configurable parameters of a SAP network-level filter for a particular IPX interface.

Note: The Configuration Manager does not allow you to change the Interface parameter you set in the IPX Configuration window. To establish a new value for the Interface parameter for a particular network-level SAP filter, you must delete that filter and configure a new filter. You can, however, reconfigure all other parameters associated with a network-level SAP filter.

To edit the configurable parameters associated with an existing network-level SAP filter, begin at the Configuration Manager window (Figure 3-1) and select the Protocols→IPX→SAP Net Levels option. The IPX SAP Network Levels window appears, as shown in Figure 3-13. From this window, proceed as follows:

1. Select the filter you want to edit by clicking on the appropriate entry in the list of network-level SAP filters.

2. Click on any parameter value you want to change; then enter a new value.
3. Click on the Apply button to save your changes.
4. Click on the Done button to exit the IPX SAP Network Levels window.

IPX SAP Network-Level Filter Parameter Descriptions

This section describes all parameters shown in the IPX SAP Network Levels window.

Parameter:	**Enable**
Default:	Enable
Options:	Enable | Disable
Function:	Specifies whether the network-level SAP filter displayed is active on this interface.
Instructions:	Select Enable to enable the network-level SAP filter. Select Disable to disable the network-level SAP filter.
MIB Object ID:	1.3.6.1.4.1.18.3.5.5.9.1.2

Parameter:	**Target Network (hex)**
Default:	None
Options:	Any valid network address in hexadecimal notation
Function:	Specifies the network address of the service that the SAP filter should recognize in its criteria for allowing certain SAP broadcasts to pass to the locally attached network segment.
Instructions:	Enter a network address of up to 8 hexadecimal characters. You can specify all networks by entering FFFFFFFF. A hexadecimal value of 0 is invalid.
MIB Object ID:	1.3.6.1.4.1.18.3.5.5.9.1.3

Parameter:	**Type (hex)**
Default:	None
Options:	Any valid Novell server type number in 4-digit hexadecimal format.
Function:	Specifies the type of server that the filter should recognize in its criteria for allowing certain SAP broadcasts to pass to the locally attached network segment.
Instructions:	Enter the server type number in 4-digit hexadecimal format. Include leading 0s. For all types, enter a value of FFFF. See Table 3-1 for a list of valid server types.
MIB Object ID:	1.3.6.1.4.1.18.3.5.5.9.1.4

Parameter:	**Action**
Default:	Advertise
Options:	Advertise | Suppress
Function:	Specifies how to process any SAP advertisement that matches the SAP filter criteria you established in the Network Number and service Type parameters.
Instructions:	Select Advertise to enable the filter to allow advertisement of services that match the SAP filter criteria you established in the Network Number and service Type parameters. Select Suppress to configure the IPX router to drop SAP advertisements that match the SAP filter criteria you established in the Network Number and server Type parameters.
MIB Object ID:	1.3.6.1.4.1.18.3.5.5.9.1.5

Deleting a SAP Network-Level Filter

To delete a SAP network-level filter:

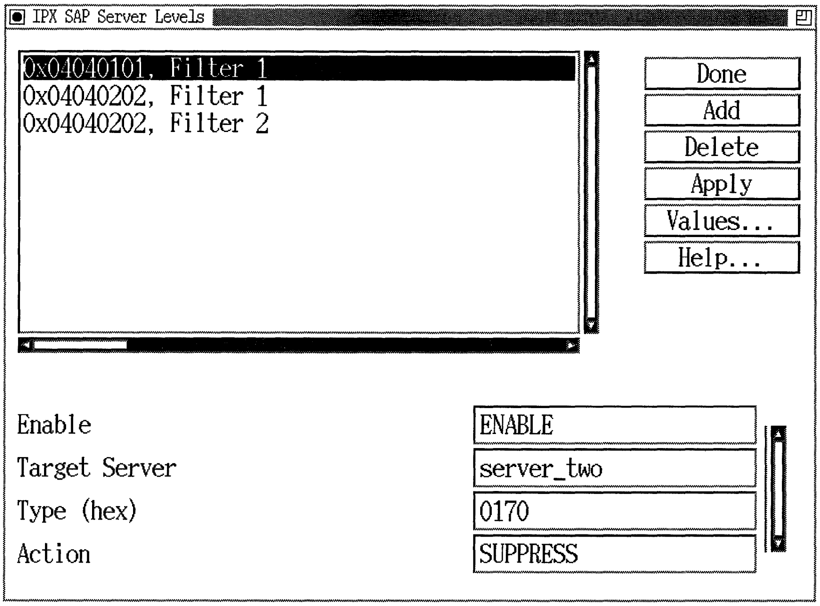
1. Select from the IPX SAP Network Levels window the filter you want to delete from the node configuration.
2. Click on the Delete button in the IPX SAP Network Levels window (see Figure 3-13).

The system software deletes the filter entry you selected, and the entry disappears from the list of SAP network-level filters in the IPX SAP Network Levels window.

Editing SAP Server-Level Filter Parameters

The SAP server-level filters function allows you to reduce network traffic by configuring server-level SAP filters.

You can add, edit, and delete up to 150 server-level SAP filters for each interface. You perform these functions from the IPX SAP Server Levels window. Begin at the Configuration Manager window (Figure 3-1) and select the Protocols➔IPX➔SAP Server Levels option. The IPX SAP Server Levels window appears (see Figure 3-15).



0x04040101, Filter 1
0x04040202, Filter 1
0x04040202, Filter 2

Enable: ENABLE
Target Server: server_two
Type (hex): 0170
Action: SUPPRESS

Figure 3-15. IPX SAP Server Levels Window

The IPX SAP Server Levels window displays each server-level SAP filter entry in the router configuration as follows:

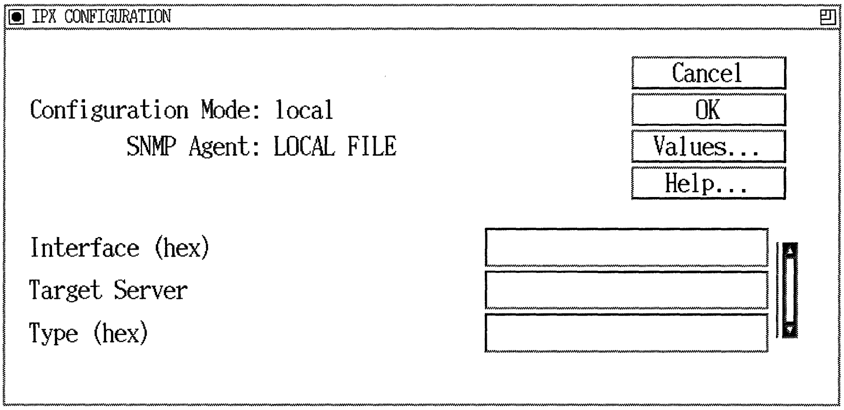
<interface / network_number>, filter <filter_no.>

Adding a SAP Server-Level Filter

To add a SAP server-level filter, first obtain from the IPX Interfaces list window the hexadecimal address of an interface that requires a server-level filter. Then, begin at the IPX SAP Server Levels window (see Figure 3-15) and proceed as follows:

1. Click on the Add button.

   The IPX Configuration window appears (see Figure 3-16):



IPX CONFIGURATION

Configuration Mode: local
SNMP Agent: LOCAL FILE

Interface (hex)
Target Server
Type (hex)

Figure 3-16. IPX Configuration Window

2. Enter a value for the Interface parameter.
3. Enter the name of the service (Target Server) that the SAP server-level filter should recognize.
4. Enter the type of service that the SAP server-level filter should recognize. (The filter should allow any frames that contain the target server name and service type information you specified in Steps 3 and 4 onto the segment associated with the interface specified in Step 2.)
5. Click on the OK button to save your entry and exit the IPX Configuration window.

Note: Site Manager does not allow you to create duplicate server-level SAP filters for the same interface.

IPX Server-Level Filter Configuration Parameter Descriptions

This section describes all parameters shown in the IPX Configuration window.

Parameter:	**Interface (hex)**
Default:	None
Options:	Any valid interface address in hexadecimal notation
Function:	Specifies the address of the interface for which you are adding a server-level SAP filter.
Instructions:	Enter an interface address of up to 8 hexadecimal characters.
MIB Object ID:	1.3.6.1.4.1.18.3.5.5.10.1.6

Parameter:	**Target Server**
Default:	None
Options:	Any valid Novell server name
Function:	Specifies the name of the service that the SAP filter should recognize in its criteria for allowing certain SAP broadcasts to pass to the locally attached network segment.
Instructions:	Enter a Novell server name. See the documentation that came with your NetWare operating system for guidelines on specifying a server name.
MIB Object ID:	1.3.6.1.4.1.18.3.5.5.10.1.3

Parameter:	**Type (hex)**
Default:	None
Options:	Any valid Novell server type number in 4-digit hexadecimal format
Function:	Specifies the type of server that the filter should recognize in its criteria for allowing certain SAP broadcasts to pass to the locally attached network segment.
Instructions:	Enter the server type number in 4-digit hexadecimal format. Include leading 0s. For all types, enter a value of FFFF. See Table 3-1 for a list of valid server types.
MIB Object ID:	1.3.6.1.4.1.18.3.5.5.10.1.4

Editing a SAP Server-Level Filter

You can edit the configurable parameters of a server-level SAP filter entry in the node configuration.

Note: Configuration Manager does not allow you to change the Interface parameter you set in the IPX Configuration window. To establish new values for the Interface parameter for a particular server-level SAP filter, you must delete that filter and configure a new filter. You can, however, reconfigure all other parameters associated with a server-level SAP filter.

To edit the configurable parameters associated with an existing server-level SAP filter, begin at the Configuration Manager window (Figure 3-1) and select the Protocols→IPX→SAP Server Levels option. The IPX SAP Server Levels window appears, as shown in Figure 3-15. From this window, proceed as follows:

1. Select the filter you want to edit by clicking on the appropriate entry in the list of filters.

2. Click on any parameter value you want to change, then enter a new value.
3. Click on the Apply button to save your changes.
4. Click on the Done button to exit the IPX SAP Server Levels window.

IPX SAP Server-Level Parameter Descriptions

This section describes how to set all parameters shown on the IPX SAP Server Levels window.

Parameter:	**Enable**
Default:	Enable
Range:	Enable | Disable
Function:	Specifies whether the server-level SAP filter displayed is active on this interface.
Instructions:	Select Enable to enable the server-level SAP filter. Select Disable to disable the server-level SAP filter.
MIB Object ID:	1.3.6.1.4.1.18.3.5.5.10.1.2

Parameter: Target Server

Default: None

Options: Any valid server name that is compatible with Novell

Function: Specifies the name of the service that the SAP filter should recognize in its criteria for allowing certain SAP broadcasts to pass to the locally attached network segment.

Instructions: Enter a server name that is compatible with Novell. See the documentation that came with your NetWare operating system for guidelines on specifying a server name.

MIB Object ID: 1.3.6.1.4.1.18.3.5.5.10.1.3

Parameter: Type (hex)

Default: None

Options: Any valid Novell server type number in 4-digit hexadecimal format.

Function: Specifies the type of server that the filter should recognize in its criteria for allowing certain SAP broadcasts to pass to the locally attached network segment.

Instructions: Enter the server type number in 4-digit hexadecimal format. Include leading 0s. For all types, enter a value of FFFF. See Table 3-1 for a list of valid server types.

MIB Object ID: 1.3.6.1.4.1.18.3.5.5.10.1.4

Parameter: Action

Default: Advertise

Options: Advertise | Suppress

Function: Specifies how to process any SAP advertisement that matches the SAP filter criteria you establish in the Target Server and server Type parameters.

Instructions: Select Advertise to enable the interface associated with the filter to route SAP advertisements that match the SAP filter criteria you established in the Target Server and server Type parameters.

Select Suppress to configure the IPX router to drop SAP advertisements that match the SAP filter criteria you established in the Target Server and server Type parameters.

MIB Object ID: 1.3.6.1.4.1.18.3.5.5.10.1.5

Deleting a SAP Server-Level Filter

To delete a SAP server-level filter:

1. Select from the IPX SAP Server Levels window (Figure 3-15) the filter you want to delete from the node configuration.
2. Click on the Delete button in the IPX SAP Server Levels window.

The system software deletes the filter entry you selected, and the entry disappears from the list of server-level SAP filters in the IPX SAP Server Levels window.

Deleting IPX from the Wellfleet Router

To delete IPX from the router, begin at the Configuration Manager window (Figure 3-1) and complete the following steps:

1. Select the Protocols→IPX→Delete IPX option.

   A confirmation window appears.

2. Select OK.

   The Configuration Manager window appears.

   IPX is no longer configured on the Wellfleet router.

Note: If you delete IPX, the connectors for those interfaces on which IPX was the *only* protocol enabled are no longer highlighted in the Configuration Manager window. Interfaces must be reconfigured for these connectors; see *Configuring Wellfleet Routers* for instructions.

Index

Bay Networks

The Merged Company of SynOptics and Wellfleet

8 Federal Street
Billerica, MA 01821

Printed in U.S.A. on Recycled Paper