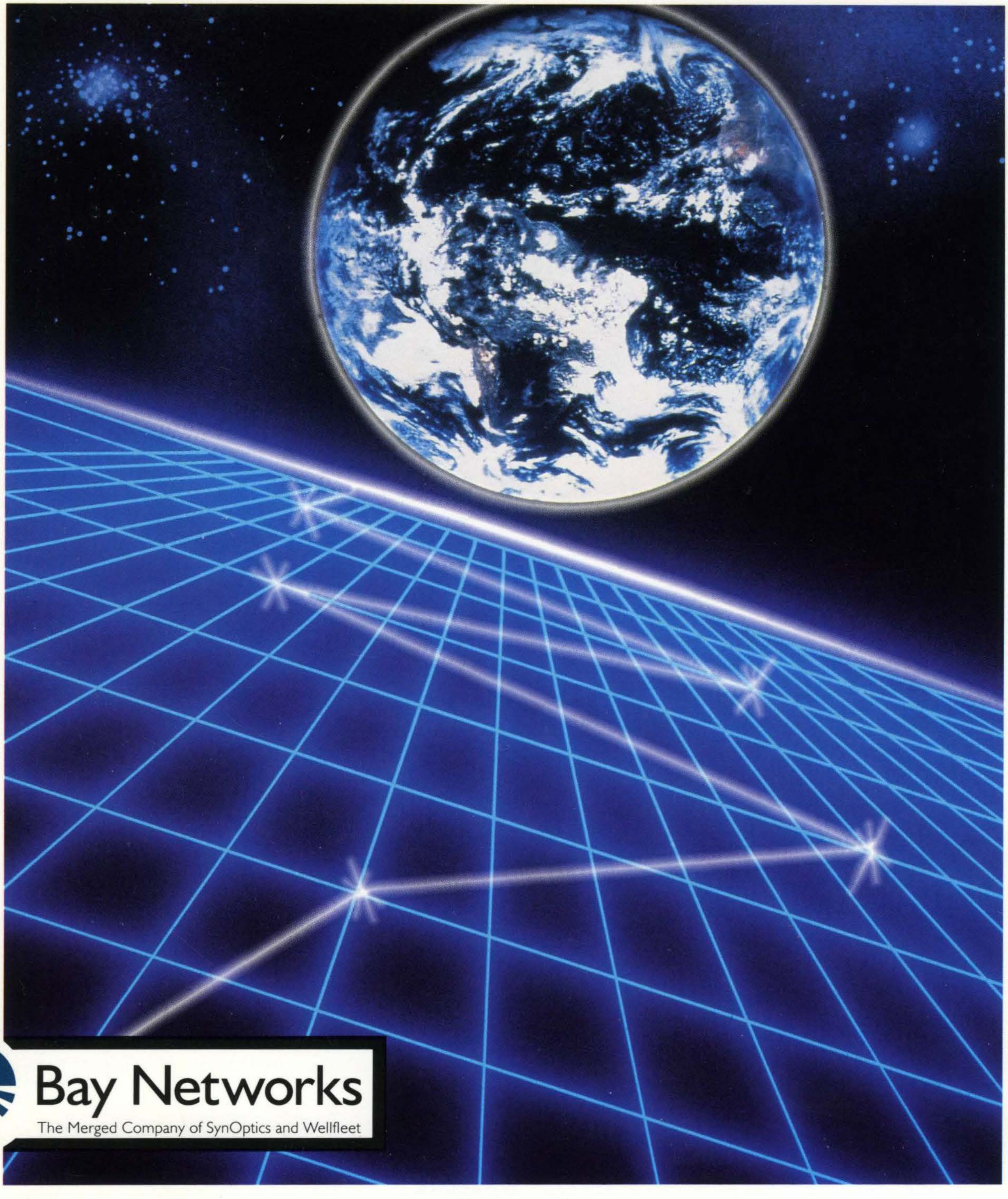



# Customizing Bridging Services

Part No. 110078 A

# Customizing Bridging Services

Router Software Version 8.10
Site Manager Software Version 2.10

Part No. 110078 Rev. A
February 1995

Bay Networks
The Merged Company of SynOptics and Wellfleet

**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
## Using Transparent Bridge Services

## Chapter 2
## Using Source Routing Bridge Services

## Chapter 4
## **Using Translation Bridge Services**

## Chapter 5
## **Using Native Mode LAN Services**



## Index

## Figures

# About This Guide

If you are responsible for configuring and managing Wellfleet® routers, you need to read this guide.

This guide describes how to customize Wellfleet router software for bridging services.

Refer to this guide for details on customizing

- Transparent bridge services (see the "Using Transparent Bridge Services" chapter)
- Source routing bridge services (see the "Using Source Routing Bridge Services" chapter)
- NetBIOS™ services (see the "Using NetBIOS Services" chapter)
- Translation bridge services (see the "Using Translation Bridge Services" chapter)

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

- Initially configuring and saving a bridging 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 bridging 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➔AppleTalk identifies the AppleTalk option in the Protocols menu. |
| **command text** | Denotes command names in text. Example: Use the **xmodem** command. |
| *italic text* | Indicates variable values in command syntax descriptions, new terms, file and directory names, and book titles. |
| `screen text` | Indicates data that appears on the screen. Example: `Set Trap Monitor Filters` |
| quotation marks (" ") | Indicate the title of a chapter or section within a book. |

| | |
|---|---|
| vertical line ( \| ) | Indicates that you enter only one of the parts of the command. The vertical line separates choices. Do not type the vertical line when entering the command.<br>Example: If the command syntax is<br>**show at routes \| nets**, you enter either<br>**show at routes** or **show at nets**, but not both. |

# Acronyms

| | |
|---|---|
| APE | all-paths explorer (frame) |
| ARE | all-routes explorer (frame) |
| ARP | Address Resolution Protocol |
| BPDU | bridge protocol data unit |
| CUGID | closed user group ID |
| DA | destination address |
| DLCI | data link connection identifier |
| DLSw | data link switching |
| DSAP | destination service access point |
| FCS | frame check sequence |
| FDDI | Fiber Distributed Data Interface |
| IEEE | Institute of Electrical and Electronic Engineers |
| IP | Internet Protocol |
| IPX | Internet Packet Exchange |
| LLC | logical link control |
| LNM | LAN Network Manager |
| MAC | media access control |
| MIB | Management Information Base |
| MTU | maximum transmission unit |
| NetBIOS | Network Basic Input/Output System |
| NML | Native Mode LAN |
| OUI | organizationally unique identifier |

| | |
|---|---|
| PPP | Point-to-Point Protocol |
| RFC | Request for Comments |
| RIF | routing information field |
| SA | source address |
| SAP | service access point |
| SMDS | Switched Multimegabit Data Services |
| SNAP | Subnetwork Access Protocol |
| SR | source routing |
| SRF | specifically routed frame |
| SSAP | session service access point |
| STE | spanning tree explorer (frame) |
| TB | transparent bridging |
| XNS | Xerox Networking System |

# Chapter 1
# Using Transparent Bridge Services

This chapter

- Contains an overview of the transparent bridge, including details on how the spanning tree algorithm works
- Describes how to edit transparent bridge parameters, using the Configuration Manager tool

# Transparent Bridge Overview

Transparent bridges are data-link layer relay devices that connect two or more networks. They use media access control (MAC) source and destination addresses to relay frames between connected networks.

**Note:** We use the terms *bridge* and *transparent bridge* interchangeably throughout this chapter.

The transparent bridge provides three primary services:

- Learns the addresses of endstations on connected networks
- Forwards or drops frames based on knowledge it acquires about endstation addresses or user-configured filters
- Ensures a loop-free topology throughout the extended network, using the spanning tree algorithm

A transparent bridge also provides some translation services, converting frames for bridging between Ethernet/802.3 LANs and FDDI LANs. Refer to "The Translation Process," later in this chapter for details on translation services.

## How the Bridge Works

The bridge receives and examines every frame transmitted on the networks to which it is attached. It learns endstation addresses by reading the source address of the endstation that transmitted the frame, and noting which LAN received the frame. The bridge enters this information into a data structure called the *forwarding table*, which the bridge constantly updates.

For example in Figure 1-1, if Node 2 transmits a frame onto the network, the bridge receives the frame and makes an update to its forwarding table. The bridge indicates whether Node 2 is in the direction of LAN A.

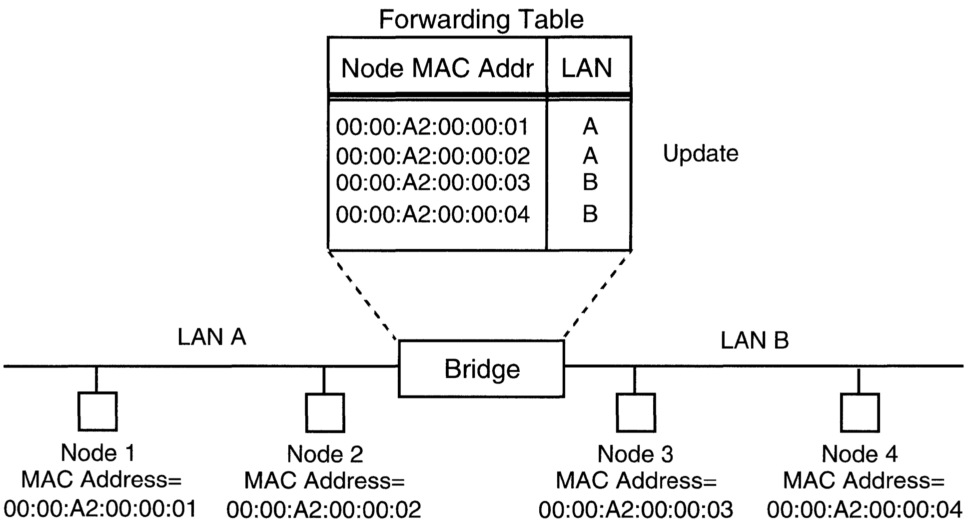



**Figure 1-1. Forwarding Table Update**

The bridge then forwards (relays to another network) or drops (discards) the frame based on the forwarding table entries. When the bridge receives a frame, it compares the frame's destination address with addresses in the forwarding table. One of these situations results:

- If the frame's destination address is on the same LAN as its source address, the bridge discards the frame; all nodes on that LAN already received this frame.
- If the frame's destination address is on a different LAN than its source address, the bridge forwards the frame to that LAN.
- If there is no match for the frame's destination address in the forwarding table, the bridge forwards the frame to all networks except the one that received the frame. This is called *flooding*.
- If the frame is destined for the bridge (for example, a spanning tree frame), the bridge forwards the frame to the appropriate bridge entity and processes it internally.

**Note:** If a frame is forwarded or flooded to a LAN using a different data-link level protocol, the bridge translates the frame to the appropriate frame format before transmission.

## The Translation Process

The transparent bridge translates frames for bridging between Ethernet or 802.3 LANs and Fiber Distributed Data Interface (FDDI) LANs. When the transparent bridge receives Ethernet or 802.3 frames destined for an FDDI LAN, it reformats those frames to the FDDI MAC frame format. The transparent bridge sets the original MAC type of the frame in the logical link control (LLC) header. Therefore, if the frame passes through a second FDDI-to-Ethernet/802.3 bridge, that bridge can translate the frame back to its original format.

- The bridge translates all Ethernet MAC frames to FDDI MAC and Institute of Electrical and Electronic Engineers (IEEE) 802.2 LLC/ Subnetwork Access Protocol (SNAP) encapsulation as specified by RFC 1042. Protocols in this category include DECnet™ Phase IV, Novell®, AppleTalk® Phase I and II, Xerox® Networking System (XNS™), Internet Package Exchange (IPX®), and Internet Protocol (IP).

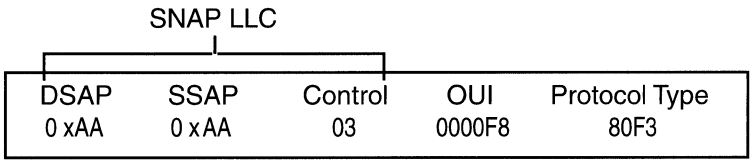
  Figure 1-2 shows the format and values of the LLC and SNAP headers of these frames after translation.

| SNAP LLC | | | | |
|---|---|---|---|---|
| DSAP | SSAP | Control | OUI | Protocol Type |
| 0 xAA | 0 xAA | 03 | 000000 | (Original Type) |

**Figure 1-2. RFC 1042 Encapsulation**

However, AppleTalk Address Resolution Protocol (ARP) frames (Ethernet frames with a protocol type equal to 80F3) require special translation by the Bridge Tunnel Service.

Figure 1-3 illustrates the LLC and SNAP headers of the AppleTalk ARP outbound frame after the Bridge Tunnel Service translation.

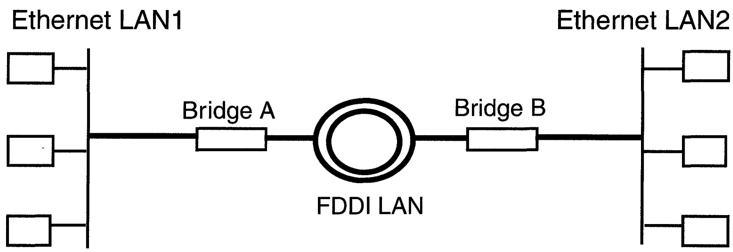



**Key**
SNAP = Subnetwork Access Protocol
LLC = logical link control
DSAP = destination service access point
SSAP = session service access point
OUI = organizationally unique identifier

**Figure 1-3. Bridge Tunnel Service Encapsulation**

- The bridge translates all IEEE 802.2 LLC by removing the length field. Protocols in this category include AppleTalk Phase 2, Novell™ Proprietary, and IP.

  Figures 1-4 and 1-5 illustrate different LAN configurations and show how Bridge A translates different types of frames originating on LAN 1 for transmission across the FDDI LAN.




## Ethernet to FDDI Translation

From Ethernet LAN

| DA | SA | TYPE =80F3 | DATA | FCS |
|---|---|---|---|---|

→ Through Bridge A to FDDI LAN

| DA | SA | SNAP LLC | | | OUI | | | TYPE =80F3 | DATA | FCS |
|---|---|---|---|---|---|---|---|---|---|---|
| | | AA | AA | 03 | 00 | 00 | 00 | | | |

Bridge A

- Extracts addressing information from the Ethernet header.
- Incorporates address information into newly generated FDDI MAC header.
- Encapsulates Ethernet data according to RFC 1042.
- Recalculates frame check sequence (FCS).

## Ethernet (AppleTalk ARP) to FDDI Translation

From Ethernet LAN

| DA | SA | TYPE =80F3 | DATA | FCS |
|---|---|---|---|---|

→ Through Bridge A to FDDI LAN

| DA | SA | SNAP LLC | | | OUI | | | TYPE =80F3 | DATA | FCS |
|---|---|---|---|---|---|---|---|---|---|---|
| | | AA | AA | 03 | 00 | 00 | F8 | | | |

Bridge A

- Extracts addressing information from the Ethernet header.
- Incorporates address information into newly generated FDDI MAC header.
- Encapsulates Ethernet within a SNAP header with an organizationally unique identifier (OUI) of 0000F8. This identifies a tunnel-encapsulated frame, specified in IEEE Draft Recommended Practice 802.1H.
- Recalculates FCS.

**Figure 1-4. Ethernet to FDDI Translation**

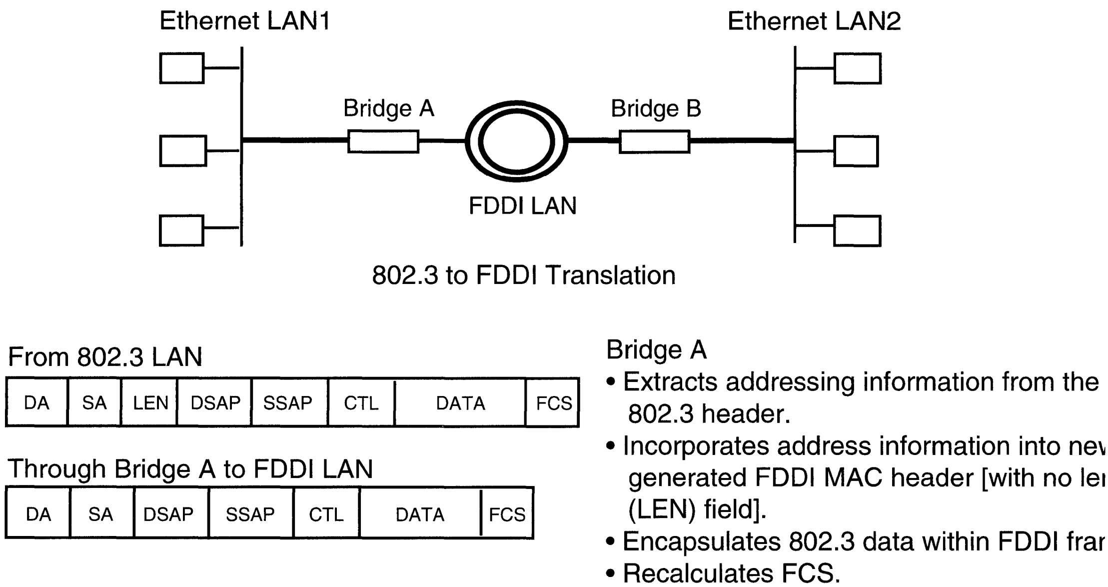



**Figure 1-5. Ethernet/802.3 to FDDI Translation**

The translation process from the FDDI LAN to Ethernet/802.3 LAN (the process Bridge B performs in Figures 1-4 and 1-5) is a mirror image of the translation process occurring on Bridge A, with one exception: the bridge translates an AppleTalk ARP frame that originates on the FDDI LAN and is destined for an 802.3 LAN as shown in Figure 1-6.

AppleTalk ARP frame originating on FDDI LAN

| DA | SA | SNAP LLC | | | OUI | TYPE | DATA | FCS |
|---|---|---|---|---|---|---|---|---|
| | | AA | AA | 03 | = 00 00 00 | =80F3 | | |

Through Bridge B to 802.3 LAN

| DA | SA | LEN | SNAP LLC | | | OUI | TYPE | DATA | FCS |
|---|---|---|---|---|---|---|---|---|---|
| | | | AA | AA | 03 | = 00 00 00 | =80F3 | | |

Bridge B

- Extracts addressing information from the FDDI MAC header
- Incorporates address information into newly generated 802.3 header
- Adds a length field
- Encapsulates FDDI data according to RFC 1042
- Recalculates FCS

**Figure 1-6. AppleTalk ARP (Originating on FDDI) to 802.3 Translation**

## Spanning Tree Algorithm

The spanning tree algorithm ensures the existence of a loop-free topology in networks that contain parallel bridges. (Refer to *Source Routing Appendix to IEEE Standard 802.1d Media Access Control (MAC) Bridges* for details on the spanning tree algorithm.) A loop occurs when there are alternate routes between hosts. If there is a loop in an extended network, bridges may forward traffic indefinitely. This can result in increased traffic and degradation in network performance.

Figure 1-7 shows an example of a network containing a loop: two parallel bridges, Bridge 1 and Bridge 2, connect LANs A and B.

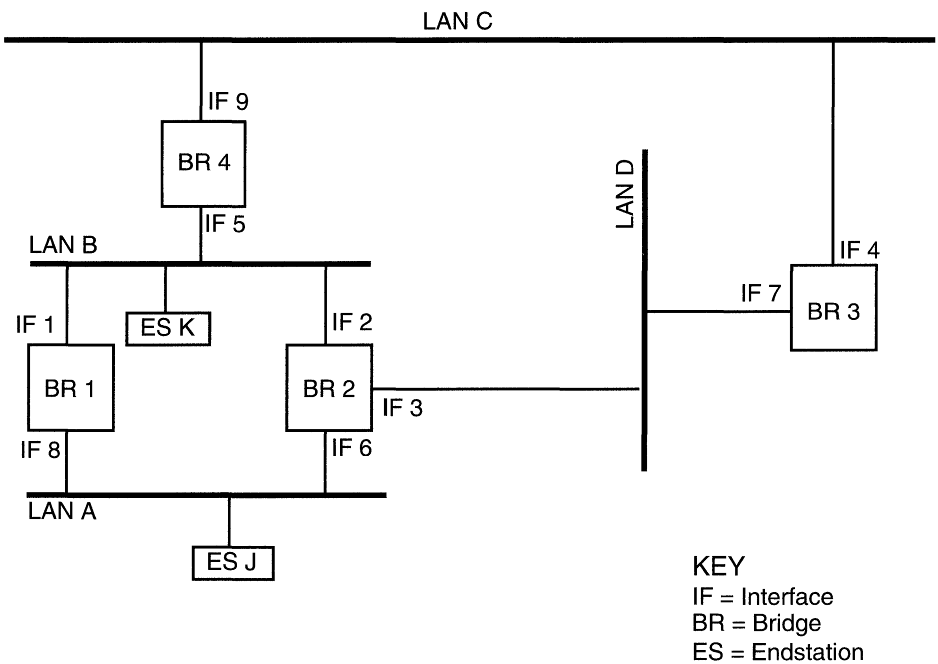



**Figure 1-7. Parallel Bridge Topology**

When Endstation J initially sends a frame to Endstation K, both Bridge 1 and Bridge 2 read the frame. Since this is the first frame sent between J and K, there is no forwarding table entry for J or K on either of the bridges. Each bridge updates its forwarding table to indicate that Endstation J is in the direction of LAN A. Then, each bridge floods the frame: Bridge 1 forwards the frame over Interface 1 and Bridge 2 forwards the frame over Interface 2. Bridge 2 also forwards the frame over Interface 3; however, to simplify the example, we do not trace this frame.

Next, Endstation K receives two copies of the frame, resulting in an inefficient use of the available bandwidth. More serious, however, is the effect of duplicate frames on the two bridges. The frame flooded by Bridge 1 onto Interface 1 is ultimately read by Bridge 2 on Interface 2. When Bridge 2 reads this frame, it updates its forwarding table to indicate that Endstation J is in the direction of LAN B. Similarly, Bridge 1 reads the frame flooded by Bridge 2 and updates its forwarding table to show that Endstation J is in the direction of LAN B. Consequently, the forwarding tables of both bridges are now corrupted and neither bridge can properly forward a frame to Endstation J.

You can eliminate this problem by implementing the spanning tree algorithm, which produces a logical tree topology out of any arrangement of bridges. The result is that a single path exists between any two endstations on an extended network. The spanning tree algorithm also provides a high degree of fault tolerance. It allows the network to automatically reconfigure the spanning tree topology if there is a bridge or data-path failure.

The spanning tree algorithm requires five values to derive the spanning tree topology. The first, a multicast address specifying all bridges on the extended network, is media-dependent and is automatically determined by the software. You assign the remaining four values, which are

- Network-unique identifier for each bridge on the extended network
- Unique identifier for each bridge/LAN interface (called a port)
- Priority specifying the relative priority of each port
- Cost for each port

After you assign these values, bridges multicast and process formatted frames (called Bridge Protocol Data Units, or BPDUs) to derive a single loop-free topology throughout the extended network. The bridges exchange BPDU frames quickly, minimizing the time that service is unavailable between hosts.

In constructing a loop-free topology, the bridges within the extended network follow these steps:

1. Elect a root bridge.

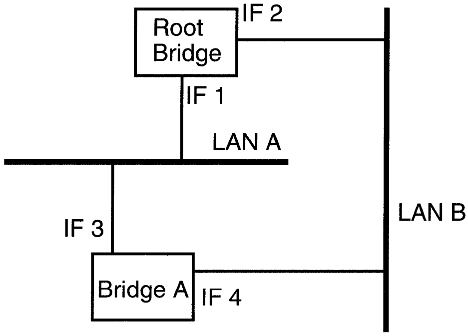
   The bridge with the lowest priority value becomes the root bridge and serves as the root of the loop-free topology. If priority values are equal, the bridge with the lowest bridge MAC address becomes the root bridge.

2. Determine path costs.

   The path cost is the cost of the path to the root bridge offered by each bridge port.

3. Select a root port and elect a designated bridge on each LAN.

   Each bridge designates the port that offers the lowest-cost path to the root bridge as the root port. In the event of equal path costs, the bridge examines the paths' interfaces to the root bridge. The port (interface) of the path with the lowest interface priority to the root bridge becomes the root port. For example, Figure 1-8 shows how Bridge A determines its root port.




Given:

Path costs from IF 3 to root bridge and from IF 4 to root bridge are equal.

---------AND--------

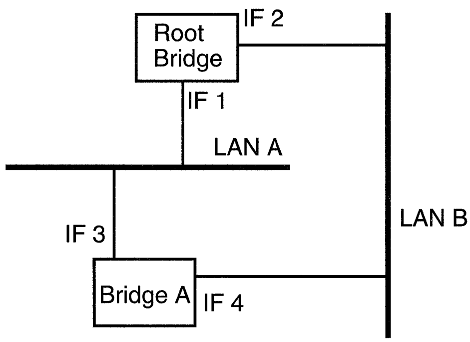
IF 1 = priority 1
IF 2 = priority 2
IF 3 = priority 3
IF 4 = priority 4

Then:

IF 3 becomes root port because IF1's priority is lower than IF 2's priority.

**Figure 1-8. Root Port Determination (Equal Path Costs)**

If the paths' interfaces to the root bridge are also equal, then the root port is the port on the bridge with the lowest priority value (for example, refer to Figure 1-9).




Given:

Path costs from IF 3 to root bridge and from IF 4 to root bridge are equal.

---------AND--------

IF 1 = priority 1 — Same priority
IF 2 = priority 1 — Same priority
IF 3 = priority 3
IF 4 = priority 2

Then:

IF 4 becomes root port because it has a better priority than IF3.

**Figure 1-9. Root Port Determination (Equal Path Costs and Root Interface Priorities)**

The spanning tree algorithm selects a bridge on each LAN as the designated bridge. The root port of this bridge has the lowest-cost path to the root bridge. All bridges turn off (set to blocking state) all of the lines except for the single line that is the shortest-cost path to the root, and any line attached to the LANs for which the bridge serves as a designated bridge.

4. Elect a designated port.

   The spanning tree algorithm selects the port that connects the designated bridge to the LAN as the designated port. If there is more than one such port, the spanning tree algorithm selects the port with the lowest priority as the designated port. This port, which carries all extended network traffic to and from the LAN, is in the forwarding state.

Thus, the spanning tree algorithm removes all redundant ports (ports providing parallel connections) from service (places in the blocking state). If there is a topological change or a bridge or data-path failure, the algorithm derives a new spanning tree that may move some ports from the blocking to the forwarding state.

For example, in Figure 1-7, if all path costs are equal and Bridge 2 has the lowest-bridge priority, followed by Bridge 3, then Bridge 4, then Bridge 1, the spanning tree algorithm may block Bridge 1/Interface 8 and Bridge 4/Interface 9 from service.

Figure 1-10 shows the resulting logical topology, which provides a loop-free topology with only a single path between any two hosts.

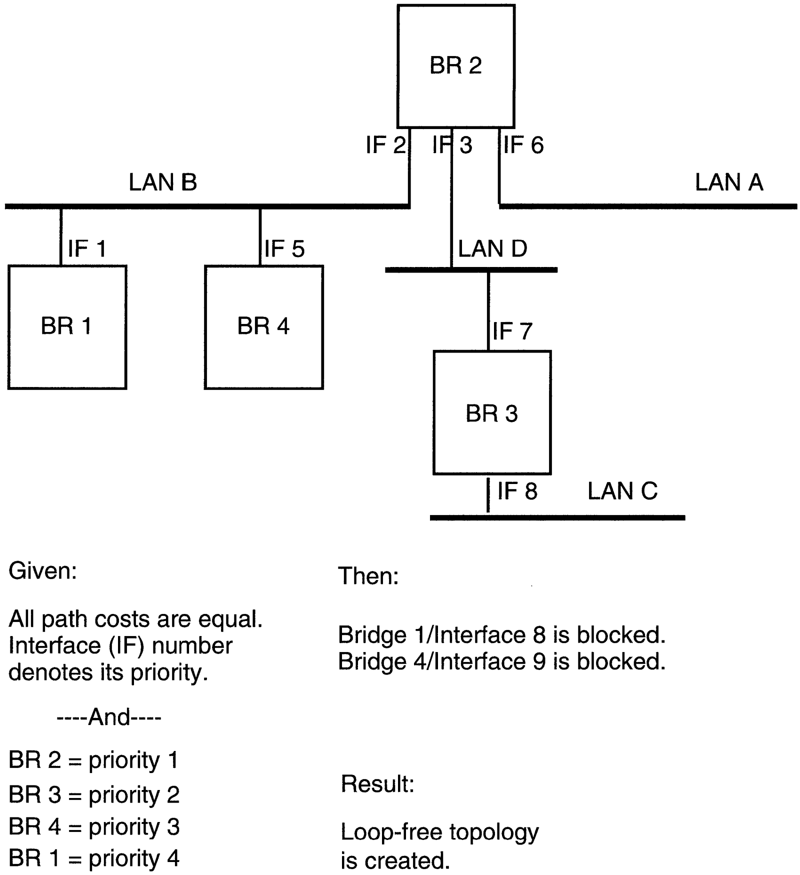
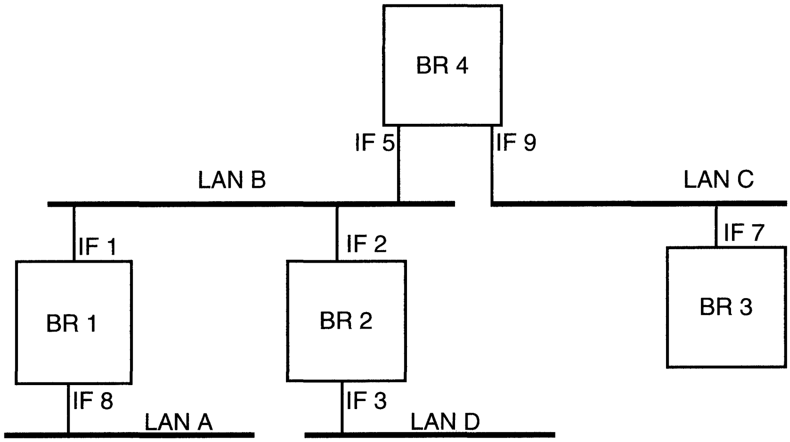



**Figure 1-10. Spanning Tree (Loop-Free) Logical Topology**

It is very important to configure the spanning tree parameters correctly. Consider the typical flow of traffic so that the logical topology that results from the spanning tree algorithm is appropriate for the network.

If, in the network shown in Figure 1-7, a majority of traffic originates on LAN A and is destined for LAN D, it is not practical to set the spanning tree parameters as shown in Figure 1-11. This figure exemplifies an inefficient spanning tree topology for this network because the traffic from LAN A must traverse Bridge 1, LAN B, and Bridge 2 to get to LAN D. LAN B is then congested with unnecessary traffic.




Given:

All path costs are equal.
Interface (IF) number denotes its priority.

----And----

BR 4 = priority 1
BR 3 = priority 2
BR 2 = priority 3
BR 1 = priority 4

Then:

Bridge 2/Interface 6 is blocked.
Bridge 3/Interface 7 is blocked.

Result:

Inefficient spanning tree topology is created.

**Figure 1-11. Inefficient Spanning Tree Topology**

## Filtering Frames

You use filters mainly for security reasons. They enable the bridge to relay or drop a particular frame based on user-selectable fields within each of the four encapsulation methods supported by the bridge. These encapsulation methods are

- Ethernet
- IEEE 802.2 logical link control
- IEEE 802.2 LLC with SNAP header
- Novell proprietary

Refer to *Configuring Filter Options for Wellfleet Routers* for details about filters and how to configure them for the bridge.

# Editing Bridge Parameters

Once you configure a circuit to support the bridge and, optionally, the spanning tree algorithm, you use the Configuration Manager tool to edit the bridge and spanning tree parameters.

This section describes how to access and edit these parameters. The instructions in this section assume that you already configured the bridge on the router. If you did not, refer to *Configuring Wellfleet Routers* for details on configuring the bridge.

**Note:** If you enable the spanning tree algorithm for your network, the algorithm reconverges if you dynamically change any of the parameters described in the following sections.

You access all bridge parameters from the Configuration Manager window (Figure 1-12). (Refer to *Using Site Manager Software* guide for details on accessing this window.

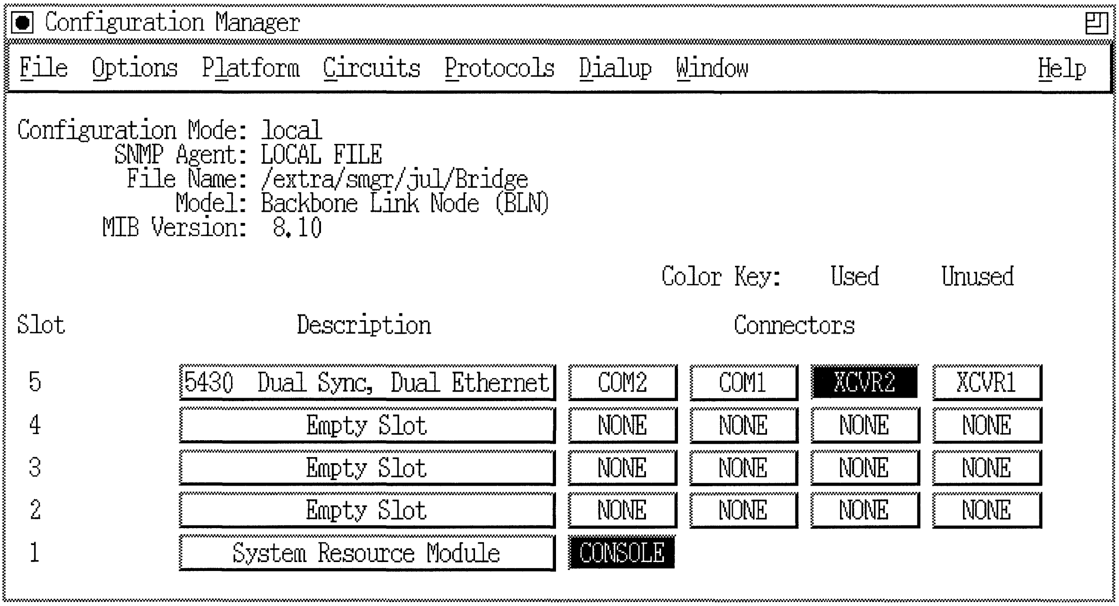



**Figure 1-12. Configuration Manager Window**

For each bridge parameter, this section provides details on the default setting, valid parameter options, 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 details on using the Technician Interface to access the MIB, refer to *Using Technician Interface Software*.

## Editing Bridge Global Parameters

To edit the bridge global parameters:

1. Select Protocols→Bridge→Global from the Configuration Manager window (refer to Figure 1-12). The Edit Bridge Global Parameters window appears (Figure 1-13).

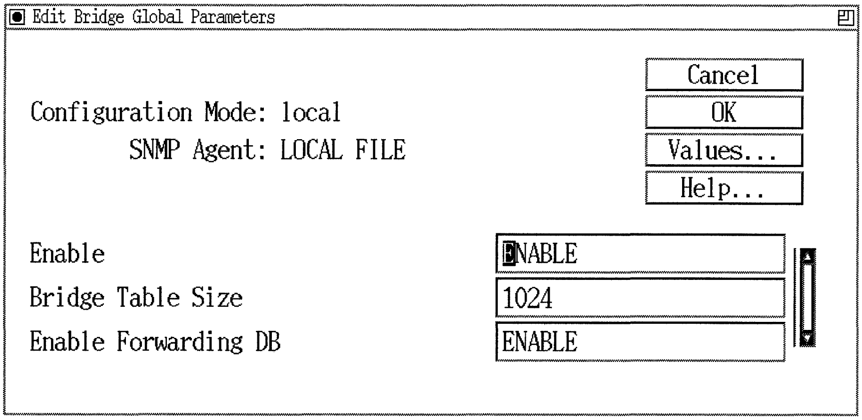



**Figure 1-13. Edit Bridge Global Parameters Window**

2. Edit the parameters, using the descriptions in the next section as a guide.

3. Click on the OK button to save your changes and exit the window. Site Manager returns you to the Configuration Manager window.

## Bridge Global Parameter Descriptions

Use these parameter descriptions as a guide when you configure the parameters in the Edit Bridge Global Parameters window (refer to Figure 1-13).

| | |
|---|---|
| **Parameter:** | **Enable** |
| Default: | Enable |
| Options: | Enable \| Disable |
| Function: | Enables or disables bridging on the entire router. |
| Instructions: | Set to Disable if you want to disable bridging for all circuits on the router. |
| MIB Object ID: | 1.3.6.1.4.1.18.3.5.1.1.1.1.2 |

**Parameter:** **Bridge Table Size**

Default: 1024 entries

Options: 1024 | 2048 | 4096 | 8192 | 16384 | 32768 | 65536 | 131072

Function: Specifies the maximum number of MAC address entries allowed in the forwarding table. If you enter an invalid value, the system rounds up or down from the invalid value to the nearest valid value.

If you increase the number of table entries, the bridge is more efficient but uses more memory.

If you save a change to this parameter in dynamic mode, the bridge disables and then re-enables itself, thereby deleting all previously learned addresses.

Instructions: Specify the table size, after accounting for the number of protocols running on your router and the size of the bridged network.

Select the 131072 option only if the router is running IP Host Only and no other protocols are running on the router. If you select 131072, the system automatically disables the next parameter, Enable Forwarding DB.

MIB Object ID: 1.3.6.1.4.1.18.3.5.1.1.1.1.5

**Parameter:** **Enable Forwarding DB**

Default: Enable

Options: Enable | Disable

Function: If you enable this parameter, the bridge maintains an additional table, equal in size to the forwarding table plus dynamically allocated memory for each MAC address. This additional table contains each MAC address in the forwarding table and the port from which the bridge learned the address. The table allows you to access MAC addresses and ports.

If you change the setting of this parameter in dynamic mode, the bridge disables and re-enables itself. If you change the setting to disable, the bridge deletes all previously learned addresses, including those in the forwarding table.

Instructions: Leave this parameter enabled if you want to view the MAC addresses in the forwarding table or the ports from which the bridge learned the addresses.

Disable this parameter if you need to improve bridge performance.

MIB Object ID: 1.3.6.1.4.1.18.3.5.1.1.1.1.6

## Editing Bridge Interface Parameters

To edit bridge interface parameters:

1. Select Protocols→Bridge→Interfaces from the Configuration Manager window (refer to Figure 1-12). The Bridge Interfaces window appears (Figure 1-14).

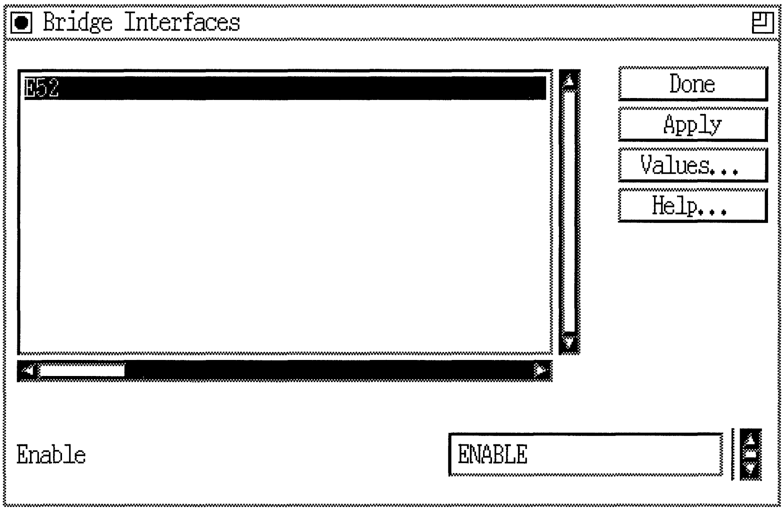



**Figure 1-14. Bridge Interfaces Window**

2. Select the interface you want to edit.
3. Edit the parameters, using the descriptions in the next section as a guide.
4. Click on the Apply button to save your changes.
5. Click on the Done button to exit the window. Site Manager returns you to the Configuration Manager window.

## Bridge Interface Parameter Descriptions

Use these parameter descriptions as a guide when you configure the parameters in the Bridge Interfaces window (refer to Figure 1-14).

**Parameter:** **Enable**

Default: If you added bridging using either the Quick Start procedure or the configuring circuits procedure, this parameter defaults to Enable. If you previously used this parameter to disable bridging on this circuit, the parameter defaults to Disable.

Options: Enable | Disable

Function: Toggles bridging on and off for this circuit only.

Instructions: This parameter does not allow you to add bridging to this circuit. To add the bridging protocol to this circuit, you must use the Configuration Manager (see *Configuring Wellfleet Routers*).

Set this parameter to either Enable or Disable.

MIB Object ID: 1.3.6.1.4.1.18.3.5.1.1.3.1.2

| | |
|---|---|
| **Parameter:** | **Translation Bridge Enable** |
| Default: | Disable |
| Options: | Enable \| Disable |
| Function: | Specifies whether this transparent bridge interface participates in a transparent-to-source-routing translation-bridged network. Make sure you enable only one interface for translation bridging and you disable this parameter for all other interfaces. Otherwise, translation bridging does not occur. |
| Instructions: | Set this parameter to Enable or Disable, depending on your interface. |
| MIB Object ID: | 1.3.6.1.4.1.18.3.5.1.1.3.1.9 |

## Editing Spanning Tree Global Parameters

To edit the spanning tree global parameters:

1. Select Protocols→Bridge→Spanning Tree→Global from the Configuration Manager window (refer to Figure 1-12). The Edit Spanning Tree Global Parameters window appears (Figure 1-15).

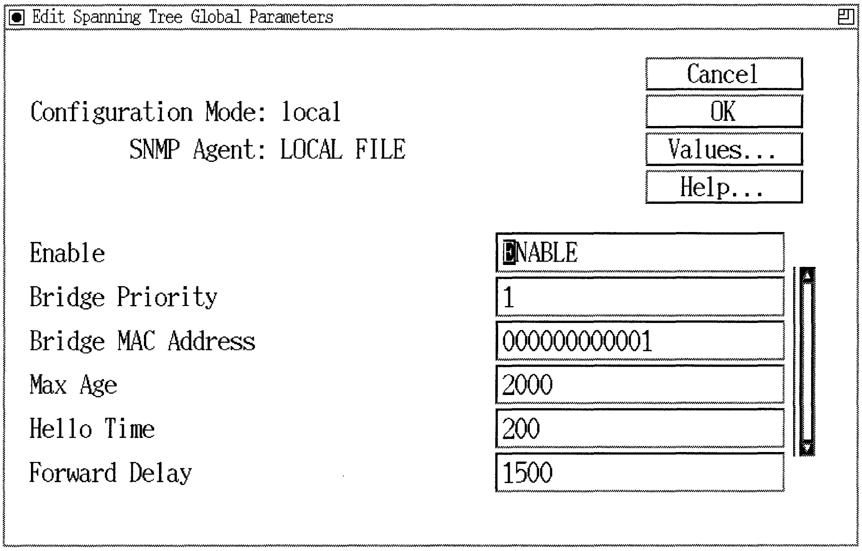



**Figure 1-15. Edit Spanning Tree Global Parameters Window**

2. Edit the parameters, using the descriptions in the next section as a guide.
3. Click on the OK button to save your changes and exit the window. Site Manager returns you to the Configuration Manager window.

## Spanning Tree Global Parameter Descriptions

Use these parameter descriptions as a guide when you configure the parameters in the Edit Spanning Tree Global Parameters window (refer to Figure 1-15).

| | |
|---|---|
| **Parameter:** | **Enable** |
| Default: | Enable |
| Options: | Enable \| Disable |
| Function: | Enables or disables spanning tree on the entire router. |
| Instructions: | Set to Disable if you want to disable spanning tree for the entire router, or to Enable if you want to enable spanning tree for the entire router. |
| MIB Object ID: | 1.3.6.1.4.1.18.3.5.1.2.1.2 |

| | |
|---|---|
| **Parameter:** | **Bridge Priority** |
| Default: | Defaults to the bridge priority that you set when you added spanning tree to this circuit. |
| Options: | 0 to 65535 (expressed as a decimal value) |
| Function: | The bridge priority and bridge MAC address form a bridge ID. The bridge ID provides a unit of comparison for use with the Spanning Tree Protocol. The root bridge is the bridge ID with the lowest value. Because of its significance in the bridge ID, the bridge priority strongly influences root bridge selection. The lower the bridge priority, the more likely that the spanning tree algorithm chooses the bridge as the Root Bridge. If there are equal bridge priority values, the bridge MAC address determines the bridge's priority; the lower the address, the higher the priority. |
| Instructions: | Either accept the current bridge priority value or assign a new one. |
| MIB Object ID: | 1.3.6.1.4.1.18.3.5.1.2.1.5 |

| | |
|---|---|
| **Parameter:** | **Bridge MAC Address** |
| Default: | Defaults to the bridge MAC address that was set when you added spanning tree to this circuit. |
| Options: | Any MAC address that is unique to the network (expressed as a 12-digit hexadecimal value) |
| Function: | The bridge priority and bridge MAC address form a bridge ID. The bridge ID provides a unit of comparison for use with the Spanning Tree Protocol. The root bridge is the bridge ID with the lowest value. Because of its significance in the bridge ID, the bridge priority strongly influences root bridge selection. The lower the bridge priority, the more likely that the spanning tree algorithm chooses the bridge as the Root Bridge. If there are equal bridge priority values, the bridge MAC address determines the bridge's priority; the lower the address, the higher the priority.<br><br>We recommend that you set this parameter to the MAC address of one of this bridge's spanning tree ports (preferably the one with the lowest priority). |
| Instructions: | Either accept the current bridge MAC address or enter a new one. |
| MIB Object ID: | 1.3.6.1.4.1.18.3.5.1.2.1.5 |

**Note:** We recommend that you do not change the following three spanning tree parameters (Max Age, Hello Time, and Forward Delay) unless absolutely necessary. However, if you do change them, you must follow these guidelines:

> 2 x (Forward Delay – 1 Second) ≥ Max Age
>
> Max Age ≥ 2 x (Hello Time + 1 Second)

If the values for Max Age, Hello Time, and Forward Delay are not the same for each bridge in your network, the root bridge parameters rule the entire topology.

| | |
|---|---|
| **Parameter:** | **Max Age** |
| Default: | 20 seconds (expressed in hundredths of a second: 2000) |
| Range: | 6 to 40 seconds |
| Function: | Specifies the maximum number of seconds that the router considers protocol information (BPDUs) valid. After this specified amount of time, the router times out and discards the information.<br>We recommend that you accept this default value; however, if you change it, you must follow the guidelines listed previously in this section. |
| Instructions: | Either accept the default value or specify a new value in the Max Age box. Make sure to express any new value in hundredths of a second. |
| MIB Object ID: | 1.3.6.1.4.1.18.3.5.1.2.1.15 |

| | |
|---|---|
| **Parameter:** | **Hello Time** |
| Default: | 2 seconds (expressed in hundredths of a second: 200) |
| Range: | 1 to 10 seconds |
| Function: | Specifies the interval in seconds between BPDUs transmitted by the bridge. BPDUs are periodic transmissions exchanged between bridges in the network to convey configuration and topology change data.<br><br>We recommend that you accept the default value; however, if you change it, you must follow the guidelines listed previously in this section. |
| Instructions: | Either accept the default value or enter a new value in the Hello Time box. Make sure you enter the new value in hundredths of a second. |
| MIB Object ID: | 1.3.6.1.4.1.18.3.5.1.2.1.16 |

| | |
|---|---|
| **Parameter:** | **Forward Delay** |
| Default: | 15 seconds (expressed in hundredths of a second: 1500) |
| Range: | 4 to 30 seconds |
| Function: | Specifies the time in seconds that a circuit spends in the listening and learning states. If you set this parameter to the minimum value, the spanning tree converges at its fastest rate.<br><br>As the spanning tree algorithm operates, it eventually places all circuits in either a forwarding (enabled) or blocking (disabled) state. In response to network topology changes, the spanning tree algorithm may change the state of specific circuits. To prevent network looping caused by sudden state changes, the spanning tree algorithm does not transition circuits directly |

from the blocking to forwarding state. Rather, it places them in two intermediate states: listening and learning.

In the listening (stand-by) state, the circuit listens for network-generated BPDUs. It receives and drops all other traffic. When the forward delay timer expires, the spanning tree algorithm places the circuit in the learning state.

In the learning state, the circuit receives both network-generated BPDUs, and endstation-generated traffic that is subjected to the learning process but is not relayed. When the forward delay timer expires, the spanning tree algorithm places the circuit in the forwarding state.

We recommend that you accept the default, 15 seconds; however, if you change the value, you must follow the guidelines listed previously in this section.

Instructions: Either accept the default value or enter a new value in the Forward Delay box. Make sure you enter the new value in hundredths of a second.

MIB Object ID: 1.3.6.1.4.1.18.3.5.1.2.1.17

## Editing Spanning Tree Interface Parameters

To edit spanning tree interface parameters:

1. Select Protocols➔Bridge➔Spanning Tree➔Interfaces from the Configuration Manager window (refer to Figure 1-12). The Spanning Tree Interfaces window appears (Figure 1-16).

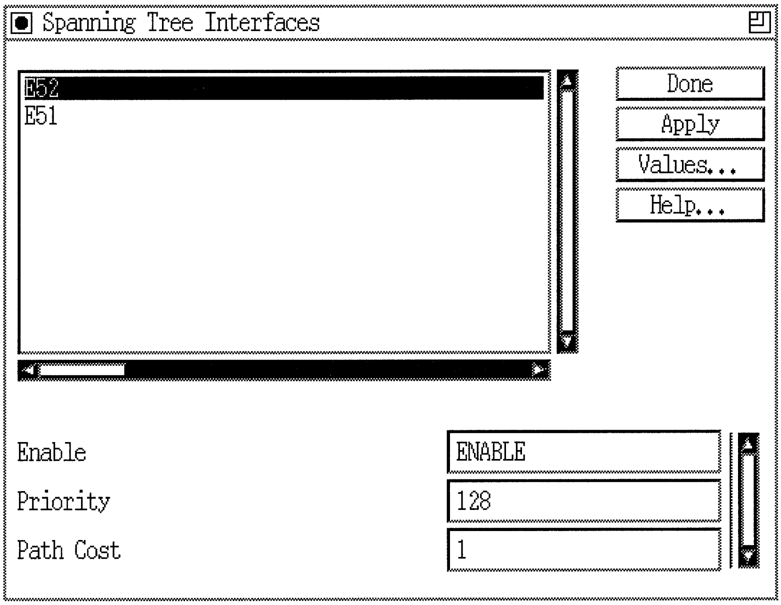



**Figure 1-16. Spanning Tree Interfaces Window**

2. Select the interface you want to edit.
3. Edit the parameters, using the descriptions in the next section as a guide.
4. Click on the Apply button to save your changes.
5. Click on the Done button to exit the window. Site Manager returns you to the Configuration Manager window.

## Spanning Tree Interface Parameter Descriptions

Use these parameter descriptions as guide when you configure the parameters on the Spanning Tree Interfaces window (refer to Figure 1-16).

| | |
|---|---|
| **Parameter:** | **Enable** |
| Default: | If you added spanning tree using either the Quick Start procedure or the configuring circuits procedure, this parameter defaults to Enable. If you previously used this parameter to disable spanning tree on this circuit, the parameter defaults to Disable. |
| Options: | Enable \| Disable |
| Function: | Toggles spanning tree on and off for this circuit only. |
| Instructions: | This parameter does not allow you to add spanning tree to this circuit. To add the spanning tree to this circuit, you must use the Configuration Manager. (Refer to *Configuring Wellfleet Routers* for details.) |
| Instructions: | Set this parameter to either Enable or Disable. |
| MIB Object ID: | 1.3.6.1.4.1.18.3.5.1.2.2.1.2 |

| | |
|---|---|
| **Parameter:** | **Priority** |
| Default: | 128 |
| Range: | 0 to 255 |
| Function: | Assigns a priority to a bridge port. This interface priority value and the bridge ID (bridge priority + bridge MAC address) determine whether this port becomes the designated port when the spanning tree algorithm converges. The lower the priority value, the higher the priority, and the more likely that this port is the designated port. |
| Instructions: | Either accept the default value or enter a new value in the Priority box. |
| MIB Object ID: | 1.3.6.1.4.1.18.3.5.1.2.2.1.4 |

| | |
|---|---|
| **Parameter:** | **Path Cost** |
| Default: | 1 |
| Range: | 1 to 65535 |
| Function: | When this port is the root port, the path cost is the contribution of the path through this port to the total cost of the path to the root for this bridge. When this port is not the root port, the path cost is added to the designated cost for the root port and is used as the value of the root path cost offered in all configuration BPDUs transmitted by the bridge.<br><br>To determine the path cost, we recommend that you use this formula:<br><br>Interface Path Cost = 1000/Attached LAN speed in Mb/s |
| Instructions: | Enter a path cost value in the Path Cost box. For example, enter 100 if the attached LAN is Ethernet (1000/10 = 100). |
| MIB Object ID: | 1.3.6.1.4.1.18.3.5.1.2.2.1.7 |

| | |
|---|---|
| **Parameter:** | **Translation Bridge Enable** |
| Default: | Disable |
| Options: | Enable \| Disable |
| Function: | Specifies whether the spanning tree protocol is part of the transparent-to-source-routing translation bridged network for this interface. |
| Instructions: | Set to Enable or Disable, depending on your network. |
| MIB Object ID: | 1.3.6.1.4.1.18.3.5.1.2.2.1.15 |

## Flushing the Forwarding Table

You can clear (flush) all MAC addresses from the bridge's forwarding table without bringing the bridge down and back up. This function is only available when you configure the bridge in dynamic mode.

To flush the tables, select the Protocols→Bridge→Flush FWD Tables option from the Configuration Manager window (refer to Figure 1-12). The system unlearns all MAC addresses it previously stored in its forwarding table and then displays a confirmation message.

# Deleting the Bridge and Spanning Tree from the Router

To delete the bridge or spanning tree from all Wellfleet router circuits on which you enabled them:

1. Select Protocols→Bridge→Delete Bridge from the Configuration Manager window (refer to Figure 1-12) to delete the bridge and spanning tree (if you enabled it). Or, if you want to delete the spanning tree only, select Protocols→Bridge→Spanning Tree→Delete Spanning Tree from this window.

   A pop-up window appears asking whether you really want to delete the bridge or spanning tree.

2. Click on the OK button. Site Manager returns you to the Configuration Manager window. The bridge and/or spanning tree is no longer configured on the Wellfleet router.

If you deleted the bridge, the connectors for those circuits on which the bridge was the only protocol enabled are no longer highlighted in the Configuration Manager window. You must reconfigure the circuits for these connectors. (Refer to *Configuring Wellfleet Routers* for details on configuring the connectors.)

# Chapter 2
# Using Source Routing Bridge Services

This chapter

- Contains an overview of source routing technology
- Describes how the Wellfleet source routing bridge works
- Includes a list of additional source routing reference material
- Lists implementation guidelines for adding source routing bridges to your network
- Describes how to edit source routing parameters and delete source routing from the router, using the Configuration Manager tool

# Source Routing Overview

Source routing networks consist of LAN segments connected by source routing bridges (Figure 2-1).

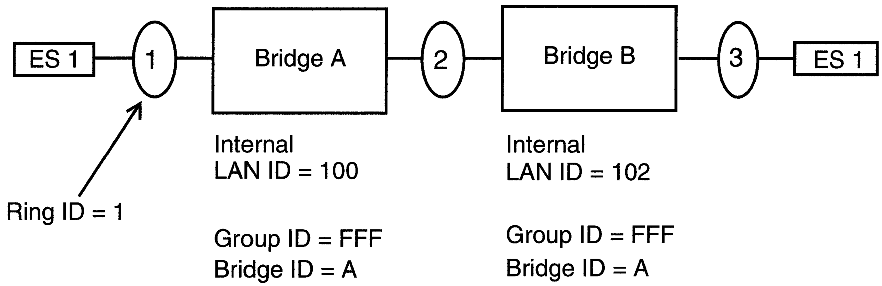



**Figure 2-1. Source Routing Network**

Each LAN segment has a unique network-wide identification number, or ring ID. Each source routing bridge also has an identification number, or bridge ID, and a unique network-wide internal or virtual LAN identification number, called an internal LAN ID.

For each Wellfleet source routing bridge, you assign an additional routing identifier called a group LAN ID. The group LAN ID serves as a routing information field (RIF) placeholder and Wellfleet identifier.

## How Source Routing Differs from Transparent Bridging

The Wellfleet source routing bridge differs from the Wellfleet transparent bridge (described in Chapter 1) in two ways:

- Source routing bridges can tolerate multiple paths between endstations in an extended network; transparent bridges require loop-free topologies.
- Source routing bridges require endstations to supply the bridging information needed to deliver a frame to a destination; transparent bridges use forwarding tables.

# How Endstations on a Source Routing Network Discover Routes

The following sections describe the three processes that endstations on a source routed network use to learn the routes to destinations. These processes are: all-paths broadcast routing, spanning tree broadcast routing, and specific routing.

## All-Paths Broadcast Routing

An endstation configured for all-paths broadcast routing generates multiple frames that traverse all paths between source and destination endstations. These frames are *all-routes explorer* (ARE) or *all-paths explorer* (APE) frames.

When an endstation receives an ARE frame, a bridge within the source routing network appends a routing designator that identifies the incoming ring ID, internal LAN ID/bridge ID, and outgoing ring ID (Figure 2-2).

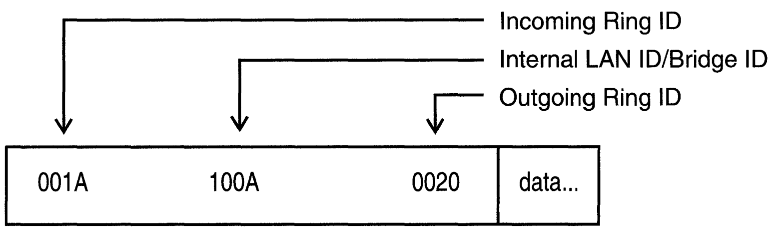



**Figure 2-2. Source Routing Designator**

After the bridge adds the routing designator, the other bridges send the frame out all ports (*floods* the frame). As a result, multiple copies of the same ARE frame can appear on a LAN, and the frame recipient can receive multiple copies of the frame (one copy for each possible path through the extended network).

Each ARE frame received by the destination endstation contains a unique sequenced list of routing designators tracing the frame's path through the source routing network.

**Note:** In a looped topology, the originating bridge may receive the ARE frame; the originating bridge discards the frame.

## Spanning Tree Broadcast Routing

An endstation configured for spanning tree broadcast routing generates a single frame that follows a loop-free path from source to destination. This frame is a *spanning tree explorer* (STE) frame.

When an endstation receives an STE frame, each bridge on the spanning tree forwards it onto all active (nonblocked) ports, except the port that received the frame. With spanning tree broadcast routing, one copy of the STE appears on each LAN and the frame recipient receives a single copy only.

## Specific Routing

When an endstation receives an ARE or STE frame, it generates a single frame, called a *specifically routed frame* (SRF). The SRF traverses a specific path back to the source endstation; it contains a list of routing designators that maps a path through the extended network from source to destination.

When an endstation receives an SRF, each bridge between the source and destination examines the list of routing designators. The bridge forwards the SRF only if the bridge itself is on the specified path. Otherwise, it ignores the frame. When the SRF reaches the original source endstation, that station removes the routing information and stores it in its internal routing table.

Once the endstations discover a route and store the information in their routing tables, the endstations send specifically routed frames across the source routed network (Figure 2-3).

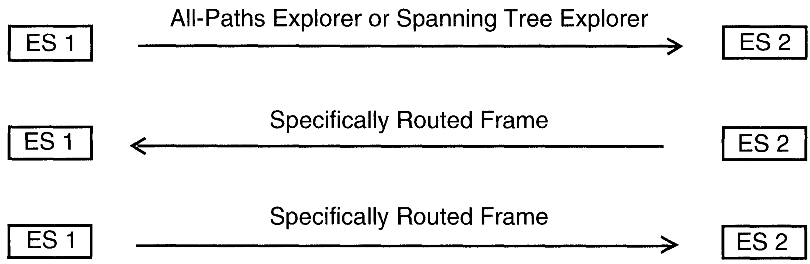



**Figure 2-3. Route Discovery**

## Source Routing over IP Networks

The Wellfleet source routing bridge supports *Internet Protocol (IP) encapsulation*. IP encapsulation allows the source routing bridge to route frames to endstations located across an IP backbone network.

These frames use standard IP transmission services and a proprietary sequence maintenance protocol that ensures error-free, in-sequence delivery of IP encapsulated frames. The IP network can consist of any standard IP equipment and media.

### How IP Encapsulation Works

When you enable IP encapsulation on a source routing bridge (thus making it an IP encapsulating bridge), you assign a single ring ID to the entire IP backbone network. The source routing bridge assigns only a single route descriptor to the frame's RIF to describe the entire internet, regardless of the IP network size that the frame traverses. Therefore, frames source routed over large IP networks can remain within maximum hop count restrictions.

Whenever a Wellfleet source routing bridge receives an explorer frame, the bridge sends it toward an IP encapsulating bridge, which resides at the edge of the IP backbone network. (For example, in Figure 2-4, Bridges A, B, and C are IP encapsulating bridges.) The IP encapsulating bridge encloses the source routed frame with an IP header before it sends the frame out onto the network. When the frame reaches a peer IP encapsulating bridge, the bridge removes the encapsulation from the frame and sends it out the appropriate source routing interfaces.

Each IP encapsulating bridge maintains a dynamic mapping of destination IP addresses to the ring and bridge IDs of their directly attached rings. When an IP encapsulating bridge receives a source routed frame, it performs these steps:

1. Checks the frame's RIF for the ring and bridge ID that immediately follow the IP network ring and bridge ID in the RIF.
2. Looks up the IP address that corresponds with this ring and bridge ID.
3. Encapsulates the frame in an IP packet with the destination IP address.
4. Sends the frame out onto the IP network.

For example, Figure 2-4 shows the IP mapping table for IP Encapsulating Bridge A.

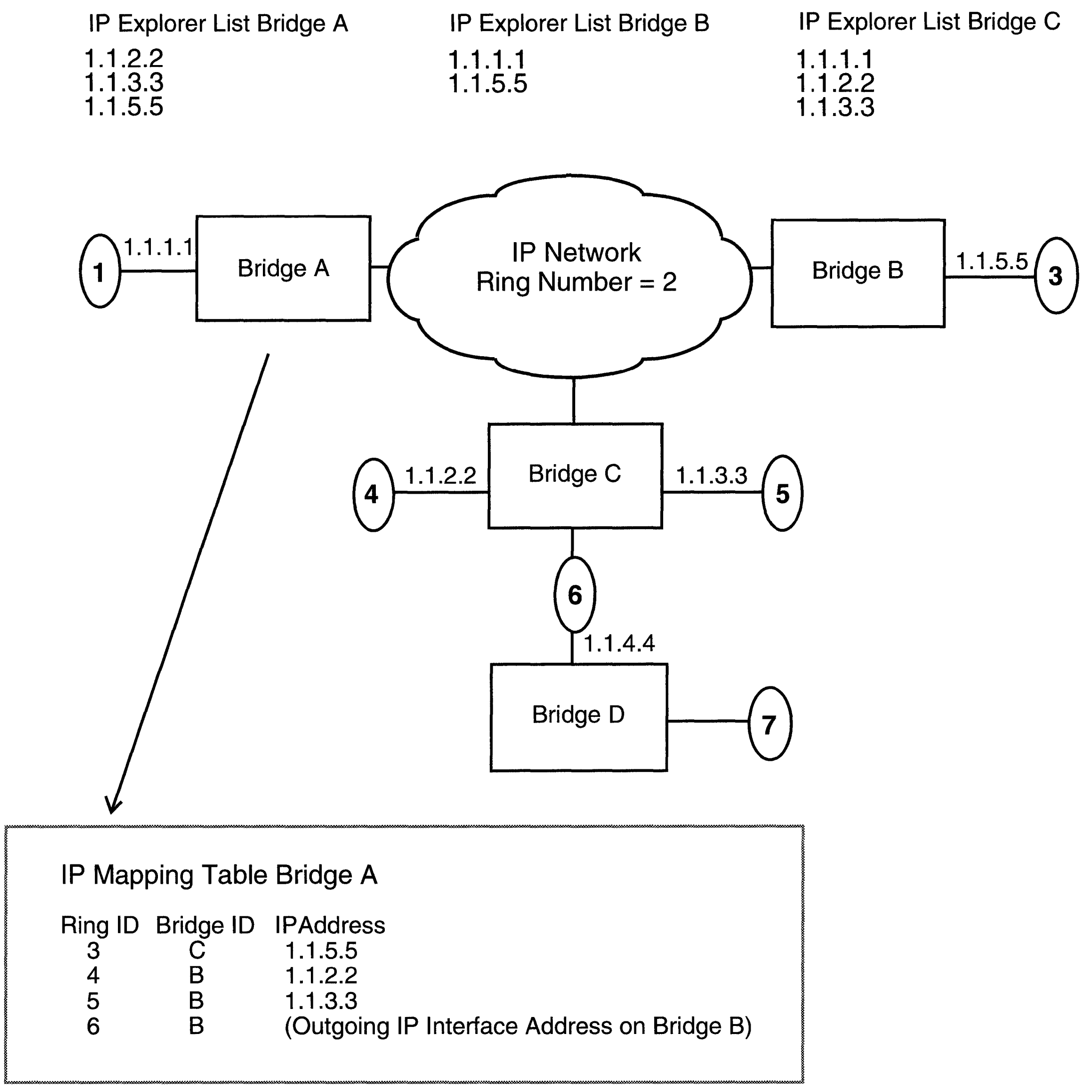



**Figure 2-4. Source Routing over an IP Network**

When Bridge A receives a source routed frame destined for an end system on Ring 4, it examines the frame's RIF and locates the next ring ID (4) that immediately follows the IP network ring ID (2), as shown in Figure 2-5.

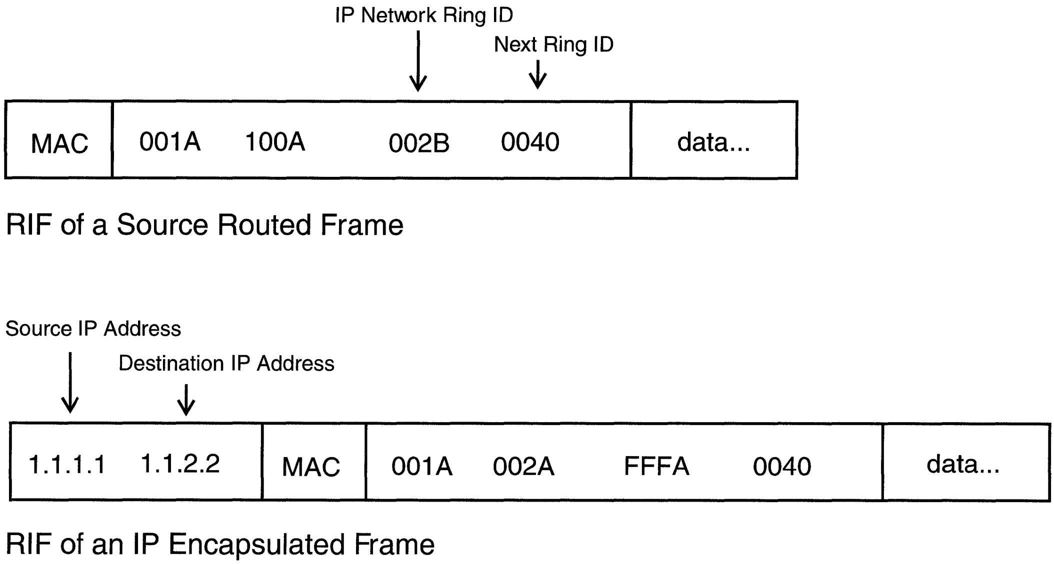



**Figure 2-5. Examining the RIF Field of an SRF**

Bridge A also examines the RIF to locate the bridge ID associated with the remote bridge used to reach Ring 4 (in this case, Bridge B). Then, Bridge A checks its mapping table for the IP address that corresponds to Ring ID 4 and Bridge B, and encapsulates the frame with an IP header. The IP header specifies its own source address, and the proper IP destination address (1.1.2.2). Finally, Bridge A forwards the packet onto the IP network.

You control which IP interfaces receive explorer frames by defining an *IP Explorer list* for each IP encapsulating bridge. For example, all of the IP encapsulating bridges that border the IP cloud in Figure 2-4 have IP explorer lists defined. Each bridge forwards explorer packets that are in its individual list toward the IP addresses. Note that the IP explorer lists for each bridge can vary. This allows you to control which IP networks receive explorer traffic.

## IP Encapsulation Features

Our implementation of IP encapsulation allows you to:

- Configure redundant IP interfaces.

  You can configure redundant IP interfaces on the same router for critical network connections (for example, interfaces 1.1.2.2 and 1.1.3.3 on Bridge B). That way, if you disable one of the interfaces, the other interface can still accept IP traffic for the network. (When you enable redundant IP interfaces, you also increase explorer traffic on the network. Therefore, enable redundant interfaces selectively to reduce the impact on your network performance.)

- Expand your IP backbone network.

  You can expand your IP backbone to include any Wellfleet IP router on the network. You specify the router's IP address in the IP explorer list for each bridge.

  For example, Bridge A currently forwards all traffic destined for Ring 7 to IP interface 1.1.3.3. That router then forwards the traffic toward Ring 6 so that the router can source route it to Ring 7. If you add IP address 1.1.4.4. to the IP Explorer list for Bridge A, then Bridge A forwards all traffic destined for Ring 7 directly to IP interface 1.1.4.4. By expanding your IP backbone, the source routing bridge can route through more stations, but still only add a single hop to a packet's RIF.

- Reduce excess broadcast traffic on your IP network.

  You can reduce the number of broadcast and explorer packets that traverse the network by constructing *directed explorer filters.* (Refer to *Configuring Wellfleet Routers* for details.)

- Configure both IP encapsulation support and source route endstation support on the same interface.

IP encapsulation support works independently of source route endstation support. However, you can enable both on the same circuit.

## Source Route Endstation Support

The Wellfleet IP, IPX, XNS, AppleTalk, and VINES routers support routing over Token Ring networks that contain one or more source routing bridges. This feature is called *source route endstation support*.

In a source routing network, every endstation that sends out a frame supplies the frame with the necessary route descriptors so that the router can source route it across the network. Thus, for routers to route packets across a source routing network, they must act like endstations; the routers must supply route descriptors for each packet before they send it out onto the network.

When you enable end-node support and a Wellfleet router running IP, IPX, XNS, AppleTalk, or VINES receives a packet and determines that the packet's next hop is across a source routing network, the router performs these steps:

1. Adds the necessary RIF information to the packet's MAC header
2. Sends the packet out onto the network where it is source routed toward the next hop

Upon receiving the packet from the Token Ring network, the peer router strips off the RIF field and continues to route the packet toward the destination network address (refer to Figure 2-6).

You configure source route end-node support for each individual routing protocol on a per-circuit basis.

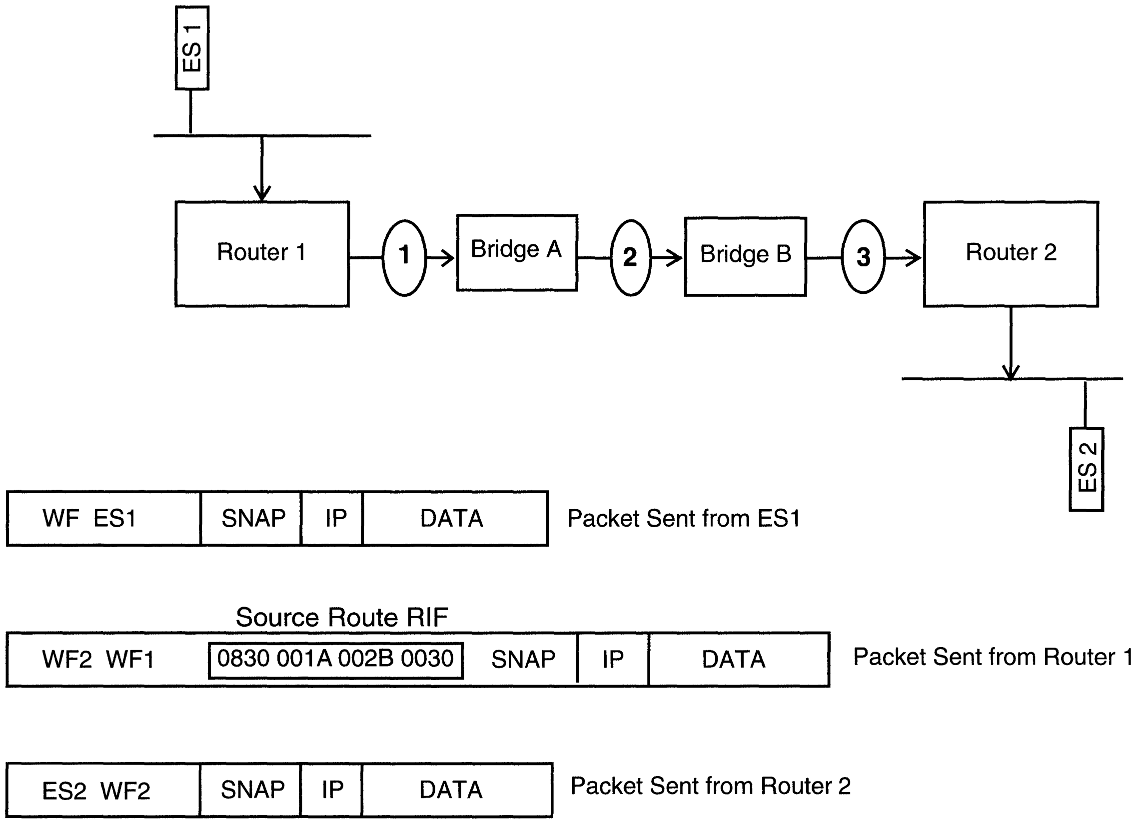



**Figure 2-6. IP Routers Source Routing across a Token Ring Network**

# How the Wellfleet Source Routing Bridge Works

This section shows examples of how the Wellfleet source routing bridge routes frames through a Token Ring network. It also describes how the source routing bridge routes frames across an IP backbone network (called IP encapsulation).

## Source Routing across a Token Ring Network

The Wellfleet source routing bridge handles incoming packets differently, depending on its position in the Token Ring network. To demonstrate, the following sections describe the routing information field (RIF) of a frame as it moves back and forth between Endstation 1 (ES1) and ES2 (Figure 2-7).

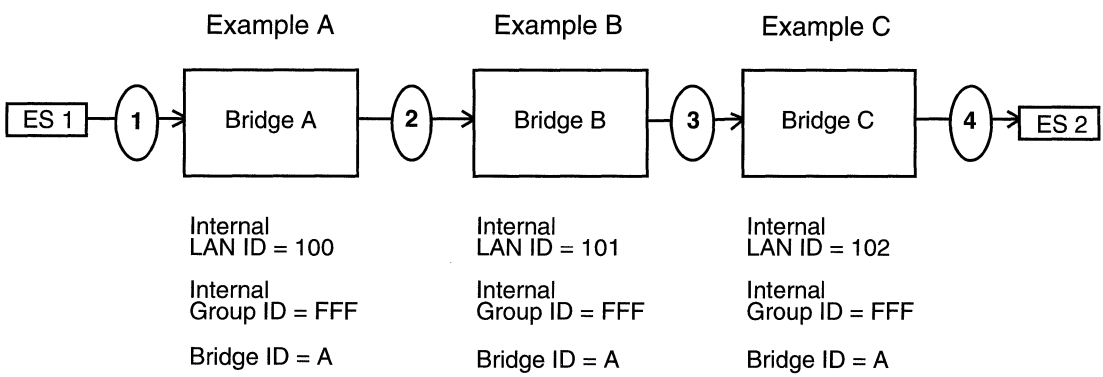



**Figure 2-7. Tracking an Explorer Frame**

First, we track the RIF of an explorer frame sent from ES1 to ES2. Then, we track the RIF of a specifically routed frame sent back from ES2 to ES1.

The size of the RIF is variable. It contains the routing information required to transmit the frame across the network.

Although the following examples show only the Wellfleet source routing bridge, other IBM-compatible source routing bridges can reside in the same network.

## How the Source Routing Bridge Handles Explorer Frames

This section describes how the Wellfleet source routing bridge handles explorer frames (AREs or STEs) sent from ES1 to ES2 (refer to Figure 2-7). Each bridge's internal LAN ID, group LAN ID, and bridge ID is in hexadecimal format below the bridge.

- Example A describes the actions of the first Wellfleet bridge.
- Examples B and C describe the actions of other Wellfleet bridges in the explorer frame's path.

### Example A: First bridge to receive the explorer frame

The frame received by Bridge A from Ring 1 did not traverse any other bridges. This bridge adds the following information in the RIF before it transmits the frame toward Ring 2 (refer to Figure 2-8):

1. Incoming ring ID/bridge ID
2. Internal LAN ID/bridge ID
3. Outgoing ring ID/bridge ID 0

### Examples B and C: Other bridges that receive the explorer frame

The explorer frame received by Bridges B and C contains internal LAN IDs and bridge numbers, indicating that this frame traversed at least one other Wellfleet bridge. These bridges perform the following steps in the RIF before transmitting the frame toward Rings 3 and 4 (refer to Figure 2-8):

1. Removes the last internal LAN ID
2. Replaces the incoming ring ID and bridge ID 0 with its own bridge ID
3. Adds its own internal LAN ID/bridge ID
4. Adds the outgoing ring ID/bridge ID 0

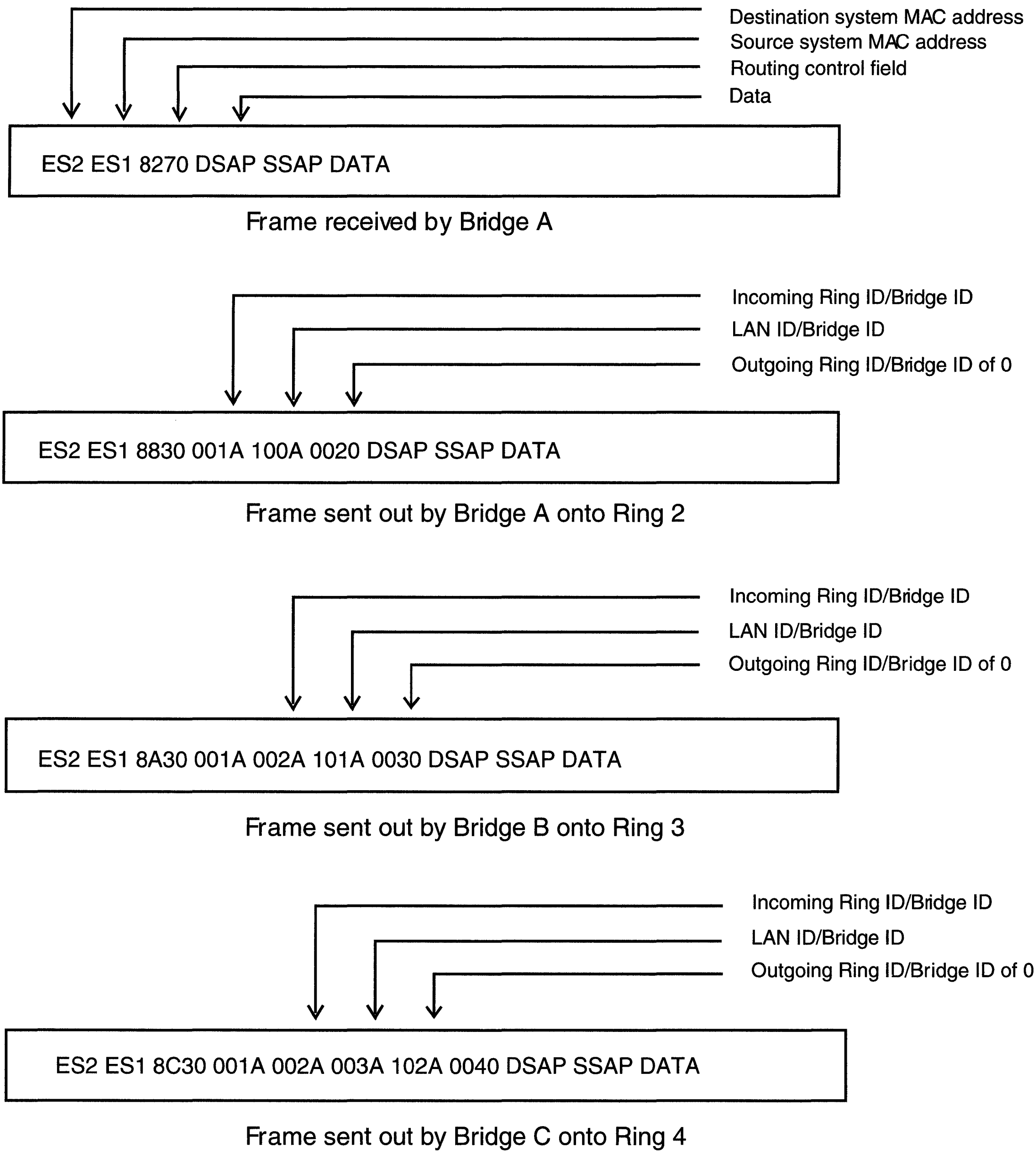



**Figure 2-8. Structure of an Explorer Frame**

## How the Source Routing Bridge Handles Specifically Routed Frames from ES2 to ES1

This section describes how the Wellfleet source routing bridge handles specifically routed frames (SRFs) sent from ES2 to ES1. Depending on the bridge's position in the network, the bridge handles the SRFs differently (Figure 2-9).

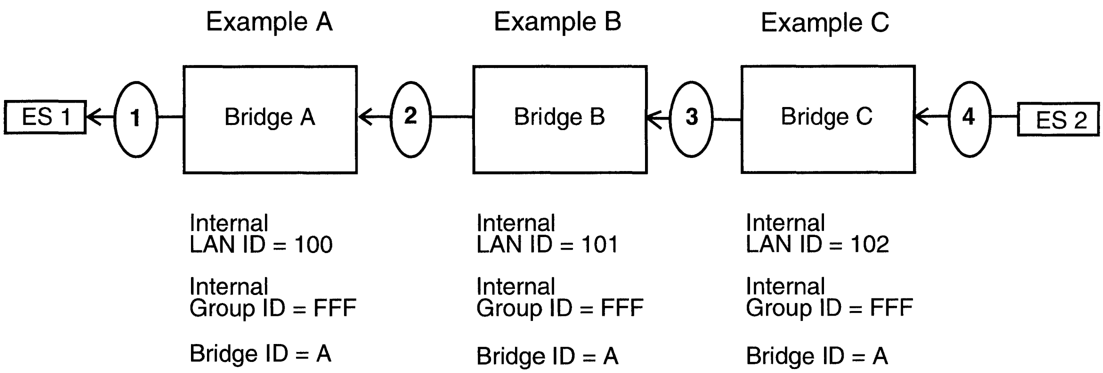



**Figure 2-9. Tracking a Specifically Routed Frame from ES2 to ES1**

If there is only a single bridge ID in the RIF, then the Wellfleet bridge transmits the frame to the outgoing circuit without modification. This is true only when the frame traverses a single Wellfleet bridge (or any combination of third-party bridges) between the source and destination end system.

If there are multiple bridge IDs in the RIF, then:

- Example A describes the actions of a Wellfleet bridge if it is the first bridge to handle the SRF.
- Example B describes the actions of a Wellfleet bridge if there are multiple bridge IDs in the RIF, and the bridge is in between the first and last Wellfleet bridge to handle the SRF.
- Example C describes the actions of a Wellfleet bridge if there are multiple bridge IDs in the RIF, and the bridge is the last Wellfleet bridge to handle the SRF.

### *Example A: First of several bridges to receive the SRF*

The frame received by Bridge C from Ring 4 did not traverse any other Wellfleet bridges (but there are multiple bridge IDs in the RIF, so it will eventually). This bridge performs the following steps in the RIF before it transmits the frame toward Ring 3 (refer to Figure 2-10):

1. Changes the destination system's MAC address at the beginning of the frame to a Wellfleet group address. This address is C000A2FFFFFF*x*, where *x* is the bridge ID of the next Wellfleet bridge specified by the RIF.
2. Removes its own internal LAN ID and inserts the group LAN ID before the last incoming ring and bridge ID listed in the RIF (refer to Figure 2-10). Eventually, the internal LAN ID of the last Wellfleet bridge along the frame's path replaces the group LAN ID.
3. Copies the destination system's MAC address into the data portion of the frame.

### *Example B: Between the first and last bridges to receive the SRF*

The frame received by Bridge B from Ring 3 traversed at least one other Wellfleet bridge. However, this is not the last Wellfleet bridge that the frame must traverse. This bridge performs the following steps in the RIF before transmitting the frame toward Ring 2 (refer to Figure 2-10):

1. Locates the bridge ID, which is at the end of the group address.
2. Changes the bridge ID at the end of the group address to the bridge ID of the next Wellfleet bridge in the RIF. (Only if it differs from the value already in place. In this example, all bridge IDs are the same, so the frame is not modified.)

### *Example C: Last of several bridges to receive the SRF*

The frame received by Bridge A is the last of several Wellfleet bridges traversed by the frame. This bridge performs the following steps in the RIF before it transmits the frame toward Ring 1 (refer to Figure 2-10):

1. Replaces the Wellfleet group address with the destination MAC address that was saved to the data field
2. Replaces the group LAN ID with its own internal LAN ID

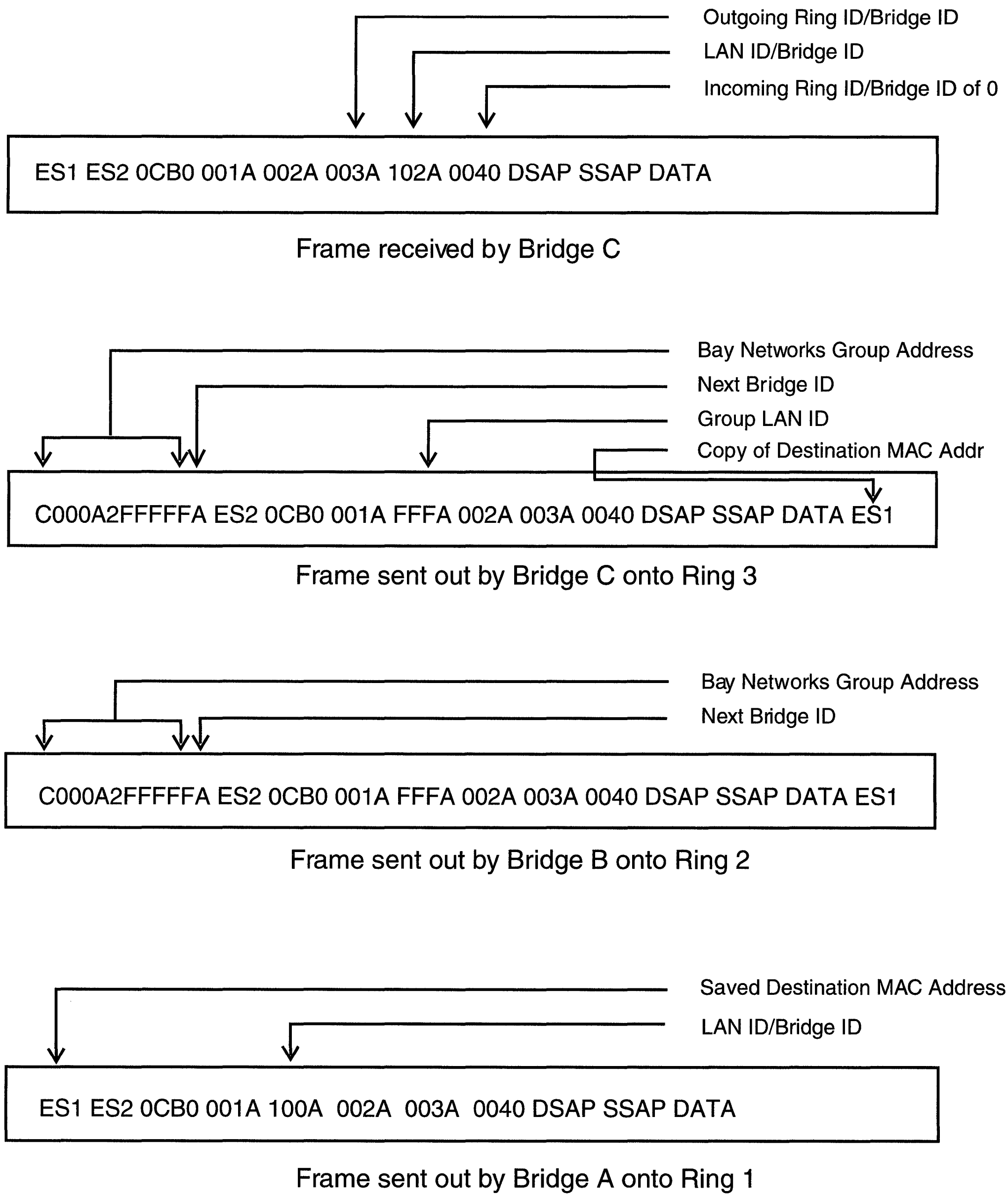



**Figure 2-10. Structure of a Specifically Routed Frame from ES2 to ES1**

## Source Routing across an IP Network

This section describes how IP encapsulation works by tracing a specifically routed frame as it is sent out from Endstation 1, traverses several bridges and an IP network, and finally arrives at Endstation 2 (Figure 2-11).

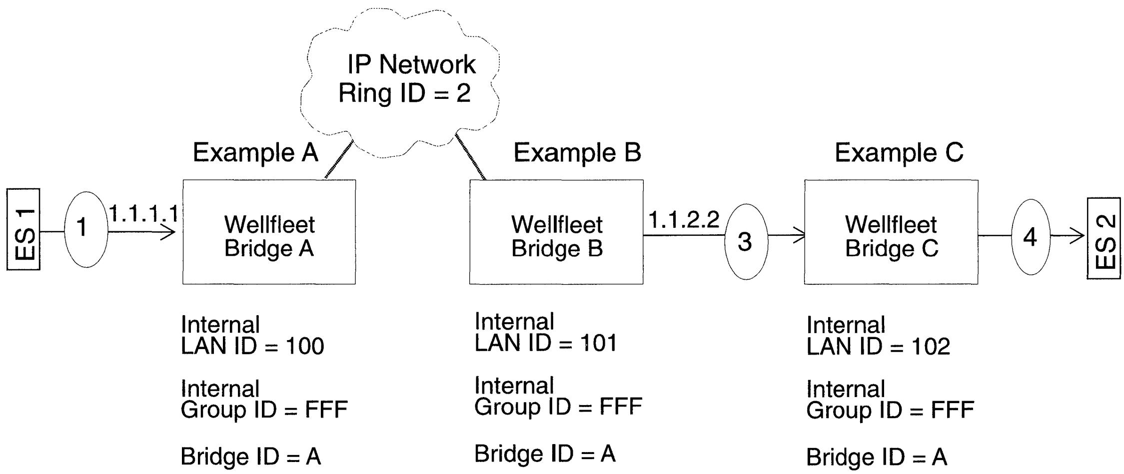



**Figure 2-11. Tracking an IP Encapsulated Frame from ES1 to ES2**

**Note:** At this point, assume that explorer packets have traversed the network and identified the paths to all reachable interfaces.

To demonstrate IP encapsulation, this section traces a specifically routed frame as it is sent out from Endstation 1 and arrives at Endstation 2:

- Example A describes the actions of the first Wellfleet bridge to handle the SRF. This bridge encapsulates the frame with an IP header before it sends the frame out onto the IP network.
- Example B describes the actions of a Wellfleet bridge that is in between the first and last Wellfleet bridges to handle the SRF. This

bridge removes the IP header from the frame before it source routes the frame to the next bridge.

- Example C describes the actions of the last bridge of several Wellfleet bridges to handle the SRF.

### *Example A: First of several bridges to receive the SRF*

Wellfleet Bridge A is the first to receive the frame from Ring 1. Bridge A performs the following steps in the RIF before it transmits the frame onto the IP network (refer to Figure 2-12):

1. Removes its own internal LAN ID.
2. Inserts the group LAN ID before the last incoming ring and bridge ID listed in the RIF (refer to Figure 2-12). Eventually, the internal LAN ID of the last Wellfleet bridge along the frame's path replaces the group LAN ID.
3. Adds an IP header containing the destination address 1.1.2.2 onto the frame and sends it toward the IP network.

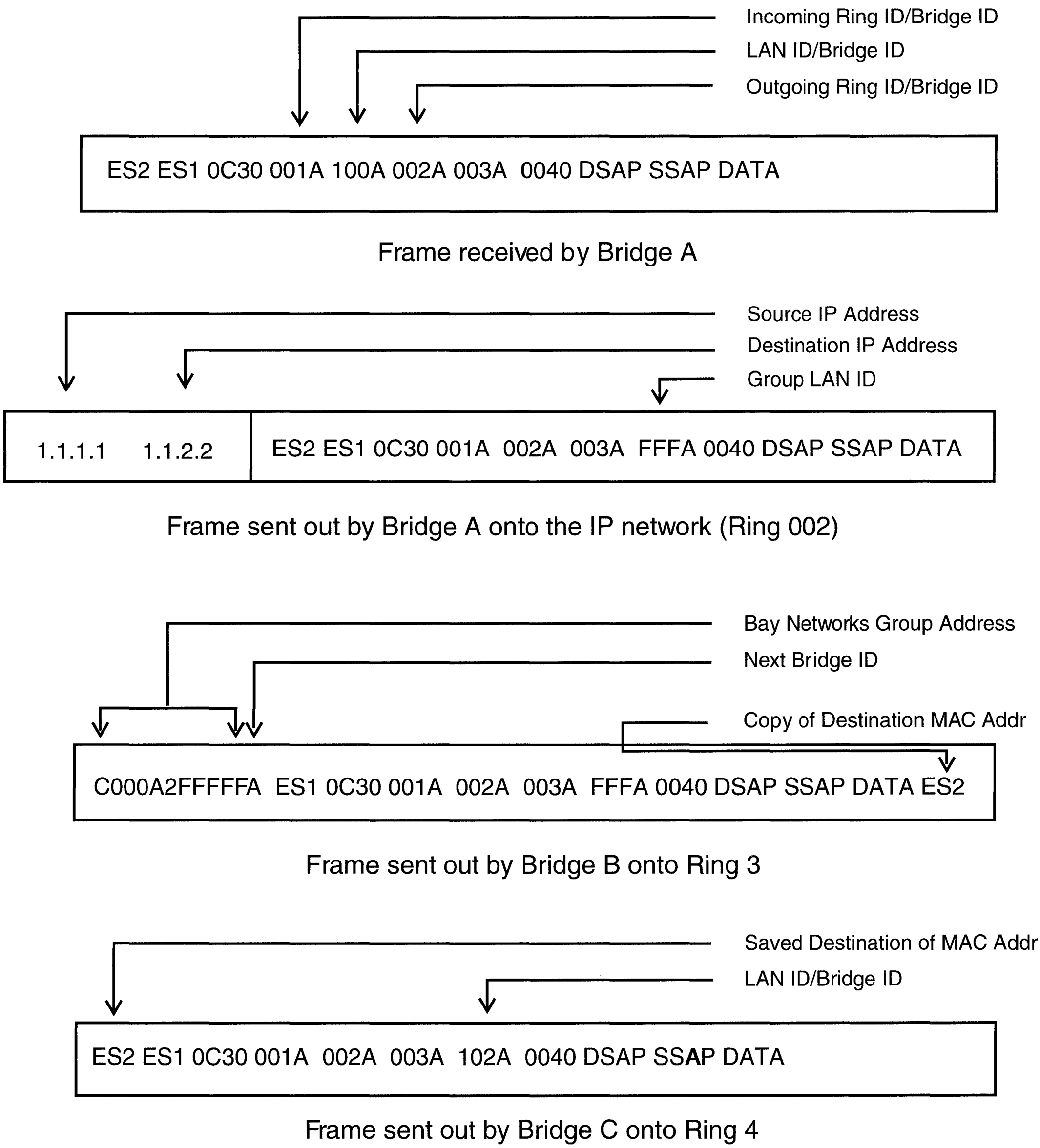



**Figure 2-12. Structure of an IP Encapsulated Frame from ES1 to ES2**

#### *Example B: Between the first and last bridges to receive the SRF*

The next Wellfleet Bridge, B, receives the frame from the IP network (Ring 2) and performs the following steps on the RIF before it transmits the frame toward Ring 3 (refer to Figure 2-12):

1. Strips the IP header from the packet.
2. Changes the destination system's MAC address at the beginning of the frame to a Wellfleet group address. This address appears as C000A2FFFFFF*x*, where *x* is the bridge ID of the next Wellfleet bridge specified by the RIF.
3. Copies the destination system's MAC address into the data portion of the frame.
4. Locates the bridge ID, which is at the end of the group address, and sends it to the bridge ID of the next Wellfleet bridge in the RIF.

#### *Example C: Last of several bridges to receive the SRF*

The last Wellfleet bridge to receive the frame performs the following steps in the RIF before it transmits the frame toward Ring 4 (refer to Figure 2-12):

1. Replaces the Wellfleet group address with the destination MAC address it saved to the data field.
2. Changes the group LAN ID to its own internal LAN ID.

## Source Routing over Frame Relay Networks

The Wellfleet source routing bridge supports source routing over frame relay networks, using RFC 1490 standard frame relay encapsulation and Wellfleet proprietary frame relay encapsulation.

To select proprietary or RFC 1490 standard frame relay encapsulation, use the Encapsulation Format parameter as described in the "Source Routing Interface Parameter Descriptions" section later in this chapter.

## Source Routing over FDDI

The Wellfleet source routing bridge supports communications between Token Ring endstations and FDDI endstations, using standard native encapsulation and proprietary encapsulation. Use Wellfleet proprietary encapsulation if you want to communicate with a Version 7 router running source routing over FDDI.

To select proprietary or standard encapsulation, use the Encapsulation Format parameter as described in the "Source Routing Interface Parameter Descriptions" section later in this chapter.

# For More Information about Source Routing

The following documentation provides technical details on Source Routing Protocol implementation:

*IBM Token Ring Network Architecture Reference. Third Edition* (SC3D-3374-D2*).* New York: IBM Corporation, September, 1989.

*Source Routing Appendix to IEEE Standard 802.1d. Media Access Control (MAC) Bridges.* Project 802.5m - Draft 71991.

Perlman, Radia. *Interconnections: Bridges and Routers*. Reading, Massachusetts: Addison-Wesley Publishing Company, First printing, May, 1992.

# Implementation Notes

This section contains some basic guidelines for adding Wellfleet source routing bridges to your network. It also describes some of the configuration features that may match your network requirements.

## Assigning Bridge IDs, Internal LAN IDs, and Group LAN IDs

When you enable the source routing bridge on the router, you must specify its bridge ID and internal LAN ID. The source routing bridge uses these routing designators and the group LAN ID to source-route packets through the network. The following sections describe each of these routing designators in detail.

### Bridge ID

The bridge ID is a standard source routing designator that identifies a bridge in the network. When you assign the bridge ID, make sure you follow these guidelines:

- Assign the same bridge ID to all other Wellfleet source routing bridges on the network unless the bridges operate in parallel.
- Assign bridge IDs to Wellfleet bridges that are *unique* among all bridges on the network.

If two or more Wellfleet bridges operate in parallel, you must assign different bridge IDs. You must also specify the other Wellfleet bridge ID in the entry list for each bridge.

For example, in Figure 2-13, Wellfleet Bridges A, C, and D all have the same bridge ID (A). However, because Bridges B and C operate in parallel, Bridge B has a different bridge ID (B). You specify this bridge ID (B) on the Bridge Entry list for Bridges A, C, and D. This ensures that the bridges know Bridge B is active on the network. Similarly, you specify the bridge ID (A) for Bridge B on the Bridge Entry list so that it knows Bridges A, C, and D are active on the network.

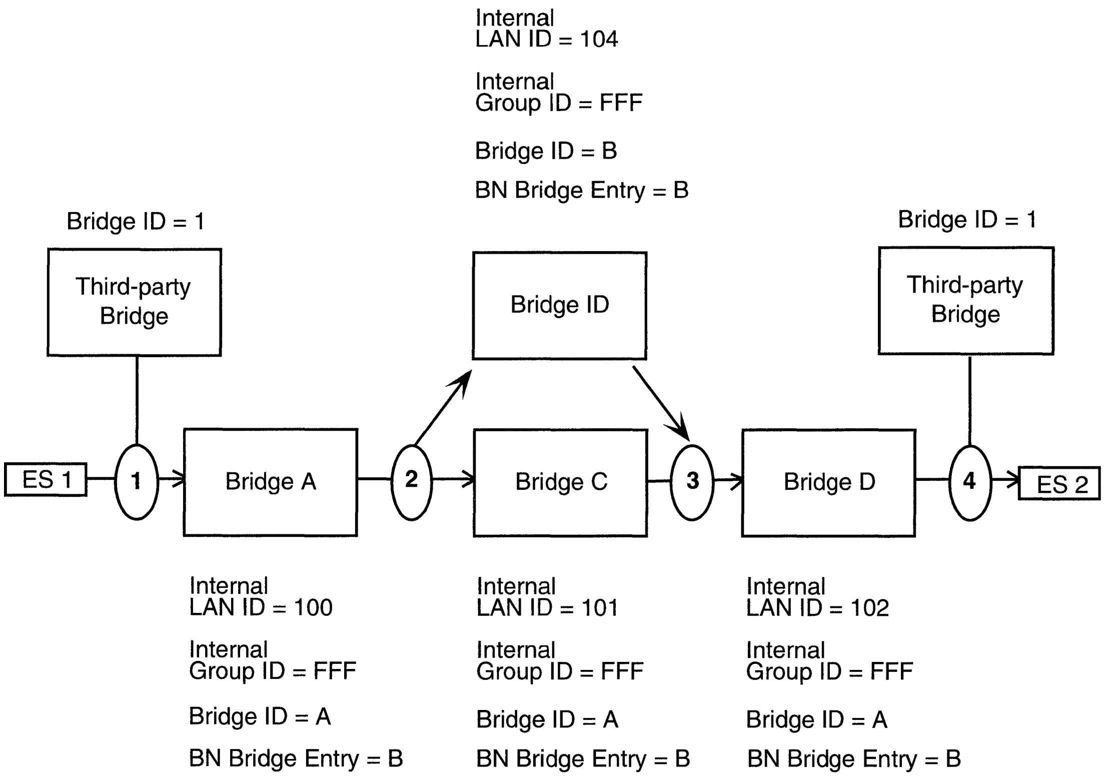



**Figure 2-13. Parallel Operation**

## Internal LAN ID

The internal LAN ID is a source routing designator that identifies the virtual LAN on which frames travel. When you configure the Wellfleet source routing bridge, you must assign a globally unique internal LAN ID to each bridge on which you enabled source routing. For example, in Figure 2-13, Source Routing Bridges A, B, C, and D all have unique internal LAN IDs.

## Group LAN ID

The group LAN ID is a Wellfleet proprietary routing designator that helps the source routing bridges in your network identify the last Wellfleet bridge in their path. When you configure the Wellfleet source routing bridge, make sure you follow these configuration guidelines:

- Assign the *same* group LAN ID to all source routing bridges in the network.
- Assign a group LAN ID to all bridges in your network. This number must be different from the LAN ID value assigned to any other bridges in the network.

# Configuring IP Encapsulation Support

IP encapsulation support allows you to source route frames between Wellfleet bridges over IP networks. When you enable IP encapsulation on the source routing bridge, make sure you follow these guidelines:

- Enable at least one IP interface on those routers through which you want to source route packets. You can enable IP on any circuit on any slot on the router; it does not have to be the same circuit on which you enabled source routing. (Refer to *Configuring Wellfleet Routers* for details on enabling IP on a circuit.)
- Configure redundant IP interfaces on different slots on the same router if you want the router to receive broadcasts for backup purposes.
- Enable source routing on the circuits of those bridges through which you want to source route frames. (Refer to *Configuring Wellfleet Routers* for details on enabling source routing on a circuit.)
- Specify a ring ID for the backbone IP network to which the source routing interface connects. You enter the IP network's ring ID for the Conn. IP NTWK Ring Number parameter for each source routing bridge. (Refer to "Editing Source Routing Interface Parameters" later in this chapter for details on accessing this parameter.) Specify the same IP network ring ID for each Wellfleet source routing bridge that connects to the network.

- Enable IP encapsulation on the source routing bridges that connect to the IP backbone. You reset the IP Encaps parameter to Enable for each source routing bridge. (Refer to "Editing Source Routing Global Parameters" later in this chapter for details on accessing this parameter.)
- Specify the IP Explorer list for each source routing interface that connects to the IP backbone.

  The IP Explorer list defines the IP addresses that will receive explorer frames from the bridge. (Refer to "Adding or Deleting an IP Address on the IP Explorer Address List" later in this chapter for details on the IP Explorer list.)
- Create directed explorer filters to reduce excess broadcast traffic on the network. (Refer to *Configuring Wellfleet Routers* for details on filters.)

# Editing Source Routing Parameters

Once you configure a circuit to support source routing, you use the Configuration Manager tool to edit the source routing parameters. This section provides information on how to access and edit these parameters.

**Note:** The instructions in this section assume that you have already configured source routing on the router. (Refer to *Configuring Wellfleet Routers* for details on configuring source routing.)

You access all source routing parameters from the Configuration Manager window (refer to Figure 2-14). Refer to *Using Site Manager Software* for details on accessing this window.

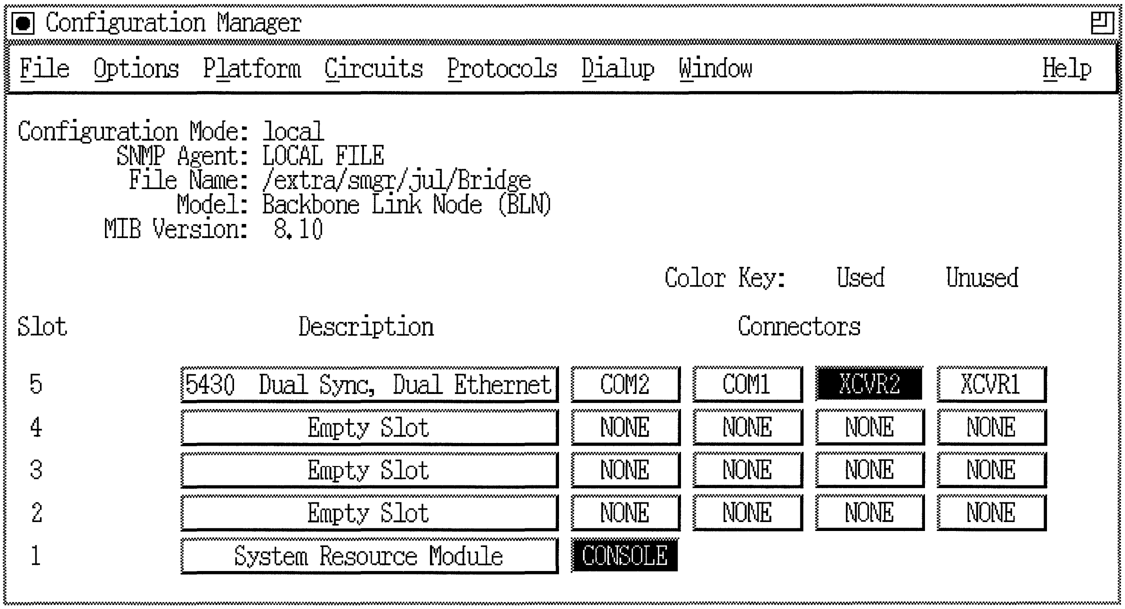



**Figure 2-14. Configuration Manager Window**

For each source routing parameter, this section provides details on the default setting, valid parameter options, 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 details on using the Technician Interface to access the MIB, refer to *Using Technician Interface Software*.

## Editing Source Routing Global Parameters

To edit source routing global parameters:

1. Select Protocols→Source Routing→Global from the Configuration Manager window (refer to Figure 2-14). The Edit Source Routing Global Parameters window appears (Figure 2-15).

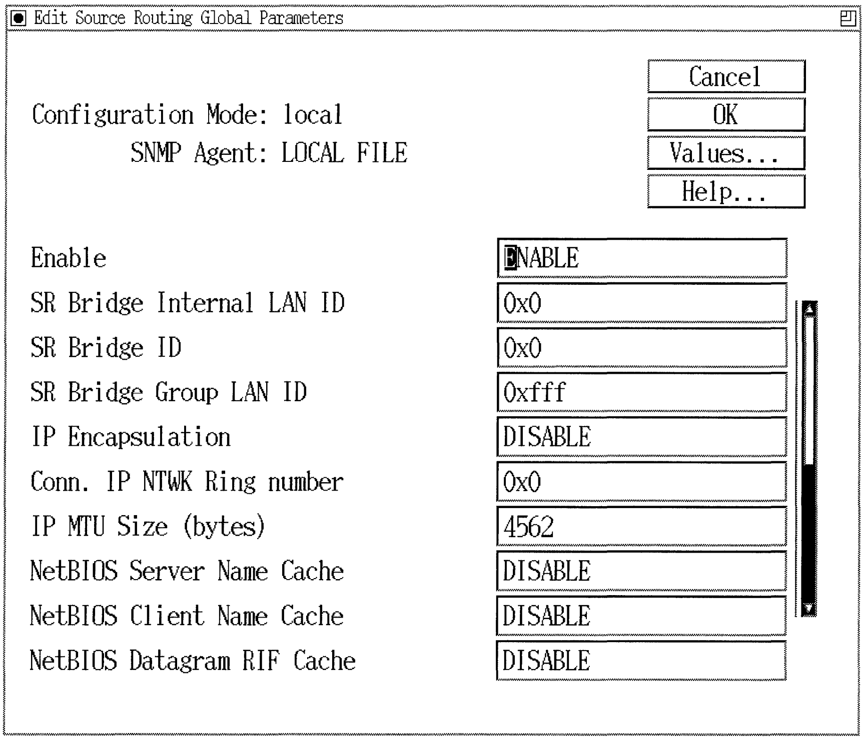



**Figure 2-15. Edit Source Routing Global Parameters Window**

2. Edit the parameters, using the descriptions in the next section as a guide. (Refer to Chapter 3 for details on editing the NetBIOS parameters.)
3. Click on the OK button to save your changes and exit the window.

## Source Routing Global Parameter Descriptions

Use these parameter descriptions as a guide when you configure the parameters on the Edit Source Routing Global Parameters window (refer to Figure 2-15). (Refer to Chapter 3 for details on configuring the NetBIOS parameters on this window.)

| | |
|---|---|
| **Parameter:** | **Enable** |
| Default: | Enable |
| Options: | Enable \| Disable |
| Function: | Enables or disables source routing on the entire router. |
| Instructions: | Set to Disable if you want to disable source routing. |
| MIB Object ID: | 1.3.6.1.4.1.18.3.5.1.1.2.1.2 |

| | |
|---|---|
| **Parameter:** | **SR Bridge Internal LAN ID** |
| Default: | 0x1 |
| Range: | 0x1 to 0x0fff |
| Function: | Specifies this bridge's internal LAN ID. |
| Instructions: | Assign an internal LAN ID that is unique among all other internal LAN IDs and ring IDs in the network. |
| MIB Object ID: | 1.3.6.1.4.1.18.3.5.1.1.2.1.4 |

| | |
|---|---|
| **Parameter:** | **SR Bridge ID** |
| Default: | 0x1 |
| Range: | 0x1 to 0x0f |
| Function: | Specifies this bridge's bridge ID and identifies the Wellfleet source routing bridges in the network. |
| Instructions: | Assign the same value to all Wellfleet source routing bridges in the network (unless two bridges operate in parallel; see the following note). The SR bridge ID must be unique among any other third-party bridge IDs in the network. |
| MIB Object ID: | 1.3.6.1.4.1.18.3.5.1.1.2.1.5 |

**Note:** If two Wellfleet source routing bridges operate in parallel, you must assign a different SR bridge ID to one of the bridges. You must also specify the SR bridge ID in the Bridge Entry list for all other Wellfleet source routing bridges in the network. (Refer to the previous section, "Assigning Bridge IDs, Internal LAN IDs, and Group LAN IDs," for details on assigning bridge IDs.)

| | |
|---|---|
| **Parameter:** | **SR Bridge Group LAN ID** |
| Default: | 0xfff |
| Range: | 0x0 to 0x0fff |
| Function: | Specifies this bridge's group LAN ID. The bridge uses the group LAN ID when transmitting specifically routed frames (SRF) between Wellfleet bridges. Together with the other routing designators, the group LAN ID helps bridges manipulate the RIF. |
| Instructions: | Assign the same group LAN ID to all Wellfleet source routing bridges in the network. The group LAN ID must be unique among any other group LAN IDs, ring IDs or internal LAN IDs in the network. |
| MIB Object ID: | 1.3.6.1.4.1.18.3.5.1.1.2.1.6 |

| | |
|---|---|
| **Parameter:** | **IP Encapsulation** |
| Default: | Disable |
| Options: | Enable \| Disable |
| Function: | Enables IP encapsulation for those packets destined for an IP network. |
| Instructions: | Enable this parameter if the bridge borders an IP network cloud and you want to source route frames across this IP network. If you enable this parameter, you must also configure the Conn. IP NTWK Ring Number parameter for IP encapsulation to occur. |
| MIB Object ID: | 1.3.6.1.4.1.18.3.5.1.1.2.1.7 |

**Note:** Refer to "Configuring IP Encapsulation Support" earlier in this chapter for details on IP encapsulation.

| | |
|---|---|
| **Parameter:** | **Conn. IP NTWK Ring Number** |
| Default: | 0x0 |
| Range: | 0x0 to 0x0fff |
| Function: | Identifies the ring ID of the IP network to which this bridge connects. |
| Instructions: | Assign the same value to all Wellfleet source routing bridges that border the IP network cloud. Make sure this value is unique among any other ring IDs, group LAN IDs, or internal LAN IDs in the network. |
| MIB Object ID: | 1.3.6.1.4.1.18.3.5.1.1.2.1.8 |

**Note:** Refer to "Configuring IP Encapsulation Support" earlier in this chapter for details on IP encapsulation.

| | |
|---|---|
| **Parameter:** | **IP MTU Size (bytes)** |
| Default: | 4562 |
| Range: | 1 to 4562 |
| Function: | Specifies the maximum MTU size for the IP network. |
| Instructions: | Select a value that equals the smallest MTU size of any of the links in the IP network. This allows the largest frame negotiation in the source routing exploration process to account for any link inside the IP cloud.<br><br>You can simply accept the default value 4562. However, if you have links in your IP network with smaller MTU sizes than the default value, the IP entity may fragment packets. For maximum performance, refer to your network configuration and calculate this value based on actual MTU sizes. |
| MIB Object ID: | 1.3.6.1.4.1.18.3.5.1.1.2.1.11 |

## Editing Source Routing Interface Parameters

To edit a source routing interface:

1. Select Protocols→Source Routing→Interfaces from the Configuration Manager window (refer to Figure 2-14). The SR Interface List window appears (Figure 2-16).

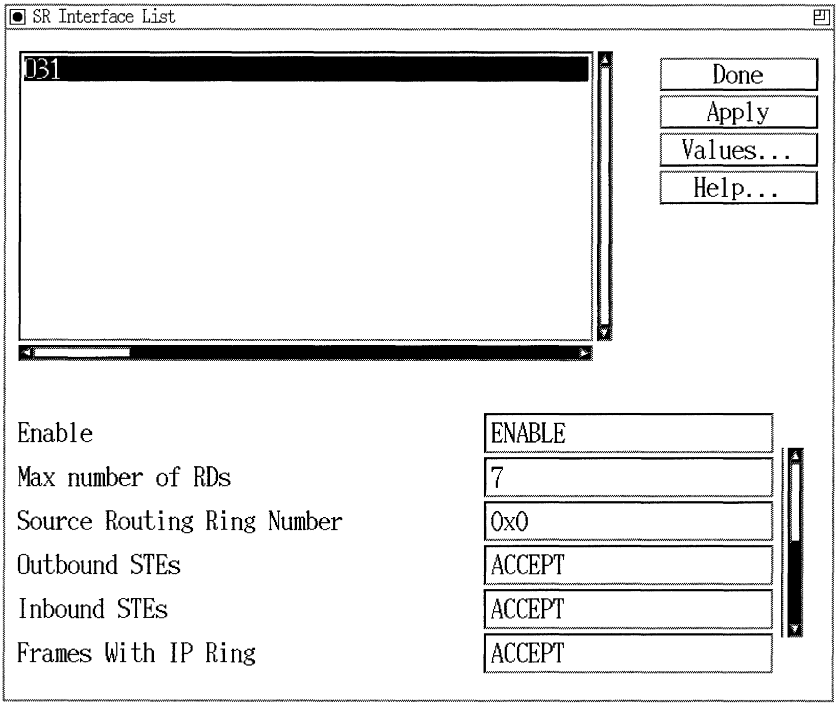



**Figure 2-16. SR Interface List Window**

2. Select the interface you want to edit.
3. Edit the parameters, using the descriptions in the next section as a guide. (Refer to Chapter 3 for descriptions of the NetBIOS parameters on this screen.)
4. Click on the Apply button to save your changes.

5. Click on the Done button to exit the window. Site Manager returns you to the Configuration Manager window.

**Note:** When you reconfigure an interface in Dynamic mode, source routing restarts on that interface.

## Source Routing Interface Parameter Descriptions

Use these parameter descriptions as a guide when you configure the parameters on the SR Interface List window (refer to Figure 2-16). (Refer to Chapter 3 for descriptions of the NetBIOS parameters on this screen.)

| | |
|---|---|
| **Parameter:** | **Enable** |
| Default: | Enable |
| Options: | Enable \| Disable |
| Function: | Enables or disables source routing over this circuit. |
| Instructions: | Set this parameter to Enable to enable source routing over this circuit. |
| MIB Object ID: | 1.3.6.1.4.1.18.3.5.1.1.2.2.1.2 |

| | |
|---|---|
| **Parameter:** | **Max number of RDs** |
| Default: | 7 |
| Range: | 2 to 7 |
| Function: | Specifies the maximum number of route descriptors allowed in incoming explorer frames. Any explorer frames received that contain more route descriptors than specified here are dropped. |
| Instructions: | Accept the default unless you want to limit the number of networks this router can reach. |
| MIB Object ID: | 1.3.6.1.4.1.18.3.5.1.1.2.2.1.5 |

| | |
|---|---|
| **Parameter:** | **Source Routing Ring Number** |
| Default: | 0x0 |
| Range: | 0x0 to 0x0fff |
| Function: | Identifies the ring number (ring ID) of this source routing circuit. |
| Instructions: | Assign a ring number (ring ID) to this source routing circuit that is unique among any other ring IDs, group LAN IDs, or internal LAN IDs in the network. |
| MIB Object ID: | 1.3.6.1.4.1.18.3.5.1.1.2.2.1.6 |

**Parameter:** **Outbound STEs**

Default: Accept

Options: Accept | Block

Function: When set to Block, the bridge drops outbound STEs on this circuit. Use this parameter to configure a static spanning tree for spanning tree explorer packets.

Instructions: Set to Block only if you do not want the bridge to forward STEs on this circuit.

MIB Object ID: 1.3.6.1.4.1.18.3.5.1.1.2.2.1.7

**Parameter:** **Inbound STEs**

Default: Accept

Options: Accept | Block

Function: Specifies if the bridge should drop single route explorer frames received on this circuit. This option will not stop single route explorer frames from being transmitted on this circuit.

Instructions: Set to Block only if you want spanning tree explorer packets to be dropped by this circuit.

MIB Object ID: 1.3.6.1.4.1.18.3.5.1.1.2.2.1.8

| | |
|---|---|
| **Parameter:** | **Frames with IP Ring** |
| Default: | Accept |
| Options: | Accept \| Block |
| Function: | Specifies if the bridge should block inbound explorer frames received on this circuit that traversed the IP network via IP encapsulation. |
| Instructions: | Set to Block only if you want to limit the route selection possibilities using IP encapsulation. |
| MIB Object ID: | 1.3.6.1.4.1.18.3.5.1.1.2.2.1.9 |

| | |
|---|---|
| **Parameter:** | **IP Address** |
| Default: | None |
| Options: | Any valid IP address |
| Function: | Shows the IP address of this interface. (If there is not IP address, this field displays 0.)<br>You can use this parameter with the IP Encaps parameter to map ring IDs to IP addresses. |
| Instructions: | If you accept the IP address displayed, then the ring ID maps to that address.<br>If you want to change the ring ID mapping to the outgoing IP interface, then enter 0.0.0.0 at this field. |
| MIB Object ID: | 1.3.6.1.4.1.18.3.5.1.1.2.2.1.10 |

**Note:** If you did not configure IP on this interface already, the system will overwrite the value you entered for this parameter when you do configure IP.

**Parameter:** **WAN Broadcast Address**

Default: -1

Options: Any valid frame relay data link connection identifier (DLCI) number

Function: Sets the DLCI number this interface uses when it sends broadcast frames over frame relay.

Instructions: Specify a DLCI number.

MIB Object ID: 1.3.6.1.4.1.18.3.5.1.1.2.2.1.23

**Parameter:** **Encapsulation Format**

Default: Proprietary

Options: Proprietary | Standard

Function: Indicates Wellfleet proprietary encapsulation format or standard encapsulation format.

Instructions: If you want to run source routing over a frame relay network, follow these instructions:

- If your Version 8 router communicates with a third-party router that supports RFC 1490, and you configured both routers to run source routing over frame relay, select Standard for RFC 1490 standard frame relay encapsulation.
- If your Version 8 router communicates with a Version 5 or Version 7 Wellfleet router, and you configured both routers to run source routing over frame relay, accept the default, Proprietary.
- If your Version 8 router communicates with another Version 8 router, and you configured both routers to run source routing over frame relay, you can select either Proprietary or Standard; however, you must set the same encapsulation format for both routers.

If you want to bridge between source routing Token Ring and FDDI endstations, refer to the following instructions:

- If your Version 8 router connects Token Ring endstations to FDDI endstations, select Standard for standard native encapsulation.
- If your Version 8 router communicates with a third-party router via an FDDI network, and each router connects to a Token Ring network, select Standard.
- If your router communicates with a Version 5 or Version 7 router via an FDDI network, and each router connects to a Token Ring network, accept the default, Proprietary.
- If your Version 8 router communicates with another Version 8 router via an FDDI network, you can select either Proprietary or Standard; however, you must set the same encapsulation format for both routers.

MIB Object ID: 1.3.6.1.4.1.18.3.5.1.1.2.2.1.24

# Adding or Deleting a Bridge ID on the Bridge Entry List

You specify a bridge ID on the Bridge Entry list if you want to configure two or more Wellfleet source routing bridges in parallel. (Refer to "Assigning Bridge IDs, Internal LAN IDs, and Group LAN IDs" in this chapter for more information). The following sections describe how to add or delete a bridge ID on the Bridge Entry list.

## Adding a Bridge Entry to the Bridge Entry List

To add a bridge ID:

1. Select Protocols➔Source Routing➔Bridge Entry from the Configuration Manager window (refer to Figure 2-14). The Source Routing Bridge IDs window appears, which lists the bridge IDs currently configured on the network (Figure 2-17).

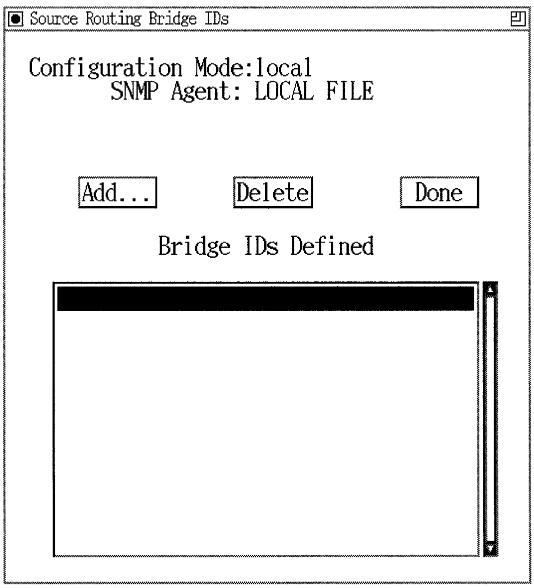



**Figure 2-17. Source Routing Bridge IDs Window**

2. Click on the Add button. The Add Bridge ID window appears (Figure 2-18).

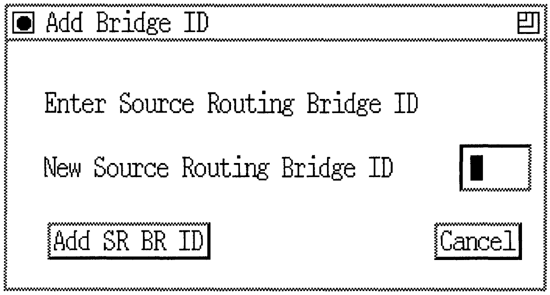



**Figure 2-18. Add Bridge ID Window**

3. Enter the new bridge ID at the New Source Routing Bridge ID field, using the description in the next section as a guide.
4. Click on the Add SR BR ID button. Site Manager returns you to the Source Routing Bridge IDs window. The bridge ID you configured now appears in the Bridge Entry list.
5. Click on the Done button to exit the window. Site Manager returns you to the Configuration Manager window.

## Source Routing Bridge ID Parameter Description

Use this parameter description as a guide when you configure the parameter on the Source Routing Bridge IDs window (refer to Figure 2-17).

| | |
|---|---|
| **Parameter:** | **New Source Routing Bridge ID** |
| Default: | None |
| Range: | 1 to 15 |
| Function: | Specifies the other active bridge IDs that exist on the network. This parameter is only necessary if you have parallel source routing bridges configured on your network. |
| Instructions: | Enter the bridge ID assigned to the parallel bridge on your network. Refer to “Assigning Bridge IDs, Internal LAN IDs, and Group LAN IDs” for details on parallel source routing bridges. |
| MIB Object ID: | 1.3.6.1.4.1.18.3.5.1.1.2.3.1.2 |

## Deleting a Bridge Entry from the Bridge Entry List

To delete a bridge ID:

1. Select Protocols→Source Routing→Bridge Entry from the Configuration Manager window (refer to Figure 2-14). The Source Routing Bridge IDs window appears, which lists the other bridge IDs currently configured on the network (refer to Figure 2-17).
2. Select a bridge ID from the list.
3. Click on the Delete button. Site Manager returns you to the Source Routing Bridge IDs window. The bridge ID you deleted no longer appears in the Bridge Entry list.
4. Click on the Done button to exit the window. Site Manager returns you to the Configuration Manager window.

# Adding or Deleting an IP Address on the IP Explorer Address List

You specify an IP address on the IP Explorer Address list if you want to source route across an IP network. The following sections describe how to add or delete an IP address on the IP Explorer Address list.

## Adding an IP Explorer Address to the IP Explorer Address List

To add an IP explorer address:

1. Select Protocols→Source Routing→Explorer Entry from the Configuration Manager window (refer to Figure 2-14). The Source Routing Bridge IP Explorer Addresses window appears (Figure 2-19), which lists the defined IP explorer addresses.

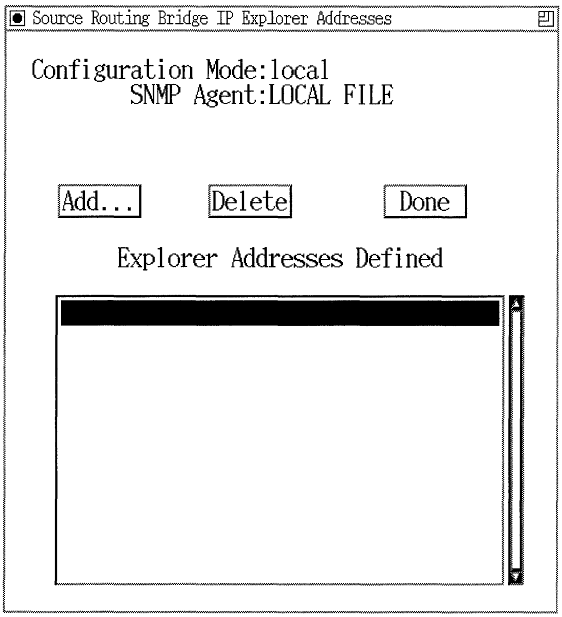



**Figure 2-19. Source Routing Bridge IP Explorer Addresses Window**

2. Click on the Add button. The Add Source Routing Explorer IP Address window appears (Figure 2-20).

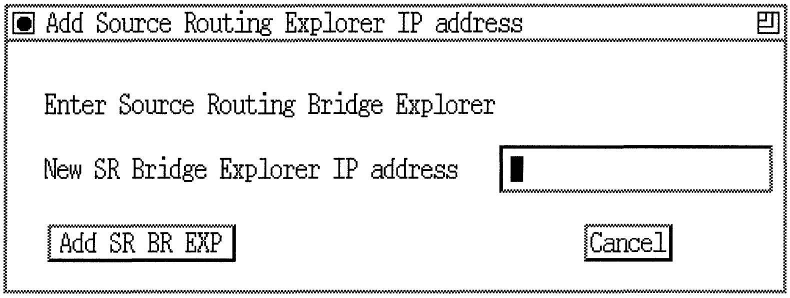



**Figure 2-20. Add Source Routing Explorer IP Address Window**

3. Enter the new IP address at the New SR Bridge Explorer IP address field, using the description in the next section as a guide.
4. Click on the Add SR BR EXP button. Site Manager returns you to the Source Routing Bridge IP Explorer Addresses window. The IP address you configured now appears on the list.
5. Click on the Done button to exit the window. Site Manager returns you to the Configuration Manager window.

## IP Explorer Address Parameter Description

Use this parameter description as a guide when you configure the parameter on the Add Source Routing IP Address window (refer to Figure 2-20).

| | |
|---|---|
| **Parameter:** | **New SR Bridge Explorer IP Address** |
| Default: | None |
| Options: | Any valid IP address. |
| Function: | Specifies a destination IP address that this bridge can use to source route packets across an IP network. |
| Instructions: | Enter a valid destination IP address. |
| MIB Object ID: | 1.3.6.1.4.1.18.3.5.1.1.2.4.1.2 |

## Deleting an IP Explorer Address

To delete an IP address from the IP Explorer Address list:

1. Select Protocols→Source Routing→Explorer Entry from the Configuration Manager window (refer to Figure 2-14). The Source Routing Bridge IP Explorer Addresses window appears (refer to Figure 2-19), which lists the defined IP explorer addresses.
2. Select an IP address from the list.
3. Click on the Delete button. Site Manager returns you to the Source Routing Bridge IP Explorer Addresses window. The IP address you deleted no longer appears in the IP Explorer Address list.
4. Click on the Done button to exit the window. Site Manager returns you to the Configuration Manager window.

## Editing Source Route Spanning Tree Parameters

To edit the source route spanning tree parameters:

1. Select Protocols→Bridge→Spanning Tree→Global from the Configuration Manager window (refer to Figure 2-14). The Edit Source Route Spanning Tree Parameters window appears (Figure 2-21).

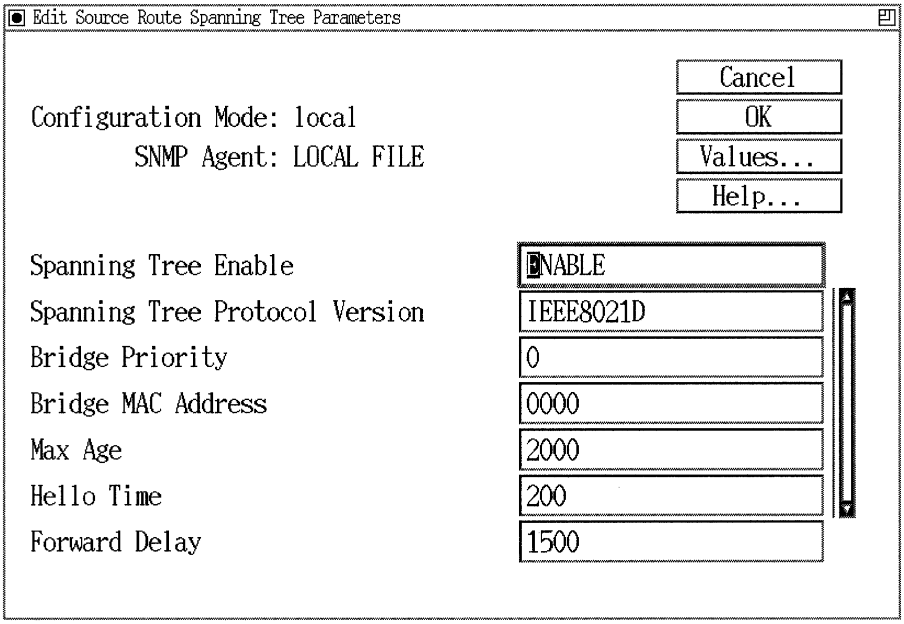



**Figure 2-21. Edit Source Route Spanning Tree Parameters Window**

2. Edit the parameters, using the descriptions in the next section as a guide.
3. Click on the OK button to save your changes and exit the window. Site Manager returns you to the Configuration Manager window.

## Source Route Spanning Tree Parameter Descriptions

Use these parameter descriptions as a guide when you configure the parameters on the Edit Source Route Spanning Tree Parameters window (refer to Figure 2-21).

| | |
|---|---|
| **Parameter:** | **Spanning Tree Enable** |
| Default: | Enable |
| Options: | Enable \| Disable |
| Function: | Enables or disables spanning tree on the entire router. |
| Instructions: | Set to Disable if you want to disable spanning tree for the entire router, or to Enable if you want to re-enable spanning tree for the entire router. |
| MIB Object ID: | 1.3.6.1.4.1.18.3.5.1.1.2.1.30 |

| | |
|---|---|
| **Parameter:** | **Spanning Tree Protocol Version** |
| Default: | IEEE8021D |
| Options: | IEEE8021D \| Unknown \| DECLB100 |
| Function: | Specifies the version of the spanning tree protocol the router is running. |
| Instructions: | Accept the default, IEEE8021D, or select one of the other options. |
| MIB Object ID: | 1.3.6.1.4.1.18.3.5.1.1.2.1.32 |

| | |
|---|---|
| **Parameter:** | **Bridge Priority** |
| Default: | Defaults to the bridge priority you set when you added spanning tree to this circuit. |
| Range: | 0 to 65535 (expressed as a decimal value) |
| Function: | The bridge priority and bridge MAC address form a bridge ID. The bridge ID provides a unit of comparison for use with the Spanning Tree Protocol. The root bridge is the bridge ID with the lowest value. Because of its significance in the bridge ID, the bridge priority strongly influences root bridge selection. The lower the bridge priority, the more likely that the spanning tree algorithm chooses the bridge as the root bridge. If there are equal bridge priority values, the bridge MAC address determines the bridge's priority; the lower the address, the higher the priority. |
| Instructions: | Either accept the current bridge priority value or assign a new one. |
| MIB Object ID: | 1.3.6.1.4.1.18.3.5.1.1.2.1.33 |

| | |
|---|---|
| **Parameter:** | **Bridge MAC Address** |
| Default: | Defaults to the bridge MAC address that you set when you added spanning tree to this circuit. |
| Options: | Any MAC address that is unique to the network (expressed as a 12-digit hexadecimal value) |
| Function: | The bridge priority and bridge MAC address form a bridge ID. The bridge ID provides a unit of comparison for use with the Spanning Tree Protocol. The root bridge is the bridge ID with the lowest value. Because of its significance in the bridge ID, the bridge priority strongly influences root bridge selection. The lower the bridge priority, the more likely that the router chooses the bridge as the root bridge. In the case of equal bridge priority values, the bridge MAC address determines the bridge's priority; the lower the address, the higher the priority.<br><br>We recommend that you set this parameter with the MAC address of one of this bridge's spanning tree ports (preferably the one with the lowest priority). |
| Instructions: | Either accept the current bridge MAC address or enter a new one. |
| MIB Object ID: | 1.3.6.1.4.1.18.3.5.1.1.2.1.33 |

**Note:** We recommend that you do not change the following three spanning tree parameters (Max Age, Hello Time, and Forward Delay) unless absolutely necessary. However, if you do change them, you must follow these guidelines.

**2 x (Forward Delay - 1 second) ≥ Max Age**

**Max Age ≥ 2 x (Hello Time + 1 second)**

If the values for Max Age, Hello Time, and Forward Delay are not the same for each bridge in your network, the root bridge parameters rule the entire topology.

| | |
|---|---|
| **Parameter:** | **Max Age** |
| Default: | 20 seconds (expressed in hundredths of a second: 2000) |
| Range: | 6 to 40 seconds |
| Function: | Specifies the maximum number of seconds that the router considers protocol information (BPDUs) valid. After this specified amount of time, the router times out and discards the information.<br>We recommend that you accept this default value; however, if you change it, you must follow the guidelines listed previously in this section. |
| Instructions: | Either accept the default value or specify a new value in the Max Age box. Make sure to express any new value in hundredths of a second. |
| MIB Object ID: | 1.3.6.1.4.1.18.3.5.1.1.2.1.43 |

| | |
|---|---|
| **Parameter:** | **Hello Time** |
| Default: | 2 seconds (expressed in hundredths of a second: 200) |
| Range: | 1 to 10 seconds |
| Function: | Specifies the interval in seconds between BPDUs transmitted by the bridge. BPDUs are periodic transmissions exchanged between bridges in the network to convey configuration and topology change data.<br><br>We recommend that you accept the default value; however, if you change it, you must follow the guidelines listed previously in this section. |
| Instructions: | Either accept the default value or enter a new value in the Hello Time box. Make sure you enter the new value in hundredths of a second. |
| MIB Object ID: | 1.3.6.1.4.1.18.3.5.1.1.2.1.44 |

| | |
|---|---|
| **Parameter:** | **Forward Delay** |
| Default: | 15 seconds (expressed in hundredths of a second: 1500) |
| Range: | 4 to 30 seconds |
| Function: | Specifies the time in seconds that a circuit spends in the listening and learning states. If you set this parameter to the minimum value, the spanning tree converges at its fastest rate.<br><br>As the spanning tree algorithm operates, it eventually places all circuits in either a forwarding (enabled) or blocking (disabled) state. In response to network topology changes, the spanning tree algorithm may change the state of specific circuits. To prevent network looping caused by sudden state changes, the spanning tree algorithm does not transition circuits directly |

from the blocking to forwarding state. Rather, it places them in two intermediate states: listening and learning.

In the listening (stand-by) state, the circuit listens for network-generated BPDUs. It receives and drops all other traffic. When the forward delay timer expires, the spanning tree algorithm places the circuit in the learning state.

In the learning state, the circuit receives both network-generated BPDUs, and endstation-generated traffic that is subjected to the learning process but is not relayed. When the forward delay timer expires, the spanning tree algorithm places the circuit in the forwarding state.

We recommend that you accept the default, 15 seconds; however, if you change the value, you must follow the guidelines listed previously in this section.

Instructions: Either accept the default value or enter a new value in the Forward Delay box. Make sure you enter the new value in hundredths of a second.

MIB Object ID: 1.3.6.1.4.1.18.3.5.1.1.2.1.45

## Editing Source Route Spanning Tree Interface Parameters

To edit the source route spanning tree interface parameters:

1. Select Protocols→Source Routing→Spanning Tree→Interfaces from the Configuration Manager window (refer to Figure 2-14). The Source Route Spanning Tree Interface List window appears (Figure 2-22).

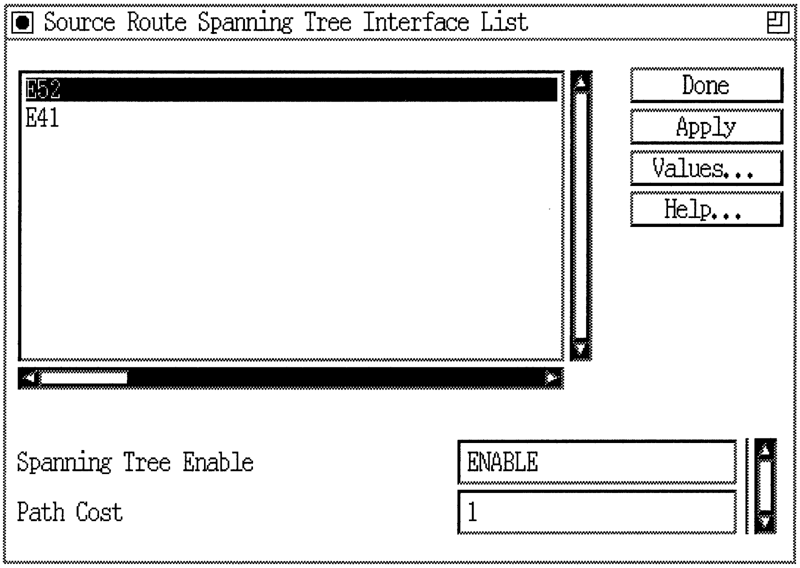



**Figure 2-22. Source Route Spanning Tree Interface Window**

2. Edit the parameters, using the descriptions in the next section as a guide.
3. Click on the OK button to save your changes.
4. Click on the Done button to exit the window. Site Manager returns you to the Configuration Manager window.

## Source Route Spanning Tree Interface Parameters Descriptions

Use these parameter descriptions as a guide when you configure the parameters on the Source Route Spanning Tree Interface List window (refer to Figure 2-22).

| | |
|---|---|
| **Parameter:** | **Spanning Tree Enable** |
| Default: | If you added spanning tree using either the Quick Start procedure or the configuring circuits procedure, this parameter defaults to Enable. If you previously used this parameter to disable spanning tree on this circuit, the parameter defaults to Disable. |
| Options: | Enable \| Disable |
| Function: | Toggles spanning tree on and off for this circuit only.<br>This parameter does not allow you to add spanning tree to this circuit. To add the spanning tree to this circuit, use the configuring circuits procedure. For instructions, see *Configuring Wellfleet Routers*. |
| Instructions: | Set this parameter to either Enable or Disable. |
| MIB Object ID: | 1.3.6.1.4.1.18.3.5.1.1.2.2.1.25 |

**Parameter:** **Path Cost**

Default: 1

Range: 1 to 65535

Function: When this port is the root port, the path cost is the contribution of the path through this port to the total cost of the path to the root for this bridge. When this port is not the root port, the router adds the path cost to the designated cost for the root port and uses it as the value of the root path cost offered in all configuration BPDUs transmitted by the bridge.

To determine the path cost, we recommend that you use this formula:

Interface Path Cost = 1000/Attached LAN speed in Mb/s

Instructions: Enter a path cost value for this interface in the Path Cost box. For example, enter 100 if the attached LAN was Ethernet (1000/10 = 100).

MIB Object ID: 1.3.6.1.4.1.18.3.5.1.1.2.2.1.28

# Deleting Source Routing from the Router

To delete source routing from all circuits on which you enabled it:

1. Select Protocols→Source Routing→Delete Source Routing from the Configuration Manager window. A window pops up and prompts:

   ```
   Do you REALLY want to delete Source Routing?
   ```

2. Select OK. Site Manager returns you to the Configuration Manager window; source routing is no longer configured on the router.

When you look at the Configuration Manager window, you see that the connectors for circuits on which source routing was the only protocol enabled are no longer highlighted. You must reconfigure the circuits for these connectors. (Refer to *Configuring Wellfleet Routers* for details on configuring the circuits.)

# Chapter 3
# Using NetBIOS Services

This chapter provides

- An overview of the Network Basic Input/Output System (NetBIOS)
- Implementation notes you should consider before you attempt to customize NetBIOS
- Instructions on how to use the Configuration Manager tool to edit the NetBIOS parameters

# NetBIOS Overview

NetBIOS is a standard mechanism for sharing services and information across a variety of transmission protocols and media.

## NetBIOS Names

Each PC application that runs over a Token Ring LAN has a NetBIOS name. Applications use NetBIOS names to start and end sessions.

You can configure a single station with multiple applications, each of which has a unique NetBIOS name. Each PC that supports an application also has a NetBIOS station name that you assign or that NetBIOS derives by internal means to that station.

NetBIOS names can consist of up to 16 alphanumeric characters. The combination of characters must be unique within the entire source routing network.

**Note:** You can configure the Wellfleet source routing bridge so that it treats NetBIOS names as though they have 15 characters, a feature useful in some environments. Refer to "NetBIOS Global Parameter Descriptions" later in this chapter for a description of the 15-Character Name Caching parameter.

### Registering Station Names

To ensure that each NetBIOS name is unique, the NetBIOS interface in each station broadcasts an *add name query* or *add group name query* frame. These frames contain each station's assigned name.

In response to the query, the NetBIOS interface in the originating station sends out an *add name response* broadcast frame. However, if the station name is the same as one already registered on the network, the NetBIOS interface sends out a *name in conflict* broadcast frame.

## Establishing Sessions

Once a NetBIOS application determines that its name is unique on the network, the application establishes a session with another NetBIOS application. The following steps describe how the application establishes the session:

1. The originating station sends out a NetBIOS *name query* to determine the route to the destination application. The query is a spanning tree explorer (STE) frame that invites a specific remote application to respond. (Refer to Chapter 2 for details on STE frames.)

2. As the name query STE frame propagates along its spanning tree route, the frame accumulates routing information field (RIF) data that traces its unique path through the loop-free topology of the network.

   - If you do not have a source routed spanning tree configured on your network, the STE propagates along all available routes to the destination application.
   - If your network has a spanning tree topology, only one copy of the name query STE frame arrives at the destination remote station.
   - If you do not have a source routed spanning tree configured on your network, multiple copies of the name query STE frame may arrive at the destination station.

   The NetBIOS interface in the destination station recognizes the name of one of its own applications in the query frame. The NetBIOS interface responds by broadcasting a name-recognized all routes explorer (ARE) frame. (Refer to Chapter 2 for details on ARE frames.)

3. As the name-recognized ARE frame propagates toward the calling station along multiple paths, each frame accumulates RIF information that traces its unique path through the network. The originating source routing interface receives multiple copies of the name-recognized frame.

4. Depending on the number of parallel paths from the destination application back to the calling application, one or more copies of the name-recognized ARE response frame arrive at the originating station. The originating station accepts only the first name-recognized frame it receives, assuming that this frame contains the RIF for the shortest path to the destination station. The calling station uses this RIF for any subsequent frames sent to the destination station. All subsequent frames associated with the impending session are specifically routed frames (SRFs). (See Chapter 2 for details on SRF frames.)
5. Based on the information gained from the name-recognized frame accepted by the originating application, the NetBIOS interface establishes a session directly between the originating and destination application. Once the session between applications is open, NetBIOS names are no longer necessary for the duration of that session.
6. When no further session transactions remain, the NetBIOS interface that serves the calling application closes the session.

## Sessionless Communication

When a NetBIOS station wants to send information that does not require a response from the destination application, the local station transmits a NetBIOS *datagram* frame. The datagram allows the NetBIOS station to communicate without establishing a session. The source station or application can send a datagram as a broadcast frame or an SRF.

## Broadcast Reduction

To increase the bandwidth available on your source routing network, the Wellfleet source routing bridge can convert broadcast frames (add name query, add group name query, name-recognized query response, and certain datagram frames) to specifically routed frames (SRFs). This process is called *broadcast reduction.*

You can customize the broadcast reduction capabilities of the source routing bridge, using these caching mechanisms:

- Client name caching
- Server name caching
- Datagram RIF caching
- Query caching
- Cache lookup
- Cache aging

The following sections describe the functions of the caching mechanisms.

## Client Name Caching

If you enable client name caching, the source routing bridge caches (learns into the NetBIOS name cache tables) the source name and associated RIF found in any name query STE frame it receives. In addition, the source routing bridge uses information cached from name query frames to convert name-recognized, datagram, or other name query broadcast frames into SRFs.

If you disable client name caching, the source routing bridge cannot cache client names and RIFs.

## Server Name Caching

If you enable server name caching, the source routing bridge caches the source name and associated RIF found in any name-recognized broadcast frame it receives. In addition, the source routing bridge uses information cached from name-recognized broadcast frames to convert name query, datagram, or other name query STE explorer frames into SRFs.

If you disable server name caching, the source routing bridge cannot cache server names and RIFs.

## Datagram RIF Caching

If you enable datagram name caching, the source routing bridge caches the source name and associated RIF found in any datagram frame it receives. In addition, the source routing bridge uses information cached from datagram broadcast frames to convert broadcast name query, name-recognized, or other datagram frames into SRFs.

If you disable datagram name caching, the source routing bridge cannot cache NetBIOS names and RIFs that it receives in datagrams.

## Query Caching

When a NetBIOS station comes up on the network, it may rebroadcast add name query and add group name query frames five to ten times at 0.5-second intervals. This increases the probability that all NetBIOS stations eventually receive these frames.

The NetBIOS query cache captures the first add name or add group name query frame it receives. The router then compares any add name or add group name query frame it receives subsequently to all of the add name and add group name query frames held in cache. If the received query matches any cached query, the router immediately discards or drops the received query. The query cache, therefore, prevents any duplicate add name query or add group name query frames from flooding the network repeatedly.

The same query caching mechanism also prevents duplicate status query frames from flooding the network.

You can adjust the maximum number of entries allowed in the query cache, using the source routing bridge's Maximum Number of Query Cache Entries global parameter. Any adjustments you make affect the number of queries that each slot can monitor.

You can also configure the router to create or disable a MIB instance for each NetBIOS query held in the query cache, using the Create MIB Instances for Cached Name global parameter. (Refer to "NetBIOS Global Parameter Descriptions" later in this chapter for a description of this parameter.) When you enable this function, you can use SNMP GET commands to view entries in the query cache table in the MIB.

Note that query caching consumes approximately 100 bytes per entry. Each cache entry remains in the query cache for a short time (approximately 3 seconds). However, if the number of NetBIOS stations and applications in your network is large, you may want to leave the query cache MIB function disabled to enhance router performance.

## Cache Lookup

The source routing bridge uses a table lookup process for name searching, which uses a fast-string hash and search mechanism. You can use the Hash Entry Count global parameter to adjust the number of entries in the hash table. (Refer to "NetBIOS Global Parameter Descriptions" later in this chapter for a description of this parameter.)

When you increase the number of entries in the hash table, you:

- Decrease the likely number of names the router must compare before it finds a specific cached name.
- Decrease the amount of time it takes the router to find a particular cached name.
- Increase memory usage.

Note that when you increase the number of entries in the hash table, you do not increase the number of names that the router can cache. You determine the number of entries, using the Max Number Query Cache Entries global parameter. (Refer to "NetBIOS Global Parameter Descriptions" later in this chapter for a description of this parameter.)

When you decrease the number of entries in the hash table, this generally produces an opposite effect on the cache lookup mechanism.

## Cache Aging

The router ages name cache and query cache entries to ensure that cached routes remain consistent with the current network topology. If the cache table lookup mechanism does not access a cache entry within the interval you set in the appropriate cache aging time parameter, the router deletes the entry from the table.

You can adjust the aging parameter for the name/RIF cache, using the Name Cache Age parameter, which is a source routing bridge global parameter. Any adjustments you make affect all instances of the source routing bridge in the router configuration.

You can also adjust the aging parameter for the query cache by means of the NetBIOS Query Cache Age, which is also a global parameter of the source routing bridge.

Refer to "NetBIOS Global Parameter Descriptions" for a description of the Cache Age Time and NetBIOS Query Cache Age parameters.

## Statically Configured NetBIOS Names

You can add static NetBIOS names and associated RIF entries into the router. These entries are independent of the name and RIF entries learned dynamically in the name cache.

The static RIF must reflect a valid learned route. Since specifying a valid RIF is a complicated procedure, we recommend that you copy a RIF that the router learned dynamically into the its name cache.

# Implementation Notes

The following sections contain information you may need to know before you configure NetBIOS on the router.

## Topologies

If you configure your source routed network to operate as a spanning tree, this may affect the client name caching feature. The following sections describe the effects on client name caching when you have a spanning tree or other topology.

### Spanning Tree Topology

If you configure your network as a source route spanning tree, you must disable client name caching on all Wellfleet routers in the network. This prevents the router from converting name-recognized broadcast frames into SRFs that contain inferior RIFs. These name-recognized broadcast frames propagate along all paths back to the querying client. The first frame that arrives at the client presents the best route to the destination application.

When you enable client name caching, the router adjacent to the destination station learns only the spanning tree RIF between the source and destination applications. This RIF may not represent the best path through your network. Furthermore, the router inserts this possibly inferior RIF into subsequent name-recognized broadcast frames that the destination station returns, increasing the traffic traversing the inferior path.

### Other Topologies

If your network design goals do not allow for a spanning tree topology, you can enable or disable client name caching, as needed, to suit the performance requirements of that network and the applications that run on it.

## NetBIOS Caches

If you use data link switching (DLSw) and source route bridge NetBIOS on the same network, the source route bridge NetBIOS does not convert frames from broadcast to SRF frames.

The source route bridge and DLSw interfaces each have NetBIOS caches, but they operate independently for each protocol. The source route bridge NetBIOS caches hold the RIFs associated with clients or servers on LAN segments attached to the local router. The DLSw NetBIOS cache holds the IP addresses associated with DLSw "peers" configured on remote routers.

Refer to *Customizing DLSw Services* for details on DLSw services.

# Editing NetBIOS Parameters

Once you configure a circuit to support source routing, you use the Configuration Manager tool to edit the NetBIOS parameters. This section describes how to access and edit these parameters.

**Note:** The instructions in this section assume that you already configured source routing on the router. If you did not, refer to *Configuring Wellfleet Routers* for details on configuring source routing.

You access all NetBIOS parameters from the Configuration Manager Window (Figure 3-1). (Refer to *Using Site Manager Software* for details on accessing this window.)

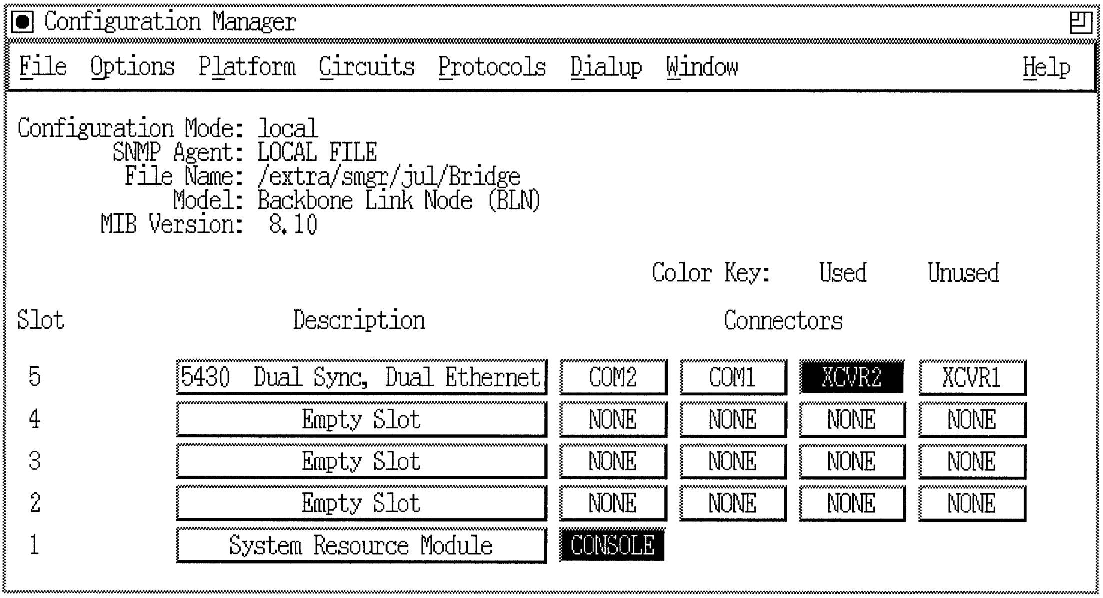



**Figure 3-1. Configuration Manager Window**

For each NetBIOS parameter, this section provides details on the default setting, valid parameter options, 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 details on using the Technician Interface to access the MIB, refer to *Using Technician Interface Software*.

## Editing NetBIOS Global Parameters

To edit the global NetBIOS parameters:

1. Select Protocols→Source Routing→Global from the Configuration Manager window (refer to Figure 3-1). The Edit Source Routing Global Parameters window appears (Figure 3-2).

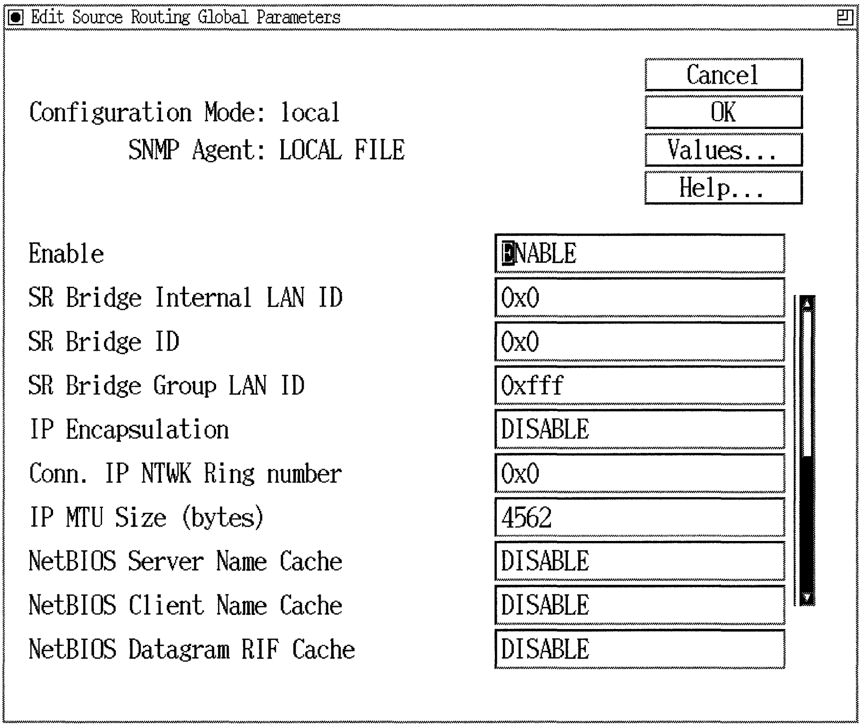



**Figure 3-2. Edit Source Routing Global Parameters Window**

2. Edit the parameters, using the descriptions in the next section as a guide. (Refer to Chapter 2 for details on editing the source routing parameters.)

3. Click on the OK button to save your changes and exit the window. Site Manager returns you to the Configuration Manager window.

## NetBIOS Global Parameter Descriptions

Use these parameter descriptions as a guide when you configure the NetBIOS parameters on the Edit Source Routing Global Parameters window (refer to Figure 3-2). (Refer to Chapter 2 for details on editing the source routing global parameters on this window.)

| | |
|---|---|
| **Parameter:** | **NetBIOS Server Name Cache** |
| Default: | Disable |
| Options: | Enable \| Disable |
| Function: | Globally enables or disables the ability of bridges to cache the source name, MAC address, and RIF path associated with each NetBIOS server that is active on the network. |
| Instructions: | Select Enable to activate NetBIOS server name, address, and RIF caching at every source routing interface configured on the node. |
| MIB Object ID: | 1.3.6.1.4.1.18.3.5.1.1.2.1.12 |

| | |
|---|---|
| **Parameter:** | **NetBIOS Client Name Cache** |
| Default: | Disable |
| Options: | Enable \| Disable |
| Function: | Globally enables or disables the ability of bridges to cache the NetBIOS source name, MAC address, and RIF path associated with each NetBIOS client that is active on the network. |
| Instructions: | Select Enable to activate NetBIOS client name, address, and RIF caching at every source routing interface configured on the node. Keep this parameter set to Disable if your network has a spanning tree topology. |
| MIB Object ID: | 1.3.6.1.4.1.18.3.5.1.1.2.1.13 |

| | |
|---|---|
| **Parameter:** | **NetBIOS Datagram RIF Cache** |
| Default: | Disable |
| Options: | Enable \| Disable |
| Function: | Globally enables or disables the ability of bridges to cache the NetBIOS source name, MAC address, and RIF path associated with each NetBIOS datagram handled by the node. |
| Instructions: | Select Enable to activate NetBIOS datagram source name, address, and RIF caching at every source routing interface configured on this node. |
| MIB Object ID: | 1.3.6.1.4.1.18.3.5.1.1.2.1.14 |

| | |
|---|---|
| **Parameter:** | **15-Character NetBIOS Name Caching** |
| Default: | Disable |
| Options: | Enable \| Disable |
| Function: | Enables or disables the ability of bridges to treat NetBIOS names either as 15- or 16-character entities. |
| Instructions: | Select Enable to activate 15-character NetBIOS name caching at every source routing interface configured on this node.<br>Select Disable if you want NetBIOS to treat names as 16-character entities. |
| MIB Object ID: | 1.3.6.1.4.1.18.3.5.1.1.2.1.15 |

**Parameter:** **Create MIB Instances for Cached Name**

Default: Enable

Options: Enable | Disable

Function: Enables or disables the ability of the system to

- Create a MIB instance for each name entry stored in the name cache.
- Delete a MIB instance for each NetBIOS name entry that ages out of the name cache.

Instructions: Select Disable if you want to release the system memory and processing resources otherwise dedicated to maintaining cached names in the MIB.

MIB Object ID: 1.3.6.1.4.1.18.3.5.1.1.2.1.16

**Parameter:** **Max Name Cache Entries**

Default: 100 entries

Range: 1 to 2147483647 entries

100 is a value suitable for networks that include up to 100 NetBIOS station names to cache. Refer to the Instructions section of this parameter description for guidelines on adjusting the value of this parameter.

Function: Specifies the maximum number of entries you need to provide in the NetBIOS name and RIF cache.

Instructions: You can adjust the value of this parameter in direct proportion to the total number of client and server names expected to be active during intervals of peak traffic load or performance demand on the router.

MIB Object ID: 1.3.6.1.4.1.18.3.5.1.1.2.1.17

| | |
|---|---|
| **Parameter:** | **Name Cache Age (secs)** |
| Default: | 300 seconds |
| Options: | The value 300 seconds, or any other value that can rapidly age infrequently referenced names out of the NetBIOS name cache |
| Function: | Specifies an age (in seconds) when inactive NetBIOS names, addresses, and RIFs expire from the NetBIOS Name Cache. |
| Instructions: | Choose an aging value that allows infrequently referenced or obsolete client and server names, addresses, and RIFs to expire from the name cache. The smaller the value, the less efficient broadcast reduction is, but the more quickly the network recovers from source routing topology changes. |
| MIB Object ID: | 1.3.6.1.4.1.18.3.5.1.1.2.1.19 |

**Parameter:** **Hash Entry Count**

Default: None

Range: 253 to 2147483648. The value 253 is suitable for networks that include up to 2500 active NetBIOS client or server names. Refer to the Instructions section of this parameter description for guidelines on Hash Entry Count settings for larger networks.

Function: Specifies the number of entries you want to allow in the RIF cache lookup tables. Each source routing bridge interface has a local table to store and retrieve the names of NetBIOS servers and clients active on the network.

Instructions: For networks that actively use up to 2500 NetBIOS client and server names, use the value 253. To determine a Hash Entry Count for larger networks:

- Divide the total number of unique NetBIOS client and server names active in the network by 10.
- Adjust the quotient to the nearest (higher or lower) prime number. (A prime number can only be divided by itself or 1 and still yield a whole-number quotient.)
- Replace the default value with the new, calculated number.

Increasing the number of hash table entries does not increase the number of names that a bridge can cache. With larger networks, increasing the size of the hash tables may, however, reduce internal cache lookup time, thereby improving overall performance.

MIB Object ID: 1.3.6.1.4.1.18.3.5.1.1.2.1.20

| | |
|---|---|
| **Parameter:** | **NetBIOS Query Cache** |
| Default: | Disable |
| Options: | Enable \| Disable |
| Function: | Globally enables or disables the ability of bridges to cache the NetBIOS source name, MAC address, and RIF path associated with each NetBIOS name query handled by the node. |
| Instructions: | Select Enable to allow source routing bridge interfaces to store names, addresses, and RIF paths associated with each NetBIOS query. |
| MIB Object ID: | 1.3.6.1.4.1.18.3.5.1.1.2.1.24 |

| | |
|---|---|
| **Parameter:** | **Create MIB Instances for Cached Query** |
| Default: | Enable |
| Options: | Enable \| Disable |
| Function: | Enables or disables the ability of the system to<br>❐ Create a MIB instance for each NetBIOS query stored in the query cache.<br>❐ Delete a MIB instance for each NetBIOS query that ages out of the name query cache. |
| Instructions: | Select Disable if you want to release system memory and processing resources otherwise dedicated to maintaining this MIB function. |
| MIB Object ID: | 1.3.6.1.4.1.18.3.5.1.1.2.1.25 |

| | |
|---|---|
| **Parameter:** | **Max Number Query Cache Entries** |
| Default: | 100 |
| Range: | The value 100 enables the router to hold (in query cache) the names, addresses, and RIF paths captured from up to 100 unique NetBIOS name query packets. Refer to the Instructions section of this parameter description for guidelines on adjusting the value of this parameter. |
| Function: | Specifies the maximum number of entries possible in the NetBIOS name query cache. |
| Instructions: | You can adjust the value of this parameter in direct proportion to the total number of NetBIOS stations that start up during intervals of peak traffic load or performance demand on the router. |
| MIB Object ID: | 1.3.6.1.4.1.18.3.5.1.1.2.1.26 |

| | |
|---|---|
| **Parameter:** | **NetBIOS Query Cache Age (secs)** |
| Default: | 15 seconds |
| Range: | 1 to 2147483648 |
| Function: | Specifies the age (in seconds) when inactive or obsolete NetBIOS name queries expire from the query cache. |
| Instructions: | Choose a query cache aging time that ensures that name queries, which are either dormant or contain obsolete RIFs, do not unnecessarily occupy or clutter the NetBIOS name query cache. Since a NetBIOS station typically transmits a query frame for 3 seconds, the default value should be sufficient. |
| MIB Object ID: | 1.3.6.1.4.1.18.3.5.1.1.2.1.28 |

## Editing NetBIOS Interface Parameters

To edit NetBIOS interface parameters:

1. Select Protocols→Source Routing→Interfaces from the Configuration Manager window (refer to Figure 3-1). The SR Interface List window appears (Figure 3-3).

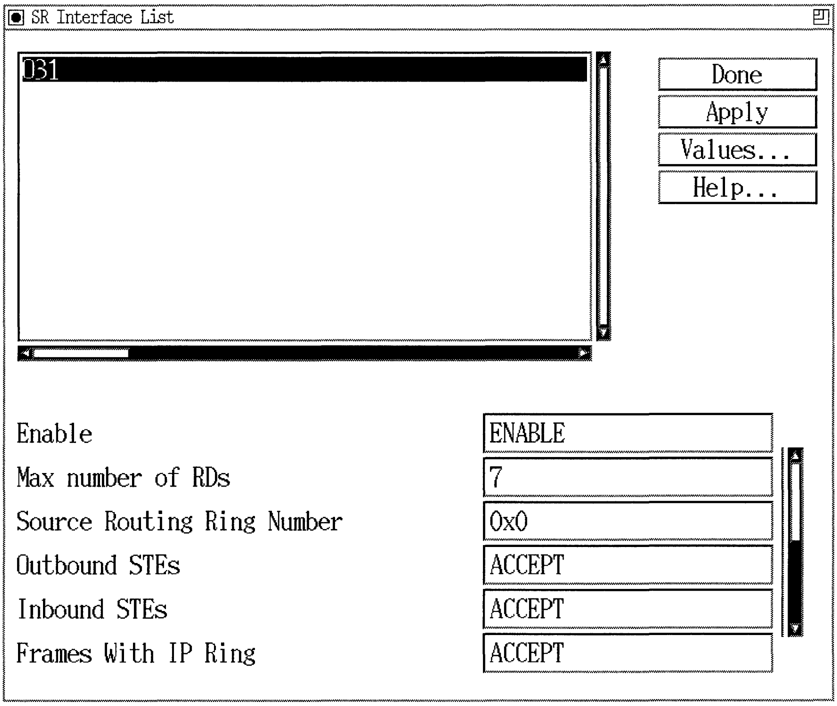



**Figure 3-3. Source Routing Interface List Window**

2. Select the interface you want to modify.
3. Edit the parameters, using the descriptions in the next section as a guide. (Refer to Chapter 2 if you want to edit the source routing interface parameters.)
4. Click on the Apply button to save your changes.

5. Click on the Done button to exit the window. Site Manager returns you to the Configuration Manager window.

## NetBIOS Interface Parameter Descriptions

Use these parameter descriptions as a guide when you configure the parameters on the SR Interface List window (refer to Figure 3-3). (Refer to Chapter 2 for details on editing the source routing interface parameters on this window.)

| | |
|---|---|
| **Parameter:** | **NetBIOS Server Name Cache** |
| Default: | Enable |
| Options: | Enable \| Disable |
| Function: | Enables or disables the ability of this bridge interface to cache the source name, MAC address, and RIF for each NetBIOS server active in the network. |
| Instructions: | Select Enable if you disabled server name caching previously, and you want to re-enable that function.<br>Select Disable if you want to release system memory and processing resources otherwise dedicated to server name caching. |
| MIB Object ID: | 1.3.6.1.4.1.18.3.5.1.1.2.2.1.17 |

| | |
|---|---|
| **Parameter:** | **NetBIOS Client Name Cache** |
| Default: | Enable |
| Options: | Enable \| Disable |
| Function: | Enables or disables the ability of this bridge interface to cache the source name, MAC address, and RIF for each NetBIOS client active in the network. |
| Instructions: | Select Enable if you disabled server name caching previously, and you want now to re-enable that function.<br>Select Disable if you want to release system memory and processing resources otherwise dedicated to client name caching.<br>Select Disable also if your network has a spanning tree topology. |
| MIB Object ID: | 1.3.6.1.4.1.18.3.5.1.1.2.2.1.18 |

| | |
|---|---|
| **Parameter:** | **NetBIOS Datagram Cache** |
| Default: | Enable |
| Options: | Enable \| Disable |
| Function: | Enables or disables the ability of this bridge interface to cache the NetBIOS source name, MAC address, and RIF associated with each NetBIOS datagram handled by the bridge. |
| Instructions: | Select Enable if you disabled datagram name caching previously, and you want now to re-enable that function.<br>Select Disable if you want to release system memory and processing resources otherwise dedicated to datagram name caching. |
| MIB Object ID: | 1.3.6.1.4.1.18.3.5.1.1.2.2.1.19 |

| | |
|---|---|
| **Parameter:** | **NetBIOS Query Cache** |
| Default: | Enable |
| Options: | Enable \| Disable |
| Function: | Enables or disables the ability of this bridge interface to cache NetBIOS queries. |
| Instructions: | Select Enable if you previously disabled name query caching on this interface only, and you want now to re-enable query caching on the interface.<br>Select Disable if you want to release system memory and processing resources otherwise dedicated to datagram name caching. |
| MIB Object ID: | 1.3.6.1.4.1.18.3.5.1.1.2.2.1.20 |

## Using Statically Configured NetBIOS Clients and Servers

The following sections describe how to add, edit, and delete statically configured NetBIOS clients and servers; refer to the appropriate section.

### Adding a Statically Configured NetBIOS Client or Server

You may want to statically configure NetBIOS names that are stable elements of your network configuration. When you statically configure a name, it reduces the use of system memory and processing resources normally required for learning and maintaining the NetBIOS names, MAC addresses, and RIFs associated with those names.

To add a statically configured NetBIOS name:

1. Select Protocols→Source Routing→NetBIOS Static Name from the Configuration Manager window (refer to Figure 3-1). The NetBIOS Static List window appears (Figure 3-4).

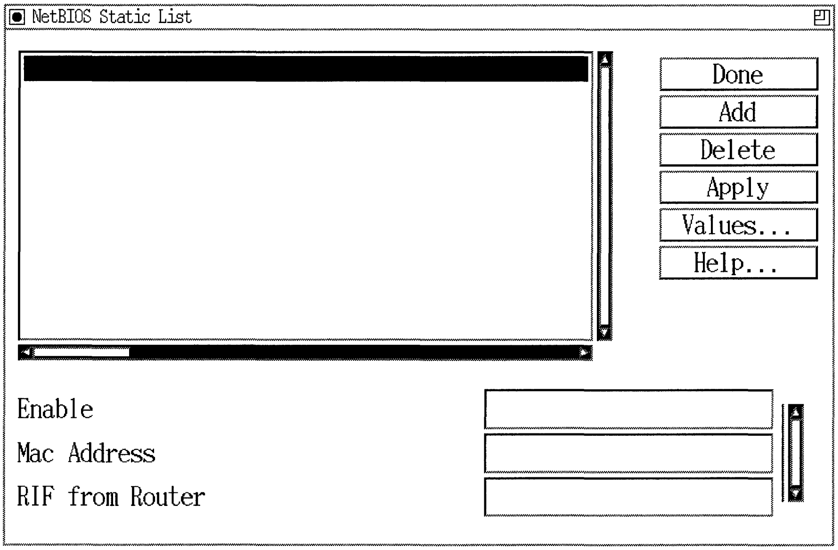



**Figure 3-4. NetBIOS Static List Window**

2. Click on the Add button. The NetBIOS window appears (Figure 3-5).

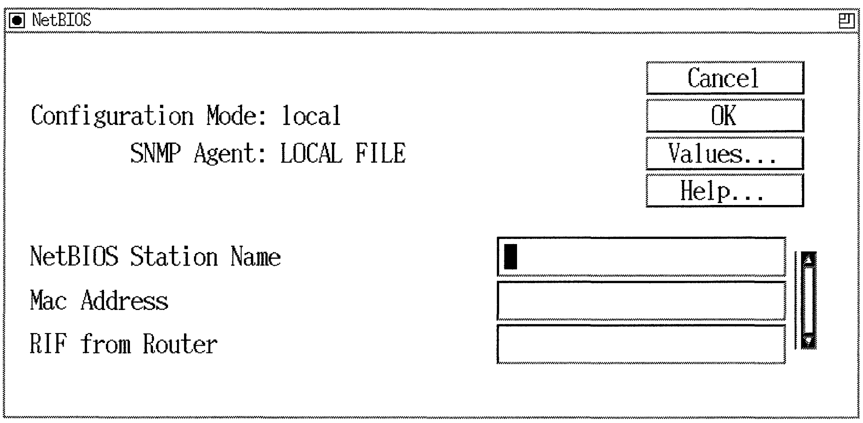



**Figure 3-5. NetBIOS Window**

3. Enter values for the parameters, using the descriptions in the next section as a guide.
4. Click on the OK button to save your changes.
5. Click on the Done button to exit the window. Site Manager returns you to the NetBIOS Static List window. (Refer to the next section to edit the parameters on this window.)

### Static Name Parameter Descriptions

Use these parameter descriptions as a guide when you configure parameters on the NetBIOS window (refer to Figure 3-5).

| | |
|---|---|
| **Parameter:** | **NetBIOS Station Name** |
| Default: | None |
| Options: | Any valid NetBIOS name |
| Function: | Specifies a NetBIOS name you want to add to the list of statically configured names that this node can reach. |
| Instructions: | Enter the NetBIOS name you want to add. The name must not exceed 16 characters. The system pads names shorter than 16 characters with ASCII space characters (0x20). |
| MIB Object ID: | 1.3.6.1.4.1.18.3.5.1.1.2.10.1.4 |

| | |
|---|---|
| **Parameter:** | **Mac Address** |
| Default: | None |
| Options: | Any valid, 48-bit MAC address |
| Function: | Specifies the MAC address of a NetBIOS name you want to add to the list of statically configured names that this node can reach. |
| Instructions: | Enter a valid, 48-bit (6-byte) MAC address of a NetBIOS client or server this node must reach. |
| MIB Object ID: | 1.3.6.1.4.1.18.3.5.1.1.2.10.1.5 |

| | |
|---|---|
| **Parameter:** | **RIF from Router** |
| Default: | None |
| Range: | Any valid RIF, with entries specified in hexadecimal format |
| Function: | Specifies the RIF required for any frame to reach a NetBIOS name you want to add. |
| Instructions: | After you add a NetBIOS name to the static list, specify the RIF from the router to the station that uses the name. First, allow the bridge to use the route discovery process to learn the correct RIF of the station. You can use the Quick Get function accessible from Site Manager's Statistics Manager tool to examine the RIF by requesting the MIB object wfBrSrNbRifEntry.wfBrSrNbRif. (Refer to *Managing Wellfleet Routers* for instructions on using the Statistics Manager tool.) Next, copy the RIF to this RIF From Router parameter. |
| MIB Object ID: | 1.3.6.1.4.1.18.3.5.1.1.2.10.1.6 |

## Editing Statically Configured NetBIOS Clients and Servers

To edit the statically configured NetBIOS clients and servers:

1. Select Protocols→Source Routing→NetBIOS Static Name from the Configuration Manager window (refer to Figure 3-1). The NetBIOS Static List window appears, which lists all of the statically configured NetBIOS clients and servers currently defined in the node configuration (refer to Figure 3-4).
2. Select the static entry you want to modify.
3. Edit the parameters, using the descriptions in the next section as a guide.
4. Click on the Apply button to save your changes.
5. Click on the Done button to exit this screen. Site Manager returns you to the Configuration Manager window.

### NetBIOS Static List Parameter Descriptions

Use these parameter descriptions as a guide when you configure the parameters on the NetBIOS Static List window (refer to Figure 3-4).

| | |
|---|---|
| **Parameter:** | **Enable** |
| Default: | Enable |
| Options: | Enable \| Disable |
| Function: | Enables or disables caching of the NetBIOS name you selected. |
| Instructions: | Select Enable to activate caching of the name you selected.<br>Select Disable to deactivate caching of the name you selected. |
| MIB Object ID: | 1.3.6.1.4.1.18.3.5.1.1.2.10.1.2 |

| | |
|---|---|
| **Parameter:** | **Mac Address** |
| Default: | None |
| Options: | Any valid, 48-bit MAC address |
| Function: | Specifies the MAC address of the NetBIOS name you selected. |
| Instructions: | Specify the MAC address of the name. |
| MIB Object ID: | 1.3.6.1.4.1.18.3.5.1.1.2.10.1.5 |

| | |
|---|---|
| **Parameter:** | **RIF from Router** |
| Default: | None |
| Options: | Any valid RIF, with route entries specified in hexadecimal format |
| Function: | Specifies the RIF required for any frame to reach the NetBIOS station you selected. |
| Instructions: | After you add a NetBIOS name to the static list, specify the RIF from the router to the station that uses the name. First, allow the bridge to use the route discovery process to learn the correct RIF of the station. You can use the Quick Get function accessible from Site Manager's Statistics Manager tool to examine the RIF by requesting the MIB object wfBrSrNbRifEntry.wfBrSrNbRif. (Refer to *Managing Wellfleet Routers* for details on using the Statistics Manager tool.) Next, copy the RIF to this RIF From Router parameter. |
| MIB Object ID: | 1.3.6.1.4.1.18.3.5.1.1.2.10.1.6 |

## Deleting a Statically Configured NetBIOS Name

To delete a statically configured NetBIOS name:

1. Select Protocols→Source Routing→NetBIOS Static Name from the Configuration Manager window (refer to Figure 3-1). The NetBIOS Static List window appears, which lists all of the statically configured NetBIOS clients and servers currently defined in the node configuration (refer to Figure 3-4).
2. Select the NetBIOS name you want to delete.
3. Click on the Delete button.

The system deletes the entry you selected and removes it from the list of NetBIOS names in the NetBIOS Static List window.

# Chapter 4
# Using Translation Bridge Services

This chapter contains

- An overview of the transparent-to-source routing translation bridge (referred to as the *translation bridge* in this chapter)
- Implementation information you should know before you use the translation bridge
- Descriptions of translation bridge parameters and instructions for editing those parameters

# Translation Bridge Overview

One kind of network uses a technique called *source routing* (SR) to bridge frames across networks. In SR networks, the station that transmits a frame includes, as part of the frame, the route that frame should traverse. The station learns the route through a route-discovery process. (Refer to Chapter 2 for details on source routing bridge services.)

Another kind of network uses a technique called *transparent bridging* (TB) to link networks. In a TB network, the bridge builds a database of node addresses to determine when it should forward or drop frames; the endstations on TB networks are not aware of forwarding routes. (Refer to Chapter 1 for details on transparent bridge services.)

The translation bridge provides a method of bridging these two kinds of networks. This allows endstations using different bridging techniques to communicate as though they use the same bridging technique.

## Databases

To connect the TB and SR networks, the translation bridge uses two databases. The following sections describe each database.

### Forwarding Database

The *forwarding table* database contains the MAC addresses for endstations on the TB network. The bridge adds addresses to the forwarding table as it learns them. The bridge learns the addresses by examining the frames transmitted on the networks with which it communicates. Thus, the forwarding table includes the addresses of all known stations on the TB network. (Refer to Chapter 1 for details on the forwarding table.)

The translation bridge expands this database to include addresses of stations it discovers on the SR network. When the transparent bridge receives a frame destined for a station on the SR network, it uses the forwarding table to forward the frame to the translation bridge.

### Route Information Field Database

The *route information field table* database includes routing information for all known stations on the SR network. The translation bridge uses this database to provide source routing information for frames it forwards from the TB network to the SR network.

### Database Aging Mechanism

The addresses in both databases have aging attributes that determine how long the addresses can remain in the databases before the translation bridge deletes them. The translation bridge resets the aging attribute for an address in the databases whenever it receives a frame from that address. When the aging attribute reaches a user-configurable value, the translation bridge deletes the address from the database. The aging mechanism allows the bridges to adapt quickly to changes in the network's configuration.

## Bridge Operations

The Wellfleet translation bridge software provides a link between the transparent bridging and source routing software on the router. The following sections describe how that link functions.

### SR Operations

To facilitate SR operations, you assign the TB network a *ring number.* To stations on the SR network, the entire TB network appears to be one additional network segment or ring, identified by this ring number. When the SR bridge receives a frame destined for this ring number, it passes it to the translation bridge.

## Routing of Explorer Frames

SR networks use explorer frames to determine the route between stations. (Refer to Chapter 2 for a description of how SR networks determine routes.)

Some stations generate all-routes explorer (ARE) frames, which are multiple frames that traverse all the possible routes between source and destination endstations. (These frames are also referred to as all-paths explorer [APE] frames.) Some stations generate a spanning-tree explorer (STE) frame, a single frame that follows a loop-free path from source to destination.

When the translation bridge receives either an STE or ARE explorer frame, it determines what to do based on the frame's source and destination addresses, as follows:

- If the frame has a group destination address, the translation bridge completes these steps:
  - The translation bridge forwards the frame to the transparent bridge, which sends it out all ports.
  - If the source address is not in the RIF table, the bridge adds the address and its routing information to the table.
  - If the source address is in the RIF table, the bridge updates its routing information.
- If the frame has a specific destination address, the translation bridge completes these steps:
  - If the source address is not in the RIF table, the translation bridge adds the address and its routing information to the table.
  - If the source address is in the RIF table, the translation bridge updates its routing information.
  - If the destination address is in the RIF table, the translation bridge discards the frame since it is intended for an SR station.

- If the destination address is not in the RIF table, but is in the forwarding table, the translation bridge converts the frame and sends it out the TB port listed in the forwarding table.
- If the destination address is not in the RIF table or the forwarding table, the translation bridge converts the frame and sends it out to all TB ports.

### Routing of Specific-Route Frames

Once an endstation on the SR network determines the route between itself and another endstation by sending out explorer frames, it can send a frame destined for that other endstation. This frame is a specifically routed frame (SRF). If the SR bridge receives an SRF that includes the ring ID of the TB network in its routing information, the SR bridge completes these steps:

- The SR bridge forwards the frame to the translation bridge, which converts the frame and forwards it to the appropriate TB network based on its destination address.
- If the SRF's source address is not already in the RIF table, the translation bridge adds it to the database and stores its routing information.

## TB Operations

When the transparent bridge receives a frame from a TB network, it determines what to do based on the frame's source and destination address, as follows:

- If the source address is not in the forwarding table, the transparent bridge adds it.
- If the destination address is in the forwarding table as a station on a TB network, the transparent bridge sends the frame to the appropriate TB port.
- If the destination address is in the forwarding table as a station on an SR network, the transparent bridge forwards the frame to the translation bridge. The translation bridge then converts the frame,

adds its routing information from the RIF table, and forwards the frame to the appropriate SR port.

- If the destination address is not in the forwarding table, the transparent bridge forwards the frame out all TB ports and to the translation bridge. The translation bridge converts the frame and sends it to the SR network as either an STE or ARE frame, depending on how you configured the translation bridge software. (Refer to the next section for details on configuring the translation bridge software for STE or ARE frames.)

**Note:** An ARE or STE frame includes the ring ID of the TB network in the route information field.

## Configuring for STE or ARE Frames

When the translation bridge software forwards a frame with an unknown destination address onto the SR network, it sends the frame as either an STE or ARE frame. By default, the translation bridge uses STE frames, so it does not overload the SR network with excessive ARE traffic. However, when the translation bridge sends STE frames, all of the traffic between the TB and SR networks follow the spanning-tree route through the SR network; this may not be the optimal route.

If you connect TB networks across a large SR network, you may want to configure the translation bridge to forward frames as ARE frames. This causes the frames to follow routes other than the spanning-tree route across the SR LAN.

# TB to SR Challenges

The translation bridge software must overcome differences in the way that TB and SR networks implement various aspects of data transmission. These differences include

- Frame formats
- Frame lengths
- MAC address formats
- LAN speed

The following sections describe how the translation bridge software accommodates these differences.

## Frame Format Selection

The Ethernet Version 2 and Ethernet 802.3 protocols transmit data, using different formats for frames. For example, in Ethernet Version 2, the first section of the frame (the *preamble*) requires eight octets. For Ethernet 802.3 frames, the preamble is seven octets long. The translation bridge converts the frames it receives from the SR network to either Ethernet Version 2 or Ethernet 802.3 format. Then the translation bridge sends the frames to the transparent bridge for forwarding.

When you configure the translation bridge, you select a default conversion, either Ethernet 802.3 or Ethernet Version 2. When the translation bridge receives a frame from the SR network, it converts the frame to the format you specified as the default. You can specify exceptions to the default so that frames destined for certain endstations use the other frame format.

## Frame Lengths

SR and TB networks often use different maximum frame lengths. For example, Ethernet networks support a maximum transmission unit (MTU) size of 1500 bytes, while Token Ring networks support much larger MTUs.

To resolve these differences, the translation bridge software specifies a maximum size of 1470 in the largest-frame-size bits of the routing information field on all frames forwarded onto the SR network. The translation bridge cannot forward frames it receives from the SR network that are longer than 1500 bytes.

## MAC Address Formats

Ethernet networks transmit the least significant bit of each byte of a MAC address first, while Token Ring networks transmit the most significant bit first. The translation bridge, therefore, reverses the bits in the source and destination addresses in the header of each frame it transfers between Ethernet and Token Ring networks. You can also define explicit mappings between Ethernet group addresses and Token Ring functional addresses. (Refer to "Editing Translation Bridge MAC Address Conversions," later in this chapter for details about MAC address conversions.)

## LAN Speeds

When the translation bridge transfers frames between networks that have different network speeds, the software automatically accommodates for variations in throughput. If the difference in speeds is significant, the translation bridge may drop some frames.

# Translation Bridge Implementation Notes

The following sections contain specific information you should know before you use the Wellfleet translation bridge.

## Protocols Supported

The translation bridge supports the transfer of logical link control (LLC)-based traffic. You can designate the service access points (SAPs) that the translation bridge accepts. By default, the translation bridge accepts traffic destined for NetBIOS (0xF0), Systems Network Architecture (SNA) (0x04, 0x08,0xFC), and LAN Network Manager (LNM) SAPs (0xF4).

## Interfaces Supported

The translation bridge can operate on all TB interfaces supported by the Wellfleet router, including

- Ethernet/802.3
- Fiber Distributed Data Interface (FDDI)
- Wellfleet serial
- Frame Relay
- Switched Multi-Megabit Data Service (SMDS)
- Point-to-Point Protocol (PPP)
- Token Ring encapsulation

The translation bridge can operate on all SR interfaces supported by the Wellfleet router except IP, but including

- Token Ring
- Wellfleet serial
- Frame relay
- SMDS
- PPP
- Ethernet/802.3 encapsulation
- FDDI encapsulation

# Loop-Free Operation

Loops occur in the network when there are several different routes between hosts. Bridges may forward traffic indefinitely around the loops, which results in degraded network performance. To eliminate loops, you can use one of the methods described in the following sections.

## Physically Disable Loops

You can discover loops in your network, using a configuration diagram of it. Then you can physically adjust the network configuration to eliminate the loops. For example, assume that Figure 4-1 is a diagram of a portion of your network.

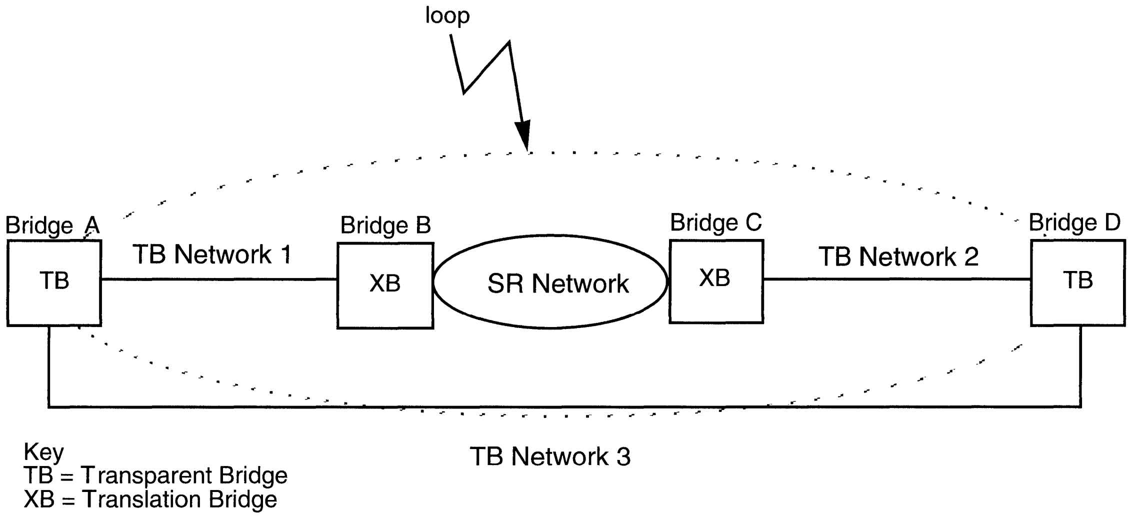



**Figure 4-1. Network Configuration with Potential Loop**

You want to send a packet from TB Network 1 to TB Network 2. As shown in the figure, there are two possible routes between these two networks:

1. Through Bridge B, across the SR network, through Bridge C, to the destination on TB Network 2.
2. Through Bridge A, across TB Network 3, through Bridge D, to the destination on TB Network 2.

To avoid continuous looping of the packet around these two paths, you can disable Bridge A or Bridge D. This eliminates the possibility of the packet using the second route. If you cannot disable a path, you can disable translation on one part of the path.

## Use the Spanning Tree Protocol

A second way to eliminate loops in the network is to use the spanning tree algorithm. This process automatically discovers and eliminates redundant paths in the network topology by disabling the appropriate bridges.

You can use the spanning tree with any TB network, but only if the translation bridge uses Token Ring interfaces to the SR network. For example, you cannot use the spanning tree algorithm with translation bridging if your interface to the SR network is Ethernet, using the Wellfleet SR encapsulation. Figure 4-2 shows an example of a spanning tree environment with translation bridging.

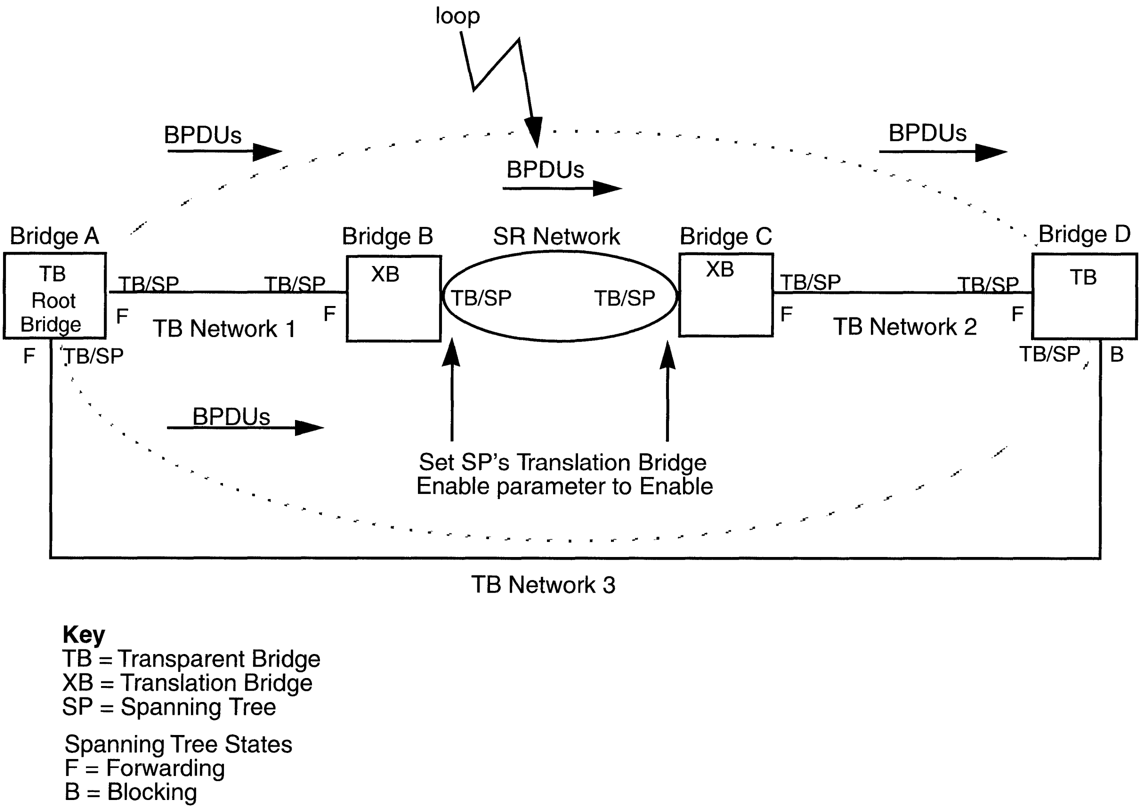



**Figure 4-2. Spanning Tree with Translation Bridging**

## Procedure for Configuring the Translation Bridge on Your Network

To configure the translation bridge to work with your network:

1. Enable the bridge on all interfaces attached to TB networks. (Refer to *Configuring Wellfleet Routers* for details on configuring protocols to run on interfaces.)
2. Enable source routing on all interfaces attached to SR networks. (Refer to *Configuring Wellfleet Routers* for details on configuring protocols to run on interfaces.)

3. Enable the translation bridge for each interface attached to an SR network if you want that interface to participate in the translation bridge. (Refer to *Configuring Wellfleet Routers* for details on configuring protocols to run on interfaces.) Use the Bridge Interfaces window to set the Translation Bridge Enable parameter to Enable. (Refer to Chapter 1 for details on configuring bridge parameters.)
4. Create the translation bridge on the router. (Refer to "Creating the Translation Bridge" later in this chapter for instructions.) Once you create the translation bridge, all TB interfaces on the router automatically participate in translation bridging.
5. Enable the spanning tree on all TB and SR interfaces on the network on which you want to use the translation bridge if you want to use the spanning tree algorithm to eliminate loops in the network. Remember that the spanning tree algorithm only works if you use Token Ring interfaces to the SR network. If you use a different kind of interface to the SR network, you have to use another method to eliminate loops. (Refer to the previous section, "Loop-Free Operation," for details on methods for eliminating loops.)
6. Set the spanning tree's Translation Bridge Enable parameter to Enable for all Token Ring SR interfaces on which you enabled spanning tree.

# Creating the Translation Bridge

To configure the translation bridge to run on the router, select Protocols→Translation Bridge→Create TB from the Configuration Manager window (Figure 4-3).

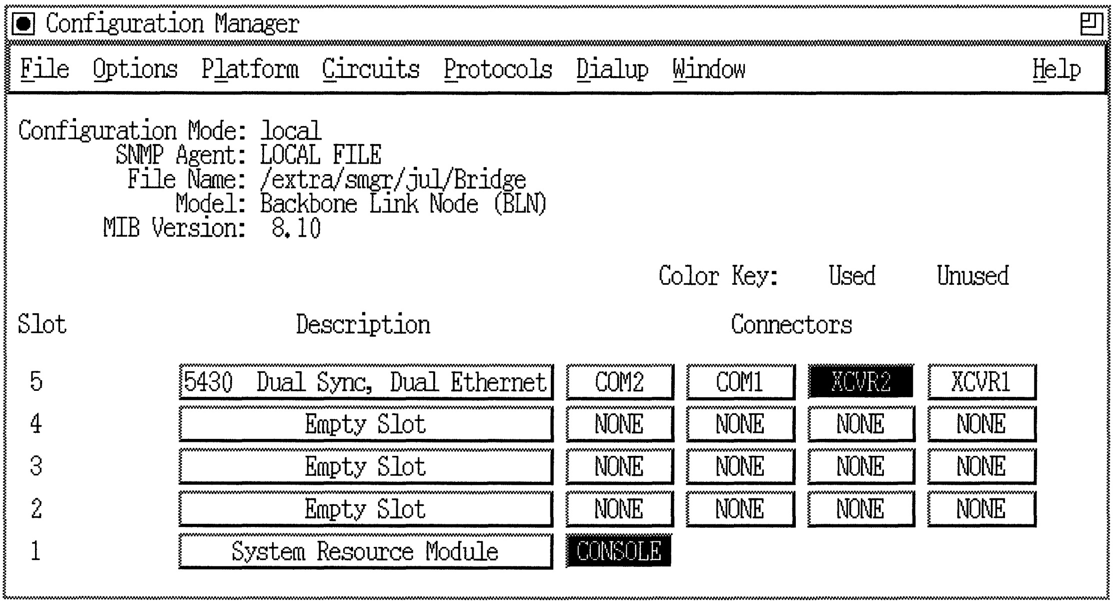



**Figure 4-3. Configuration Manager Window**

You can now operate the translation bridge on the router. Refer to the next section for details on optimizing translation bridge performance for your network.

# Editing Translation Bridge Parameters

Once you configure the translation bridge to operate on the router, you use the Configuration Manager tool to edit the translation bridge parameters. This section describes how to edit the translation bridge parameters.

You access the translation bridge parameters from the Configuration Manager window (refer to Figure 4-3).

For each translation bridge parameter, this section provides details on the default setting, valid parameter options, 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 details on using the Technician Interface to access the MIB, refer to *Using Technician Interface Software*.

## Editing Translation Bridge Global Parameters

To edit the translation bridge global parameters:

1. Select Protocols→Global Protocols→Translation Bridge→Global from the Configuration Manager window (refer to Figure 4-3). The Edit Translation Bridge Global Parameters window appears (Figure 4-4).

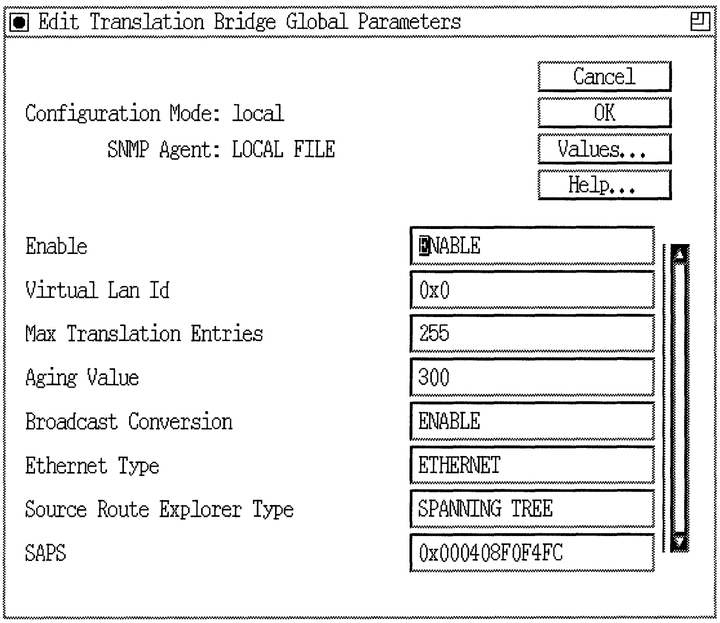



**Figure 4-4. Edit Translation Bridge Global Parameters Window**

2. Edit the parameters, using the descriptions in the next section as a guide.

3. Click on the OK button to save your changes and exit the window. Site Manager returns you to the Configuration Manager window.

## Translation Bridge Global Parameter Descriptions

Use these parameter descriptions as a guide when you configure the parameters on the Edit Translation Bridge Global Parameters window (refer to Figure 4-4).

| | |
|---|---|
| **Parameter:** | **Enable** |
| Default: | Enable |
| Options: | Enable \| Disable |
| Function: | Toggles on and off the translation bridge for the router. |
| Instructions: | Set to Disable to turn off translation bridging for the entire router. |
| MIB Object ID: | 1.3.6.1.4.1.18.3.5.1.1.2.11.2 |

| | |
|---|---|
| **Parameter:** | **Virtual LAN ID** |
| Default: | 0x0 |
| Range: | 0 to 0x0fff |
| Function: | Assigns the transparently bridged network a ring number. To stations on the source routing network, the entire transparently bridged network appears to be one additional network segment or ring, identified by this ring number. When the SR bridge receives a frame destined for this ring number, it passes it to the translation bridge. |
| Instructions: | Specify a ring number that is not already being used by the source routing network. The number you use should not be the same as any LAN ID, group LAN ID, or internal LAN ID number that is configured on any of the SR bridges on the network. We recommend that you configure the same ring number on all translation bridges on the network. |
| MIB Object ID: | 1.3.6.1.4.1.18.3.5.1.1.2.11.3 |

| | |
|---|---|
| **Parameter:** | **Max Translation Entries** |
| Default: | 255 |
| Options: | Any integer value |
| Function: | Specifies the maximum number of source routing addresses with routing information that the translation bridge can store in its RIF table. |
| Instructions: | Enter the number of addresses that the translation bridge can store in its RIF table. Ideally, this number should be equal to or greater than the number of stations on the source routed network that will communicate with stations on the transparently bridged network. If there is not enough room in the RIF table, the translation bridge does not store routing information for some stations. When the translation bridge receives traffic for those stations, it forwards the traffic as explorer frames.<br><br>However, the more entries allowed in the RIF table, the more memory the translation bridges may consume. |
| MIB Object ID: | 1.3.6.1.4.1.18.3.5.1.1.2.11.4 |

| | |
|---|---|
| **Parameter:** | **Aging Value** |
| Default: | 300 seconds |
| Options: | Any integer value |
| Function: | Specifies how long an address entry remains in the translation bridge's forwarding or RIF table when no data from that address has been received. |
| Instructions: | Specify the number of seconds that inactive addresses should be retained.<br>The larger you make this value, the more time it takes the bridge to adjust to changes in the network.<br>The smaller you make this value, the more processing the translation bridge must perform to delete and then relist infrequently used addresses. |
| MIB Object ID: | 1.3.6.1.4.1.18.3.5.1.1.2.11.6 |

| | |
|---|---|
| **Parameter:** | **Broadcast Conversion** |
| Default: | Enable |
| Options: | Enable \| Disable |
| Function: | If you enable this feature, when the translation bridge receives a frame destined for the 802.3 broadcast address (0xFFFFFFFFFFFF), it converts the address to the 802.5 broadcast address (0xC000FFFFFFFF), and vice versa. |
| Instructions: | Set to Disable if you do not want the translation bridge to convert the broadcast address. |
| MIB Object ID: | 1.3.6.1.4.1.18.3.5.1.1.2.11.7 |

| | |
|---|---|
| **Parameter:** | **Ethernet Type** |
| Default: | Ethernet |
| Options: | Ethernet \| IEEE8023 |
| Function: | Specifies the default type of frame to be sent to the transparently bridged network, either Ethernet Version 2 (Ethernet) or Ethernet 802.3 (IEEE 8023). |
| Instructions: | Specify the frame type that will be used by most of the Ethernet endstations on the network. (You can indicate specific addresses that use the other Ethernet type. Refer to "Editing Translation Bridge Station Type" later in this chapter.) |
| MIB Object ID: | 1.3.6.1.4.1.18.3.5.1.1.2.11.8 |

| | |
|---|---|
| **Parameter:** | **Source Route Explorer Type** |
| Default: | Spanning Tree |
| Options: | Spanning Tree \| All Routes |
| Function: | When the translation bridge software forwards a frame with an unknown destination address onto the source routed network, it sends the frame as either an STE (spanning tree explorer) or ARE (all-routes explorer) frame. By default, the translation bridge is configured to use STE frames, so as not to burden the source routed network with excessive ARE traffic. Using STE frames, however, forces all traffic flowing over the translation bridge to follow the spanning tree route through the network, which may not be the optimal route. |
| Instructions: | If you are connecting transparently bridged networks across a large source routed network, you may want to configure the translation bridge to forward frames as AREs, so that frames can follow routes other than the spanning tree route across the source routed LAN. Consider, however, that AREs may generate an unacceptable level of traffic on the larger network. |
| MIB Object ID: | 1.3.6.1.4.1.18.3.5.1.1.2.11.9 |

| | |
|---|---|
| **Parameter:** | **SAPS** |
| Default: | 000408F0F4FC |
| Options: | Any hexadecimal value |
| Function: | The translation bridge supports the transfer of LLC-based traffic, as indicated by the SAP (service access point) value. This parameter allows you to designate the SAPs that identify the protocols you want the translation bridge to accept and translate. By default, the translation bridge accepts NetBIOS, SNA, and LNM (LAN Network Manager) SAPs. |
| Instructions: | Specify SAPs that the translation bridge will accept. |
| MIB Object ID: | 1.3.6.1.4.1.18.3.5.1.1.2.11.10 |

## Editing Translation Bridge MAC Address Conversions

Token Ring networks use functional addresses for frames addressed to more than one station; Ethernet networks use multicast addresses for these frames. The Translation Bridge Address Mapping window allows you to map Token Ring functional addresses to Ethernet multicast addresses.

When the translation bridge receives a multicast frame from an Ethernet network destined for a Token Ring network, it translates the frame's multicast address to the mapped Token Ring functional address. The translation bridge converts the addresses of functional frames going in the other direction, from Token Ring to Ethernet, to the mapped multicast address.

**Note:** You do not need to map functional addresses that are bit-reversed versions of the multicast addresses. The translation bridge handles these conversions automatically.

## Adding an Address Mapping

To add an address mapping:

1. Select Protocols→Global Protocols→Translation Bridge→MAC Address Conversions from the Configuration Manager window (refer to Figure 4-3). The Address Mapping List window appears (Figure 4-5).

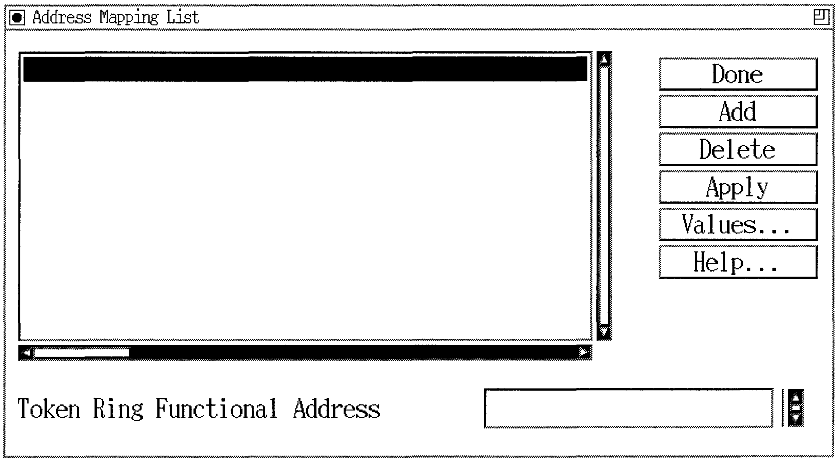



**Figure 4-5. Address Mapping List Window**

2. Click on the Add button. The Translation Bridge Address Mapping window appears (Figure 4-6).

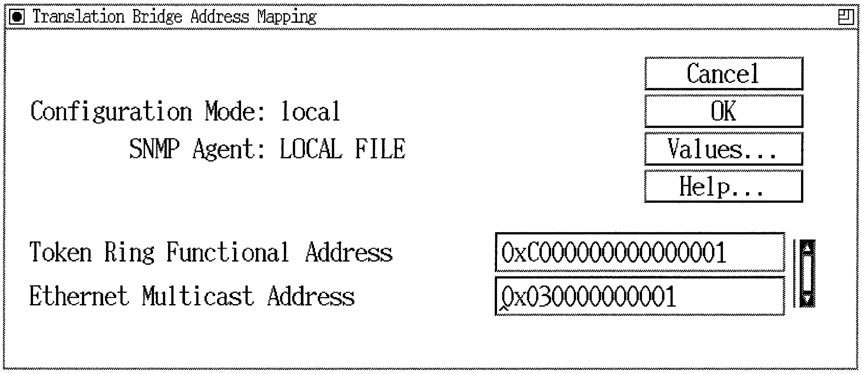



**Figure 4-6. Translation Bridge Address Mapping Window**

3. Edit the parameters, using the descriptions in the next section as a guide.
4. Click on the OK button to save your changes and exit the window. Site Manager returns you to the Translation Bridge Address Mapping List window.

## Translation Bridge Address Mapping Parameter Descriptions

Use these parameter descriptions as a guide when you configure the parameters on the Address Mapping List and Translation Bridge Address Mapping windows (refer to Figure 4-5 and Figure 4-6).

| | |
|---|---|
| **Parameter:** | **Token Ring Functional Address** |
| Default: | None |
| Options: | Any valid functional address |
| Function: | Indicates the functional address of the Token Ring station. |
| Instructions: | Enter a valid functional address. |
| MIB Object ID: | 1.3.6.1.4.1.18.3.5.1.1.2.12.1.3 |

| | |
|---|---|
| **Parameter:** | **Ethernet Multicast Address** |
| Default: | None |
| Options: | Any valid Ethernet Multicast address |
| Function: | Indicates the Ethernet Multicast address. |
| Instructions: | Enter a valid Ethernet Multicast address. |
| MIB Object ID: | 1.3.6.1.4.1.18.3.5.1.1.2.12.1.2 |

## Deleting an Address Mapping

To delete an address mapping:

1. Select Protocols→Global Protocols→Translation Bridge→MAC Address Conversions from the Configuration Manager window (refer to Figure 4-3). The Address Mapping List window appears (refer to Figure 4-5).
2. Select the address you want to delete. Then click on the Delete button.
3. Click on the Apply button to save your changes.
4. Click on the Done button to exit the window. Site Manager returns you to the Configuration Manager window.

# Editing Translation Bridge Station Type

This section describes how to configure the translation bridge so that it always translates frames destined for certain Ethernet endstations into a particular Ethernet type, regardless of how you configure the Ethernet Type parameter.

## Adding a New Address to the Station List

To add a new address to the station list:

1. Select the Protocols→Global Protocols→Translation Bridge→ Ethernet Type List option from the Configuration Manager window (refer to Figure 4-3). The Ethernet Station Type List window appears (Figure 4-7).

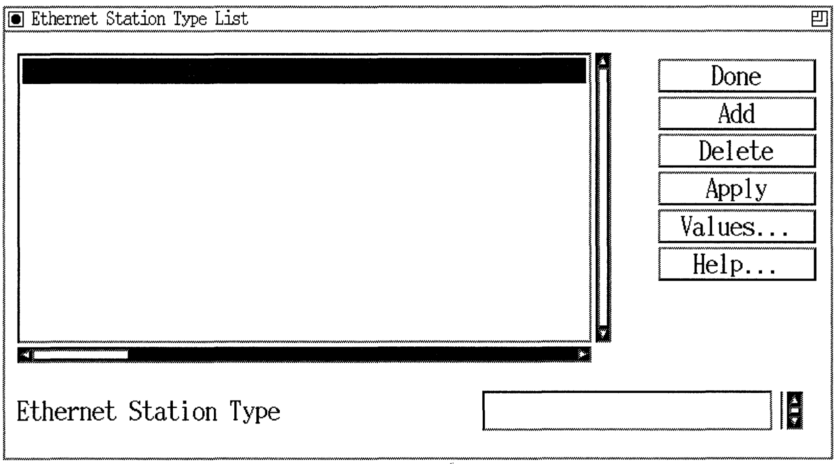



**Figure 4-7. Ethernet Station Type List Window**

2. Click on the Add button. The Translation Bridge (Ethernet) Address Mapping window appears (Figure 4-8).

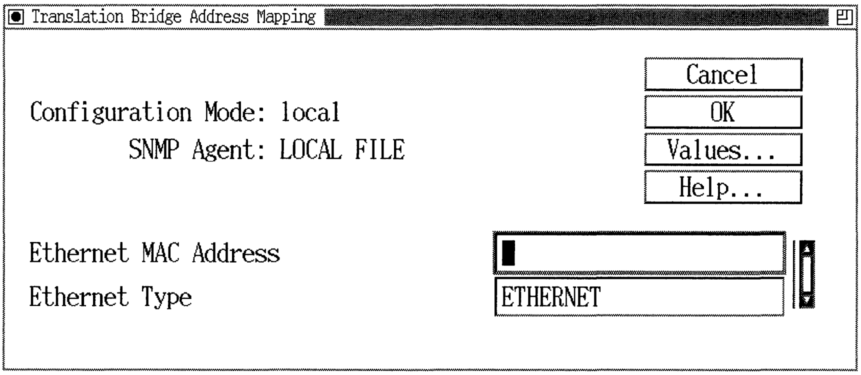



**Figure 4-8. Translation Bridge Station Type Add Window**

3. Edit the parameters, using the descriptions in the next section as a guide.
4. Click on the OK button to save your changes and exit the window. Site Manager returns you to the Ethernet Station Type List window.
5. Click on the Done button to exit the window. Site Manager returns you to the Configuration Manager window.

## Translation Bridge Ethernet Address Mapping Parameter Descriptions

Use these parameter descriptions as a guide when you configure the parameters on the Translation Bridge (Ethernet) Address Mapping window (refer to Figure 4-8).

| | |
|---|---|
| **Parameter:** | **Ethernet MAC Address** |
| Default: | None |
| Options: | Any valid Ethernet MAC address |
| Function: | Indicates the address of the station whose type you want to specify. |
| Instructions: | Enter the Ethernet MAC address of the desired station. |
| MIB Object ID: | 1.3.6.1.4.1.18.3.5.1.1.2.14.1.2 |

| | |
|---|---|
| **Parameter:** | **Ethernet Type** |
| Default: | Ethernet |
| Options: | Ethernet \| IEEE8023 |
| Function: | Specifies the type of frame you want to use for this station, either Ethernet Version 2 (Ethernet) or Ethernet 802.3 (IEEE8023). |
| Instructions: | Select the type you want to use for this station. |
| MIB Object ID: | 1.3.6.1.4.1.18.3.5.1.1.2.14.1.3 |

### Deleting a Station

To delete a station from the station list:

1. Select Protocols→Global Protocols→Translation Bridge→ Ethernet Type List from the Configuration Manager window (refer to Figure 4-3). The Ethernet Station Type List window appears (refer to Figure 4-7).
2. Select the address you want to delete. Then click on the Delete button.
3. Click on the Apply button to save your changes.
4. Click on the Done button to exit the window. Site Manager returns you to the Configuration Manager window.

## Deleting the Translation Bridge from the Router

To delete the translation bridge from the router, select Protocols→ Global Protocols→Translation Bridge→Delete TB from the Configuration Manager window (refer to Figure 4-3).

The translation bridge is no longer enabled on the router.

# Chapter 5
# Using Native Mode LAN Services

This chapter provides an overview of Native Mode LAN (NML) services. It also describes how to use Site Manager to

- Edit NML interface parameters
- Assign an access list to a port

# Native Mode LAN Overview

Native Mode LAN services allow you, as a network administrator, to define closed user groups within a shared bridging environment.

Each NML closed user group consists of multiple LANs and is identified by a closed user group ID (CUGID). You assign the group CUGID to each port that supports a LAN belonging to the closed user group and provide each port with an access list that contains the CUGID. A CUGID is a value in the range of 0-$2^{31}$.

You select a single CUGID for the group and assign the value to each NML-configured port that provides a bridge connection for a LAN in the group. You can also create a range of CUGIDs for the group and assign a different CUGID to each port.

The shared network in Figure 5-1 includes two closed user groups, Star and Moon. Closed User Group Star consists of two local area networks: LAN A on the West Side and LAN C on the East Side. Closed User Group Moon contains three local area networks distributed between the East Side and the West Side: LAN B, LAN D, and LAN E.

Each LAN in a closed user group is connected to a bridge through an NML port. LAN A in the Star Closed User Group, for example, connects to Bridge 1 on NML Port 1. LAN C connects to Bridge 2 through NML Port 6.

NML Port 1 and NML Port 6 are assigned the Star CUGID. They are also provided with an access list that contains the Star CUGID.

An NML port adds its CUGID to each frame that enters the bridge from a closed user group and uses its access list to validate the CUGID on each frame that attempts to exit the bridge through the port. In this way, traffic on the LANs within a closed user group is restricted to frames that bear the group's CUGID.

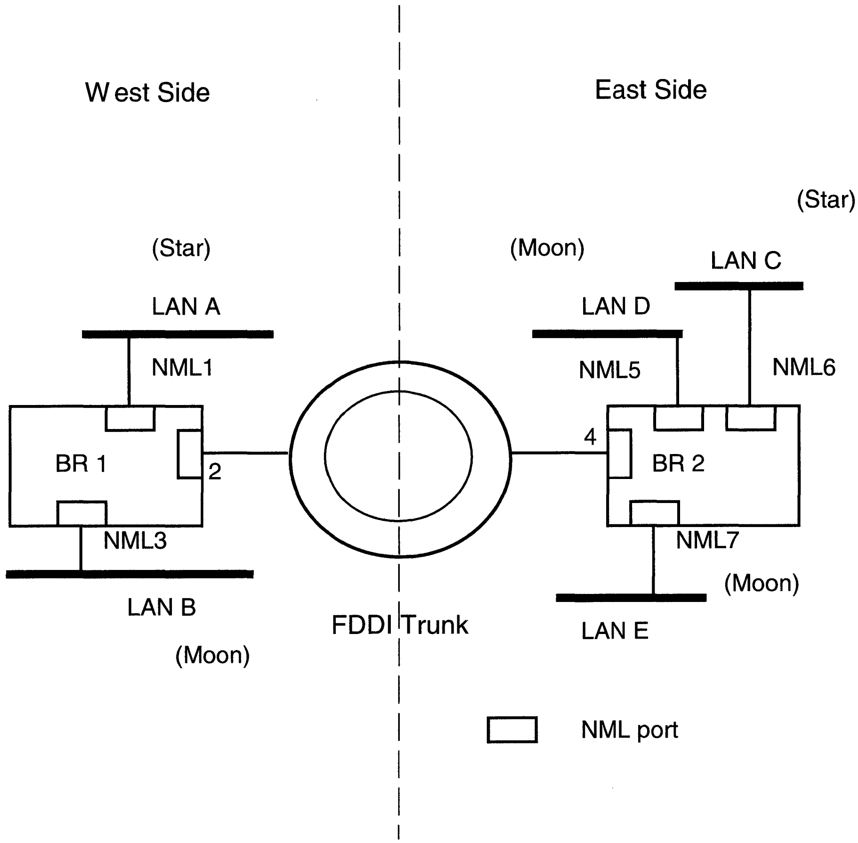



**Figure 5-1. NML Closed User Groups**

In Figure 5-1, for example, consider what happens when a member of the Star Closed User Group on LAN A sends a frame to another member of the Star group located on LAN C.

1. The frame, properly addressed, enters Bridge 1 through NML Port 1.
2. Port 1 labels the frame with the Star CUGID.
3. Bridge 1 forwards the frame to Bridge 2 over the FDDI trunk.

4. The frame attempts to exit Bridge 2 through Port 6. Port 6 examines the CUGID on the frame. The CUGID on the frame matches the CUGID on the port's access list. Port 6 forwards the frame to LAN C in the Star Closed User Group.

## Defining a Closed User Group

To define a closed user group:

1. Select a CUGID for the closed user group.
2. Create an NML port for each LAN in the closed user group by adding the NML protocol to an existing bridge circuit. (Refer to Chapter 2 in *Configuring Wellfleet Routers* for details.)
3. Assign the group CUGID to each port and specify other NML port parameters. Refer to "Editing NML Service Parameters" later in this chapter for details.
4. Provide each NML port with an access list containing the group CUGID. Refer to "Assigning an Access List to a Port" later in this chapter for details.

# Implementation Notes

The following sections describe some Native Mode LAN configuration features.

## Defining a Closed User Group that Permits Overlapping Network Traffic

In an NML environment, overlapping traffic occurs when members of one closed group are allowed to exchange information with users on some, but not all, LANs of another closed group.

To permit overlapping traffic on a LAN that is part of a closed user group, you assign an access list to the LAN's NML port that contains the CUGID for all groups that are allowed access to the LAN. This requires the use of unique CUGIDs for each involved port.

For example, members of the Star group need to exchange information with Moon group members on LAN E. To define LAN E as a LAN that permits overlapping traffic, you assign NML Port 7 an access list that includes both Moon CUGIDs and Star CUGIDs.

## Controlling NML Traffic on a Network Trunk

Network trunks carry the frames of all closed user groups. In Figure 5-1, for example, the FDDI link between Bridge 1 and Bridge 2 is a network trunk. The NML service allows you to control traffic on a trunk by blocking access to the trunk by frames that originate from LANs that you specify. If you determine, for example, that frames originating from a LAN that is part of a given closed user group can never reach their destination via the trunk, you can block the frames from traveling on the trunk. This feature helps reduce network traffic on the trunk by eliminating useless frames.

For example, the Moon user group in Figure 5-1 closes its office on the West Side, dismantling LAN B and NML Port 3. To ensure that no frames destined for Port 3 get onto the FDDI trunk (needlessly increasing the traffic load), you create an NML trunk port, Port 4, and provide it with an access list that contains the CUGIDs of the remaining Moon ports. The NML port checks the CUGID of all frames that attempt to exit from the bridge onto the trunk and drops all frames containing a Moon CUGID.

**Note:** We strongly recommend that you avoid using this feature in conjunction with the spanning tree algorithm.

# Editing NML Parameters

Once you configure a circuit to support NML, you can use the Configuration Manager tool to edit the NML parameters. This section describes how to edit these parameters.

**Note:** The instructions in this section assume that you already configured NML on the router. If you did not, refer to *Configuring Wellfleet Routers* for details.

For each NML parameter, this section provides details on the default setting, valid parameter options, 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 details on using the Technician Interface to access the MIB, refer to *Using Technician Interface Software*.

You access all NML parameters from the Configuration Manager window (Figure 5-2). Refer to the *Configuring Wellfleet Routers* guide for details on accessing this window.

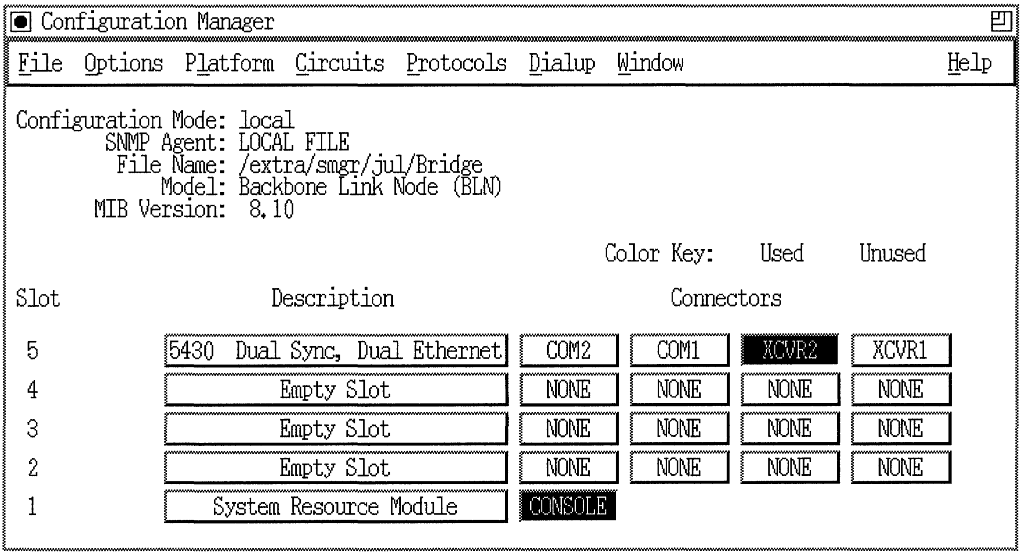



**Figure 5-2. Configuration Manager Window**

# Editing NML Interface Parameters

To edit NML interface parameters:

1. Select Protocols→NML→Interfaces from the Configuration Manager window (refer to Figure 5-2). The NML Interfaces window appears (Figure 5-3).

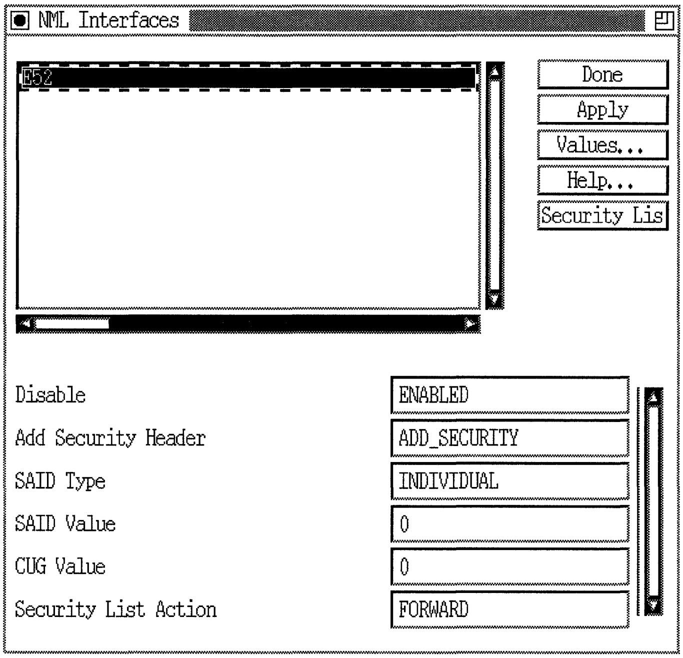



**Figure 5-3. NML Interfaces Window**

2. Edit the parameters, using the descriptions in the next section as a guide.
3. Click on the OK button to save your changes and exit the window. Site Manager returns you to the Configuration Manager window.

## NML Interface Parameter Descriptions

Use the following descriptions as a guide when you configure the parameters on the NML Interfaces window (refer to Figure 5-3).

| | |
|---|---|
| **Parameter:** | **Disabled** |
| Default: | Enabled |
| Options: | Enabled \| Disabled |
| Function: | Enables and disables the NML service on this circuit. |
| Instructions: | Set to Disable if you want to temporarily disable NML on this circuit rather than delete it. Set to Enable if you previously disabled NML but now want to re-enable it. |
| MIB Object ID: | 1.3.6.1.4.1.18.3.5.1.1.5.2.1.2 |

**Parameter:** **Add Security Header**

Default: Add Security

Options: No Security | Add Security | Check Security

Function: Specifies whether the NML port adds a CUGID to frames entering the bridge and performs an access check on frames that exit the bridge.

*Add Security*. The NML port adds a CUGID to every frame that enters the bridge on the circuit and performs an access check on every frame that attempts to exit from the bridge on the circuit. Depending on the option you specify for the Security List Action parameter, the NML port forwards or drops the exiting frame. In forwarding a frame, the NML port strips off the CUGID.

*Check Security*. The NML port performs an access check on each frame that attempts to exit from the bridge on the circuit. Depending on the option you specify for the Security List Action parameter, the NML port forwards or drops the exiting frame. The NML port forwards the frame with the CUGID in place. It does not strip off the identifier.

*No Security*. The port performs no access validation.

Instructions: Specify Add Security for a circuit that provides a bridge connection for a LAN belonging to a closed user group.

Specify Check Security for a circuit that provides a bridge connection for a network trunk. For information about NML services for network trunks, refer to "Controlling NML Traffic on a Network Trunk."

MIB Object ID: 1.3.6.1.4.1.18.3.5.1.1.5.2.1.4

| | |
|---|---|
| **Parameter:** | **SAID Type** |
| Default: | Individual |
| Options: | Individual \| Group |
| Function: | Ignored by Bay Networks. Supplied for 802.10 interoperability. |
| Instructions: | None |
| MIB Object ID: | 1.3.6.1.4.1.18.3.5.1.1.5.2.1.5 |

| | |
|---|---|
| **Parameter:** | **SAID Value** |
| Default: | 0 |
| Options: | 0 to $2^{31}$ (2,147,483,648) |
| Function: | Ignored by Bay Networks. Supplied for 802.10 interoperability. |
| Instructions: | None |
| MIB Object ID: | 1.3.6.1.4.1.18.3.5.1.1.5.2.1.6 |

| | |
|---|---|
| **Parameter:** | **CUG Value** |
| Default: | 0 |
| Options: | A decimal value or a set of values in the range 0 to $2^{31}$ (2,147,483,648) |
| Function: | Specifies the CUGID that you assign to the circuit. |
| Instructions: | In most cases, you create a single CUGID for the closed user group and assign the value to each circuit that supports the group. If you need to specify different access requirements for certain LANs in the closed user group, create a range of CUGIDs and assign a different one to each LAN. |
| MIB Object ID: | 1.3.6.1.4.1.18.3.5.1.1.5.2.1.7 |

| | |
|---|---|
| **Parameter:** | **Security List Action** |
| Default: | Forward |
| Options: | Drop \| Forward |
| Function: | Specifies whether the NML port forwards or drops a frame when it finds a match on the access list. |
| Instructions: | If the access list is an inclusive CUGID list, specify forward. The port forwards to the attached LAN all frames labelled with the CUGID. If the list is an exclusive list. specify drop. The Port drops all frames labelled with the CUGID. |
| MIB Object ID: | 1.3.6.1.4.1.18.3.5.1.1.5.2.1.8 |

# Assigning an Access List to a Port

To validate a frame that is attempting to exit through an NML port, the port consults an access list. If the CUGID on the frame matches a CUGID on the list, the port takes the action you have specified: forwarding the frame and discarding the CUGID, forwarding the frame and retaining the CUGID, or dropping the frame.

You create an inclusive list or an exclusive list for each NML port that supports the closed user group. When the port finds a match on an inclusive list, it forwards the frame. When the NML port finds a match on an exclusive list, it drops the frame.

To assign an access list to a port so that you can specify a start and end range of CUGIDs for the circuit on which the port is located:

1. Select Protocols→NML→Interfaces from the Configuration Manager window (refer to Figure 5-2). The NML Interfaces window appears (refer to Figure 5-3).
2. Click on the Security List button. The NML Filters window appears (refer to Figure 5-4).

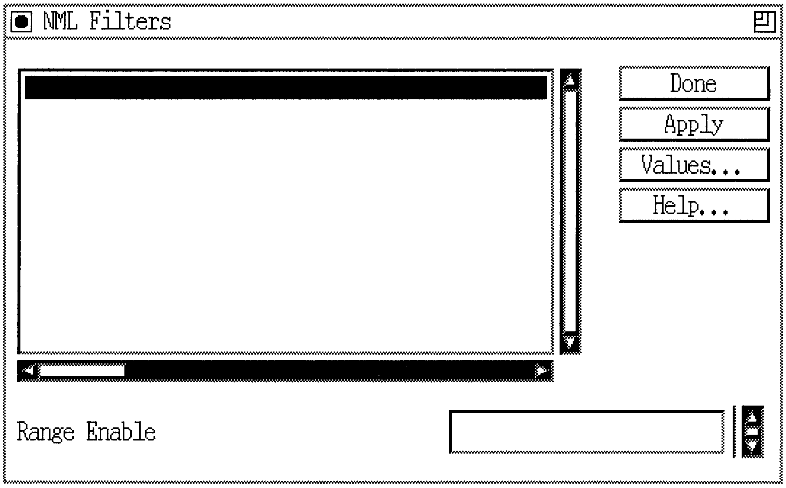



**Figure 5-4. NML Filters Window**

3. Select the circuit to which you want to add an access list.
4. Click on the Add button to add a security range. The NML Add Security Range window appears (Figure 5-5).

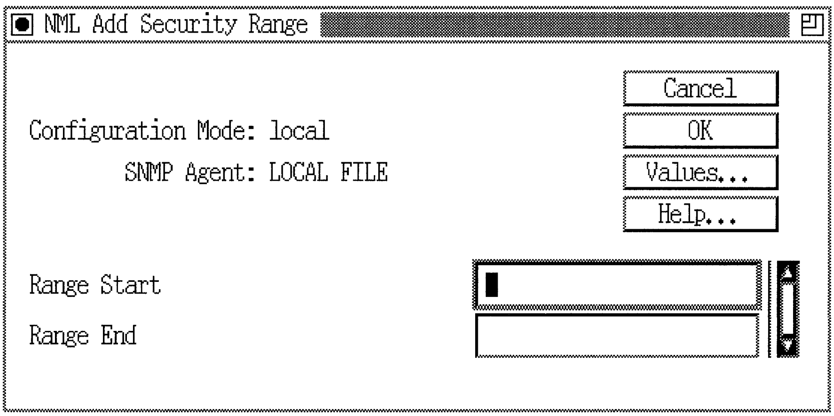



**Figure 5-5. NML Add Security Range Window**

5. Specify a CUGID or a range of CUGIDs, using the parameter descriptions in the next section as a guide.
6. Click on the OK button. Site Manager returns you to the NML Filters window.

**Note:** If you want to disable the ranges you just set, skip to Step 5 in the next section, "Enabling Ranges." Otherwise, continue to Step 7 in this section.

7. Repeat Steps 3 to 6 to add additional start and end ranges.
8. Click on the Apply button to save your changes. Then click on the Done button to exit the window. Site Manager returns you to the NML Interfaces window.
9. Click on the Done button to save your changes and exit the window.

## NML Add Security Range Parameters

Use these parameter descriptions as a guide when you add security ranges for a selected circuit on the NML Add Security Range window (refer to Figure 5-5).

| | |
|---|---|
| **Parameter:** | **Range Start** |
| Default: | None |
| Options: | 0 to $2^{31}$ (2,147,483,648) |
| Function: | Indicates the start of the CUGID range. |
| Instructions: | Enter a value between 0 and $2^{31}$. |
| MIB Object ID: | N/A |

| | |
|---|---|
| **Parameter:** | **Range End** |
| Default: | None |
| Options: | 0 to $2^{31}$ (2,147,483,648) |
| Function: | Indicates the end CUGID range. |
| Instructions: | Enter a value between 0 and $2^{31}$. |
| MIB Object ID: | N/A |

## Enabling Ranges

To enable or disable the ranges you set for a selected circuit:

1. Select the Circuits→Edit Circuits option from the Configuration Manager window (refer to Figure 5-2). The Circuit List window appears (Figure 5-6).

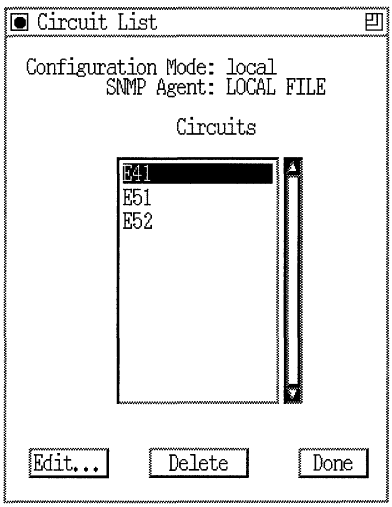



**Figure 5-6. Circuit List Window**

2. Select the circuit whose access list you want to view.

3. Click on the Edit button. The Circuit Definition window appears, with the circuit you selected highlighted (Figure 5-7).

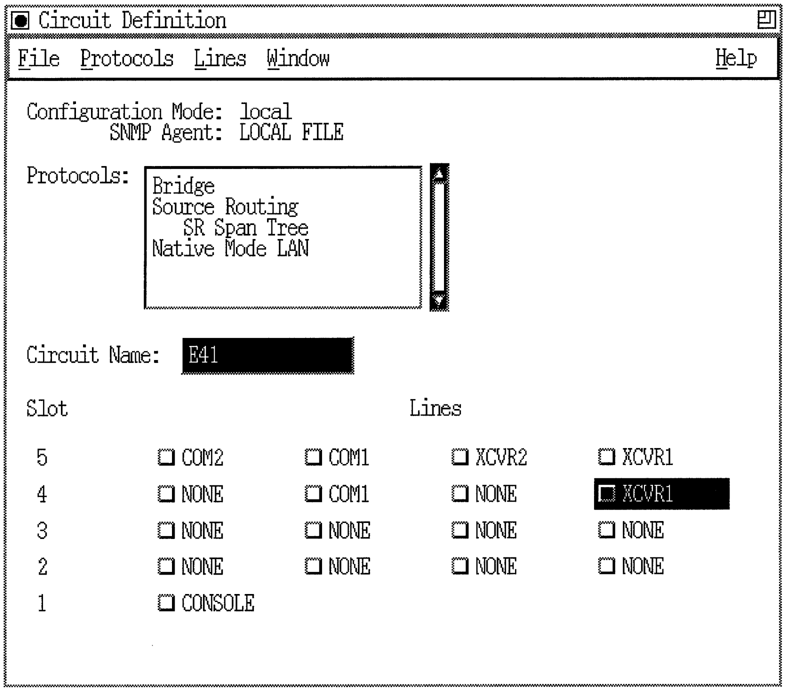



**Figure 5-7. Circuit Definition Window**

4. Select the Protocol➔Edit NML➔Security List option from this window. The NML Filters window appears (refer to Figure 5-4).
5. Set the Range Enable parameter to Enable or Disable, depending on whether you want the ranges you just set for the specified circuit enabled or disabled. Use the parameter description in the next section as a guide.
6. Click on the Done button to save your changes and exit the screen and save your changes.

**Note:** You cannot enable or disable specific ranges in a circuit.

### Range Enable Parameter Description

Use this parameter description as a guide when you enable or disable ranges for a selected circuit on the NML Filters window (refer to Figure 5-4).

| | |
|---|---|
| **Parameter:** | **Range Enable** |
| Default: | Enable |
| Options: | Enable \| Disable |
| Function: | Indicates whether you want the ranges you specified enabled or disabled. |
| Instructions: | Accept the default, Enable, or specify Disable. |
| MIB Object ID: | N/A |

## Deleting NML from the Router

To delete NML from the router:

1. Select Protocols➔NML➔Delete NML from the Configuration Manager window (refer to Figure 5-2). A message appears that prompts:

   ```
   Do you REALLY want to delete NML?
   ```

2. Click on the OK button. You are returned to the Configuration Manager window. NML is no longer configured on the router.

# Index

## Numbers



## A



## B

## C



## D



## E

## F



## G



## H



## I



## L



## M

## N

## O



## P



## Q



## R

## S

## T

## V



## W

Bay Networks
The Merged Company of SynOptics and Wellfleet
8 Federal Street
Billerica, MA 01821