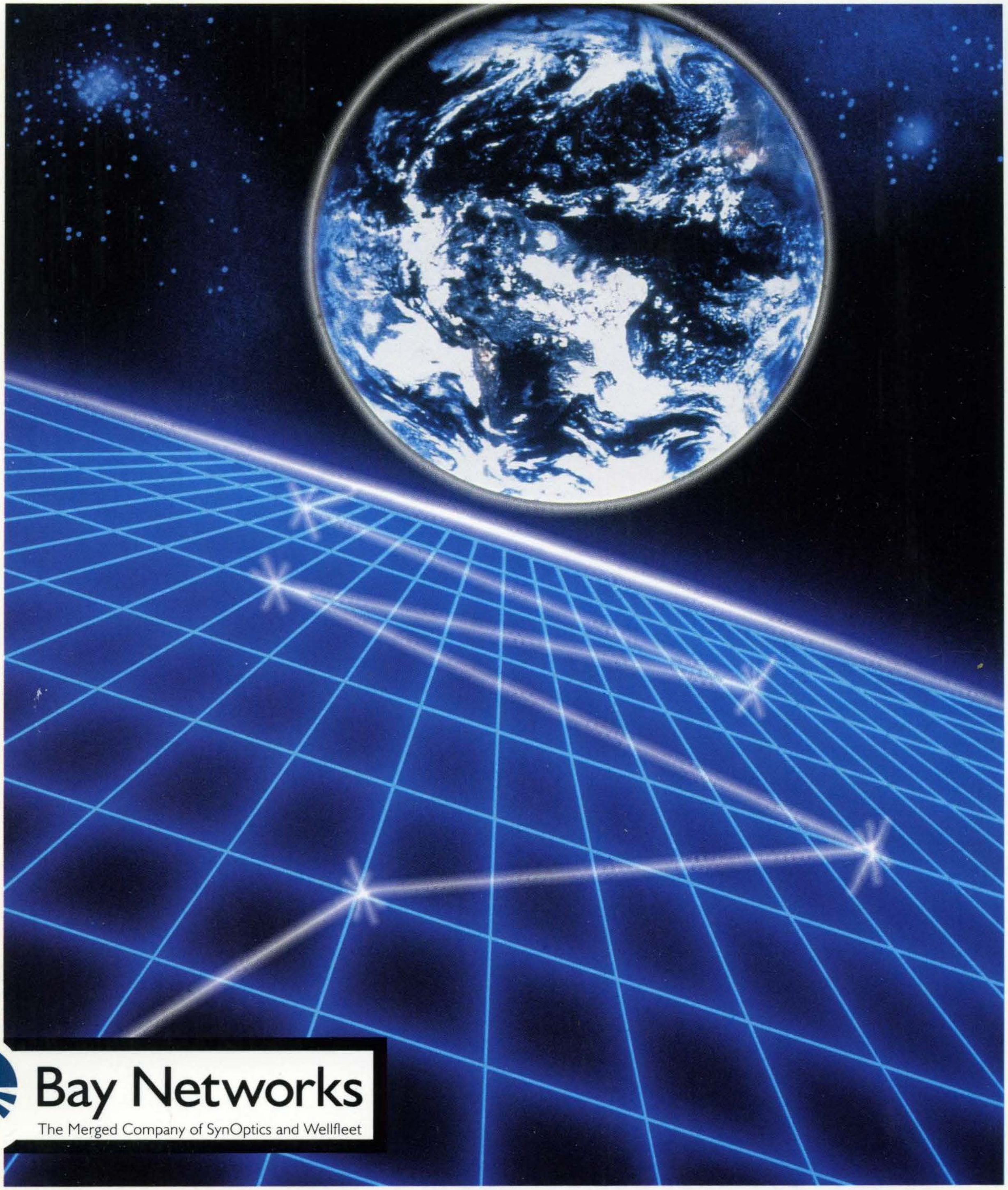


Bay Networks

The Merged Company of SynOptics and Wellfleet

Customizing SNMP, BOOTP, and RARP Services

Part No. 110080 A

Customizing SNMP, BOOTP, and RARP Services

Router Software Version 8.10
Site Manager Software Version 2.10

Part No. 110080 Rev. A
February 1995

Bay Networks
The Merged Company of SynOptics and Wellfleet

Restricted Rights Legend

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

Notice for All Other Executive Agencies

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

Trademarks of Bay Networks, Inc.

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

Third-Party Trademarks

3Com is a registered trademark of 3Com Corporation.

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

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

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

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

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

Fastmac and MADGE are trademarks of Madge Networks, Ltd.

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

HP is a registered trademark of Hewlett-Packard Company.

Intel is a registered trademark of Intel Corporation.

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

MCI is a registered trademark of MCI Communications Corporation.

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

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

Motorola is a registered trademark of Motorola, Inc.

NetBIOS is a trademark of Micro Computer Systems, Inc.

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

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

VINES is a registered trademark of Banyan Systems Incorporated.

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

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

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

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

Bay Networks Software License

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

1. Upon delivery of the Software, Bay Networks grants to licensee a personal, nontransferable, nonexclusive license to use the Software with the Equipment with which or for which it was originally acquired, including use at any of licensee's facilities to which the Equipment may be transferred, for the useful life of the Equipment unless earlier terminated by default or cancellation. Use of the Software shall be limited to such Equipment and to such facility. Software which is licensed for use on hardware not offered by Bay Networks is not subject to restricted use on any Equipment, however, unless otherwise specified on the Documentation, each licensed copy of such Software may only be installed on one hardware item at any time.

2. Licensee may use the Software with backup Equipment only if the Equipment with which or for which it was acquired is inoperative.

3. Licensee may make a single copy of the Software (but not firmware) for safekeeping (archives) or backup purposes.

4. Licensee may modify Software (but not firmware), or combine it with other software, subject to the provision that those portions of the resulting software which incorporate Software are subject to the restrictions of this license. Licensee shall not make the resulting software available for use by any third party.

5. Neither title nor ownership to Software passes to licensee.

6. Licensee shall not provide, or otherwise make available, any Software, in whole or in part, in any form, to any third party. Third parties do not include consultants, subcontractors, or agents of licensee who have licensee's permission to use the Software at licensee's facility, and who have agreed in writing to use the Software only in accordance with the restrictions of this license.

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

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

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

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

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

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

Contents

Chapter 1
Customizing Router Software for SNMP Services

Chapter 2
Customizing Router Software for BOOTP Services

Chapter 3
Customizing Router Software for RARP Services

Index

Figures

Tables

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 router software for the Simple Network Management Protocol (SNMP), Bootstrap Protocol (BOOTP) and Reverse Address Resolution Protocol (RARP) services.

For information and instructions about the following topics, refer to the book *Configuring Wellfleet Routers*:

- Initially configuring and saving an IP 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 IP interface (with SNMP, BOOTP or RARP enabled).
- ❒ 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.

user entry text — Denotes text that you need to enter. Example: Start up the Windows environment by entering the following after the prompt: **win**

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. Example: If the command syntax is **show at routes | nets**, you enter either **show at routes** or **show at nets**, but not both.

Acronyms

ANSI	American National Standards Institute
ARP	Address Resolution Protocol
ATM	Asynchronous Transfer Mode
BOOTP	Bootstrap Protocol
CMIP	Common Management Information Protocol
FDDI	Fiber Distributed Data Interface
IEEE	Institute of Electrical and Electronic Engineers
ILI	intelligent link interface
IS-IS	Intermediate System to Intermediate System
MAC	Media Access Control
MOM	maintenance operations module
MOP	Maintenance Operations Protocol
OSI	Open Systems Interconnection
OSPF	open shortest path first
PCMCIA	Personal Computer Memory Card International Association
PVCs	permanent virtual circuits
RARP	Reverse Address Resolution Protocol
RIP	Routing Information Protocol
SNAP	Subnetwork Access Protocol
SNMP	Simple Network Management Protocol
SRM	system resource modules
SVCs	switched virtual circuits
TCP/IP	Transmission Control Protocol/Internet Protocol
TFTP	Trivial File Transfer Protocol

Chapter 1
Customizing Router Software for SNMP Services

You can tailor your router software to take advantage of a variety of SNMP services. Refer to this chapter for the following information:

- Overview of the Simple Network Management Protocol (SNMP)
- Additional resources that describe SNMP
- Features of the Bay Networks implementation of SNMP
- Accessing and editing SNMP parameters

SNMP Overview

SNMP is a simple request/response protocol that communicates management information between two types of SNMP software entities: SNMP *applications* (also called *SNMP managers*) and SNMP *agents*.

SNMP *applications* run in a network management center and issue queries to gather information about the status, configuration, and performance of external network devices (called *network elements* in SNMP terminology). The Wellfleet Site Manager software is an example of a network management center, and the Wellfleet BN® (backbone node) router is an example of a network element.

SNMP *agents* run in network elements (for example, in the BN) and respond to network management center queries (for example, from Site Manager). In addition, agent software sends unsolicited reports (called *traps*) back to the network management center when certain network activity occurs.

For security reasons, the SNMP agent validates each request from an application entity before responding to the request. The validation procedure consists of verifying that the application entity belongs to an SNMP *community* with access privileges to the agent.

An SNMP community is a logical relationship between an SNMP agent and one or more SNMP managers. The community has a name, and all members of a community have the same access privileges: either read-only (members can view configuration and performance information) or read-write (members can view configuration and performance information, as well as change the configuration).

All SNMP message exchanges consist of a community name and a data field, which contains the SNMP operation and its associated operands. You can configure the SNMP agent to receive requests and send responses only from managers that are members of a known community. If the agent knows the community name in the SNMP message and knows that the application entity generating the request is a member of that community, it considers the message to be authentic and gives it the access allowed for members of that community. Thus, the SNMP community prevents unauthorized managers from viewing or changing the configuration of a router.

For More Information about SNMP

The following documents provide more detail about SNMP design and implementation:

Rose, Marshall T. *The Simple Book.* Englewood Cliffs, New Jersey: Prentice Hall, Inc., 1991.

Stallings, William. *SNMP, SNMP v2, and CMIP. The Practical Guide to Network-Management Standards.* Reading, Mass.: Addison-Wesley Publishing Co., Inc., 1993.

SNMP Implementation Notes

This section contains information about features specific to the Bay Networks implementation of SNMP.

IP

SNMP uses the IP protocol to transport its messages. You must enable IP in order to use SNMP.

Thresholds

SNMP uses a MIB (management information base) to manage the router. The MIB includes an extensive collection of statistics (MIB *variables*) that track the router's performance and provide early warnings of abnormal operating conditions.

The Site Manager threshold feature allows you to specify that when certain statistics reach certain thresholds, the system automatically notifies the network manager.

You can set a threshold for any integer, counter, gauge, or time-tick variable in the MIB. Using the threshold parameters (refer to "Editing Threshold Parameters" later in this chapter), you select the polling interval, which specifies how often the system checks the statistic to see if its value has reached the threshold. You also set three threshold values (high, medium, and low) and specify the threshold action as *Lessthan* or *Greaterthan*.

When the statistic reaches the threshold, the system generates an event. You specify the severity level at which you want the system to log the event. Depending on how you configure the SNMP trap parameters (refer to "Configuring Traps" later in this chapter), SNMP may also send the threshold exception as an SNMP trap.

Threshold Example

For example, you may want SNMP to warn you if the collision rate for an interface becomes excessive. The MIB variable wfCSMACDCerr tracks the number of collisions. Using the threshold parameters, you set a threshold for wfCSMACDCerr. You also set the polling interval to five seconds, to indicate that the system should check variables for which you have configured thresholds every five seconds. You set the threshold action to *Greaterthan* and set the threshold levels and severity of events to the values listed in Table 1-1.

Table 1-1. Example of Threshold and Severity Settings

Threshold Level	Low	Medium	High
Number of collisions per second	5	20	40
Severity of event	INFO	INFO	WARNING

When you add this threshold to the MIB, the system polls the variable wfCSMACDCerr every five seconds and responds as follows:

- If its value is greater than 5, but less than or equal to 20, the system logs an informational event indicating that the low threshold has been exceeded.
- If its value is greater than 20 but less than or equal to 40, the system logs an informational event indicating that a medium threshold has been exceeded.
- If its value is greater than 40, the system logs a warning event indicating that a high threshold has been exceeded.

By default, the threshold event messages include the OID (object identifier) of the variable on which the threshold was exceeded, the value of the variable, and the threshold level exceeded. In other words, if the wfCSMACDCerr variable has a value of 9 in this example, the system generates an event message similar to the following one:

```
   #1:08/27/93 10:53:20.802 INFO SLOT 2 STA CODE: 6

Object 1.3.6.1.4.1.18.4.3.1.1.28.2.1 with value = 9
units/ hour is > low threshold.
```

You can, however, identify objects more easily by configuring the software to report the object name rather than the OID in the event message. To configure the software to report the object name in the event message, use the threshold label parameter (refer to the section "Threshold Interface Parameter Descriptions" later in this chapter). For example if you enter **wfCSMACDCerr** as the threshold label parameter, the system generates an event message similar to the following one:

```
   #1:08/27/93 10:53:20.802 INFO SLOT 2 STA CODE: 6

Object wfCSMACDCerr with value = 9 units/ hour is > low
threshold.
```

If the collision rate stays above a threshold for an extended period of time, the system continues to generate a new event every five seconds. You can specify the maximum number of event messages you want the system to generate before it changes the threshold's state to *held*.

When the threshold is in a held state, the system does not generate new events unless the statistic exceeds the threshold at a different level. If the statistic does not exceed any threshold for a specified number of polling periods, the system no longer considers the threshold held.

Polling statistics to determine whether they have reached a threshold and reporting events when thresholds are exceeded requires router processing capacity. Please be aware that the more thresholds you set and the shorter the polling interval you specify, the greater the likelihood that router performance will be affected.

Traps

Using the SNMP trap parameters, you can configure which event log messages the agent sends to the network management station as traps. You select the traps the agent sends based on slot, protocol entity, and severity level. You can also specify up to 50 *exceptions*, traps that the agent always sends or never sends regardless of slot and regardless of how you configure the trap parameters. Refer to "Editing Trap Parameters" later in this chapter for information on how to specify which traps the agent sends.

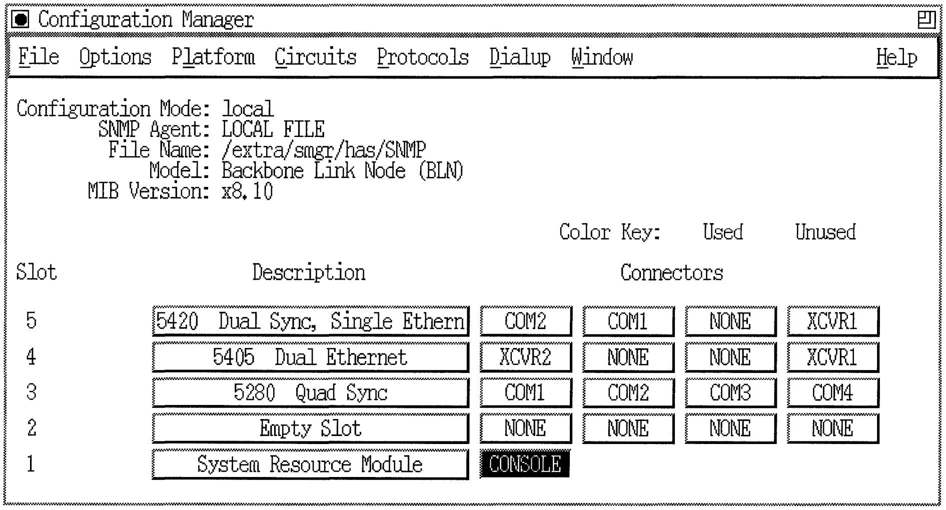
Accessing SNMP Parameters

Use the Configuration Manager to edit or customize SNMP parameters for IP interfaces.

Note: The instructions in this section assume that you have already configured at least one IP interface. If you have *not* yet configured an IP interface, or want to add additional IP interfaces, refer to the book *Configuring Wellfleet Router*s for instructions.

You access all SNMP parameters from the Configuration Manager window (Figure 1-1). Refer to the book *Configuring Wellfleet Routers* for instructions on accessing this window.

This section describes the default setting for each SNMP parameter, all valid setting options, the parameter function, and instructions for setting the parameter.



```
Configuration Mode: local
        SNMP Agent: LOCAL FILE
         File Name: /extra/smgr/has/SNMP
             Model: Backbone Link Node (BLN)
       MIB Version: x8.10
```

Color Key: Used Unused

Slot	Description	Connectors			
5	5420 Dual Sync, Single Ethern	COM2	COM1	NONE	XCVR1
4	5405 Dual Ethernet	XCVR2	NONE	NONE	XCVR1
3	5280 Quad Sync	COM1	COM2	COM3	COM4
2	Empty Slot	NONE	NONE	NONE	NONE
1	System Resource Module	CONSOLE			

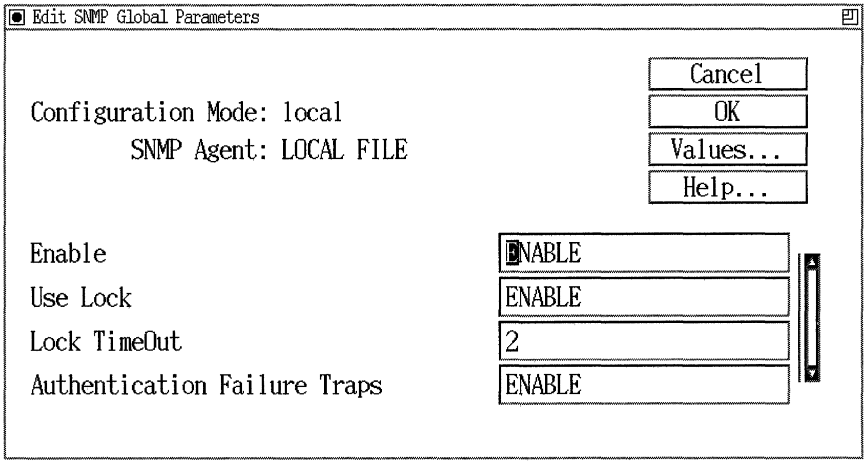
Figure 1-1. Configuration Manager Window

Editing SNMP Global Parameters

To edit SNMP global parameters, begin at the Configuration Manager window (Figure 1-1) and complete the following steps:

1. Select the Protocols→IP→SNMP→Global option.

   The Edit SNMP Global Parameters window appears (Figure 1-2).



Configuration Mode: local

SNMP Agent: LOCAL FILE

Enable	ENABLE
Use Lock	ENABLE
Lock TimeOut	2
Authentication Failure Traps	ENABLE

Figure 1-2. Edit SNMP Global Parameters Window

2. Edit the parameters on this screen, referring to the descriptions following this procedure for guidelines.
3. Click on the OK button when you have configured all values.

SNMP Global Parameter Descriptions

Use the following descriptions as guidelines when setting SNMP global parameters.

Parameter:	**Enable**
Default:	Enable
Options:	Enable | Disable
Function:	Specifies the state of the SNMP agent software on all interfaces that support IP.
Instructions:	Select Enable to enable the SNMP agent software. Select Disable to disable the SNMP agent software.
MIB Object ID:	1.3.6.1.4.1.18.3.5.3.5.1.1

Caution: When you disable the SNMP agent software in dynamic mode, you immediately prohibit the Site Manager from communicating with the router.

Parameter: Use Lock

Default: Enable

Options: Enable | Disable

Function: Specifies whether the agent software responds to multiple network management centers issuing simultaneous SNMP SETs to the router.

Instructions: Select Enable to prohibit the agent software from responding to simultaneous SNMP SETs from multiple network management centers. The agent software responds to the first SNMP SET it receives and locks out subsequent SETs from other network management centers for the duration of the value you specify as the Lock TimeOut. During this lock-out time, the agent software responds to SETs from the network management center that holds the lock; however, it will respond to SETs from other managers with an SNMP genErr GetResponse PDU. Locked out managers log the SNMP genErr GetResponse PDUs as SNMP SET ERROR messages.

Select Disable to allow the router to respond to simultaneous SETs from multiple network management centers.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.5.1.2

Parameter: Lock TimeOut

Default: 2 minutes

Range: 1 to 60 minutes

Function: Specifies the maximum number of minutes the router allows an idle network management center to hold a lock on it. During this time, the agent locks out SNMP SETs from other network management centers. The lock timer is reset each time the locking manager issues a SET.

Instructions: Enter the number of minutes only if you set Use Lock to Enable.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.5.1.4

Parameter: Authentication Failure Traps

Default: Enable

Options: Enable | Disable

Function: Specifies whether the router attempts to generate an Authentication Failure trap when it receives an SNMP message from an SNMP manager falsely claiming to be in a particular community or specifying an unknown community.

Instructions: Select Enable to enable the router to generate Authentication Failure traps. If you select Enable, you must configure an SNMP manager to receive the trap.

Select Disable to prohibit the router from generating Authentication Failure traps.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.5.1.35

Editing SNMP Community Parameters

This section describes how to add, edit, and delete the SNMP communities to which the SNMP agent responds or sends traps. It also describes how to select which managers are members of a particular community.

Note: When you add the first IP interface during a local configuration, the Site Manager automatically creates a read-write public community with a wild card manager (0.0.0.0). Therefore, your router is always SNMP manageable. For security reasons, we recommend that you replace the public community and wild card manager with a unique community configured with a limited list of managers.

Adding an SNMP Community

To add an SNMP community, begin at the Configuration Manager window (refer to Figure 1-1) and complete the following steps:

1. Select the Protocols→IP→SNMP→Communities option.

   The SNMP Community List window appears (Figure 1-3).

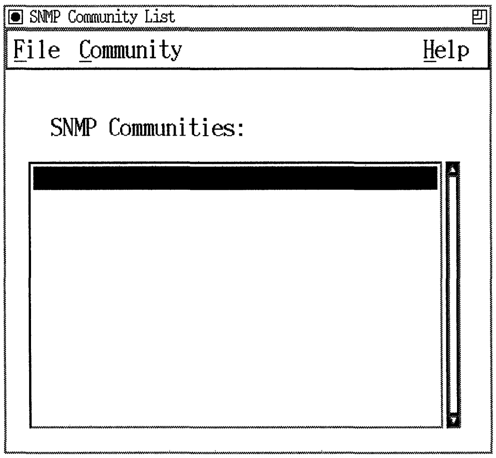
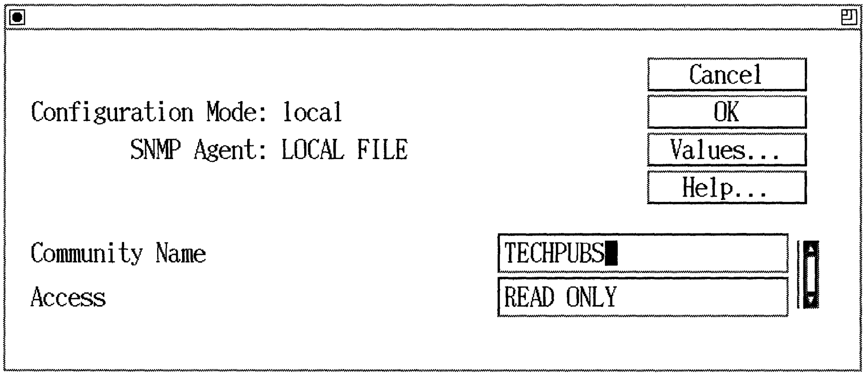


Figure 1-3. SNMP Community List Window

2. Select the Community→Add Community option to display the SNMP Community window (Figure 1-4).



Configuration Mode: local
SNMP Agent: LOCAL FILE

Community Name: TECHPUBS

Access: READ ONLY

Figure 1-4. SNMP Community Window

3. Edit the parameters on this screen, referring to the descriptions following this procedure for guidelines.
4. Click on the OK button to add the SNMP community.
5. Specify the members of the community; refer to the section "Editing SNMP Community Parameters," later in this chapter, for instructions.

SNMP Community Parameter Descriptions

Use the following descriptions as guidelines when setting SNMP Community parameters.

Parameter:	**Community Name**
Default:	None
Range:	Printable ASCII characters
Function:	Specifies the name of the SNMP community.
Instructions:	Enter the SNMP community name.
MIB Object ID:	1.3.6.1.4.1.18.3.5.3.5.2.1.3

Parameter:	**Access**
Default:	Read Only
Options:	Read Only | Read-Write
Function:	Specifies the access privileges that the router grants to all members of this SNMP community.
Instructions:	Select Read Only to allow all members of this community to only view configuration and performance information about this router. Select Read-Write to allow all members of this community to both view configuration and performance information about this router and to change the router's configuration.
MIB Object ID:	1.3.6.1.4.1.18.3.5.3.5.2.1.4

Editing an SNMP Community

To edit an SNMP community, begin at the Configuration Manager window (refer to Figure 1-1) and complete the following steps:

1. Select the Protocols→IP→SNMP→Communities option.

   The SNMP Community List window appears (refer to Figure 1-3).

2. Select the community you want to edit.
3. Select the Community→Edit Community option to display the relevant SNMP Community window (refer to Figure 1-4).

   You can change both the name and the access privilege for the community. Refer to the previous section, "Adding an SNMP Community," for instructions on how to configure these parameters.

   If you want to add, edit, or delete community members from this community, refer to the section "Configuring SNMP Community Members" later in this chapter.

Deleting an SNMP Community

To delete an SNMP community, begin at the Configuration Manager window (refer to Figure 1-1) and complete the following steps:

1. Select the Protocols→IP→SNMP→Communities option.

   The SNMP Community List window appears (refer to Figure 1-3).

2. Select the community you want to delete.
3. Select the Community→Delete Community option to display the Delete SNMP Community window.
4. Verify that the proper SNMP community name appears and click on the Delete button to delete the community.

Configuring SNMP Community Members

You can add, edit, and delete a particular SNMP community's members (called *managers*).

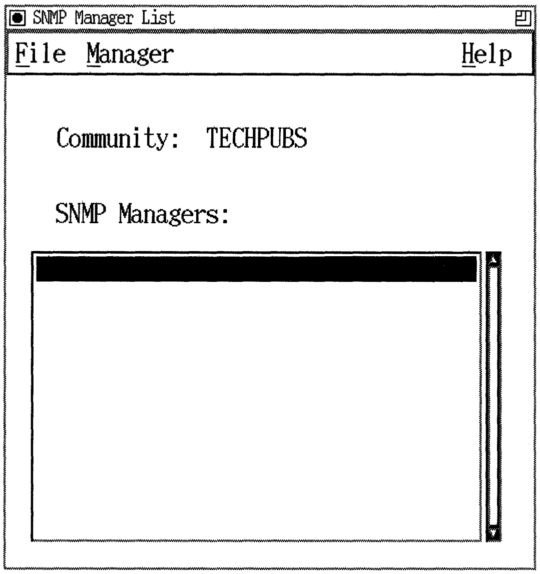
Adding a Manager

To add a manager, begin at the Configuration Manager window (refer to Figure 1-1) and complete the following steps:

1. Select the Protocols➔IP➔SNMP➔Communities option.

   The SNMP Community List window appears (refer to Figure 1-3).

2. Select the community to which you want to add managers.
3. Select the Community➔Managers option to display the SNMP Manager List window for that community (Figure 1-5).

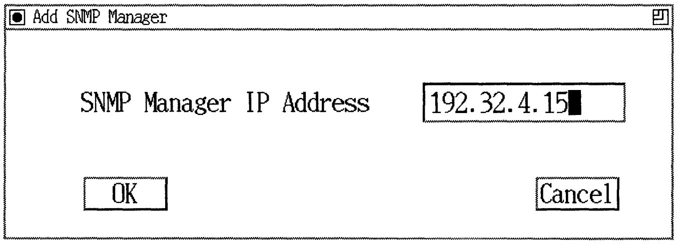


Community: TECHPUBS

SNMP Managers:

Figure 1-5. SNMP Manager List Window

4. Select the Manager→Add Manager option to display the Add SNMP Manager window (Figure 1-6).



SNMP Manager IP Address 192.32.4.15

Figure 1-6. Add SNMP Manager Window

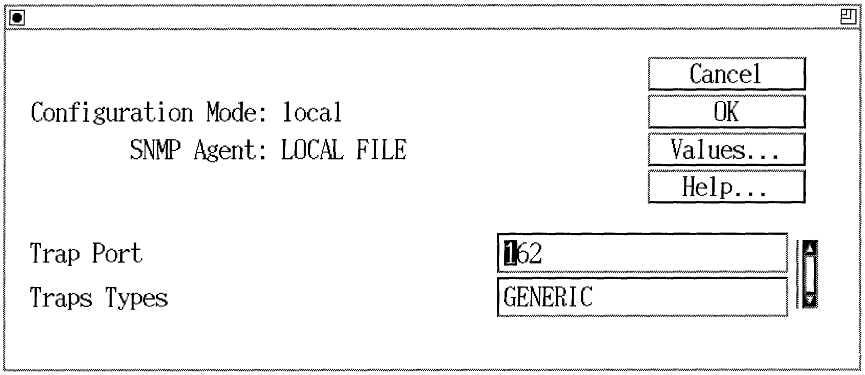
5. Type in the IP address of the SNMP manager you want to add.
6. Click on the OK button.
7. Configure the manager to receive traps from the router agent software; refer to the following section, "Editing a Manager," for instructions.

Editing a Manager

When you edit a manager, you determine whether the manager receives traps and what types of traps the router agent software transmits to that manager. To edit a manager, begin at the Configuration Manager window (refer to Figure 1-1) and complete the following steps:

1. Select the Protocols→IP→SNMP→Communities option.

   The SNMP Community List window appears (refer to Figure 1-3).
2. Select the community for which you want to edit the manager.
3. Select the Community→Managers option to display the SNMP Manager List window for that community (refer to Figure 1-5).
4. Select the manager you want to edit.
5. Select the Manager→Edit Manager option to display the SNMP Manager window (Figure 1-7).



Configuration Mode: local

SNMP Agent: LOCAL FILE

Trap Port: 162

Traps Types: GENERIC

Figure 1-7. SNMP Manager Window

6. Edit the parameters on this screen, referring to the parameter descriptions following this procedure for guidelines.
7. Click on the OK button when all parameters are configured.

SNMP Manager Parameter Descriptions

Use the following descriptions as guidelines when setting SNMP Manager parameters.

Parameter:	**Trap Port**
Default:	162
Range:	1 to 9999
Function:	Specifies the number of the port on the managing station to which the agent software transmits traps.
Instructions:	The standard port number for trap messages is 162; however, you may enter a different port number. Be sure not to specify a port that is used by another application.
MIB Object ID:	1.3.6.1.4.1.18.3.5.3.5.3.1.5

Parameter:	**Traps Types**
Default:	Generic
Options:	None | Generic | Specific | All
Function:	Specifies the type of trap the agent software transmits to this manager.
Instructions:	Select None to prohibit the agent software from transmitting traps to this manager. Select Generic to configure the agent software to transmit the well-defined SNMP traps (cold start, warm start, and Authentication Failure traps) to the manager. The well-defined cold start and warm start traps are automatically enabled in the SNMP agent software; however, you must enable the Authentication Failure Traps parameter for the agent software to transmit such traps to this manager. Select Specific to configure the agent software to transmit all log event traps that you have enabled to this manager. Select All to transmit to this manager cold start and warm start traps, as well as all traps that you have enabled.
MIB Object ID:	1.3.6.1.4.1.18.3.5.3.5.3.1.6

Deleting a Manager

To delete a manager from an SNMP community, begin at the Configuration Manager window (refer to Figure 1-1) and complete the following steps:

1. Select the Protocols➔IP➔SNMP➔Communities option.

   The SNMP Community List window appears (refer to Figure 1-3).

2. Select the community from which you want to delete the manager.
3. Select the Community➔Managers option to display the SNMP Manager List window for that community (refer to Figure 1-5).

4. Select the manager you want to delete.
5. Select the Manager→Delete Manager option to display the Delete SNMP Manager window.
6. Verify that the proper manager IP address appears.
7. Click on the Delete button.

Editing Threshold Parameters

You can configure thresholds for any integer, counter, gauge, or time-tick variable in the MIB. Refer to the section "SNMP Implementation Notes" earlier in this chapter for more information about using thresholds.

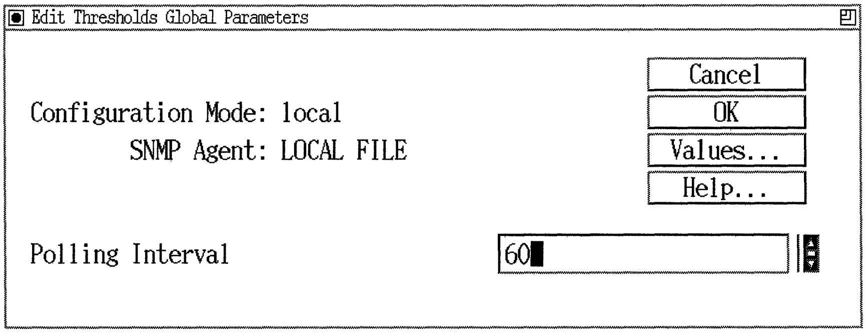
This section describes all individual threshold parameters, and how to configure the threshold polling interval.

Configuring the Threshold Polling Interval

To set the polling interval, begin at the Configuration Manager window (refer to Figure 1-1) and complete the following steps:

1. Select the Protocols→Global Protocols→Thresholds→Global option.

   The Edit Thresholds Global Parameters window appears (Figure 1-8).



Configuration Mode: local
SNMP Agent: LOCAL FILE

Polling Interval 60

Figure 1-8. Edit Thresholds Global Parameters Window

2. Specify the polling interval, referring to the description following this procedure for guidelines.
3. Click on the OK button when you have entered a value.

Threshold Polling Interval Parameter Description

Use the following description as a guideline when setting Threshold Global parameters.

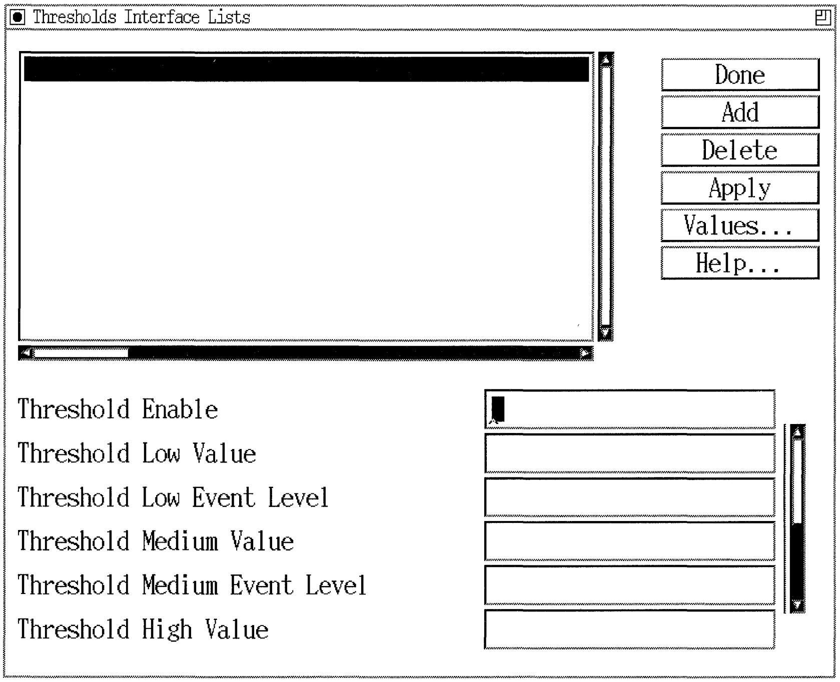
Parameter:	**Polling Interval**
Default:	60 seconds
Range:	5 seconds minimum; no maximum value
Function:	Sets the time interval at which the statistic is polled to determine whether the threshold has been reached.
Instructions:	Specify the number of seconds for the polling interval. Keep in mind that the more often the statistic is polled, the more memory is required to manage the thresholds for this statistic.
MIB Object ID:	1.3.6.1.4.1.18.3.3.2.6.1.2

Configuring a Threshold

To set a threshold, begin at the Configuration Manager window (refer to Figure 1-1) and complete the following steps:

1. Select the Protocols➔Global Protocols➔Thresholds➔Thresholds option.

   The Thresholds Interface Lists window appears (Figure 1-9).



Threshold Enable

Threshold Low Value

Threshold Low Event Level

Threshold Medium Value

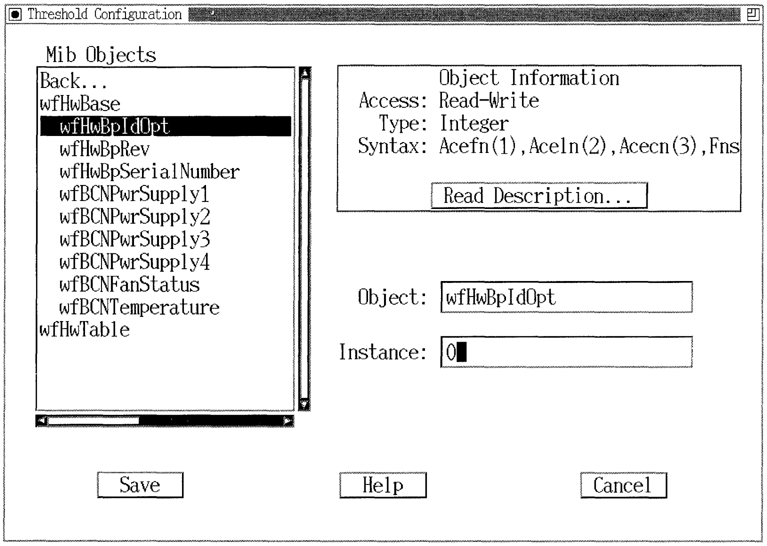
Threshold Medium Event Level

Threshold High Value

Figure 1-9. Thresholds Interface Lists Window

2. Click on the Add button.

   The Threshold Configuration window appears (Figure 1-10), displaying a list of all MIB variables supported by the agent software.



Threshold Configuration

Mib Objects

Back...
wfHwBase
 wfHwBpIdOpt
 wfHwBpRev
 wfHwBpSerialNumber
 wfBCNPwrSupply1
 wfBCNPwrSupply2
 wfBCNPwrSupply3
 wfBCNPwrSupply4
 wfBCNFanStatus
 wfBCNTemperature
wfHwTable

Object Information
Access: Read-Write
Type: Integer
Syntax: Acefn(1),Aceln(2),Acecn(3),Fns

Object: wfHwBpIdOpt

Instance: 0

Figure 1-10. Threshold Configuration Window

3. Select the variable to which you want to apply a threshold.

Note: For complete information about how to navigate through the MIB Variable List window, refer to the statistics section of the book *Managing Wellfleet Routers*.

4. Type in the instance identifier for the variable, if required.
5. Click on the Save button.
6. Edit the Threshold Interface parameters.

   Refer to the parameter descriptions following this procedure for guidelines.
7. Click on the Apply button when you have finished editing the Threshold Interface parameters.
8. Repeat steps 2 to 7 for other thresholds you want to add.
9. Click on the Done button when you have finished adding thresholds.

Threshold Interface Parameter Descriptions

Use the following descriptions as guidelines when setting Threshold Configuration parameters.

Parameter: **Threshold Enable**

Default: Enable

Options: Enable | Disable

Function: Toggles on and off the threshold for the statistic.

Instructions: Select Disable if you want the threshold for this statistic to be ignored.

MIB Object ID: 1.3.6.1.4.1.18.3.3.2.6.2.1.2

Parameter: **Threshold Low Value**

Default: 0

Range: Any integer value

Function: Sets the level of the low threshold for this statistic.

Instructions: Specify the level at which you want the system to generate a low-threshold exception event.

MIB Object ID: 1.3.6.1.4.1.18.3.3.2.6.2.1.5

Parameter: **Threshold Low Event Level**

Default: Info

Options: Info | Warning | Debug

Function: Specifies the severity level assigned to an event message generated when a low threshold is exceeded.

Instructions: Select Info if you want low-threshold exceptions to generate informational events.

Select Warning if you want low-threshold exceptions to generate warning events.

Select Debug if you want low-threshold exceptions to generate debugging events.

MIB Object ID: 1.3.6.1.4.1.18.3.3.2.6.2.1.6

Parameter: **Threshold Medium Value**

Default: 0

Range: Any integer value

Function: Sets the level of the medium threshold for this statistic.

Instructions: Specify the level at which you want the system to generate a medium-threshold exception event.

MIB Object ID: 1.3.6.1.4.1.18.3.3.2.6.2.1.7

Parameter: **Threshold Medium Event Level**

Default: Info

Options: Info | Warning | Debug

Function: Specifies the severity level assigned to an event message generated when a medium threshold is exceeded.

Instructions: Select Info if you want medium-threshold exceptions to generate informational events.

Select Warning if you want medium-threshold exceptions to generate warning events.

Select Debug if you want medium-threshold exceptions to generate debugging events.

MIB Object ID: 1.3.6.1.4.1.18.3.3.2.6.2.1.8

Parameter: **Threshold High Value**

Default: 0 units

Range: Any integer value

Function: Sets the level of the high threshold for this statistic.

Instructions: Specify the level at which you want the system to generate a high-threshold exception event.

MIB Object ID: 1.3.6.1.4.1.18.3.3.2.6.2.1.9

Parameter:	**Threshold High Event Level**
Default:	Info
Options:	Info | Warning | Debug
Function:	Specifies the severity level assigned to an event message generated when a high threshold is exceeded.
Instructions:	Select Info if you want high-threshold exceptions to generate informational events. Select Warning if you want high-threshold exceptions to generate warning events. Select Debug if you want high-threshold exceptions to generate debugging events.
MIB Object ID:	1.3.6.1.4.1.18.3.3.2.6.2.1.10

Parameter:	**Threshold Units**
Default:	Persecond
Options:	Persecond | Absolute
Function:	Specifies the units used to determine whether a threshold has been exceeded.
Instructions:	Select Persecond if you want a threshold event to be generated when the statistic's rate of change *per second* reaches one of the three thresholds. Select Absolute if you want a threshold event to be generated when the value of the statistic reaches one of the three thresholds.
MIB Object ID:	1.3.6.1.4.1.18.3.3.2.6.2.1.12

Parameter: **Threshold Action**

Default: Greaterthan

Options: Greaterthan | Lessthan

Function: Specifies how the thresholds should be evaluated with respect to the threshold values.

Instructions: Select Greaterthan if you want threshold events to be generated when the value of the statistic is *greater than* the thresholds specified.

Select Lessthan if you want threshold events to be generated when the value of the statistic is *less than* the thresholds specified.

MIB Object ID: 1.3.6.1.4.1.18.3.3.2.6.2.1.13

Parameter: **Threshold Max Successive Alarms**

Default: 5 units

Range: Any integer value

Function: Specifies the maximum number of successive alarms that can be generated for this statistic. A successive alarm is defined as two or more polling periods when an alarm is generated as a result of an exception at the same threshold level.

Instructions: Specify the maximum number of successive alarms. When the maximum number of alarms is exceeded, the threshold is marked as held. No more alarms are generated until either the threshold is crossed at a different level or no threshold is crossed for the number of polling intervals specified by Threshold HoldDown Intervals.

MIB Object ID: 1.3.6.1.4.1.18.3.3.2.6.2.1.14

Parameter:	**Threshold HoldDown Intervals**
Default:	1 unit
Range:	Any integer value
Function:	Specifies the number of exception-free polling intervals through which a statistic in a held state must pass before the statistic is no longer considered held.
Instructions:	Specify the number of exception-free polling intervals. The lower the number you select, the more likely you are to get repetitive event messages generated for a statistic that is intermittently exceeding thresholds.
MIB Object ID:	1.3.6.1.4.1.18.3.3.2.6.2.1.15

Parameter: **Threshold Label**

Default: ASN.1 object identifier

Options: ASN.1 or String identifier

Function: This parameter lets you enter the name of the object in string format to replace the ASN.1 identifier. The string you enter appears in the log file, making it easier to identify the object that is the subject of the trap. For example, if you enter the object name **wfSyncTxOctets.2.1** in the Threshold Label field, the log file will contain a report such as

```
Object wfSyncTxOctets.2.1 with value =
235 units/sec is > low threshold
```

Instructions: Type the name of the object. For example, to display `wfSyncTxOctets.2.1` in the log file, type **wfSyncTXOctets.2.1**. You can type any name that you want to appear in the log file. For example, instead of the name *wfSyncTXOctets.2.1*, you could enter **Sync Transmits in Octets**. If you leave this field empty, the ASN.1 identifier for the object appears in the log file.

MIB Object ID: 1.3.6.1.4.1.18.3.3.2.6.2.1.22

Editing Trap Parameters

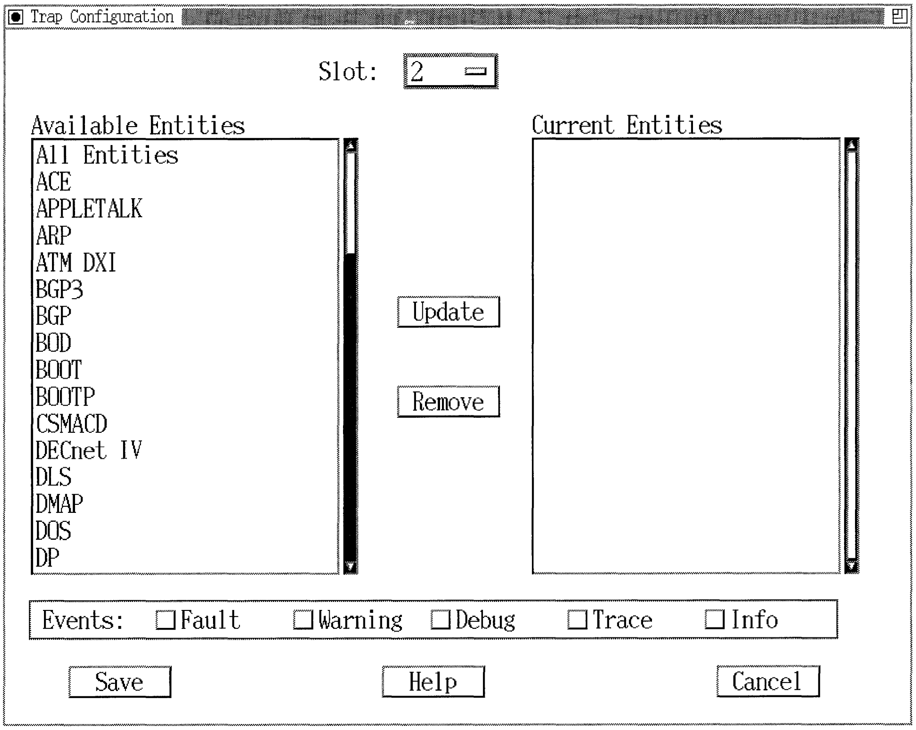
You can specify which traps the SNMP agent sends to the network management station.

Configuring Traps

To specify which traps the agent sends based on slot, protocol entity, and severity level, begin at the Configuration Manager window (refer to Figure 1-1) and complete the following steps:

1. Select the Protocols→IP→SNMP→Trap Configuration→Interfaces option.

   The Trap Configuration window appears (Figure 1-11).



Trap Configuration

Slot: 2

Available Entities

All Entities
ACE
APPLETALK
ARP
ATM DXI
BGP3
BGP
BOD
BOOT
BOOTP
CSMACD
DECnet IV
DLS
DMAP
DOS
DP

Current Entities

Events: □ Fault □ Warning □ Debug □ Trace □ Info

Figure 1-11. Trap Configuration Window

2. Select the slot for which you want to configure traps by clicking on the bar in the Slot box.
3. Choose the entities for which you want to configure traps by selecting the entity name from the Available Entities column, a comprehensive list of all protocols available, regardless of the platform or software you are using.

   If you want to configure traps for all entities running on this slot, select All Entities.
4. Select the severity levels for which you want to receive traps by clicking on the Events boxes at the bottom of the screen.
5. Click on Update to move the entity name to the Current Entities column, thereby indicating that you want to receive traps for this entity at the specified severity levels.

   (To move an entity name out of this column, select the entity name and then click on Remove.)
6. Click on Save when you are done with this screen.

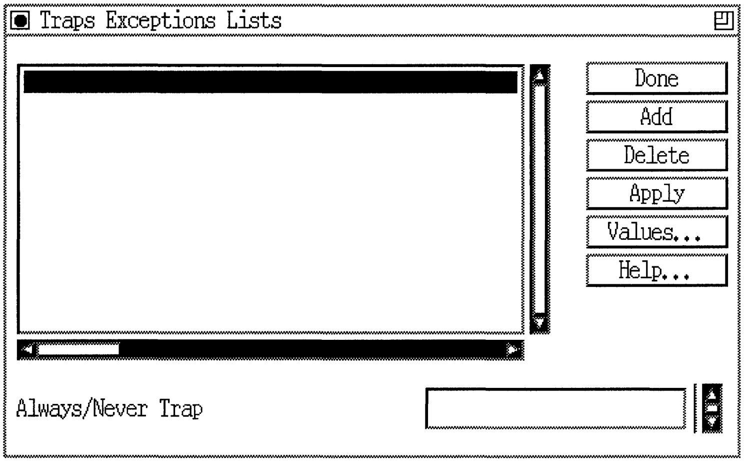
Configuring Exceptions

You can configure up to 50 exceptions, which specify that the SNMP agent always sends or never sends certain traps to the network management station regardless of what you have selected on the Trap Configuration window and *regardless of slot*.

To add an exception, begin at the Configuration Manager window (refer to Figure 1-1) and complete the following steps:

1. Select the Protocols→IP→SNMP→Trap Configuration→Exceptions option.

   The Traps Exceptions Lists window appears (Figure 1-12).

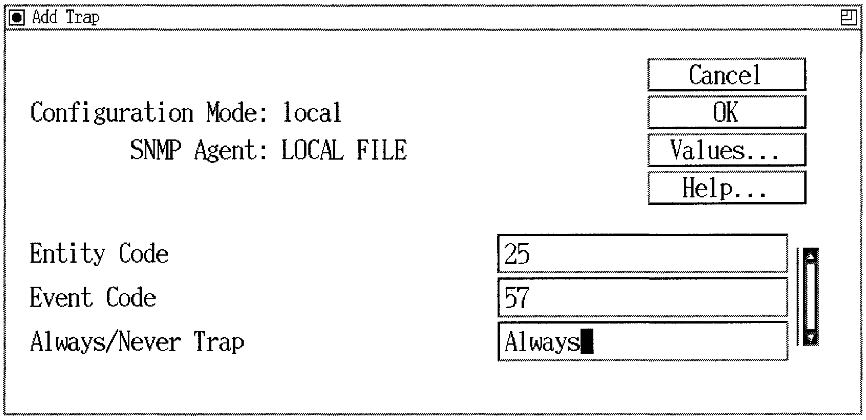


Always/Never Trap

Figure 1-12. Traps Exceptions Lists Window

2. Click on the Add button.

   The Add Trap window appears (Figure 1-13).



Configuration Mode: local
SNMP Agent: LOCAL FILE

Entity Code 25
Event Code 57
Always/Never Trap Always

Figure 1-13. Add Trap Window

3. Edit the parameters on this screen, using the descriptions that follow this procedure as guidelines.
4. Click on the OK button when done.

Trap Interface Parameter Descriptions

Use the following descriptions as a guideline when setting the Add Trap parameters.

Parameter: **Entity Code**

Default: None

Range: Any valid entity code

Function: Specifies the entity code for the event for which you want to configure an exception.

Instructions: Enter the entity code of the event for which you want to configure an exception. Refer to *Event Messages for Wellfleet Routers* for entity codes.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.5.6.1.3

Parameter: **Event Code**

Default: None

Range: Any valid event code

Function: Specifies the code number for the event for which you want to configure an exception.

Instructions: Enter the event code number for the event for which you want to configure an exception. Refer to *Event Messages for Wellfleet Routers* for event codes.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.5.6.1.4

Parameter:	**Always | Never Trap**
Default:	None
Options:	Always | Never
Function:	Specifies whether the SNMP agent always sends or never sends the trap you have entered to the network management station. The instructions you specify in this field override the settings in the Trap Configuration window and affect traps sent from every slot in the router.
Instructions:	Select Always or Never.
MIB Object ID:	1.3.6.1.4.1.18.3.5.3.5.6.1.2

Deleting Exceptions

To delete an exception, begin at the Configuration Manager window (refer to Figure 1-1) and complete the following steps:

1. Select the Protocols➔IP➔SNMP➔Trap Configuration➔Exceptions option.

   The Trap Exceptions Lists window appears (refer to Figure 1-12).

2. Select the trap for which you want to delete the exception.
3. Click on the Delete button.

Chapter 2
Customizing Router Software for BOOTP Services

Using Bootstrap services, you can arrange for your diskless clients to boot from a server located on either their own or another (physical) network. Refer to this chapter for the following information:

- Overview of the Bootstrap Protocol (BOOTP) Relay Agent
- Accessing and editing BOOTP parameters

BOOTP Relay Agent Overview

BOOTP allows a diskless client to request a boot file from a server on the same network or on a different physical network. The requested boot file is then transferred using a transfer protocol (for example, Trivial File Transfer Protocol) from the server host to the diskless client.

The BOOTP *relay agent* (also referred to as BOOTP Gateway or BOOTP Pass-Thru) allows the Wellfleet router to transfer BOOTP packets between diskless client nodes and servers on *different physical networks*, enabling the clients to boot off of remote servers. The client issues a BOOTREQUEST packet to the server, requesting that the server allow the client to boot from it. The server issues a BOOTREPLY packet in response to a BOOTREQUEST packet and sends it to the client. Figure 2-1 shows the fields in the BOOTREQUEST and BOOTREPLY packets.

<table>
<tr><td>Operation (1)</td><td>Hardware type (1)</td><td>Hardware address length (1)</td><td>Hops (1)</td></tr>
<tr><td colspan="4">Transaction ID (4)</td></tr>
<tr><td colspan="2">Seconds (2)</td><td colspan="2">Unused (2)</td></tr>
<tr><td colspan="4">Client IP address (4)</td></tr>
<tr><td colspan="4">Your IP address (4)</td></tr>
<tr><td colspan="4">Server IP address (4)</td></tr>
<tr><td colspan="4">Gateway IP address (16)</td></tr>
<tr><td colspan="4">Client hardware address (16)</td></tr>
<tr><td colspan="4">Server name (64)</td></tr>
<tr><td colspan="4">File name (128)</td></tr>
<tr><td colspan="4">Vendor-specific area (64)</td></tr>
</table>

Figure 2-1. BOOTREQUEST and BOOTREPLY Fields

When a client and a server are on the same physical network, the BOOTP relay agent is not involved in the BOOTP packet exchange. The client transmits a BOOTREQUEST packet to the IP limited broadcast address (255.255.255.255). The server sends a BOOTREPLY packet to the client. Depending on the server's implementation, the packet is addressed to either the limited broadcast or the client's IP address.

When the client and the server are not on the same physical network, a relay agent is required to route the BOOTREQUEST and BOOTREPLY packets to their correct destinations. For example, the client issues a BOOTREQUEST packet that has an IP destination address of 255.255.255.255 (a packet addressed to any other address will be dropped). If an IP network interface on a Wellfleet router is configured to act as a BOOTP relay agent, the interface receives the packet.

The router examines the *seconds* and *hops* fields in the BOOTP packet. The *seconds* field contains the minimum number of seconds that the router waits before forwarding a BOOTREQUEST packet. The *hops* field contains the maximum number of hops that a packet can take between the source and destination devices. If the packet has traversed more hops than is allowed, or if the timer has expired, the router discards the packet.

If the router does not discard the packet, it examines the *gateway IP address* field in the packet. (This field is zero if the client is on a directly attached network.) The router writes the IP address of the interface that received the packet to the *gateway IP address* and the *IP source address* fields and the *hops* field is incremented by 1. The relay agent then determines which networks are to receive this packet and broadcasts it through the appropriate network interfaces.

In addition to receiving BOOTREQUEST packets from clients, the router also receives BOOTREPLY packets from servers. The server sends a BOOTREPLY packet to one of the router's network interfaces that has the BOOTP relay agent implemented on it. The BOOTP server obtains the address of the interface from the *gateway IP address* field in the BOOTREQUEST packet. The UDP destination port number is *BOOTP server.* The *gateway IP address* field in the BOOTP header must be the same as the IP destination address. If it is not the same, the packet is discarded.

If the received BOOTREPLY is acceptable, the UDP destination port is changed to BOOTP client. If the *client IP address* field is not zero, that address is used as the destination IP address and the packet is sent. If the client knows its IP address, it should reply to Address Resolution Protocols (ARPs). If the client does not know its IP address, the router sends the packet using the IP address in the *your IP address* field and the MAC address in the *client hardware address* field.

Configuring a Network Interface with BOOTP

You configure a BOOTP relay agent on individual network interfaces, controlling the following aspects of each relay agent:

- The interfaces to use for broadcasting BOOTREQUEST packets received on a particular interface.
- A maximum value for the *hops* field in a BOOTREQUEST packet. The router discards packets containing a larger *hops* field to prevent broadcast loops.
- A minimum value for the *seconds* field in a BOOTREQUEST packet. The router discards packets containing a smaller value. This feature is useful if the relay agent is supposed to act only after BOOTP attempts on the local network have failed.

Implementation Notes

This section describes implementation notes you should keep in mind when you configure BOOTP for the router.

- You can configure a BOOTP relay agent only on a numbered network interface. Also, for the BOOTP relay agent to operate, you must configure the router in forwarding mode. For instructions on numbering a network interface, refer to the book *Configuring Wellfleet Routers*. For instructions on configuring the router in forwarding mode, refer to the book *Customizing IP Services*.
- You can enhance BOOTP relay agent operation by using traffic filters. For example, a network segment may have two types of clients: one set that is supposed to boot only using servers on the local network and another set that boots from remote servers. You could set up a traffic filter to drop any BOOTREQUEST packets from the first set, as follows:

- *Protocol:* UDP
- *UDP destination port:* BOOTP server
- *User-defined field for the client hardware address in the BOOTP header:* all MAC addresses of clients in the local group
- *action:* DROP

The user-defined field has the following attributes:

- *Reference:* after IP header
- *Offset:* 224 bits (7 longwords into the BOOTP header)
- *Length:* depends on the media (48 bits for LANs)

For instructions on configuring traffic filters, refer to the book *Configuring Filter Options for Wellfleet Routers.*

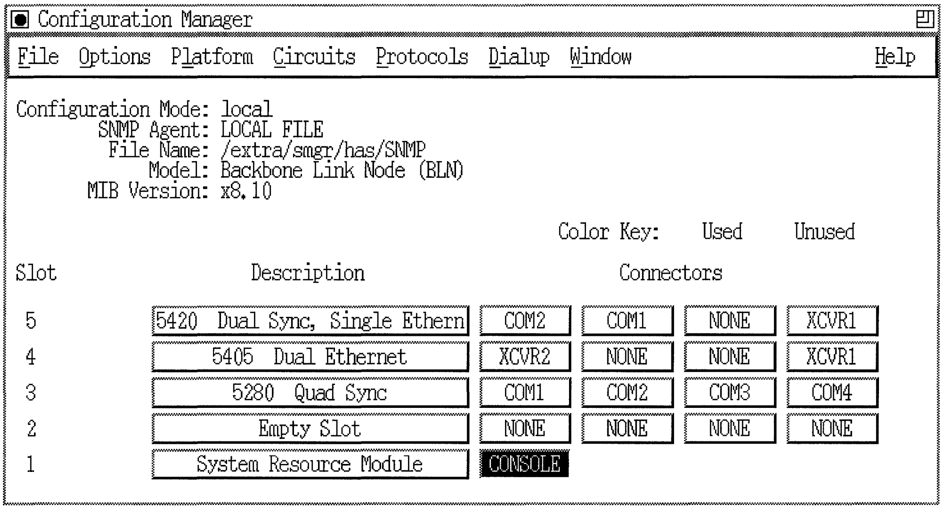
Accessing BOOTP Parameters

Use the Configuration Manager to edit or customize BOOTP parameters for IP interfaces.

Note: The instructions in this section assume that you have already configured at least one IP interface on which you have enabled BOOTP. If you have *not* yet configured an IP interface, or want to add additional IP interfaces, refer to the book *Configuring Wellfleet Routers* for instructions.

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

This section describes the default setting for each BOOTP parameter, all valid setting options, the parameter function, and instructions for setting the parameter.



Configuration Mode: local
SNMP Agent: LOCAL FILE
File Name: /extra/smgr/has/SNMP
Model: Backbone Link Node (BLN)
MIB Version: x8.10

Slot	Description	Connectors			
5	5420 Dual Sync, Single Ethern	COM2	COM1	NONE	XCVR1
4	5405 Dual Ethernet	XCVR2	NONE	NONE	XCVR1
3	5280 Quad Sync	COM1	COM2	COM3	COM4
2	Empty Slot	NONE	NONE	NONE	NONE
1	System Resource Module	CONSOLE			

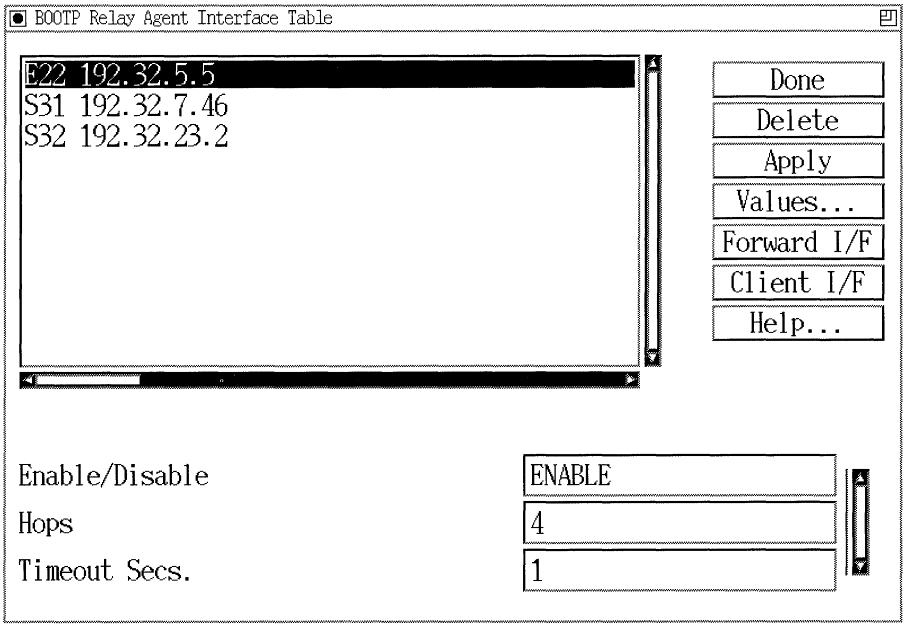
Figure 2-2. Configuration Manager Window

Editing BOOTP Relay Agent Parameters

To edit BOOTP relay agent parameters, begin at the Configuration Manager window (Figure 2-2) and proceed as follows:

1. Select the Protocols→IP→BOOTP→ Relay Agent Interface Table option.

   The BOOTP Relay Agent Interface Table window appears (Figure 2-3). This window lists all the IP interfaces on the router that have BOOTP configured on them.



E22 192.32.5.5
S31 192.32.7.46
S32 192.32.23.2

Enable/Disable ENABLE
Hops 4
Timeout Secs. 1

Figure 2-3. BOOTP Relay Agent Interface Table Window

2. Click on the interface for which you want to edit BOOTP parameters.
3. Edit the parameters you want to change.

   Refer to the descriptions following this procedure for guidelines on editing BOOTP parameters.
4. Click on the Apply button to implement your changes.

   If you wish, you can create the BOOTP relay agent forwarding table and the BOOTP client interface table from this window. To create the relay agent forwarding table, refer to “Creating the BOOTP Relay Agent Forwarding Table,” later in this chapter. To create the client interface table, refer to “Creating the BOOTP Client Interface Table,” later in this chapter.
5. Click on the Done button to exit the window.

Parameter: **Enable | Disable**

Default: Enable

Options: Enable | Disable

Function: Specifies whether BOOTP is enabled on the specified network interface.

Instructions: Accept the default, Enable, to enable BOOTP on the network interface. Select Disable to disable BOOTP on the network interface.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.8.3.1.1.2

Parameter: **Hops**

Default: 4

Range: 1 to 16 hops

Function: Specifies the maximum number of hops from the client to the server. A hop is the logical distance between two devices. If the value in the *hops* field of a BOOTREQUEST packet is greater than the number you specify for the Hops parameter, the router drops the packet.

Instructions: Accept the default of 4 hops or specify a number between 1 and 16, inclusive.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.8.3.1.1.5

Parameter: **Timeout Secs.**

Default: 0 second

Range: 0 to 65535 seconds

Function: Specifies the minimum number of seconds that the router waits before forwarding a BOOTREQUEST packet. If the value in the *seconds* field of a BOOTREQUEST packet is less than the value you specify for the Timeout Secs. parameter, the router drops the packet.

Instructions: Accept the default, 0, or specify a number between 1 and 65535, inclusive.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.8.3.1.1.6

Creating the BOOTP Relay Agent Forwarding Table

The BOOTP relay agent forwarding table allows you to specify the IP interface that receives the BOOTREQUEST packets from the external network (incoming IP interface), and the IP interface that passes the BOOTREQUEST packets out the router to the destination device (outgoing IP interface).

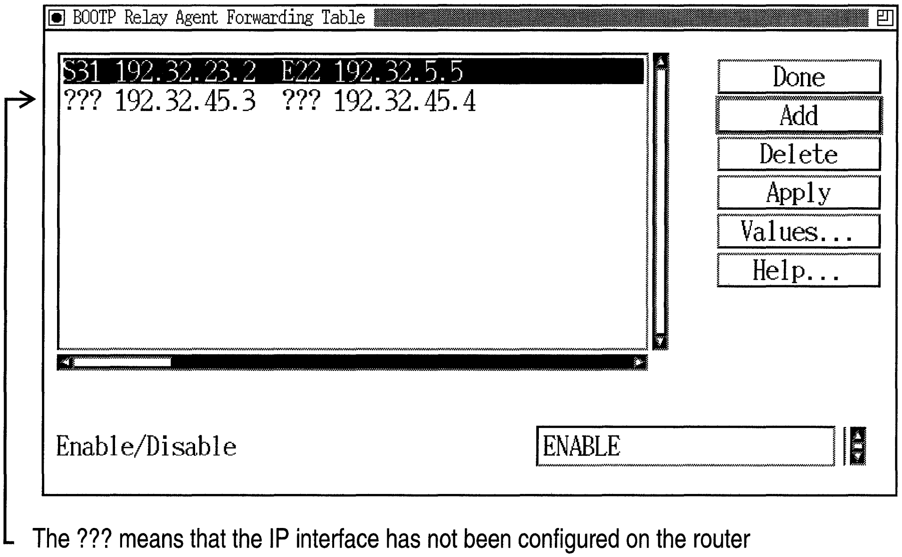
Depending on the configuration of your network, you can specify

- One incoming IP interface to forward packets to multiple outgoing IP interfaces
- Multiple incoming interfaces to forward to multiple outgoing interfaces
- Multiple incoming interfaces to forward to one outgoing interface

To create the BOOTP relay agent forwarding table, begin at the BOOTP Relay Agent Interface Table window (refer to Figure 2-3) and proceed as follows:

1. Click on the Forward I/F button.

   The BOOTP Relay Agent Forwarding Table window appears (Figure 2-4).



BOOTP Relay Agent Forwarding Table

```
S31 192.32.23.2   E22 192.32.5.5
??? 192.32.45.3   ??? 192.32.45.4
```

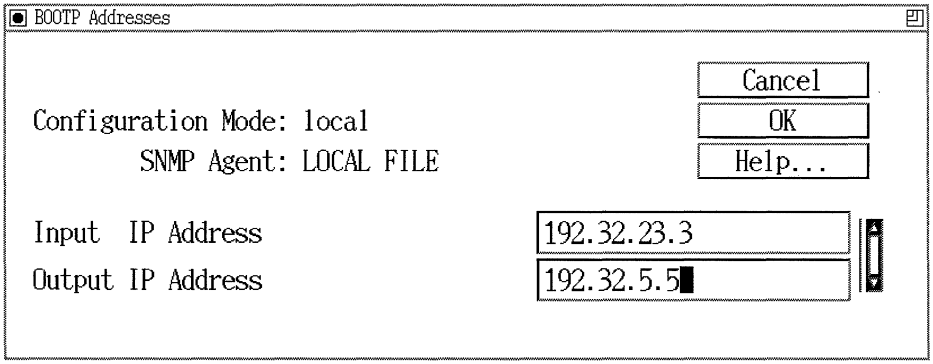
Enable/Disable ENABLE

The ??? means that the IP interface has not been configured on the router

Figure 2-4. BOOTP Relay Agent Forwarding Table Window

2. Click on the Add button.

   The BOOTP Addresses window appears (Figure 2-5).



BOOTP Addresses

Configuration Mode: local
SNMP Agent: LOCAL FILE

Input IP Address 192.32.23.3
Output IP Address 192.32.5.5

Figure 2-5. BOOTP Addresses Window

3. Specify the input IP address and output IP address parameters.
4. Click on the OK button.

   The BOOTP Relay Agent Forwarding Table window now lists the relay agent you added. Note that if you entered an IP address that has not yet been configured on the router, "`???`" appears before the output IP address (e.g., `??? 111.111.111.111`). When you add the IP address to the system, Site Manager replaces the "`???`" with the appropriate address.
5. Click on the Done button to exit the window.

Parameter: **Input IP Address**
Default: None
Range: Any valid IP address
Function: Specifies the IP interface that receives BOOTREQUEST packets from an external network. This interface must have BOOTP configured on it.
Instructions: Enter an IP address for the IP interface that has BOOTP configured on it.
MIB Object ID: 1.3.6.1.4.1.18.3.5.3.8.3.2.1.3

Parameter: **Output IP Address**
Default: None
Range: Any valid IP address
Function: Specifies the IP interface that forwards BOOTREQUEST packets to an external network.
Instructions: Enter the appropriate IP address.
MIB Object ID: 1.3.6.1.4.1.18.3.5.3.8.3.2.1.4

Parameter:	**Enable | Disable**
Default:	Enable
Options:	Enable | Disable
Function:	Specifies whether the Input IP Address/Output IP Address pair is enabled.
Instructions:	Accept the default, Enable, to enable BOOTP forwarding for the address pair. Select Disable to disable BOOTP forwarding for the address pair.
MIB Object ID:	1.3.6.1.4.1.18.3.5.3.8.3.2.1.2

Disabling an Input/Output Address Pair

To enable or disable an input/output IP address pair, begin at the BOOTP Relay Agent Forwarding Table window (refer to Figure 2-4) and proceed as follows:

1. Edit the Enable | Disable parameter as described in the previous section.
2. Click on the Apply button to implement your changes.
3. Click on the Done button to exit the BOOTP Relay Agent Forwarding Table window.

Deleting an Input/Output Address Pair

To delete an input/output address pair, begin at the BOOTP Relay Agent Forwarding Table window (refer to Figure 2-4) and proceed as follows:

1. Click on the address pair to select it.
2. Click on the Delete button.

   The BOOTP Relay Agent Forwarding Table window no longer displays the address pair.
3. Click on the Done button to exit the window.

Creating the BOOTP Client Interface Table

You must create a BOOTP client interface table if you intend to configure an Access Node to use EZ-Install over a frame relay permanent virtual circuit (PVC) in group access mode. You do not need to create this table if the frame relay PVC is configured to operate in direct access mode.

The BOOTP client interface table allows you to specify and pair the IP address of a remote Access Node that will boot via EZ-Install with the local Data Link Connection Identifier (DLCI) of its frame relay group access PVC.

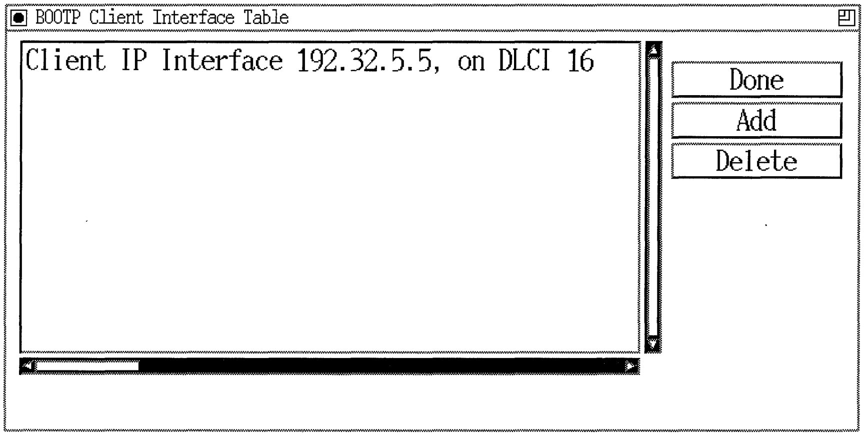
For information about configuring an AN to use EZ-Install, refer to *Installing and Starting AN Routers*.

For information about DLCI and frame relay, refer to *Customizing Frame Relay Services*.

To create the BOOTP client interface table, begin at the BOOTP Relay Agent Interface Table window (refer to Figure 2-3) and proceed as follows:

1. Click on the Client I/F button.

   The BOOTP Client Interface Table window appears (Figure 2-6).



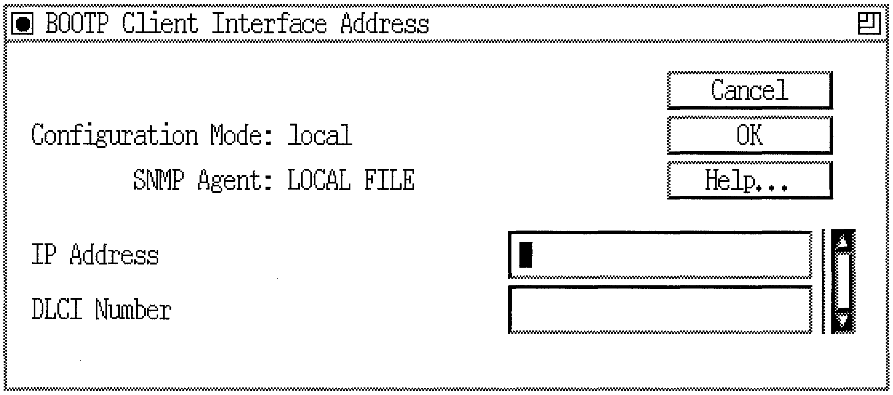
BOOTP Client Interface Table

Client IP Interface 192.32.5.5, on DLCI 16

Figure 2-6. BOOTP Client Interface Table Window

2. Click on the Add button.

   The BOOTP Client Interface Address window appears (Figure 2-7).



BOOTP Client Interface Address

Configuration Mode: local

SNMP Agent: LOCAL FILE

IP Address

DLCI Number

Figure 2-7. BOOTP Client Interface Address Window

3. Enter values for the Boot Node IP Address and DLCI Number parameters, using the descriptions following this procedure for guidelines.
4. Click on the OK button.

   The BOOTP Client Interface Table window now lists the client IP interface and the DLCI number you added.
5. Click on the Done button to exit the window.

BOOTP Client Interface Address Parameter Descriptions

Use the following descriptions as guidelines when setting BOOTP Client Interface Address parameters.

Parameter:	**IP Address**
Default:	None
Range:	Any valid IP address
Function:	Specifies the IP address of the remote Access Node that will boot using EZ-Install over a frame relay group access PVC connection to the router.
Instructions:	Enter the IP address of the remote Access Node router.
MIB Object ID:	1.3.6.1.4.1.18.3.5.3.8.1.1.1.3

Parameter:	**DLCI Number**
Default:	None
Range:	16 to 1007
Function:	Specifies the frame relay PVC identification number whose destination is the remote Access Node that will boot using EZ-Install. The frame relay network uses the DLCI number to direct data flow.
Instructions:	Enter the DLCI number, in decimal format, for the group access PVC to the remote Access Node. Use the DLCI number assigned by your frame relay service provider.
MIB Object ID:	1.3.6.1.4.1.18.3.5.3.8.1.1.1.2

Deleting the BOOTP Relay Agent from an IP Interface

To delete a BOOTP relay agent, begin at the Configuration Manager window (refer to Figure 2-2) and proceed as follows:

1. Select the Protocols➔IP➔BOOTP➔Relay Agent Interface Table option.

   The BOOTP Relay Agent Interface Table window appears (refer to Figure 2-3).

2. Click on the interface from which you want to delete BOOTP.
3. Click on the Delete button.

   The BOOTP relay agent and all of the forwarding table entries that you specified are deleted from the selected interface.

Deleting BOOTP Globally

To globally delete BOOTP on the router, begin at the Configuration Manager window (refer to Figure 2-2) and proceed as follows:

1. Select the Protocols→IP→BOOTP→Delete option.
2. Click on the Delete button.

   BOOTP is globally deleted from the router.

Chapter 3
Customizing Router Software for RARP Services

You can transform your router into a RARP server that assigns IP addresses to its clients on the local area net. Refer to this chapter for the following information:

- Overview of the Reverse Address Resolution Protocol (RARP)
- Accessing and editing RARP parameters

RARP Overview

RARP allows the Wellfleet router to act as a RARP server. A RARP address server supplies client hosts on the same physical or logical LAN with IP addresses (Figure 3-1).

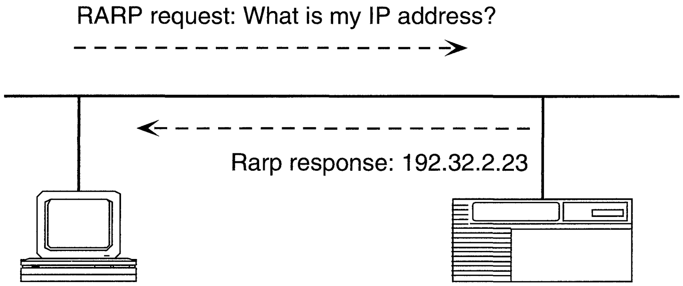

RARP request: What is my IP address?
Rarp response: 192.32.2.23

Figure 3-1. RARP Server Supplying an IP Address

When you enable RARP support on the router, you define a MAC address-to-IP address mapping table. When a client host needs to be assigned an IP address, it broadcasts a RARP request specifying its MAC address. Upon receiving a RARP request, the router refers to its MAC address-to-IP address mapping table, then sends the host a response packet containing the corresponding IP address. The client host uses the IP address specified in the response packet as its IP address.

You can configure RARP support on Ethernet, Token Ring, and FDDI interfaces.

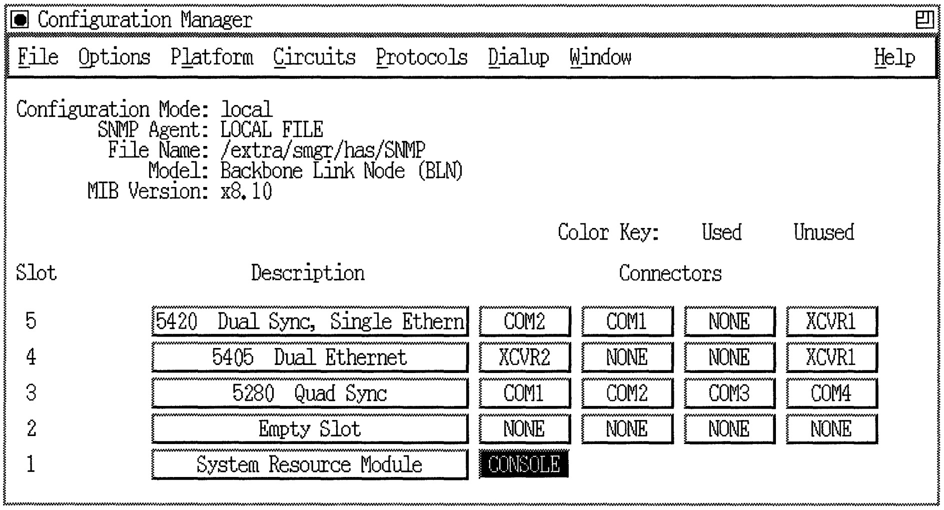
Accessing RARP Parameters

This section describes how to use the Configuration Manager tool to edit, or customize, RARP parameters.

Note: The instructions in this section assume that you have already configured at least one IP interface on which you have enabled RARP. If you have *not* yet configured an IP interface, or want to add additional IP interfaces, refer to *Configuring Wellfleet Router*s for instructions.

You access all RARP parameters from the Configuration Manager window (Figure 3-2). Refer to *Configuring Wellfleet Routers* for instructions on accessing this window.

This section describes the default setting for each RARP parameter, all valid setting options, the parameter function, and instructions for setting the parameter.



```
Configuration Mode: local
        SNMP Agent: LOCAL FILE
         File Name: /extra/smgr/has/SNMP
             Model: Backbone Link Node (BLN)
       MIB Version: x8.10
```

Color Key: Used Unused

Slot	Description	Connectors			
5	5420 Dual Sync, Single Ethern	COM2	COM1	NONE	XCVR1
4	5405 Dual Ethernet	XCVR2	NONE	NONE	XCVR1
3	5280 Quad Sync	COM1	COM2	COM3	COM4
2	Empty Slot	NONE	NONE	NONE	NONE
1	System Resource Module	CONSOLE			

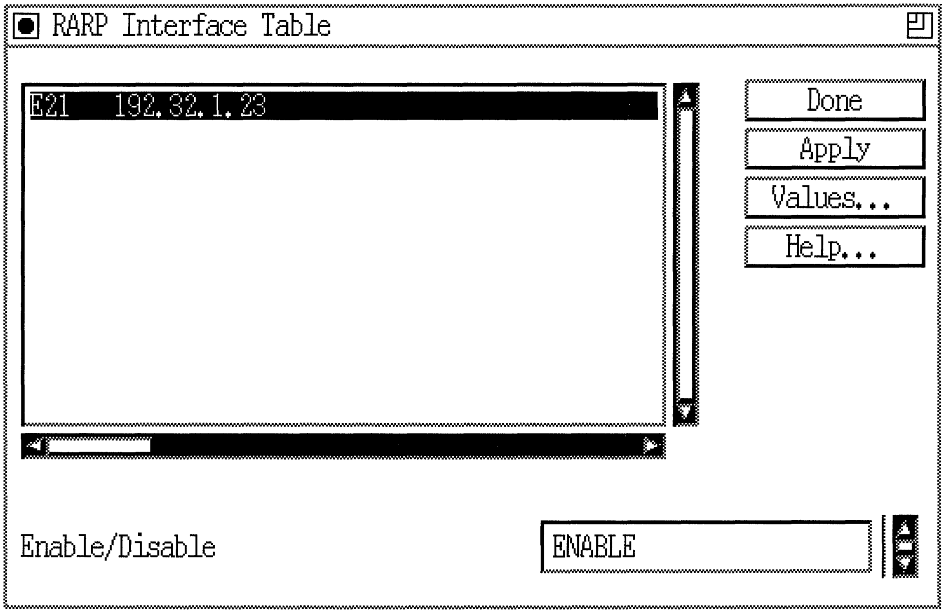
Figure 3-2. Configuration Manager Window

Disabling and Re-Enabling RARP Interfaces

To disable and/or re-enable individual RARP interfaces, begin at the Configuration Manager window (Figure 3-2) and proceed as follows:

1. Select the Protocols→IP→Reverse ARP→Interface Table option.

   The RARP Interface Table window appears (Figure 3-3).



E21 192.32.1.23

Enable/Disable ENABLE

Figure 3-3. RARP Interface Table

This window lists all RARP interfaces configured on the router.

2. Click on the RARP interface you want to select from the list of interfaces.
3. Select Enable in the parameter box to re-enable a disabled interface; select Disable to disable an interface.
4. Click on the Apply button to implement your change.
5. Click on the Done button to exit the window.

Following is a description of the RARP interface Enable | Disable parameter:

Parameter:	**Enable | Disable**
Default:	Enable
Options:	Enable | Disable
Function:	Depending on the option you choose, Site Manager re-enables or disables the RARP interface currently selected in the list of interfaces.
Instructions:	Select Enable in the parameter box to re-enable a disabled interface; select Disable to disable an interface.
MIB Object ID:	1.3.6.1.4.1.18.3.5.3.9.3.1.2

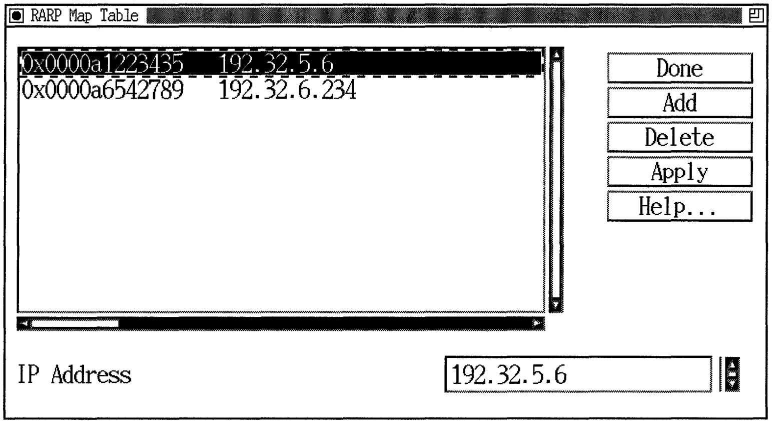
Defining the RARP Mapping Table

To define the router's MAC address-to-IP address RARP mapping table, begin at the Configuration Manager window (refer to Figure 3-2) and proceed as follows:

1. Select the Protocols➔IP➔Reverse ARP➔Map Table option.

   The RARP Map Table window appears (Figure 3-4).

   Each entry listed corresponds to a client host on the network that can use the router's RARP services.



RARP Map Table

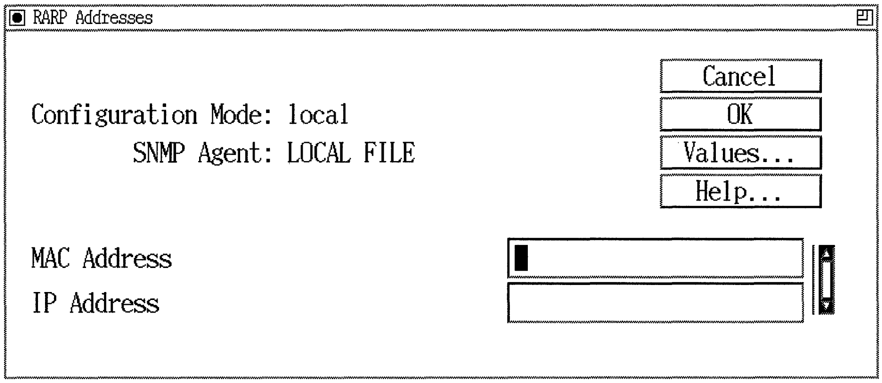
```
0x0000a1223435   192.32.5.6
0x0000a6542789   192.32.6.234
```

IP Address 192.32.5.6

Figure 3-4. RARP Map Table Window

2. Click on the Add button to add a new entry to the table.

   The RARP Addresses window appears (Figure 3-5).



RARP Addresses

Configuration Mode: local
SNMP Agent: LOCAL FILE

MAC Address

IP Address

Figure 3-5. RARP Addresses Window

3. Specify a MAC address and a corresponding IP address for the client host.

   The MAC address and IP address parameters are described following these instructions.

4. Click on the OK button.

   The RARP Map Table window now displays the entry you defined.

5. Click on the Done button to exit the window.

RARP Address Parameters

Use the following descriptions as guidelines when setting the RARP address parameters.

Parameter:	**MAC Address**
Default:	None
Range:	Any valid MAC address
Function:	Specifies the MAC address of a client host that will use the RARP services of this router. The client host will include the MAC address you specify here in RARP requests it broadcasts to the router.
Instructions:	Enter the MAC address of a client host.
MIB Object ID:	1.3.6.1.4.1.18.3.5.3.9.2.1.2

Parameter: **IP Address**

Default: None

Range: Any valid IP address

Function: Specifies the corresponding IP address for the client host identified by the MAC Address parameter.

When the router receives a RARP request from the client host, the router assigns the specified IP Address to the client host and includes it in a response packet.

Instructions: Enter the IP address corresponding to the MAC address you specified for the MAC Address parameter.

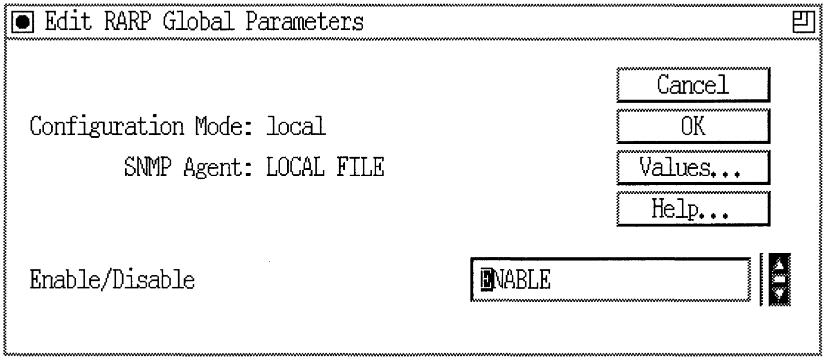
MIB Object ID: 1.3.6.1.4.1.18.3.5.3.9.2.1.3

Disabling RARP Globally

To globally disable RARP from all of the router interfaces on which it is configured, begin at the Configuration Manager window (refer to Figure 3-2) and proceed as follows:

1. Select the Protocols→IP→Reverse ARP→Globals option.

   The Edit RARP Global Parameters window appears (Figure 3-6).



Edit RARP Global Parameters

Configuration Mode: local
SNMP Agent: LOCAL FILE

Enable/Disable ENABLE

Figure 3-6. Edit RARP Global Parameters Window

2. Set the Enable | Disable parameter to Disable to disable RARP globally; set it to Enable if you previously disabled RARP and now want to re-enable it.
3. Click on the OK button to save your changes and exit the window.

Deleting RARP Globally

To globally delete RARP from all of the router's interfaces on which it is configured, begin at the Configuration Manager window (refer to Figure 3-2) and proceed as follows:

1. Select the Protocols→IP→Reverse ARP→Delete RARP option.
2. Click on the OK button to confirm the deletion.

RARP is no longer configured on the router.

Index