

**Bay Networks**

The Merged Company of SynOptics and Wellfleet

# Managing Wellfleet Routers

Part No. 110077 A

# Managing Wellfleet Routers

Router Software Version 8.10  
Site Manager Software Version 2.10

Part No. 110077 Rev. A  
February 1995



**Bay Networks**

The Merged Company of SynOptics and Wellfleet

---

**Copyright © 1995 Bay Networks, Inc.**

All rights reserved. Printed in USA. February 1995.

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

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

**Restricted Rights Legend**

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

**Notice for All Other Executive Agencies**

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

**Trademarks of Bay Networks, Inc.**

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

**Third-Party Trademarks**

3Com is a registered trademark of 3Com Corporation.

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

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

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

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

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

Fastmac and MADGE are trademarks of Madge Networks, Ltd.

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

HP is a registered trademark of Hewlett-Packard Company.

Intel is a registered trademark of Intel Corporation.

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

MCI is a registered trademark of MCI Communications Corporation.

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

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

Motorola is a registered trademark of Motorola, Inc.

NetBIOS is a trademark of Micro Computer Systems, Inc.

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

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

VINES is a registered trademark of Banyan Systems Incorporated.

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

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

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

---

# Bay Networks 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

### Overview of Router Management

Configuring the Router .....	1-2
Monitoring Traps and Events .....	1-3
Viewing Trap Messages .....	1-5
Viewing Event Messages .....	1-8
Monitoring Statistics .....	1-11
Using the Quick Get Tool .....	1-12
Using the Screen Manager Tool .....	1-13
Using the Launch Facility Tool .....	1-13
Using the Screen Builder Tool .....	1-13
Using Online Help .....	1-14
Locating Statistics Files .....	1-14
Managing Router Files .....	1-15
Monitoring Changes to Router Configuration Files .....	1-15
Customizing Router Software Images .....	1-17
Performing Administrative Functions .....	1-17

Tracking Network Availability and Response Time .....	1-18
Keeping a Log .....	1-19

## Chapter 2

### Using the Trap Monitor

Connecting to a Router .....	2-2
Configuring the Router's SNMP Agent .....	2-3
Identifying Site Manager as an SNMP Manager .....	2-3
Saving a Configuration .....	2-6
Running Multiple Network Management Applications .....	2-6
Configuring Traps Sent by a Router .....	2-8
Specifying Traps by Category .....	2-8
Specifying Traps by Entity .....	2-11
Specifying Traps by Event Type .....	2-12
Enabling an SNMP Agent .....	2-14
Viewing Trap Messages .....	2-16
Using the Trap Monitor .....	2-16
Displaying the Trap History File .....	2-16
Filtering Trap Messages .....	2-18
Filtering by Severity .....	2-19
Filtering by Router IP Address .....	2-19
Clearing the Trap Monitor Window .....	2-21
Clearing the Trap History File .....	2-21
Saving Trap Messages .....	2-22

## Chapter 3

### Using the Events Manager

Connecting to a Router .....	3-2
Displaying Event Logs .....	3-3
Displaying the Current Log .....	3-3
Displaying a Remote Log .....	3-5
Displaying a Local Log .....	3-6
Filtering Event Messages .....	3-7
Filtering by Severity, Slot, and Entity .....	3-7
Filtering by Router IP Address .....	3-9
Searching for an Event Message .....	3-9
Refreshing the Events Manager Window .....	3-10
Clearing the Events Manager Window .....	3-10
Saving Event Messages .....	3-10
Clearing the Current Event Log .....	3-12

## Chapter 4

### Using the Statistics Manager

Accessing Statistics .....	4-2
Connecting to a Router .....	4-3
Viewing the Wellfleet MIB .....	4-3
Using the MIB Browser .....	4-5
Getting Instances of Selected Objects .....	4-7



Defining the Current Screen List .....	4-12
Adding Statistics Screens .....	4-13
Removing Statistics Screens .....	4-15
Displaying Statistics Screens .....	4-15
Refreshing Active Statistics Screens .....	4-17
Specifying Circuit Mode Statistics Polling Rate .....	4-17
Zeroing Circuit Mode Statistics .....	4-18
Zeroing All Counters in a Screen .....	4-18
Zeroing All Counters in a Specific Row .....	4-20
Stopping Statistics Retrieval .....	4-21
Creating Statistics Filters .....	4-21
Using Display Filters .....	4-23
Using Retrieval Filters .....	4-26
Searching for Statistics Information .....	4-28
Saving Statistics Information .....	4-29
Building Custom Statistics Screens .....	4-30
Designing Statistics Screens .....	4-30
Displaying Custom Statistics Screens .....	4-35
Editing Custom Statistics Screens .....	4-36
Retrieving a Statistics Screen File .....	4-36
Editing a Statistics Screen File .....	4-37
For More Information .....	4-38

## Chapter 5

### Using the Router Files Manager

Displaying the Contents of a Volume .....	5-2
Active Volumes .....	5-3
Available and Contiguous Free Space .....	5-4
Default Filenames .....	5-4
Connecting to a Router .....	5-7
Naming a File .....	5-8
Copying a File .....	5-9
Examining the Router Destination Volume .....	5-9
Verifying Adequate Free Space .....	5-9
Creating the Copy .....	5-10
Deleting a File .....	5-12
Transferring a File .....	5-13
Setting Up Multiple Routers .....	5-15
Getting a File .....	5-18
Putting a File .....	5-19
Choosing the Routers .....	5-20
Examining the Router Destination Volume .....	5-21
Verifying Adequate Free Space on the Destination Volume .....	5-21
Transferring Files to the Destination Volume .....	5-22
Backing Up Router Software Files to a Host Computer .....	5-24
Modifying config Files in Remote Configuration Mode .....	5-24
Compacting File Space on a Memory Card or Flash SIMM .....	5-26

Formatting a Memory Card or Flash SIMM .....	5-27
Partitioning Media on Wellfleet Routers .....	5-28
Creating a Partition .....	5-29
Deleting a Partition .....	5-32

## Chapter 6

### Using the Report Generator and Audit Trail Feature

Generating Configuration File Reports .....	6-2
Generating Reports from Site Manager .....	6-2
Generating Configuration File Reports from UNIX .....	6-10
Generating Configuration File Reports from Windows .....	6-11
Maintaining an Audit Trail Log .....	6-13
Editing the Audit Trail Configuration File .....	6-13
Viewing an Audit Trail Log File .....	6-15

## Chapter 7

### Performing Administrative Functions

Displaying Software Versions .....	7-2
Router Booting Procedures .....	7-3
FN/LN/CN Router Boot Prerequisite .....	7-3
Booting a Router .....	7-4
Booting a Processor Module .....	7-6
Clearing the Event Log .....	7-8
Setting a Router's Date and Time .....	7-8

Pinging a Remote Device .....	7-10
IP Ping .....	7-10
IP Ping Responses .....	7-12
IPX Ping .....	7-13
IPX Ping Responses .....	7-15
OSI Ping .....	7-16
OSI Ping Responses .....	7-17
VINES Ping .....	7-18
VINES Ping Responses .....	7-20
AppleTalk Ping .....	7-21
AppleTalk Ping Responses .....	7-22
Reallocating Memory Partitions for a Processor Module .....	7-24
Partitioning Overview .....	7-24
Repartitioning Global and Local Memory .....	7-26

## Chapter 8

### Using the Ping MIB

Configuring IP Ping Requests .....	8-2
Specifying Values for Ping at Intervals Parameters .....	8-7
Deleting Ping Requests .....	8-12
Specifying Source Routes .....	8-12
Changing or Deleting Source Route Addresses .....	8-15
Reviewing IP Ping Statistics .....	8-16
Removing Entries from the Ping MIB .....	8-16

**Appendix A**  
**Using UNIX Commands to Start Site Manager**

**Appendix B**  
**Configuring a Router with a New Link Module**

Copying the Configuration File .....	B-2
Transferring the Configuration File to a Local Directory .....	B-4
Editing the Configuration File .....	B-5
Transferring the Edited Configuration File to the Router .....	B-9
Rebooting the Router with the Edited Configuration File .....	B-11
Deleting the Old Configuration File from the Router .....	B-11
Renaming the Edited Configuration File to the Default .....	B-12

**Index**

## Figures

Figure 1-1.	Wellfleet Trap Monitor Window .....	1-6
Figure 1-2.	Wellfleet Events Manager Window .....	1-9
Figure 1-3.	Statistics Manager Tools Menu .....	1-11
Figure 1-4.	Administration Menu .....	1-18
Figure 2-1.	Router Connection Options Window .....	2-2
Figure 2-2.	Configuration Manager Window .....	2-4
Figure 2-3.	SNMP Communities List .....	2-4
Figure 2-4.	SNMP Manager List .....	2-5
Figure 2-5.	Add SNMP Manager Window .....	2-5
Figure 2-6.	Trap Port and Trap Types Window .....	2-7
Figure 2-7.	Specifying a Trap Category .....	2-9
Figure 2-8.	Trap Configuration Window .....	2-11
Figure 2-9.	Traps Exceptions List .....	2-12
Figure 2-10.	Add Trap Window .....	2-13
Figure 2-11.	Traps Exceptions Lists Window .....	2-14
Figure 2-12.	Edit SNMP Global Parameters Window .....	2-15
Figure 2-13.	Enabling an SNMP Agent .....	2-15
Figure 2-14.	Wellfleet Trap Monitor Window .....	2-18
Figure 2-15.	Selected Trap-Type Window .....	2-19
Figure 2-16.	Address Filters Window .....	2-20
Figure 2-17.	Sample Address Filters Window .....	2-21
Figure 2-18.	Saving Traps to a File .....	2-22
Figure 3-1.	Router Connection Options Window .....	3-2
Figure 3-2.	Wellfleet Events Manager Window .....	3-4
Figure 3-3.	Load Remote Log File Window .....	3-5

Figure 3-4. Load Local Log Window .....	3-6
Figure 3-5. Filtering Parameters Window .....	3-8
Figure 3-6. Find Text Pattern Window .....	3-9
Figure 3-7. Save Log Window .....	3-11
Figure 3-8. Confirmation Window .....	3-12
Figure 4-1. Statistics Manager Window .....	4-2
Figure 4-2. Router Connection Options Window .....	4-3
Figure 4-3. Quick Get Facility Window .....	4-4
Figure 4-4. MIB Tree for System Group .....	4-5
Figure 4-5. Sample Quick Get Facility Window .....	4-7
Figure 4-6. All Instances Retrieved (Unfiltered) without Instance IDs .....	4-9
Figure 4-7. All Instances Retrieved (Unfiltered) with Instance IDs .....	4-10
Figure 4-8. Specific Instances Retrieved without Instance IDs .....	4-11
Figure 4-9. Specific Instances Retrieved with Instance IDs .....	4-12
Figure 4-10. Screen Manager Window .....	4-13
Figure 4-11. Example of Filename and Screen Description .....	4-14
Figure 4-12. Selecting a Screen .....	4-16
Figure 4-13. Statistics Screen .....	4-17
Figure 4-14. Polling Rate Window .....	4-18
Figure 4-15. Zeroing All Counters in a Screen .....	4-19
Figure 4-16. Zeroing All Counters in a Specific Row .....	4-20
Figure 4-17. Display Filters Window .....	4-23
Figure 4-18. Statistics Window Unfiltered .....	4-24
Figure 4-19. Sample Display Filters Window .....	4-25
Figure 4-20. Statistics Screen after Filter Implemented .....	4-26
Figure 4-21. Retrieval Filters Window .....	4-27

Figure 4-22. Statistics Screen After Implementing a Retrieval Filter .....	4-28
Figure 4-23. Search Options Window .....	4-29
Figure 4-24. Screen Builder Facility Window .....	4-31
Figure 4-25. Screen Builder Column Total Window .....	4-33
Figure 4-26. Selecting Columns to Total .....	4-33
Figure 4-27. Statistics Save/Load Screen .....	4-34
Figure 5-1. Router Files Manager Window .....	5-2
Figure 5-2. Router Connection Options Window .....	5-7
Figure 5-3. Copy File Window for Source Filename .....	5-11
Figure 5-4. Copy File Window for Destination Filename .....	5-11
Figure 5-5. Deleting Router Files .....	5-13
Figure 5-6. Selecting the TFTP Option .....	5-13
Figure 5-7. Multiple Router Setup Window .....	5-15
Figure 5-8. Adding Routers to the Current Routers List .....	5-16
Figure 5-9. Adding Routers to the Current Routers List .....	5-17
Figure 5-10. TFTP Get File Window .....	5-19
Figure 5-11. TFTP Put File Selection Window .....	5-23
Figure 5-12. Create Partition Confirmation Window .....	5-30
Figure 5-13. Volume Identifiers for Partitioned Media .....	5-31
Figure 5-14. Delete Partition Confirmation Window .....	5-32
Figure 6-1. Configuration Report Generator Window .....	6-2
Figure 6-2. Select Configuration File Window .....	6-5
Figure 6-3. Save Report File As Window .....	6-6
Figure 6-4. Report Template File Window .....	6-7
Figure 6-5. Sample Configuration File Report .....	6-9
Figure 6-6. Default Audit Trail Configuration File .....	6-14



Figure 6-7. Sample Audit Trail Log File .....	6-16
Figure 7-1. Displaying Version Information .....	7-2
Figure 7-2. Boot Router Window .....	7-4
Figure 7-3. Reset Slot Window .....	7-6
Figure 7-4. Selecting a Slot .....	7-6
Figure 7-5. Router Date and Time Window .....	7-9
Figure 7-6. Selecting Ping from Router Option .....	7-10
Figure 7-7. IP Ping Window .....	7-11
Figure 7-8. Ping Is Alive Window .....	7-12
Figure 7-9. Ping Does Not Respond Window .....	7-12
Figure 7-10. IPX Ping Window .....	7-14
Figure 7-11. OSI Ping Window .....	7-16
Figure 7-12. VINES Ping Window .....	7-19
Figure 7-13. AppleTalk Ping Window .....	7-21
Figure 7-14. Specifying Router Connection Options .....	7-26
Figure 7-15. Kernel Configuration Window .....	7-27
Figure 8-1. Router Connection Options Window .....	8-2
Figure 8-2. File Selection Window .....	8-3
Figure 8-3. Configuration Manager Window .....	8-4
Figure 8-4. Ping at Intervals Window .....	8-5
Figure 8-5. IP Ping Parameters Window .....	8-6
Figure 8-6. Source Route Entries Window .....	8-13
Figure 8-7. Source Ping Parameters Window .....	8-13
Figure 8-8. Completed Source Route Entries .....	8-14
Figure B-1. Router Files Manager Window .....	B-2
Figure B-2. Copy File Window Source Filename .....	B-3

Figure B-3.	Copy File Window/Destination Filename .....	B-3
Figure B-4.	TFTP Get File Window .....	B-4
Figure B-5.	File Selection Window .....	B-5
Figure B-6.	Wellfleet Configuration Manager Window .....	B-6
Figure B-7.	Circuit List Window .....	B-7
Figure B-8.	Module List Window .....	B-8
Figure B-9.	Confirming a Circuit Delete Request .....	B-8
Figure B-10.	File Save Confirmation Window .....	B-9
Figure B-11.	TFTP Put File Selection Window .....	B-10

## Tables

Table 1-1.	Comparing Trap Messages and Event Messages .....	1-3
Table 1-2.	Trap Message Details .....	1-7
Table 1-3.	Event Message Details .....	1-10
Table 1-4.	Statistics Manager Tools .....	1-12
Table 2-1.	Restarting Site Manager on a New Port .....	2-8
Table 2-2.	Categories of Traps .....	2-10
Table 2-3.	Entering Values in the Add Trap Window .....	2-13
Table 4-1.	Finding MIB Information .....	4-6
Table 5-1.	Default Router Filenames .....	5-5
Table 6-1.	Output Format Options .....	6-3
Table 8-1.	Default Ping MIB Statistics Screens .....	8-16
Table A-1.	Site Manager Startup Commands .....	A-2
Table A-2.	Site Manager Startup Command Options .....	A-3



---

# About This Guide

If you are responsible for configuring and managing Wellfleet™ routers, you need to read this guide. This guide is intended for experienced network operators. It describes how to manage Wellfleet routers using Wellfleet's Site Manager application. It assumes that the reader has a technical understanding of data communications and a basic understanding of how Site Manager works.

Refer to this guide for instruction on

- ❑ Accessing and viewing trap messages and event messages
- ❑ Responding to trap messages and event messages
- ❑ Accessing and viewing statistics
- ❑ Accessing and using files to boot routers
- ❑ Basic system administration
- ❑ Editing a configuration file after replacing a link module

**Note:** The Site Manager windows shown in this book are from an X Window System™ UNIX® environment. Minor variations in screen appearance may occur from platform to platform.

## Before You Begin

Refer to the guide *Quick-Starting Wellfleet Routers* for information on how to install Site Manager on your computer.

Refer to the guide *Using Site Manager Software* for an introduction to Bay Networks' network management application.

Refer to the guide *Configuring Wellfleet Routers* for information on how to use the Configuration Manager tool.

Refer to the guide *Customizing SNMP, BOOTP, and RARP Services* for more information on SNMP.

## 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

- angle brackets (< >)      Indicate that you choose the text to enter based on the description inside the brackets. Do not type the brackets when entering the command. Example: if command syntax is **ping** <ip\_address>, you enter **ping 192.32.10.12**
- arrow character (→)      Separates menu and option names in instructions. Example: **Protocols→AppleTalk** identifies the AppleTalk option in the Protocols menu.
- brackets ([ ])              Indicate optional elements. You can choose none, one, or all of the options.

---

<b>user entry text</b>	Denotes text that you need to enter. Example: Start up the Windows environment by entering the following after the prompt: <b>win</b>
<b>command text</b>	Denotes command names in text. Example: Use the <b>xmodem</b> command.
<i>italic text</i>	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
ellipsis points	Horizontal (. . .) and vertical ( : ) ellipsis points indicate omitted information.
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 <b>show at routes   nets</b> , you enter either <b>show at routes</b> or <b>show at nets</b> , but not both.

## Acronyms

ACE	Advanced Communications Engine
ALN	Bay Networks' Access Link Node
AN	Bay Networks' Access Node Router
ARP	Address Resolution Protocol
ASN	Access Stack Node
BCN	Bay Networks' Backbone Concentrator Node Router
BGP	Border Gateway Protocol
BLN	Bay Networks' Backbone Link Node Router
BLN-2	Bay Networks' Backbone Link Node-2 Router
BOOTP	Bootstrap Protocol
CSMA/CD	Carrier Sense Multiple Access/Carrier Detect
CLNP	Connectionless Network Protocol

---

DLSw	data link switching
DMAP	direct memory access processor
DOS	disk operating system
EGP	Exterior Gateway Protocol
FDDI	Fiber Distributed Data Interface
FN	Bay Networks' Feeder Node Router
FRE	fast routing engine
GAME	Bay Networks' Gate Access Management Entity
HSSI	High Speed Serial Interface
ICMP	Internet Control Message Protocol
IP	Internet Protocol
IPX	Internet Packet Exchange Protocol
LLC	logical link control
MIB	management information base
NSAP	network service access point
NVFS	Nonvolatile file system
NVRAM	Nonvolatile read access memory
OSI	Open Systems Interconnection
OSPF	Open Shortest Path First
PCMCIA	Personal Computer Memory Card International Association
PPP	Point-to-Point Protocol
PPX	parallel packet express
RFC	Request for Comment
SIMM	Single Inline Memory Module
SMDS	Switched Multimegabit Data Service
SNMP	Simple Network Management Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol
TFTP	Trivial File Transfer Protocol
UDP	User Datagram Protocol
VINES	Virtual Networking System
XNS	Xerox Networking Systems Protocol

---

# Chapter 1

## Overview of Router Management

To manage your Wellfleet routers, you can use Site Manager to do the following:

- ❑ Configure the router
- ❑ Monitor traps and events
- ❑ Monitor statistics
- ❑ Manage router files
- ❑ Monitor changes to router configuration files
- ❑ Customize router software images
- ❑ Perform administrative functions
- ❑ Track network availability and response time



## Configuring the Router

You can configure your router remotely using the Configuration Manager tool in Site Manager. The Configuration Manager lets you do the following:

- ❑ Add network interfaces to the router using default values
- ❑ Customize network interfaces for your network environment
- ❑ Configure inbound and outbound traffic filters on interfaces
- ❑ Assign priorities to certain types of traffic that an interface receives
- ❑ Reconfigure the router's connection to the Technician Interface (TI)
- ❑ Specify a router's hardware configuration
- ❑ Specify administrative information about the router

To access the Configuration Manager tool, select Tools→Configuration Manager from the Site Manager main window. You must then specify the operating mode (Local File, Remote File, or Dynamic):

- ❑ Use Local File mode to create or edit a configuration file locally on the Site Manager workstation for later implementation on the router.
- ❑ Use Remote File mode if you can access the router over the network but want to implement the configuration at a later date.
- ❑ Use Dynamic mode if you can access the router over the network and want to configure the system in real time.

For more information on using the Configuration Manager, refer to *Configuring Wellfleet Routers*.

## Monitoring Traps and Events

Two types of messages help you manage a router:

- *Trap messages* provide real-time information on the operating status of the routers running on your network. Routers using the Simple Network Management Protocol (SNMP), an industry standard, produce trap messages. You use the Trap Monitor to view these messages.
- *Event messages* also provide information on the operating status of the routers running on your network; however, event messages provide a more detailed description. You use the Events Manager to display event messages.

For an overview of how your routers are functioning, use the Trap Monitor first; then use the Events Manager for more complete event descriptions.

Table 1-1 compares trap and event messages. Refer to *Event Messages for Wellfleet Routers* for information on how to respond to messages.

**Table 1-1. Comparing Trap Messages and Event Messages**

Trap Messages	Event Messages
Real-time display	Detailed display (not in real time)
SNMP-standard	Wellfleet-specific
Usually view before event messages	Usually view after trap messages
Expensive to view (but fast)	Inexpensive to view (but slower)
Brief messages provided	Descriptive messages provided (see <i>Event Messages for Wellfleet Routers</i> )

*continued on the next page*

**Table 1-1. Comparing Trap Messages and Event Messages** *(continued)*

Trap Messages	Event Messages
Real-time display	Detailed display (not in real time)
No list of messages provided	List of messages and recommended responses provided (see <i>Event Messages for Wellfleet Routers</i> )
Use Configuration Manager to configure SNMP agent to send messages to Trap Monitor  Use Trap Monitor to view and filter messages	Use Events Manager to view and filter messages
Can configure SNMP agent to send event messages to Trap Monitor	Cannot configure SNMP agent to send trap messages to Events Manager
Can save messages to ASCII file	Can save messages to ASCII file
Stored in workstation's trap history file	Stored in router's event log
Stamped with workstation's time	Stamped with router's time

## Viewing Trap Messages

You view trap messages in real time using the Trap Monitor tool. To access the Trap Monitor, select Tools→Trap Monitor from the Site Manager main window. The Trap Monitor lets you view event messages along with trap messages.

Before using the Trap Monitor, you must use the Configuration Manager to do the following:

- ❑ Specify the Internet Protocol (IP) address of your Site Manager workstation.
- ❑ Configure the SNMP agent located inside your router to send specified trap messages to the Site Manager workstation.
- ❑ If you use more than one network management application, change the trap port assigned to your Site Manager application so that Site Manager will continue to receive trap messages from the router.

The Trap Monitor tool receives trap messages from all SNMP agents on the network that are configured to send the messages. Once you configure an agent to send SNMP trap messages to your Site Manager workstation, a trap history file saves a running history of these messages. The Trap Monitor dynamically displays trap messages from the trap history file after you load the file into the Trap Monitor window. Chapter 2 describes how to load the file into the Trap Monitor window.

Figure 1-1 shows a sample Trap Monitor window and Table 1-2 describes the window contents.

Timestamp	Node	Slot	Entity	Severity	Description
Dec 27 22:43:25	192.32.156.10	4	CSMACD	(W)	"Connector XCVR1 carrier lost."
Dec 27 22:43:29	192.32.156.10	4	CSMACD	(W)	"Connector XCVR1 carrier lost."
Dec 27 22:43:35	192.32.156.10	4	CSMACD	(W)	"Connector XCVR1 carrier lost."
Dec 27 22:43:39	192.32.156.10	4	CSMACD	(W)	"Connector XCVR1 carrier lost."
Dec 27 22:43:46	192.32.156.10	4	CSMACD	(W)	"Connector XCVR1 carrier lost."
Dec 27 22:43:50	192.32.156.10	4	CSMACD	(W)	"Connector XCVR1 carrier lost."
Dec 27 22:43:56	192.32.156.10	4	CSMACD	(W)	"Connector XCVR1 carrier lost."
Dec 27 22:44:00	192.32.156.10	4	CSMACD	(W)	"Connector XCVR1 carrier lost."
Dec 27 22:44:07	192.32.156.10	4	CSMACD	(W)	"Connector XCVR1 carrier lost."
Dec 27 22:44:11	192.32.156.10	4	CSMACD	(W)	"Connector XCVR1 carrier lost."
Dec 27 22:44:17	192.32.156.10	4	CSMACD	(W)	"Connector XCVR1 carrier lost."
Dec 27 22:44:21	192.32.156.10	4	CSMACD	(W)	"Connector XCVR1 carrier lost."

Figure 1-1. Wellfleet Trap Monitor Window

**Table 1-2. Trap Message Details**

Item	Description
Timestamp	Date and time that the Site Manager workstation received the trap message
Node	IP address of the router whose SNMP agent generated the trap message
Slot	Slot hosting the entity that generated the trap message
Entity	Abbreviated name of entity that generated the trap message
Severity	Severity level of trap message: Fault, Warning, Information, Debug, or Trace. First letter is used (for example, W stands for Warning)
Description	Text describing the trap

You can use the entity, severity, slot, and node to filter the types of trap messages you want to view in the Trap Monitor window.

The Trap Monitor tool lets you do the following:

- ❑ Save the trap messages you see in the Trap Monitor window to an ASCII file on your workstation. You can view or print the file later.
- ❑ Clear the Trap Monitor window to display only the latest messages or empty the trap history file entirely to start a new log.

You can configure the SNMP agent to send specified trap messages to the Trap Monitor window as follows:

Configuring the SNMP Agent
By category—none, generic, specific, all
By entity
By event message (entity/event code)

**Note:** To save routing resources, configure the SNMP agent so that it sends only important data, such as fault, warning, and information messages.

For more information about using the Trap Monitor, see Chapter 2.

## Viewing Event Messages

You view event messages using the Events Manager tool. To access the Events Manager, select Tools→Events Manager from the Site Manager main window. Each time you want to view the most current version of a router's event log, you must use the Events Manager to retrieve the event log. The Events Manager does not display event messages in real time.

The Events Manager lets you view event messages from the router whose IP address you specify in the Wellfleet Site Manager window or from the Options menu in the Events Manager window.

Figure 1-2 shows a sample Events Manager window and Table 1-3 describes its contents.

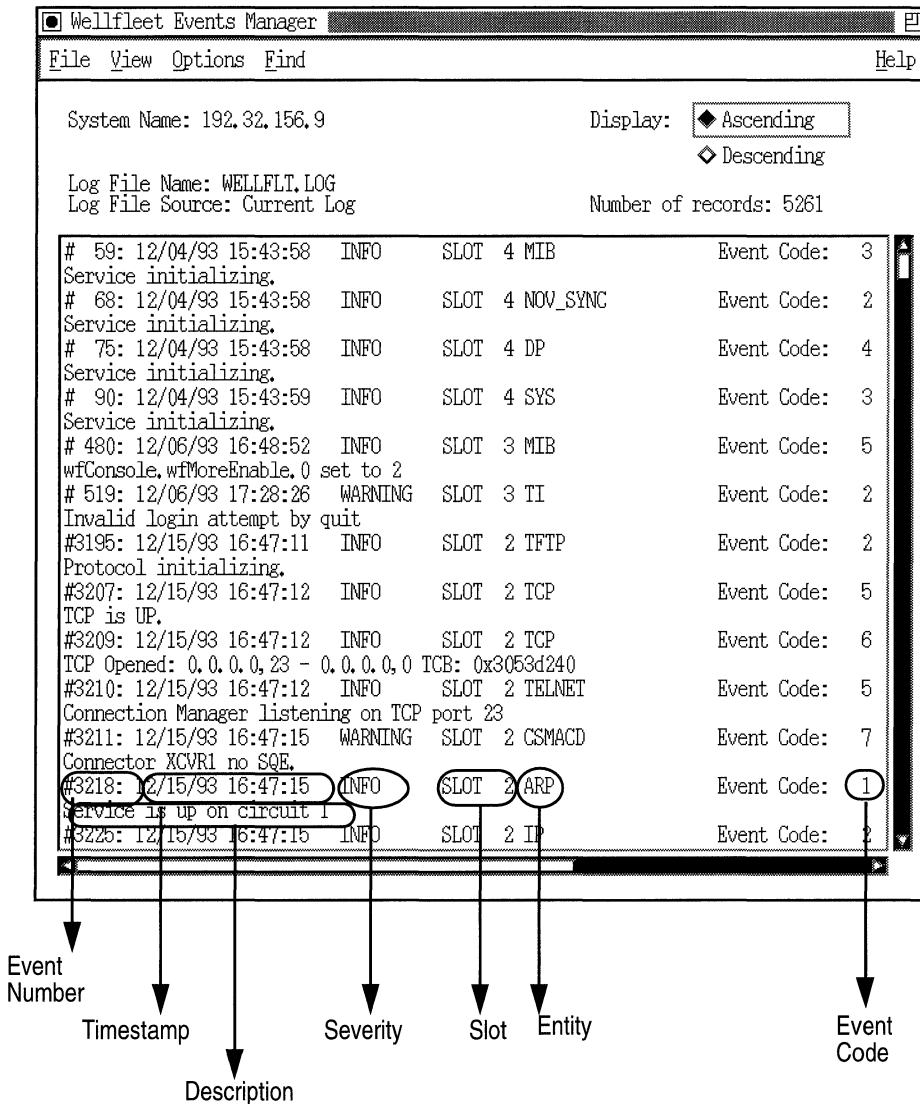


Figure 1-2. Wellfleet Events Manager Window



**Table 1-3. Event Message Details**

Detail	Description
Event number	Event's place in the event log (See the Number of Records field for the total count.)
Timestamp	Date and time the event occurred, as recorded by the router
Severity	Severity level of event message
Slot	Slot hosting the entity that generated the event message
Entity	Abbreviated name of entity that generated the event message
Event code	Event code, as shown in <i>Event Messages for Wellfleet Routers</i>
Description	Text describing the event

You can use the router IP address, entity, severity, and slot to filter event messages in the Events Manager window.

You can use the entity and event code to look up an event message in *Event Messages for Wellfleet Routers*.

The Events Manager lets you do the following:

- Search for messages in the log displayed.
- Save the event messages you see in the Events Manager window to an ASCII file on your workstation. You can then view or print the file later.
- Reload an event log saved in binary format back into the Events Manager window. (Storing a log on a diskette or memory card inside the router saves the log in binary format.)
- Clear the events displayed in the Events Manager window.

For more information on using the Events Manager, see Chapter 3.

## Monitoring Statistics

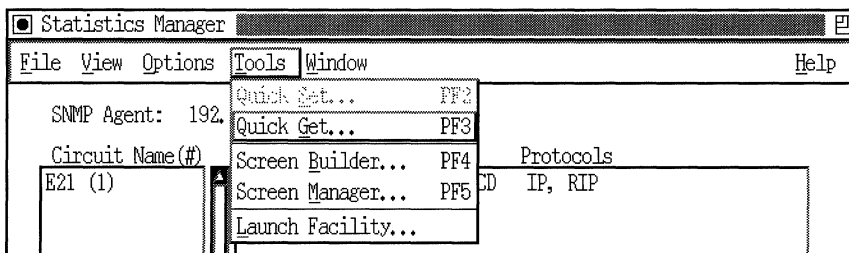
Site Manager uses an SNMP-based polling mechanism to request the following:

- ❑ Real-time data link layer statistics providing circuit information
- ❑ Network layer statistics providing protocol information

When it receives this data, Site Manager displays the information in a statistics window. Using the Statistics Manager tool, you can do the following:

- ❑ Connect to a router
- ❑ View the Wellfleet Management Information Base (MIB)
- ❑ Display statistics screens
- ❑ Build custom statistics screens
- ❑ Edit custom statistics screens
- ❑ Add or remove statistics screens from the current screen list

To access the Statistics Manager tool, select Tools→Statistics Manager from the Site Manager main window. The Statistics Manager provides four tools that you can access from the Statistics Manager's Tools menu (Figure 1-3). Table 1-4 describes these tools.



**Figure 1-3. Statistics Manager Tools Menu**

**Note:** The Quick Set tool is not a selectable option at this time.

**Table 1-4. Statistics Manager Tools**

Tool	Function
Quick Get	Lets you view objects in the Management Information Base (MIB)
Screen Builder	Lets you design your own custom statistics screens
Screen Manager	Lets you manage your statistics screen database and specify a current statistics screen list
Launch Facility	Lets you select statistics screens from the current screen list and launch (or display) the screens

The following sections describe each of these tools, as well as how to get online help. Later, we describe where the Statistics Manager stores default and custom-built statistics files on your UNIX workstation or PC.

For more information on using the Statistics Manager, see Chapter 4.

## Using the Quick Get Tool

You use Quick Get to view the MIB and retrieve instances of selected MIB objects from the router. The Wellfleet MIB is a Wellfleet proprietary database that contains the router's configuration parameters and statistics.

Quick Get includes a *MIB Browser*, which you use to scroll though the MIB and select those objects about which you want to retrieve information. Quick Get retrieves all instances of the specified MIB objects and displays the statistics in a window.

Quick Get helps you debug your network (for example, if you want to monitor MIB objects). It is also an easy way to view the MIB and decide which objects you want to include on your customized statistics screens.

## Using the Screen Manager Tool

You use the Screen Manager to manage the statistics screen database and to define a *current screen list*. The database contains over 75 default statistics screens. In addition, you can design and save up to 4,000 customized screens. The current screen list is a subset of the entire database of statistics screens — usually those you use most often. It can contain both default and custom-built screens. Note that you can display only those statistics screens that you have added to the current screen list.

## Using the Launch Facility Tool

You use the Launch Facility tool to display any statistics screens that are on the current screen list. When you launch a statistics screen, Site Manager polls the router for all instances of the MIB objects specified on the screen, then formats and displays the data in columns.

There are two types of statistics screens:

- ❑ **Circuit mode:** The Statistics Manager continually polls the router for statistics and updates the statistics screen with new data. You determine how often the Statistics Manager retrieves these statistics by specifying a polling rate.
- ❑ **Table mode:** The Statistics Manager retrieves statistics from the router only once — when you launch the screen. You must refresh the screen each time you want to update it with new data.

## Using the Screen Builder Tool

You use the Screen Builder to create custom statistics screens. The MIB Browser lets you select up to nine objects to include on the screen.

For each object you select, you design how the statistics appear on the screen. The screen shows each object's statistics in a single column below a column heading.

The Screen Builder lets you specify the following:

- A name for the column heading
- The column width
- The format in which the screen displays the statistics (decimal or hexadecimal)

You can also use the Screen Builder to edit custom screens. For example, you can redefine how to display statistics, or you can add or delete objects from the screen.

## Using Online Help

Site Manager provides online help for each Statistics Manager tool. To get help, click on the Help button at the bottom of the screen. To exit the Help window, click on OK.

## Locating Statistics Files

Depending on whether you load Site Manager on a UNIX or DOS computer, the Statistics Manager stores all statistics screen files in one of the following directories.

<b>Platform</b>	<b>Default Screen Directory</b>	<b>Custom Screen Directory</b>
UNIX	<i>/usr/wf/lib/.wfscrns</i>	<i>\$(HOME)/.wfscrns</i>
DOS	<i>\wf\lib\wfscrns</i>	<i>\wf\wfscrns</i>

For more information on using the Statistics Manager, refer to Chapter 4.

## Managing Router Files

You can display a list of the system files stored on a Wellfleet router's active volume using the Router Files Manager tool. The Router Files Manager lets you

- ❑ Display the files on all disk volumes in a Wellfleet router
- ❑ Transfer and copy files between volumes on a Wellfleet router's disk, and between the router and the Site Manager workstation
- ❑ Delete files from a Wellfleet router's disk volume
- ❑ Compact Wellfleet memory cards
- ❑ Partition the nonvolatile file system (NVFS) on Wellfleet Access Node (AN) or Access Stack Node (ASN) routers

To access the Router Files Manager, select Tools→Router Files Manager from the Site Manager main window. For more information about using the Router Files Manager, refer to Chapter 5.

## Monitoring Changes to Router Configuration Files

Two features are available for you to track changes to router configuration files:

- ❑ The Report Generator tool
- ❑ The audit trail feature

The Report Generator tool translates the router's binary configuration file to an ASCII file. You can use any standard text editor to view and print the file. You can also use source comparison utilities to compare one report with another to detect configuration changes. To access the Report Generator tool, select Tools→Report Generator from the Site Manager main window.

In organizations where network managers at branch locations share router management responsibilities, central administrators can use audit trail logs to monitor configuration changes. An audit trail log is an ASCII file that describes the changes made to a router configuration

file. Each router you audit has its own audit trail log file. Whenever someone changes a router configuration file, the audit trail feature (if enabled for that router) appends the changes to the audit trail log.

**Note:** The audit trail feature keeps track of router configuration changes made in remote mode or dynamic mode only. The feature does not track changes made in local mode, or those made using the Technician Interface (TI).

With audit trail logging enabled, when you configure the router in remote mode, Site Manager does the following once you save your configuration changes:

- ❑ Transfers the configuration file to the router, as usual
- ❑ Creates the audit trail log file (if it doesn't already exist)
- ❑ Appends the configuration changes to the audit trail log file

If you configure the router in dynamic mode, Site Manager does the following each time an SNMP SET occurs:

- ❑ Updates the configuration on the router.
- ❑ Logs the SET to the audit trail log file. Site Manager creates the audit trail log file (if it does not already exist), and appends the changes to the file.

**Note:** To prevent an audit trail log file from becoming too large, you should periodically delete old information in it or delete the file itself.

You can configure the audit trail feature to send you (and other network managers) a copy of the audit trail log file whenever Site Manager updates it with new information. For routers configured in dynamic mode, the audit trail feature sends the log file after every tenth SNMP set.

For more information on using the Report Generator tool and the audit trail feature, refer to Chapter 6.

## Customizing Router Software Images

Site Manager provides a tool, the Image Builder, that lets you customize the *router software images* you receive from Bay Networks. A router software image is a group of executable files that operates the protocols on your network in conjunction with a Wellfleet router. You can do the following to modify a router software image:

- ❑ Remove a protocol that you do not use. For example, you might want to remove protocols to make more space available on the media that contains the router software image. Alternatively, you can add protocols that you inadvertently removed.
- ❑ Replace an existing image with an entirely new one.

To access the Image Builder, select Tools→Image Builder. For more information on using the Image Builder tool, refer to *Modifying Software Images for Wellfleet Routers*.

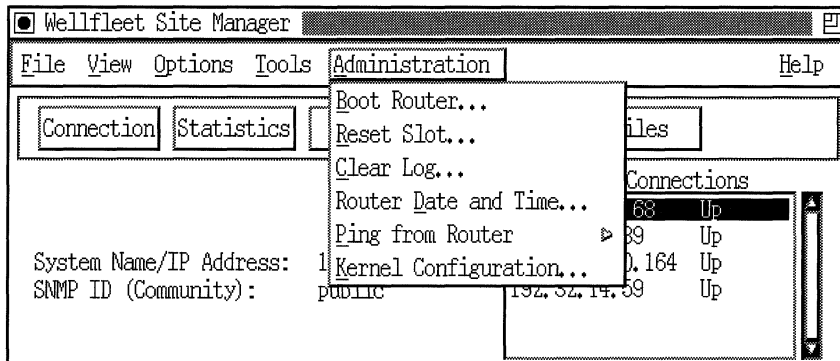
## Performing Administrative Functions

You can perform the following administrative tasks from Site Manager:

- ❑ Booting (warm-starting) the router
- ❑ Resetting (warm-starting) a single processor module in the router
- ❑ Clearing the router's event log
- ❑ Setting the router's date and time
- ❑ Testing the router's connection to a remote device on the network using one of five protocols: IP, IPX<sup>®</sup>, OSI, VINES<sup>®</sup>, or AppleTalk<sup>®</sup>
- ❑ Configuring the kernel; that is, reallocating the global and local memory on FRE2 and ACE32 processor modules, Access Nodes, and Access Feeder Nodes



You can perform these tasks using the Site Manager Administration menu (Figure 1-4).



**Figure 1-4. Administration Menu**

For more information about using each of the administrative functions, refer to Chapter 7.

## Tracking Network Availability and Response Time

You can track network availability and response time using the Ping MIB. The Ping MIB is a group of tables that store the following information for one or more ping requests:

- ❑ General ping information, such as the address you want to ping, whether you want to use trace routing and source routing, and the frequency of the ping.
- ❑ Trace route data that shows the IP addresses the ping went through to reach its destination.
- ❑ Source route data, which contains the IP addresses that you want the ping to go through instead of those in the routing table.
- ❑ History data about previous pings that you chose to initiate at specific intervals. See Chapter 8 for information on setting ping intervals.

To use the Ping MIB, you must first define the IP addresses that you want to ping. You can enter the addresses of routers, host computers, or any device on the network. The Ping MIB stores the results of the ping requests. You can then monitor those results using the Statistics Manager in Site Manager. You might also create your own application to query the Ping MIB, analyze the data, and generate reports of the information. You can also use such applications as IBM<sup>®</sup> NetView<sup>®</sup>/6000, SunNet Manager, and HP<sup>®</sup> OpenView to work with the Ping MIB.

For more information on using the Ping MIB, refer to Chapter 8.

## Keeping a Log

You should make several copies of the log on the next page to organize your management files. Keep the log in a handy place near your Site Manager workstation. Use this log to list the filenames and directories of all your configuration files, trap history files, and event logs.



---

# Chapter 2

## Using the Trap Monitor

For general information about monitoring traps, see “Monitoring Traps and Events” in Chapter 1. For specific information about using buttons, windows, and other Site Manager features, refer to *Using Site Manager Software*.

Use the Trap Monitor to do the following:

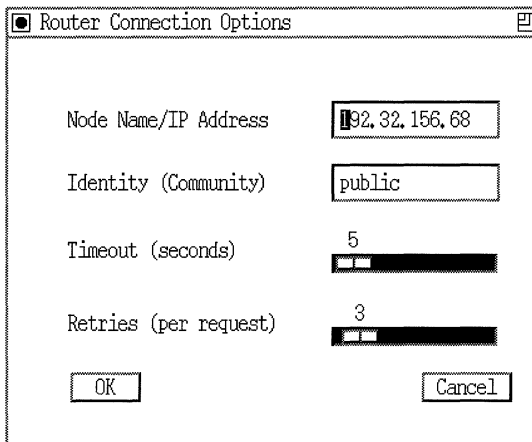
- ❑ Display the trap history file
- ❑ Filter trap messages
- ❑ Clear the Trap Monitor window
- ❑ Clear the trap history file
- ❑ Save trap messages

## Connecting to a Router

Before you can use the Trap Monitor tool, you must configure the Simple Network Management Protocol (SNMP) agent inside the router to send specified trap messages to the Trap Monitor. To do this, you must first connect to the router as follows:

1. From the Wellfleet Site Manager window, select Options→Router Connection.

The Router Connection Options window appears (Figure 2-1).



The screenshot shows a dialog box titled "Router Connection Options". It contains the following fields and values:

- Node Name/IP Address: 192.32.156.68
- Identity (Community): public
- Timeout (seconds): 5
- Retries (per request): 3

At the bottom of the dialog are two buttons: "OK" and "Cancel".

**Figure 2-1. Router Connection Options Window**

2. In the Node Name/IP Address field, type the IP address of the router you want to configure. Then click on OK.

The Wellfleet Site Manager window displays the router's system information.

## Configuring the Router's SNMP Agent

You must configure the SNMP agent in a router such that it will

- ❑ Recognize your Site Manager workstation as a valid SNMP manager
- ❑ Send specified trap messages to your Site Manager workstation

To configure the SNMP agent, use the Configuration Manager tool, which you also use to

- ❑ Enable the SNMP agent on the router
- ❑ Save the result of your configuration entries on the router

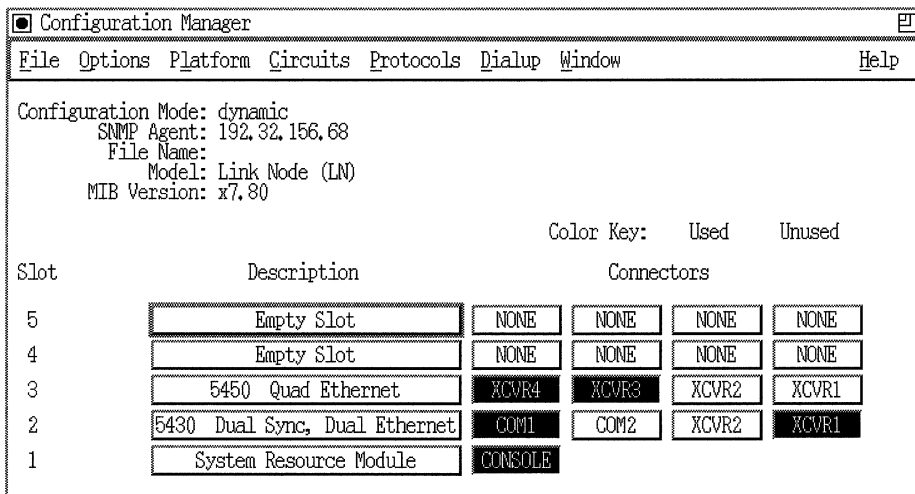
This section explains briefly how to accomplish these tasks. For more information on how to customize traps a router sends, refer to *Customizing SNMP, BOOTP, and RARP Services*.

### Identifying Site Manager as an SNMP Manager

To configure the router's SNMP agent to send trap messages to your Site Manager workstation, you must first tell the router to recognize your Site Manager workstation as a valid SNMP manager.

1. From the Wellfleet Site Manager window, select Tools→Configuration Manager. Then select Local File, Remote File, or Dynamic mode.

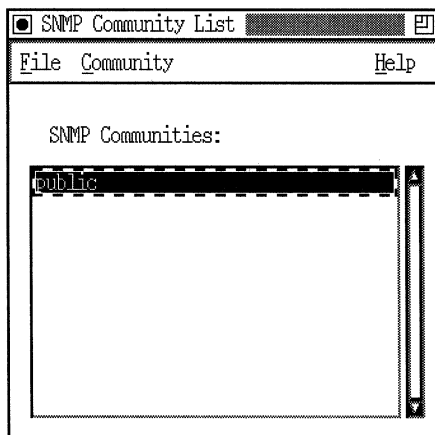
The Configuration Manager window appears (Figure 2-2).



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

- From the Configuration Manager window, select Protocols→IP→SNMP→Communities.

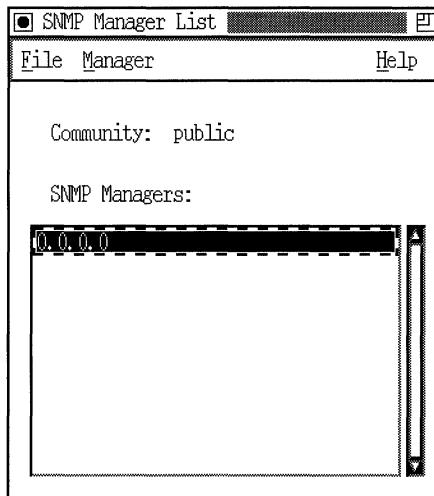
The SNMP Community List window appears (Figure 2-3).



**Figure 2-3. SNMP Communities List**

3. From the SNMP Community List window, select Community→Managers.

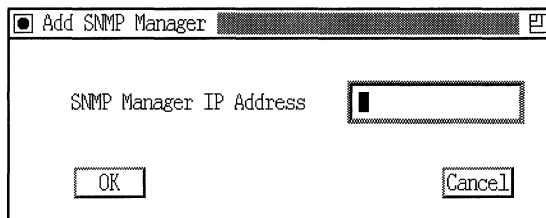
The SNMP Manager List window appears (Figure 2-4).



**Figure 2-4. SNMP Manager List**

4. From the SNMP Manager List window, select Manager→Add Manager.

The Add SNMP Manager window appears (Figure 2-5).



**Figure 2-5. Add SNMP Manager Window**



5. Type the IP address of your Site Manager workstation. Then click on OK.

The SNMP Manager List window displays your workstation's IP address.

6. Save this configuration to a file and volume on the router.

## Saving a Configuration

To save a configuration to a file and volume on the router, select File→Save or File→Save As from the Wellfleet Configuration Manager window. Exiting from the Configuration Manager window also prompts you to save a configuration. Specify the filename and router volume, then select Save. Note the name and router volume you specified.

Refer to *Configuring Wellfleet Routers* for more information on using the Configuration Manager tool.

## Running Multiple Network Management Applications

If you are running another network management application (besides Site Manager) on your workstation, you must configure Site Manager to receive trap messages via another port on your Site Manager workstation. This is necessary for the following reasons:

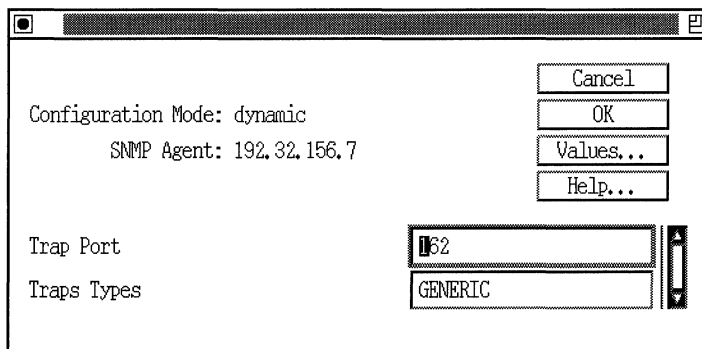
- ❑ The router can only send trap messages to one network management application at a time.
- ❑ Only one application can map to a port at a time.

**Note:** By default, a network management application installed on your workstation binds to UDP (User Datagram Protocol) port 162. This port is dedicated to receiving SNMP traps from the SNMP agent. Since Site Manager is the preferred network management application for receiving trap messages, we recommend that, when running another manager, you configure Site Manager to bind to an alternative UDP port where Site Manager can continue to receive trap messages.

To configure the SNMP agent to send trap messages to Site Manager via a different port, follow these steps:

1. From the Configuration Manager window, select Protocols→IP→SNMP→Communities.
2. From the SNMP Community List window that appears, select Community→Managers.
3. From the SNMP Manager List window, select Manager→Edit Manager.

The Trap Port and Trap Types window appears with the default value 162 (Figure 2-6).



**Figure 2-6. Trap Port and Trap Types Window**

4. To select a port number, use the Values button or type a port number in the Trap Port field.

You can enter any port number on your Site Manager workstation, as long as another application is not using that port.

5. Click on OK in the Trap Port and Trap Types window.
6. Save this configuration to a file and volume on the router. For information, see the previous section, "Saving a Configuration."
7. Exit Site Manager by selecting File→Exit from the Wellfleet Site Manager window.

- Restart Site Manager using either the UNIX or DOS commands shown in Table 2-1.

**Table 2-1. Restarting Site Manager on a New Port**

Platform	Steps
UNIX	<ol style="list-style-type: none"><li>Open a command line window.</li><li>Enter <b>wfsm -e</b> <i>&lt;port number&gt;</i> at the prompt.</li></ol>
DOS	<ol style="list-style-type: none"><li>Select the PC/Site Manager icon.</li><li>Select File→Properties.</li><li>Add <b>-e</b> <i>&lt;port number&gt;</i> to the end of the command line.</li><li>Double-click on the PC/Site Manager icon.</li></ol>

**Note:** You must specify the new port number every time you restart Site Manager.

## Configuring Traps Sent by a Router

You can specify by category, entity, or event the types of trap messages you want a router to send to your Site Manager workstation.

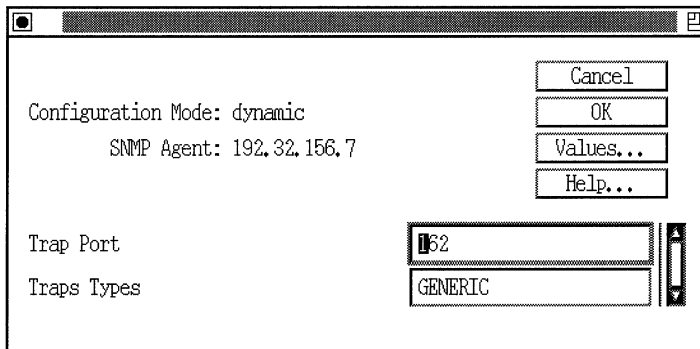
### Specifying Traps by Category

You can configure a router to send

- All traps
- Generic traps
- Specific traps
- No traps

To specify the trap types you want to receive at your workstation, follow these steps:

1. From the Configuration Manager window, select Protocols→IP→SNMP→Communities.
2. From the SNMP Communities List window that appears, select Community→Managers.
3. From the SNMP Manager List window that appears, select Manager→Edit Manager. The Trap Types and Trap Port window appears with the default value GENERIC in the Trap Types field (Figure 2-7).



**Figure 2-7. Specifying a Trap Category**

4. Click in the Trap Types field. Use the Values button to select an option; then click on OK in the Values Selection window. Table 2-2 describes the different trap types.

**Table 2-2. Categories of Traps**

Category	Description
NONE	Prohibits the SNMP agent from transmitting traps to this manager.
GENERIC	<p>Configures the agent to transmit well-defined SNMP traps (cold-start, warm-start, and authentication failure traps).</p> <p>The agent is automatically enabled to send cold-start and warm-start traps. However, you must enable the Authentication Failure Trap parameter if you want the agent to transmit authentication failure traps as well.</p>
SPECIFIC	Configures the agent to transmit all enabled trap message types (fault, warning, debug, information, and trace traps) from the protocol entities on your network.
ALL	Configures the agent to transmit cold-start and warm-start traps, as well as all other enabled traps (authentication failure, fault, warning, debug, information, and trace traps).

**Note:** You will usually want to select **GENERIC** or **SPECIFIC** when you configure the SNMP agent to send traps. These options minimize the agent's use of router resources.

5. Click on OK in the Trap Port and Trap Types window.
6. Save this configuration to a file and volume on the router.

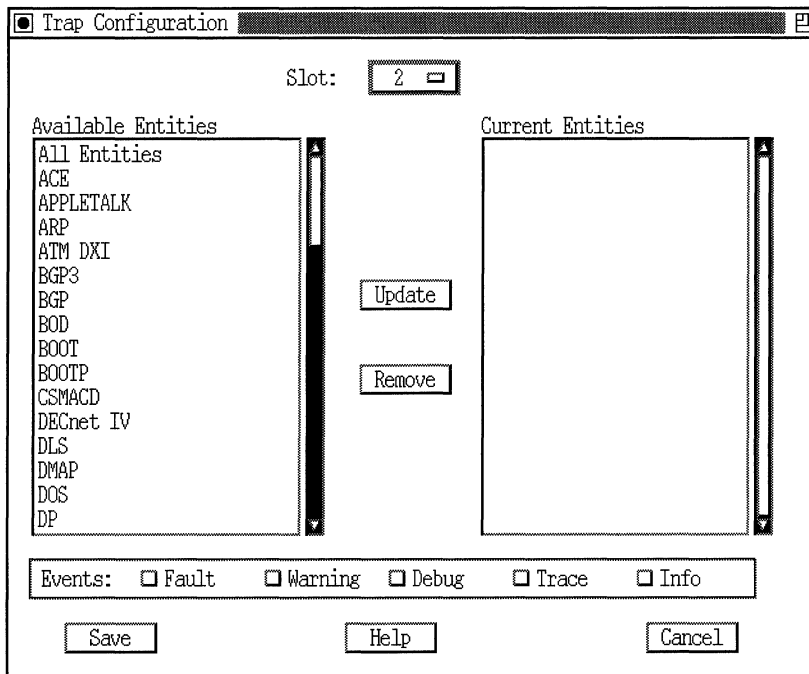
**Note:** If you select **SPECIFIC**, you must further specify by entity the kinds of trap messages you want the SNMP agent to send to your workstation. Proceed to the section "Specifying Traps by Entity."

## Specifying Traps by Entity

If you configure an SNMP agent to send SPECIFIC trap types to your Site Manager workstation, you must specify which protocols (entities) will send which trap types (fault, warning, information, debug, or trace) to your workstation. Proceed as follows:

1. From the Wellfleet Configuration Manager window, select Protocols→IP→SNMP→Trap Configuration→Interfaces.

The Trap Configuration window appears (Figure 2-8).



**Figure 2-8. Trap Configuration Window**

2. Select the appropriate slot.
3. Select an entity whose trap messages you want to receive at your Site Manager workstation.

4. Select the severity levels for that entity's trap messages.
5. Click on Update.  
The entity and severity levels are added to the Current Entities field.
6. Repeat Steps 2 through 5 for every entity whose trap messages you want to receive at your Site Manager workstation. Then click on Save.
7. Save this configuration to a file and volume on the router.

The entities you select will now send the trap types you selected to your workstation.

### Specifying Traps by Event Type

You can configure a router to always (or never) send trap messages that you designate by their unique entity code and event number. Proceed as follows:

1. From the Wellfleet Configuration Manager window, select Protocols→IP→SNMP→Trap Configuration→Exceptions.

The Traps Exceptions Lists window appears (Figure 2-9).

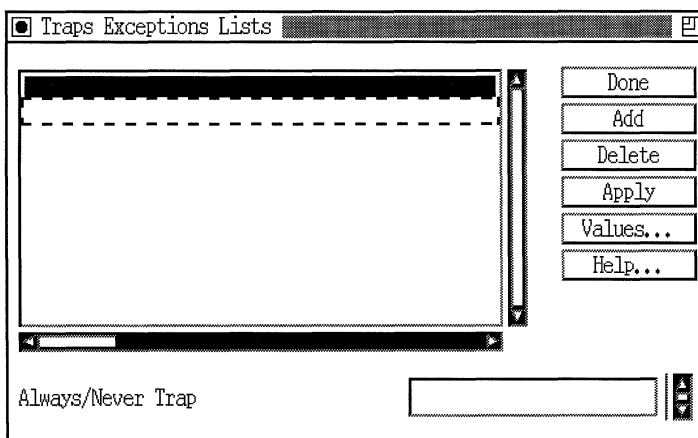
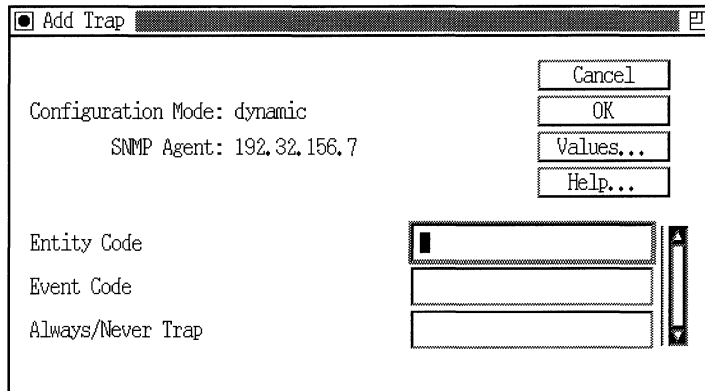


Figure 2-9. Traps Exceptions List

- To add an event message to the list of trap messages sent to your router, click on Add in the Traps Exceptions Lists window.

The Add Trap window appears (Figure 2-10).



**Figure 2-10. Add Trap Window**

- To determine which Entity Code and Event Code values to specify, refer to *Event Messages for Wellfleet Routers*.
- Use the Values button to enter values in the three fields shown in the Add Trap window. Table 2-3 shows the values you should enter.

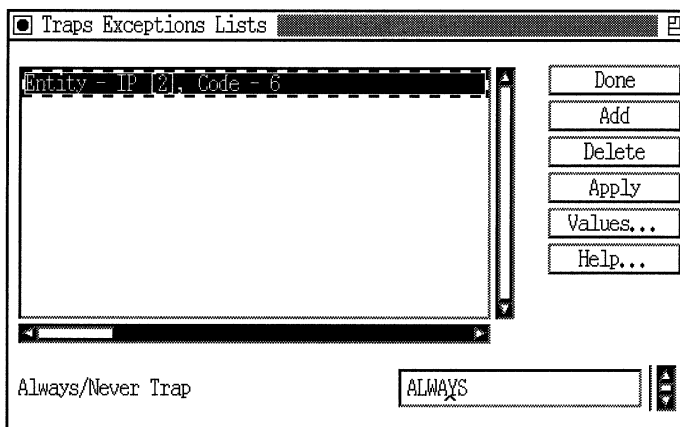
**Table 2-3. Entering Values in the Add Trap Window**

Field	Value
Entity Code	Enter a value between 0 and 61.
Event Code	Enter a value between 0 and 255.
Always/Never Trap	Enter ALWAYS.

- Click on OK in the Add Trap window.



The entity's event type appears in the Traps Exceptions Lists window (Figure 2-11).



**Figure 2-11. Traps Exceptions Lists Window**

You have now specified a particular entity's event message to be sent to your Site Manager workstation's Trap Monitor.

6. Repeat this procedure for every entity's event message you want sent to the Trap Monitor.
7. Click on the Apply and Done buttons.
8. Save this configuration to a file and volume on the router.

You have now configured the SNMP agent inside each specified router to send event messages, along with trap messages, to your Site Manager workstation's Trap Monitor.

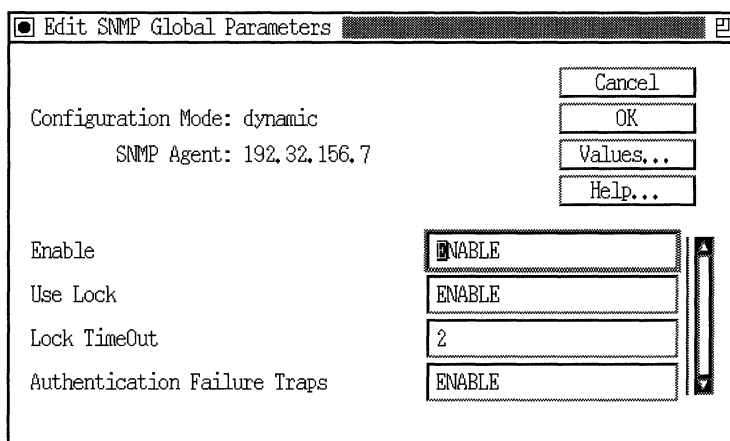
## Enabling an SNMP Agent

By default, the SNMP agent is always enabled. However, if the agent is disabled at some point, you will have to enable it. To enable an SNMP

agent to send trap messages to your Site Manager workstation, follow this procedure:

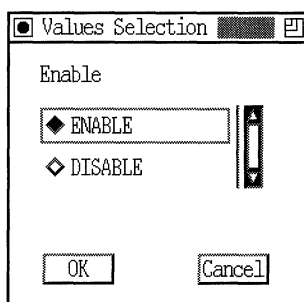
1. From the Wellfleet Configuration Manager window, select Protocols→IP→SNMP→Global.

The Edit SNMP Global Parameters window appears (Figure 2-12).



**Figure 2-12. Edit SNMP Global Parameters Window**

2. Use the Values button and select the Enable option from the Values Selection window (Figure 2-13). Then click on OK.



**Figure 2-13. Enabling an SNMP Agent**

3. Save this configuration to a file and volume on the router.

You have now configured this router's SNMP agent to send trap messages to your Site Manager workstation.

## Viewing Trap Messages

Your Site Manager workstation receives all types of trap messages that routers in your network are configured to send. However, the Trap Monitor tool lets you choose, from all trap messages received by the workstation, which traps you want to view in the Trap Monitor window. You can filter trap message types by severity or by IP address (using address filters).

The next section describes how to configure the Trap Monitor to receive trap messages from routers throughout your network.

## Using the Trap Monitor

The Trap Monitor tool lets you filter and view trap messages. Before you use the Trap Monitor tool to view trap messages, configure the SNMP agent in each router to send trap messages, as described earlier. The agent running in the router sends only the trap types that you enable in the router configuration. The Trap Monitor running in your Site Manager workstation subsequently filters and displays a subset of all the trap messages it receives from routers in your network.

**Note:** If you configure your routers to send traps, do not exit the Trap Monitor window. Otherwise, the routers log this message:

```
ICMP Destination unreachable
```

## Displaying the Trap History File

The trap history file contains trap messages that you specified be sent to your Site Manager workstation. The Trap Monitor dynamically

displays trap messages from this file after you load the trap history file into the Wellfleet Trap Monitor window.

Use the Load History File feature to display all trap messages since you last cleared the history file.

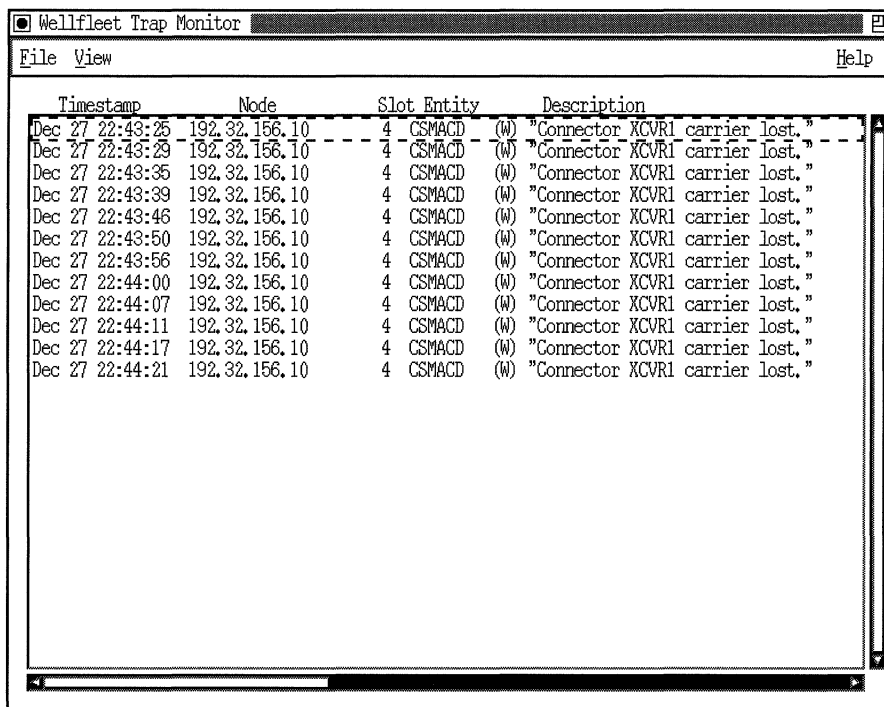
1. From the Wellfleet Site Manager window, select Tools→Trap Monitor.

The Wellfleet Trap Monitor window appears.

2. From the Wellfleet Trap Monitor window, select File→Load History File.

The Wellfleet Trap Monitor window displays incoming trap messages, along with trap messages logged since you last cleared the history file.

Figure 2-14 shows a Wellfleet Trap Monitor window with messages.



The screenshot shows a window titled "Wellfleet Trap Monitor" with a menu bar containing "File", "View", and "Help". The main area displays a table of trap messages with the following columns: Timestamp, Node, Slot, Entity, and Description. The messages are all of type "Connector XCVRI carrier lost." and originate from node 192.32.156.10.

Timestamp	Node	Slot	Entity	Description
Dec 27 22:43:25	192.32.156.10	4	CSMACD (W)	"Connector XCVRI carrier lost."
Dec 27 22:43:29	192.32.156.10	4	CSMACD (W)	"Connector XCVRI carrier lost."
Dec 27 22:43:35	192.32.156.10	4	CSMACD (W)	"Connector XCVRI carrier lost."
Dec 27 22:43:39	192.32.156.10	4	CSMACD (W)	"Connector XCVRI carrier lost."
Dec 27 22:43:46	192.32.156.10	4	CSMACD (W)	"Connector XCVRI carrier lost."
Dec 27 22:43:50	192.32.156.10	4	CSMACD (W)	"Connector XCVRI carrier lost."
Dec 27 22:43:56	192.32.156.10	4	CSMACD (W)	"Connector XCVRI carrier lost."
Dec 27 22:44:00	192.32.156.10	4	CSMACD (W)	"Connector XCVRI carrier lost."
Dec 27 22:44:07	192.32.156.10	4	CSMACD (W)	"Connector XCVRI carrier lost."
Dec 27 22:44:11	192.32.156.10	4	CSMACD (W)	"Connector XCVRI carrier lost."
Dec 27 22:44:17	192.32.156.10	4	CSMACD (W)	"Connector XCVRI carrier lost."
Dec 27 22:44:21	192.32.156.10	4	CSMACD (W)	"Connector XCVRI carrier lost."

Figure 2-14. Wellfleet Trap Monitor Window

You can scroll through the trap messages using the scroll bars on the bottom and right side of the window.

## Filtering Trap Messages

The Trap Monitor gives you two viewing options:

- Select Trap Types
- Set Address Filters

Using these options, you can filter by severity or by router IP address all trap messages that the Trap Monitor tool receives. The Trap Monitor displays only those trap types that you specify.

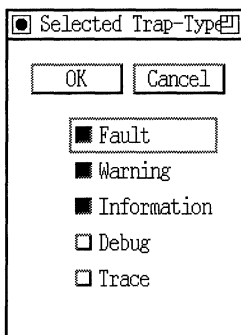
---

## Filtering by Severity

To filter trap messages by type (fault, warning, information, debug, or trace), proceed as follows:

1. From the Wellfleet Trap Monitor window, select View→Select Trap Types.

The Selected Trap-Type window appears (Figure 2-15).



**Figure 2-15. Selected Trap-Type Window**

2. Select the trap types you want the Trap Monitor to display, then click on OK.

**Note:** The fault, warning, and information types are usually the most useful types to select.

The Wellfleet Trap Monitor window displays only those trap messages that you specify. Refer to the later section “Clearing the Trap Monitor Window” to learn how to remove unwanted messages from the window.

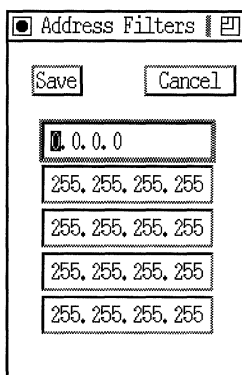
## Filtering by Router IP Address

Filtering messages by IP source address specifies which routers’ trap messages you want to appear in the Trap Monitor window. Specifying a full IP address causes the Trap Monitor to show trap messages that originate from the SNMP agent at that address only.

Specifying a partial IP address causes the Trap Monitor to show trap messages from all router SNMP agents that have the same partial IP address that you specify in the address filters window.

To configure an address filter from the Wellfleet Trap Monitor window, follow these steps:

1. Select View→Set Address Filters. The Address Filters window appears (Figure 2-16).



**Figure 2-16. Address Filters Window**

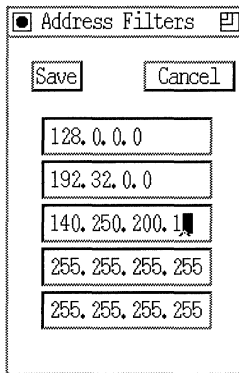
A default address filter of 0.0.0.0 causes the Trap Monitor to display trap messages from all Wellfleet routers that you configure to send trap messages to your Site Manager workstation.

The default address filter entry, 255.255.255.255, is merely a placeholder for an IP address that you choose to enter.

2. In the Address Filters window, specify one or more IP addresses and/or address filters.

You can enter as many as five complete IP addresses or address filters. The remaining fields must display the placeholder IP number 255.255.255.255.

Figure 2-17 shows a sample Address Filters window.



**Figure 2-17. Sample Address Filters Window**

With this configuration, you can view trap messages from all routers with IP addresses starting with 128. and 192.32., along with those from the router at IP address 140.250.200.1.

3. Click on Save.

Once you save the filter entries, the Trap Monitor displays trap messages only from those routers with an IP address that matches the value you specify in the Address Filters window.

## Clearing the Trap Monitor Window

To clear the Wellfleet Trap Monitor window, select **View**→**Clear Window**. The Trap Monitor clears the window of all trap messages.

Since the system constantly updates the trap history file, new trap messages appear right away.

## Clearing the Trap History File

The trap history file can hold only a fixed number of messages. When it reaches its limit, it starts overwriting the log at the beginning. The Trap Monitor lets you empty the current trap history file so that you can start a new log of trap messages.



From the Wellfleet Trap Monitor window, select File→Clear History File.

The Trap Monitor updates the trap history file and begins immediately to store new trap messages.

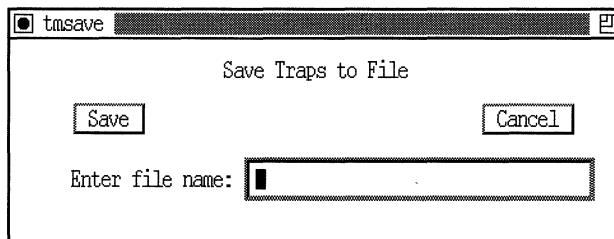
## Saving Trap Messages

The Trap Monitor lets you save the traps currently displayed in the Wellfleet Trap Monitor window to an ASCII file on your Site Manager workstation. You can later view, edit, or print this file.

To save trap messages to an ASCII file, proceed as follows:

1. From the Wellfleet Trap Monitor window, select File→Save Traps.

The Trap Monitor prompts you to name the file (Figure 2-18).



**Figure 2-18. Saving Traps to a File**

2. Type a directory and filename; then click on Save.

The system saves the log to an ASCII file on your computer. (If you do not specify a directory, the system saves the file to your local directory.) The Wellfleet Trap Monitor window reappears.

**Note:** You cannot reload an ASCII file back into the Trap Monitor.

---

# Chapter 3

## Using the Events Manager

For general information about monitoring events, see “Monitoring Traps and Events” in Chapter 1. For specific information about using buttons, windows, and other Site Manager features, refer to *Using Site Manager Software*.

Use the Events Manager to do the following:

- Display event logs
- Filter event messages
- Search for an event message
- Refresh the Events Manager window
- Clear the Events Manager window
- Save event messages
- Clear the current event log

## Connecting to a Router

When you view a router's event messages, you can connect to the router from either the Wellfleet Site Manager window or the Wellfleet Events Manager window.

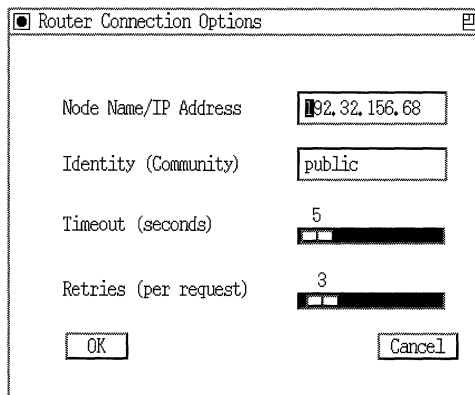
To connect to a router using the Events Manager, proceed as follows:

1. Select **Tools**→**Events Manager** from the Wellfleet Site Manager window.

The Events Manager window appears.

2. From the Wellfleet Events Manager window, select **Options**→**Router Connection**.

The Router Connection Options window appears (Figure 3-1).



**Figure 3-1. Router Connection Options Window**

3. In the Node Name/IP Address field, type the IP address of the router to which you want to connect. Then click on OK.

The Wellfleet Events Manager window displays the specified IP address.

## Displaying Event Logs

You must know how to load an event log into the Wellfleet Events Manager window, as event messages do not appear in the window until you retrieve this log. There are three types of event logs that you can load into the Events Manager:

- Current:** The log in the router's memory
- Remote:** The log on the router's flash card or floppy diskette
- Local:** The log transferred and saved (in binary format) to the Site Manager workstation

When you retrieve an event log file using Site Manager, you are using the Trivial File Transfer Protocol (TFTP) to transfer this file from the router's memory to the Site Manager workstation.

## Displaying the Current Log

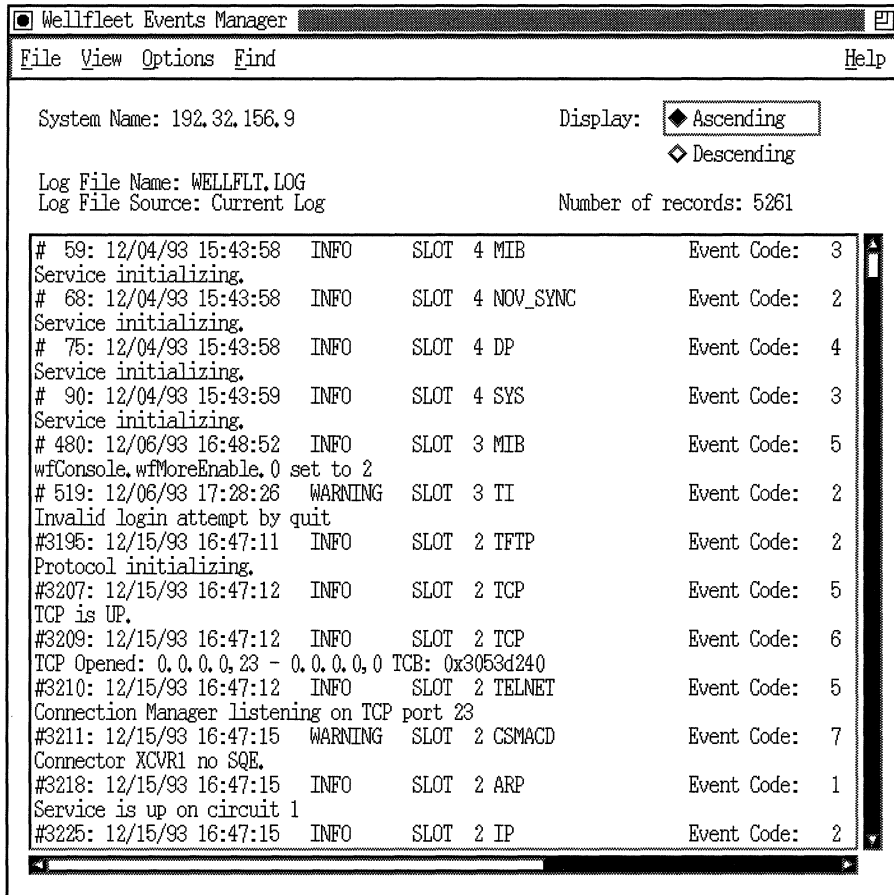
The current log is the temporary log file in the router's memory.

Before you display these event messages, you must first connect to the router whose event log you want to view. Then, to display the current log in the router's memory, select **File→Get Current Log File** from the Wellfleet Events Manager window.

Event messages appear in the Wellfleet Events Manager window, along with the following information (Figure 3-2):

- `WELLFLT.LOG` appears in the Log Filename field.
- `Current Log` appears in the Log File Source field.
- The total number of events appears in the Number of Records field.

Refer to *Event Messages for Wellfleet Routers* for a listing of event messages and suggested responses.



**Figure 3-2. Wellfleet Events Manager Window**

You can scroll through the event messages using the scroll bars on the bottom and right side of the window. Select Ascending to display events from the latest to the earliest time that they occurred. Select Descending to display events from earliest to latest.

---

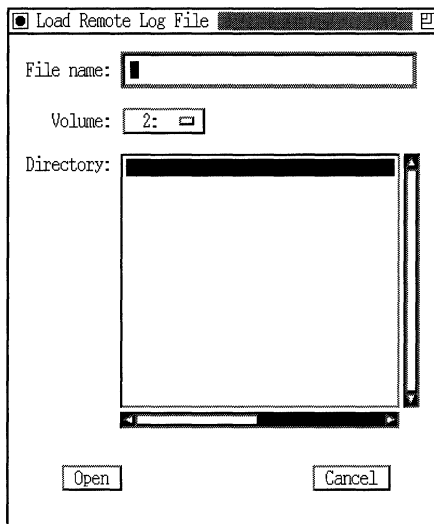
## Displaying a Remote Log

A remote log resides on the router's memory card or floppy diskette. To display a remote log, you must retrieve the log from the router's media.

Before you display any event messages, you must connect to the router whose event messages you want to view. After doing this, proceed as follows:

1. From the Wellfleet Events Manager window, select **File**→**Get Remote Log File**.

The Load Remote Log File window appears (Figure 3-3).



**Figure 3-3. Load Remote Log File Window**

2. Select the volume that contains the log file from the Volume pull-down menu.
3. Enter the filename.
4. Click on Open.

The router transfers the file to the Site Manager workstation, where Site Manager displays the events listed in the file in the Wellfleet Events Manager window. Along with event messages from the router's memory card or diskette, the following data appears in the Wellfleet Events Manager window:

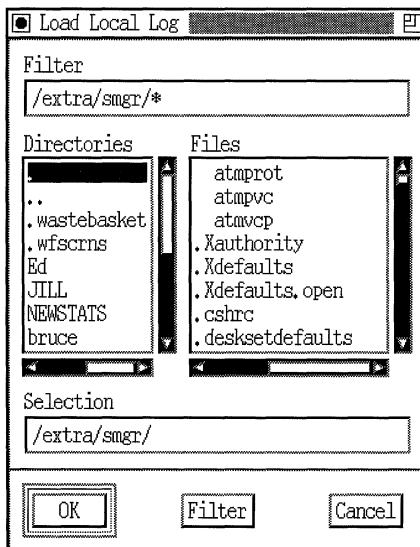
- ❑ The filename you selected appears in the Log Filename field.
- ❑ Remote Log appears in the Log File Source field.
- ❑ The total number of events appears in the Number of records field.

## Displaying a Local Log

A local log resides on the hard drive of your Site Manager workstation. Before you display any event messages, you must connect to the router whose event log you want to view. After doing this, proceed as follows:

1. From the Wellfleet Events Manager window, select File→Load Local Log File.

A Load Local Log window appears (Figure 3-4).



**Figure 3-4. Load Local Log Window**

2. Select the directory that contains the log file in the Directories box until the path to the directory appears in the Selection window.
3. Select or type in the filename in the Selection box after the pathname.
4. Click on OK.

Along with the event messages from this file, the following data appears in the Wellfleet Events Manager window:

- The filename you selected appears in the Log Filename field.
- The name Local Log appears in the Log File Source field.
- The total number of events appears in the Number of records field.

## Filtering Event Messages

You can specify the types of event messages that appear in the Wellfleet Events Manager window by specifying *filters*. You can filter the event messages by router IP address, severity, slot, or entity. The Filters feature in the Trap Monitor window specifically filters for severity, slot, and entity.

**Note:** Filtering does not affect how events are logged in the router's memory. Event messages are filtered only in the Events Manager window, not in their source.

### Filtering by Severity, Slot, and Entity

Filter the event messages shown in the Wellfleet Events Manager window as follows:

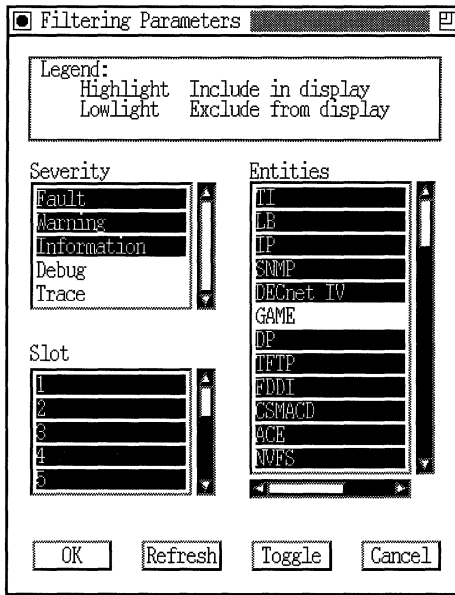
1. Display events in the Wellfleet Events Manager window.
2. Select View→Filters.

The Filtering Parameters window appears (Figure 3-5).

This window highlights the activated parameters. You can use the Toggle button to quickly switch between highlighted and nonhighlighted options.

---





**Figure 3-5. Filtering Parameters Window**

You can change the filtering setup by highlighting any Severity, Slot, or Entities parameter you want included in the next event log display. You can then do the following:

- Click on Refresh to refilter the event messages in the Events Manager window.
  - Click on OK to save the changes you made in the Filtering Parameters window without automatically refiltering the event messages in the Events Manager window.
3. Select the parameters you are interested in. Then click on Refresh or OK.

Notice that the number of records does not change; a complete listing of the number of event messages is always provided.

**Note:** We recommend filtering for trace events only when you diagnose network problems. You do not need to filter for debug events.

---

## Filtering by Router IP Address

Filtering by router IP address requires that you connect to a router from the Wellfleet Site Manager window or Wellfleet Events Manager window. See the earlier section “Connecting to a Router.” Then display a current event log, remote event log, or local event log using the File menu. See “Displaying Event Logs,” described earlier.

Event messages appear in the Wellfleet Events Manager window. You have effectively “filtered” a log by router IP address.

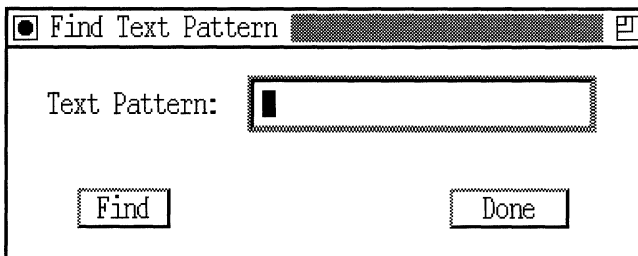
## Searching for an Event Message

The Events Manager provides Find and Find Next options for locating an event that contains text that you specify.

Locate an event containing the text you specify as follows:

1. Display events in the Wellfleet Events Manager window.
2. Select Find→Find.

The Find Text Pattern window appears (Figure 3-6).



**Figure 3-6.** Find Text Pattern Window

3. Type the text you want to find.

You can type up to 255 characters (including spaces) in this box.

**Note:** The Find Text Pattern window is case-sensitive.

4. Click on Find.

Site Manager searches from the first event highlighted in the log to the first instance of the text pattern and highlights the event that contains the text pattern.

5. Select Find→Find Next to find the next instance of the same text pattern.

## Refreshing the Events Manager Window

To redisplay a log file in Site Manager's memory after you set up new filters, select View→Refresh Display from the Wellfleet Events Manager window.

The Events Manager displays the events that match the filters you last saved, according to the setting of the Ascending/Descending option in the Wellfleet Events Manager window.

## Clearing the Events Manager Window

To clear the events in the Wellfleet Events Manager window, select View→Clear Window.

The Wellfleet Events Manager window clears and remains empty until the next time you load an event log or refresh the display.

## Saving Event Messages

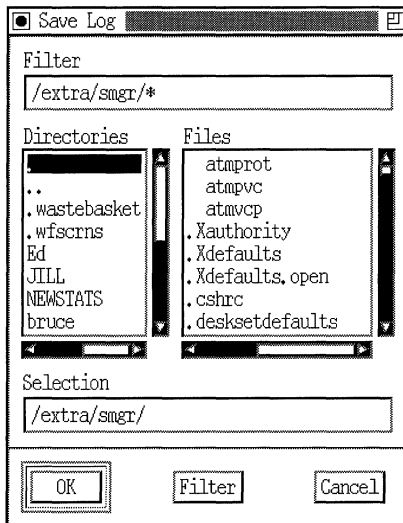
You can save the event messages that appear in the Wellfleet Events Manager window to an ASCII file on your Site Manager workstation. You can then print the log using any tool on your workstation.

To save an event log to an ASCII file, follow these steps:

1. Display the event log in the Wellfleet Events Manager window.
2. Filter the event messages displayed.

3. Select File→Save Output to Disk.

The Save Log window appears (Figure 3-7).



**Figure 3-7. Save Log Window**

4. Select the directory path in which you want to save the file.

The path appears in the Selection window.

5. Enter the filename in the Selection window after the path.

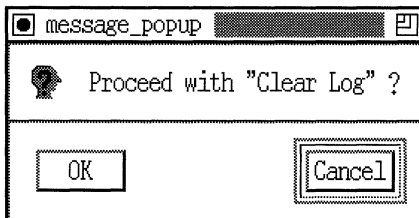
6. Click on OK.

The Events Manager saves the log to an ASCII file in the specified local directory. (If you do not specify a directory, the file is automatically saved to your local directory.)

**Note:** For viewing purposes, you can reload into the Events Manager event logs stored in binary format. You cannot reload into the Events Manager event logs stored in ASCII format.

## Clearing the Current Event Log

The router's event log can hold only a fixed number of messages. When it reaches its limit, it starts overwriting the log at the beginning. To clear a router's current event log, select Administration→Clear Log from the Wellfleet Site Manager window. A confirmation window appears (Figure 3-8).



**Figure 3-8. Confirmation Window**

Click on OK in the confirmation window to delete all the event messages that are currently stored in the router's memory. Site Manager enters a message in the event log indicating that it has cleared the log. New event messages automatically start filling the event log again.

---

# Chapter 4

## Using the Statistics Manager

For general information about monitoring router statistics, see “Monitoring Statistics” in Chapter 1. For specific information about using buttons, windows, and other Site Manager features, refer to *Using Site Manager Software*.

Use the Statistics Manager to do the following:

- ❑ Access statistics
- ❑ Connect to a router
- ❑ View the Wellfleet MIB
- ❑ Define the current screen list
- ❑ Display statistics screens
- ❑ Create statistics filters
- ❑ Search for statistics information
- ❑ Save statistics information
- ❑ Build custom statistics screens

## Accessing Statistics

You access all router statistics from the Statistics Manager window. To access this window, begin at the Wellfleet Site Manager window and select Tools→Statistics Manager. The Statistics Manager window appears (Figure 4-1).

The screenshot shows a window titled "Statistics Manager" with a menu bar containing "File", "View", "Options", "Tools", "Window", and "Help". Below the menu bar, it displays "SNMP Agent: 192.32.156.9". The main content is a table with the following data:

Circuit Name(#)	Slot	Connector	Type	Protocols
E21 (1)	2	1	CSMACD	IP, RIP
O31 (2)	3	1	TOKEN	SR, LLC2, LSS
O31.1lc2 (3)	3	1	TOKEN	LLC2, LSS, DLS, LLC2 (VC)
E22 (4)	2	2	CSMACD	LB, SPT, IP, RIP, EGP, OSPF
S31 (5)	3	1	SYNC	FR, PRQ
S32 (6)	3	2	SYNC	PPP, OSI
S41 (7)	4	1	SYNC	SMDS, AT
S42 (8)	4	2	SYNC	X25
xvc4.2.204102.0	4	2	SYNC	OSI, X25 (VC)

Figure 4-1. Statistics Manager Window

**Note:** The Statistics Manager requires an active connection to a target router to display router statistics. The next section describes how to use the Statistics Manager tool to establish or change a connection to a router.

The Statistics Manager window displays the current router's configuration. That is, it displays the circuit type and location of the router's network interfaces and the bridging and routing protocols that are enabled on each interface.

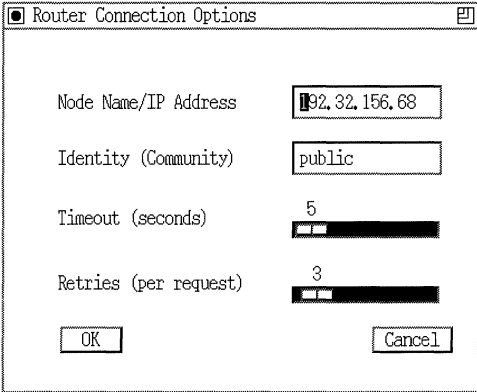
---

## Connecting to a Router

To connect to a router from the Statistics Manager window, proceed as follows:

1. Select Options→Router Connection.

The Router Connection Options window appears (Figure 4-2).



The screenshot shows a dialog box titled "Router Connection Options". It contains the following fields and values:

Field	Value
Node Name/IP Address	192.32.156.68
Identity (Community)	public
Timeout (seconds)	5
Retries (per request)	3

Buttons: OK, Cancel

**Figure 4-2. Router Connection Options Window**

2. Specify the target router's IP address in the Node Name/IP Address field. Then click on OK.

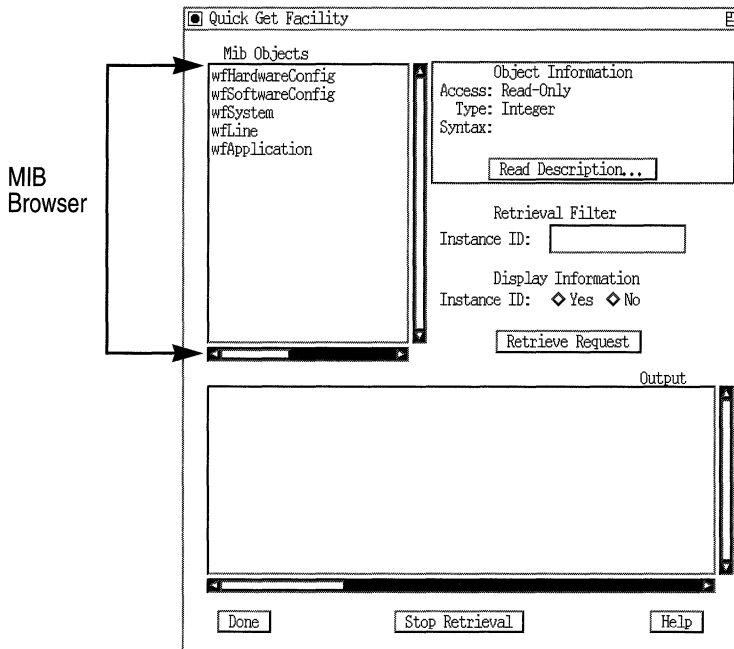
The SNMP Agent field in the Statistics Manager window displays the IP address of the router you specified. (See Figure 4-1.)

## Viewing the Wellfleet MIB

You view the Wellfleet Management Information Base (MIB) using the Quick Get tool. Quick Get includes a MIB Browser tool that lets you scroll through and select up to ten objects from the MIB. You then use Quick Get to get all instances of objects you select and to display that information in columns in the Quick Get Facility window.



To access the Quick Get Facility window, begin at the Statistics Manager window and select Tools→Quick Get. The Quick Get Facility window appears (Figure 4-3).



**Figure 4-3. Quick Get Facility Window**

The MIB Browser operates the MIB Objects window located in the top left corner of the window.

## Using the MIB Browser

The Wellfleet MIB is organized as a hierarchical tree. When you first activate Quick Get, the MIB Browser displays the five object groups at the top of the tree:

- wfHardwareConfig
- wfSoftwareConfig
- wfSystem
- wfLine
- wfApplication

Beneath these five object groups, related objects are organized in subordinate object groups, or tables (for example, Figure 4-4 shows part of the MIB tree for the *wfSystem* object group). The prefix *wf* that precedes each MIB object indicates that it is a Wellfleet enterprise-specific object.

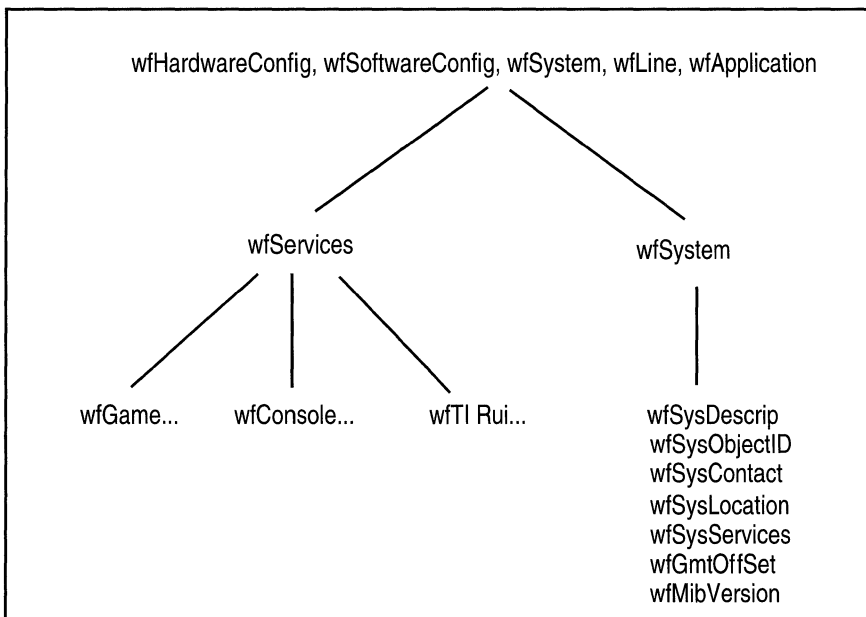


Figure 4-4. MIB Tree for System Group

To access individual objects, first select the top-level object group. The MIB Browser brings you down one level in the tree and displays subordinate object groups. Continue selecting object groups and descending through the MIB tree until the MIB Browser displays the individual objects that you want to select.

You can differentiate between object groups and individual objects by noting their position in the MIB Browser window. Object groups are flush left with the window; individual objects are indented slightly.

Use the scroll bar to scroll through the MIB. To move backward in the MIB tree, select the Back option. Table 4-1 describes where to find different types of MIB information.

**Table 4-1. Finding MIB Information**

Top-Level MIB Object Group	Types of Objects/Information	Example
wfHardwareConfig	Objects pertaining to router hardware configuration	Router backplane ID, power supply, temperature, serial number
wfSoftwareConfig	Objects pertaining to the type of protocol and driver software that is loaded, and information required to load the software	Interface drivers
wfSystem	Objects pertaining to the router system software	System record, console, remote console, circuit name table
wfLines	Objects pertaining to drivers and lines	FDDI tables, line state, line traffic
wfApplication	LAN, WAN, and Bridge information	Routing tables, packet information, protocol state information

## Getting Instances of Selected Objects

You can select and retrieve instances for as many as ten MIB objects at one time. To locate individual objects, find the object group or table that logically categorizes the objects you are interested in.

Proceed as follows:

1. Select the top-level object group to which the objects belong.

The MIB Objects field displays a list of subordinate groups. For example, when you select *wfApplication*, the objects shown in Figure 4-5 appear.

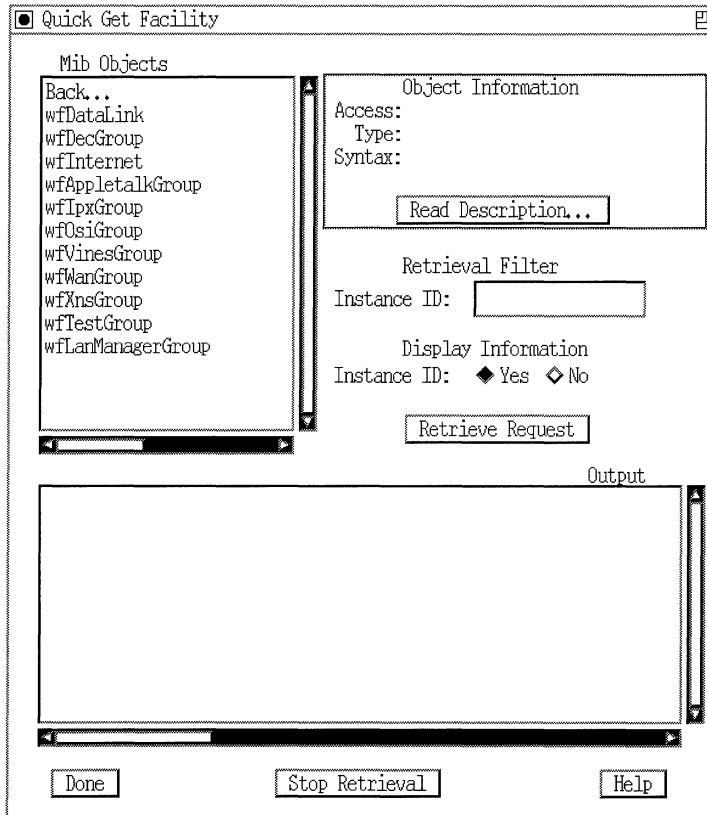


Figure 4-5. Sample Quick Get Facility Window

2. Select additional object groups or tables until you reach the individual objects you are interested in.

For example, to see the current state of all IP interfaces configured on the router, select *wfInternet*, *wfIpRouting*, *wfIpGroup*, *wfIpInterfaceTable*. Then select the *wfIPInterfaceState* and *wfIPInterfaceAddr* objects located beneath the *wfIpInterfaceTable* group.

3. Select each object in which you are interested. Note that selectable objects are indented.

When you select an individual object, the Object Information field at the top right of the Quick Get Facility window displays the following information about that object:

Access	Whether the object is user-configurable (read-write) or nonconfigurable (read-only)
Type	The type of object (integer, octet, string)
Syntax	The possible values for the object

Click on Read Description to display a Statistics Help window that contains a more detailed description of the object. Click on OK to exit the Statistics Help window.

To deselect an object listed under MIB Objects, select the object again.

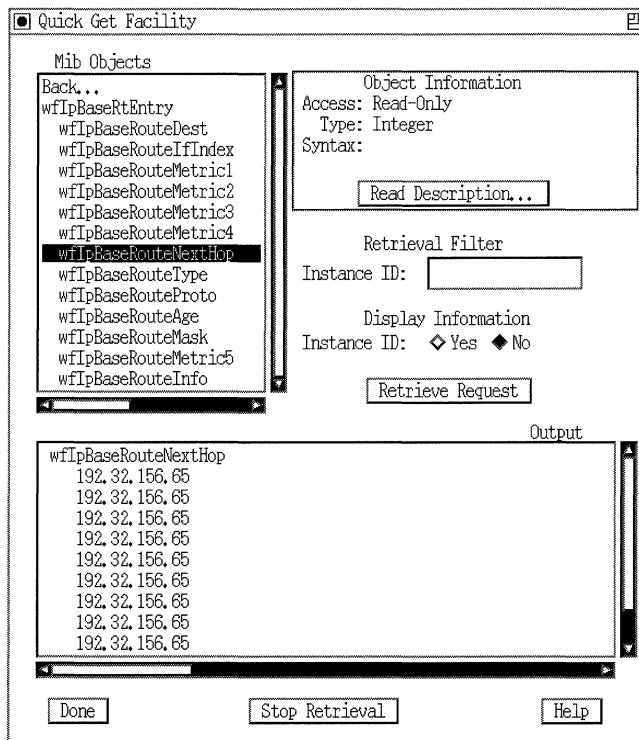
4. Use selections in the Display Information and Retrieval Filter fields of the Quick Get Facility window to determine the format of MIB objects retrieved to the Output field of that window.

You can use the Quick Get Facility to display

- All (unfiltered) or specific (filtered) instances of MIB objects selected in the Mib Objects field
- All (filtered or unfiltered) instances of selected MIB objects, with or without their associated instance IDs

To display without instance IDs all instances of MIB objects selected in the Mib Objects field (Figure 4-6):

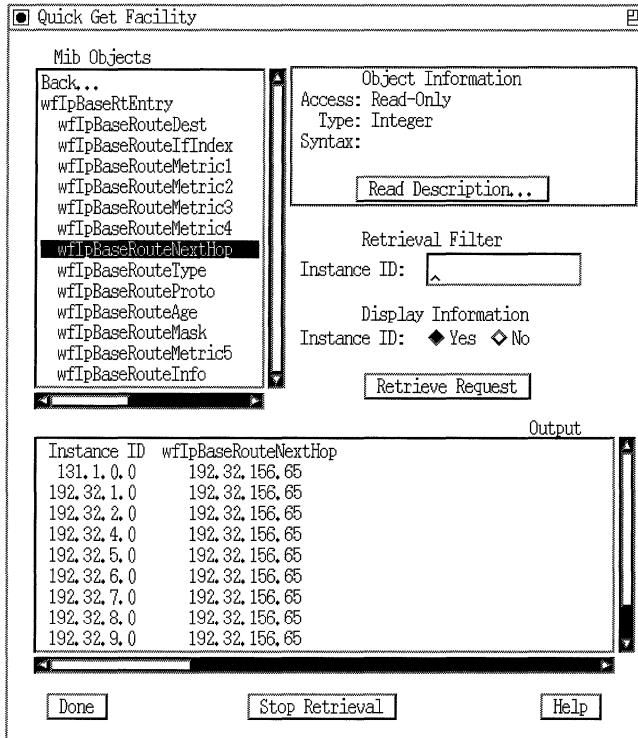
- a. Leave the Retrieval Filter field blank.
- b. Select No in the Display Information field.
- c. Click on the Retrieve Request button.



**Figure 4-6. All Instances Retrieved (Unfiltered) without Instance IDs**

To display with instance IDs all instances of MIB objects selected in the Mib Objects field (Figure 4-7):

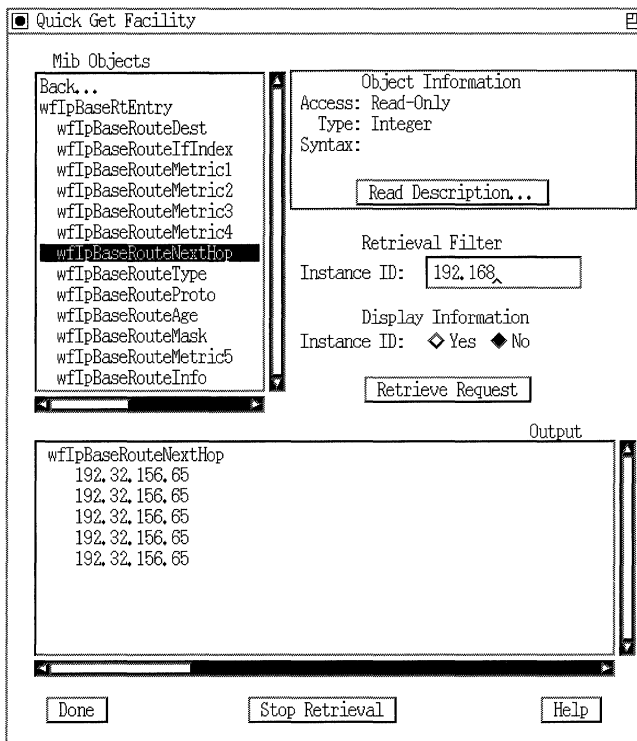
- a. Leave the Retrieval Filter field blank.
- b. Select Yes in the Display Information field.
- c. Click on the Retrieve Request button.



**Figure 4-7. All Instances Retrieved (Unfiltered) with Instance IDs**

To display without instance IDs only specific (filtered) instances of MIB objects selected in the Mib Objects field (Figure 4-8):

- Enter all or part of the instance ID for the desired MIB object(s) in the Retrieval Filter field. (Entering more of the instance ID narrows the object search.)
- Select No in the Display Information field.
- Click on the Retrieve Request button.

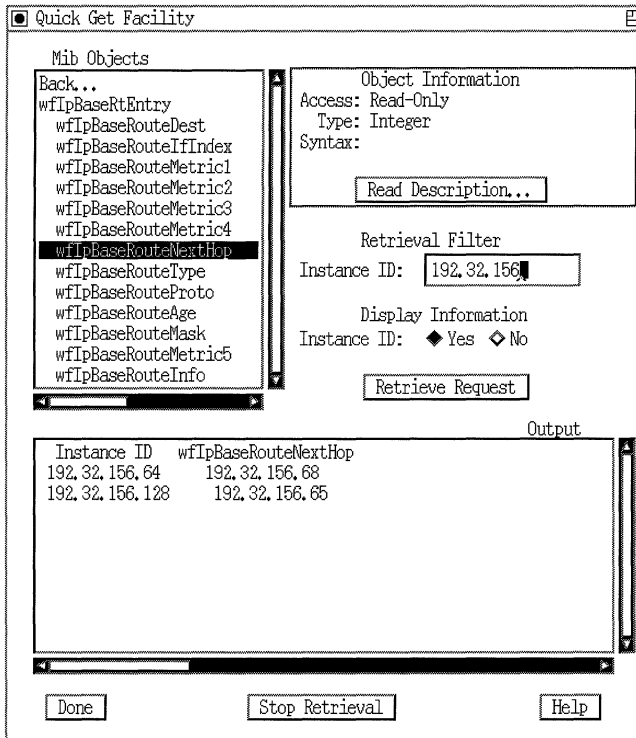


**Figure 4-8. Specific Instances Retrieved without Instance IDs**

To display without instance IDs only specific (filtered) instances of MIB objects selected in the Mib Objects field (Figure 4-9):

- a. Enter all or part of the instance ID for the desired MIB object(s) in the Retrieval Filter field. (Entering more of the instance ID narrows the object search.)
- b. Select Yes in the Display Information field.
- c. Click on the Retrieve Request button.





**Figure 4-9. Specific Instances Retrieved with Instance IDs**

5. Click on Stop Retrieval to halt retrieval of MIB objects selected in the Mib Objects field.
6. Click on Retrieve Request each time you want to refresh the information displayed in the Output field.
7. To exit the Quick Get Facility window, click on Done.

## Defining the Current Screen List

The current screen list is a subset of the default statistics screens and any custom statistics screens you build. (More information follows on the Screen Builder tool you use to custom design router statistics screens.)

**Note:** When you first use the Statistics Manager, the current screen list is empty. To view router statistics, you must add statistics screens to the current screen list.

To manage your statistics screen database most effectively, add to the current screen list only those statistics screens that you use most often.

## Adding Statistics Screens

To add a statistics screen to the current screen list, follow these steps:

1. From the Statistics Manager window, select Tools→Screen Manager.

The Screen Manager window appears (Figure 4-10).

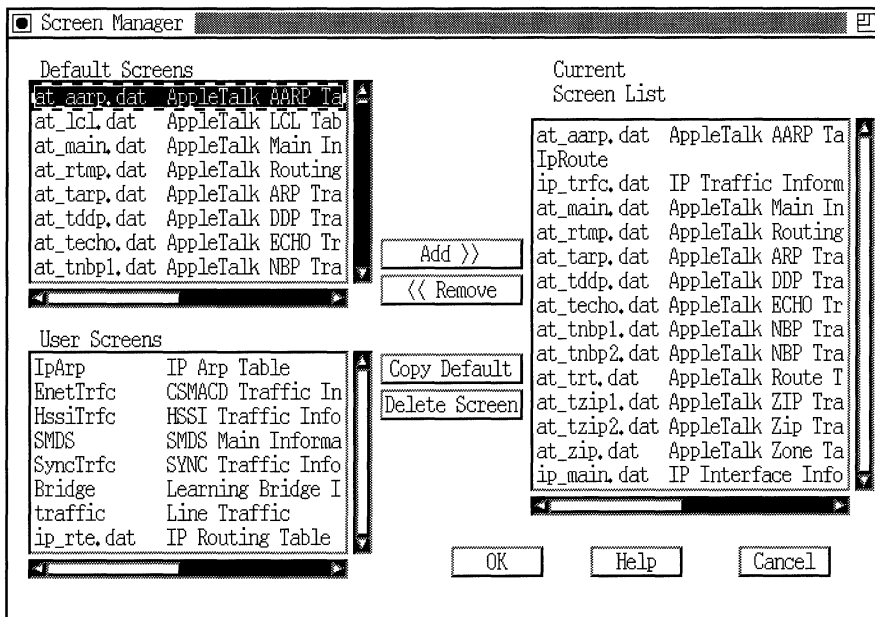
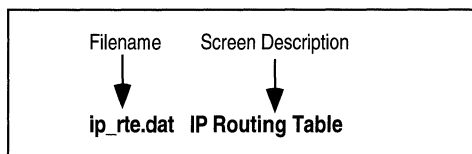


Figure 4-10. Screen Manager Window

The Screen Manager displays the default statistics screens, grouped by protocol. Use the scroll bar to scroll through the list. If you have not yet built any custom statistics screens, then the User Screens list is empty. Later, it will display any custom screens you create using the Screen Builder.

The Statistics Manager identifies each default statistics screen using a filename with the *.dat* extension, followed by a description that describes the type of data the screen displays. In the example shown in Figure 4-11 the statistics screen displays IP routing statistics.



**Figure 4-11. Example of Filename and Screen Description**

2. Highlight the statistics screen you want to add to the Current Screen List, then click on Add.

The Current Screen List can contain both default screens and custom screens at the same time, so you can add statistics screens from either list. The Statistics Manager updates the Current Screen List to include the statistics screen that you add.

Repeat steps 1 and 2 to add additional statistics screens to the current screen list.

3. Click on OK to update the current screen list and save your changes, or click on Cancel to exit the Screen Manager window without saving the changes.

You can use the Launch Facility to display any screen on the current screen list. For instructions, see “Displaying Statistics Screens” later in this chapter.

## Removing Statistics Screens

To remove a statistics screen from the Current Screen List, follow these steps:

1. From the Statistics Manager window, select Tools→Screen Manager.

The Screen Manager window appears.

2. Highlight the statistics screen you want to remove from the current screen list. Then click on Remove.

The Statistics Manager removes the statistics screen you select. Repeat Steps 1 and 2 to remove additional statistics screens.

3. Click on OK to exit the window and save your changes, or click on Cancel to exit without saving the changes.

## Displaying Statistics Screens

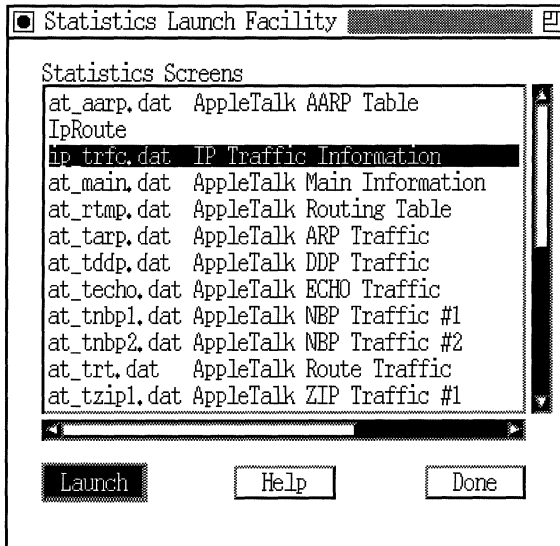
Use the Launch Facility to display statistics screens.

**Note:** Before you can display a statistics screen, you must add it to the current screen list. For instructions, see the previous section, “Defining the Current Screen List.”

To display a statistics screen, follow these steps:

1. From the Statistics Manager window, select Tools→Launch Facility.

The Statistics Launch Facility window displays the statistics screens that are in the Current Screen List (Figure 4-12).



**Figure 4-12. Selecting a Screen**

2. Select one of the statistics screens and click on Launch.

Once you launch the statistics screen, Site Manager begins retrieving the specified MIB objects from the router. After a short time, a statistics screen appears, such as the one shown in Figure 4-13.

Circuit Name	IP Address	State	Datagrams RCVD	Datagrams XMIT
S31	1.0.0.1	Down	0	0
E24	192.32.156.65	Up	37399568	39536304
O41	192.32.156.129	Up	417463	458611
E21	192.32.180.43	Up	39508309	34535891

Figure 4-13. Statistics Screen

## Refreshing Active Statistics Screens

To update a statistics screen, select View→Refresh Display.

The Statistics Manager retrieves the MIB objects from the router and updates the statistics screen with the new data.

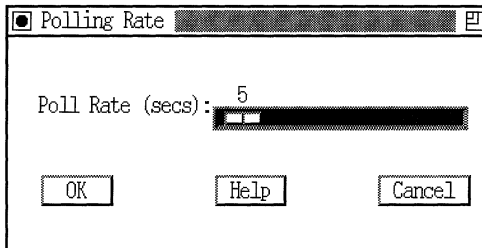
## Specifying Circuit Mode Statistics Polling Rate

A circuit mode statistics screen is one that the Statistics Manager continually updates with new data. When viewing a circuit mode screen, you can specify how often the Statistics Manager polls the router to update the data.

To specify the polling rate, begin at a statistics screen and proceed as follows:

1. Select Options→Poll Rate.

The Polling Rate window appears (Figure 4-14).



**Figure 4-14. Polling Rate Window**

2. Use the sliderbar to specify a polling rate; then click on OK.

## Zeroing Circuit Mode Statistics

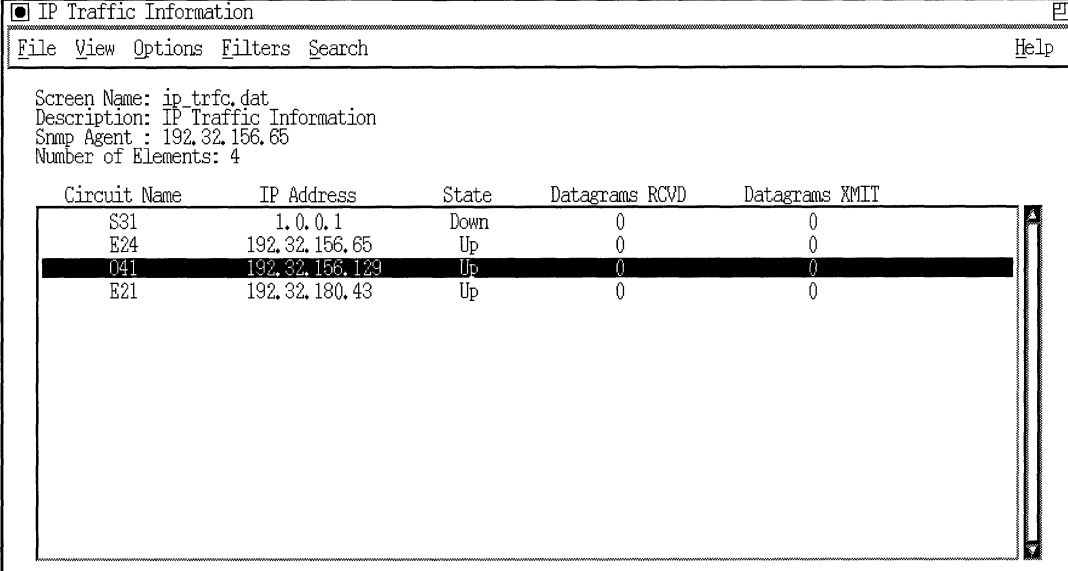
You can reset all counters in a circuit mode statistics screen to zero through the Zero All Counters menu option. You can also reset all counters in a selected row to zero through the Zero Current Row Counters menu option.

**Note:** These functions affect only the values displayed in Site Manager circuit mode statistics windows, and have no effect on the actual value of counter objects in a router MIB.

## Zeroing All Counters in a Screen

To clear all counters in a circuit mode statistics screen, select Options→Zero All Counters.

Figure 4-15 shows a typical response to the Zero All Counters option.



IP Traffic Information

File View Options Filters Search Help

Screen Name: ip\_trfc.dat  
Description: IP Traffic Information  
Snmp Agent : 192.32.156.65  
Number of Elements: 4

Circuit Name	IP Address	State	Datagrams RCVD	Datagrams XMIT
S31	1.0.0.1	Down	0	0
E24	192.32.156.65	Up	0	0
041	192.32.156.129	Up	0	0
E21	192.32.180.43	Up	0	0

**Figure 4-15. Zeroing All Counters in a Screen**

**Note:** In this example, the counters Datagrams RCVD and Datagrams XMIT reset to zero *in the statistics screen*. This type of reset has no effect on the actual, current values of these counter objects in the router MIB.

The Zero All Counters command stores the value of every counter object in the display at reset time. Each stored value provides a reference point for counter values displayed following the reset; that is, after resetting all counters in the display.

- The Statistics Manager displays only the difference between the counter value at reset time (the last known reference value) and the actual, current (MIB) value of the same counter.
- The counter values in display reflect *the amount of change* incurred beyond the reference values stored at reset time.



## Zeroing All Counters in a Specific Row

To clear all counters in a specific row of a circuit mode statistics screen, select a row, then select Options→Zero Current Row Counter.

Figure 4-16 shows a typical response to the Zero Current Row Counters option.

IP Traffic Information

File View Options Filters Search Help

Screen Name: ip\_trfc.dat  
 Description: IP Traffic Information  
 Snmp Agent : 192.32.156.65  
 Number of Elements: 4

Circuit Name	IP Address	State	Datagrams RCVD	Datagrams XMIT
S31	1.0.0.1	Down	0	0
E24	192.32.156.65	Up	37248589	39398833
O41	192.32.156.129	Up	0	0
E21	192.32.180.43	Up	39370380	34388427

**Figure 4-16. Zeroing All Counters in a Specific Row**

The counters Datagrams RCVD and Datagrams XMIT reset to zero in the selected row. The reset has no effect on the actual, current values of these counter objects in the router MIB.

The Zero Current Row Counters command stores the value of every counter object displayed in the selected row at reset time. Each stored value provides a reference point for counter values displayed in the selected row following the reset. That is, after resetting all counters in a display row

- The Statistics Manager displays only the difference between the counter value at reset time (the last known reference value) and the actual, current (MIB) value of the same counter.
- The counter values in display reflect *the amount of change* incurred beyond the reference values stored at reset time.

## Stopping Statistics Retrieval

To stop the Statistics Manager from collecting any further statistics in the current screen, select View→Stop Retrieval.

## Creating Statistics Filters

You can set a *display filter* or a *retrieval filter* for each Statistics screen you open from the Statistics Manager Launch Facility.

Without filtering, the Statistics Manager polls a router for the values of all MIB objects defined in the currently active Statistics screen. The screen subsequently shows the values of those objects, as determined by the data returned by the router.

A *display filter* is a software mechanism that enables the Statistics Manager to search the entire contents of the currently active Statistics screen and then

- *Show* only those rows that contain an object that in turn contains a string matching in value to the filter string. (This is the display filter's Display option.)
- *Hide* only those rows that contain an object that in turn contains a string matching in value to the filter string. (This is the display filter's No Display option.)

Specifying a longer display filter string narrows the number of match possibilities available from the currently active Statistics screen.

A *retrieval filter* is a software mechanism that enables the Statistics Manager to poll a router for only a subset of specific MIB objects. These objects have Instance IDs that match the full or partial Instance ID you enter in the Retrieval Filter window.

The currently active Statistics screen subsequently displays the values of those objects, as determined by the data returned by the polled router. The Statistics Manager polls only one router in each Statistics window.

The retrieval filtering mechanism for a statistics screen works substantially in the same way as does the retrieval filtering mechanism for the Quick Get Facility. That is, specifying more of the instance ID in the Retrieval Filter window causes the workstation to solicit a smaller number of objects from a router. This, in turn, typically reduces the number of objects displayed in the active Statistics screen.

Using retrieval filters to collect statistics across your network reduces

- The amount of processing overhead performed by your Site Manager workstation and any polled router
- The amount of network bandwidth consumed for the purpose of periodic polling and poll responses

You can use display filters and retrieval filters in various combinations. For example, you could

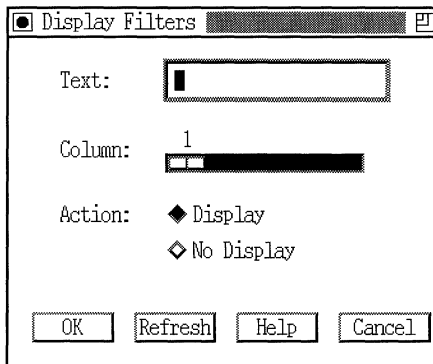
- Use a retrieval filter first to solicit from routers in your network the values of certain MIB objects
- Apply a display filter to hide or show objects in the resulting Statistics screen

## Using Display Filters

To create a display filter, begin from a statistics screen, then

1. Select Filters→Display Filters.

The Display Filters window prompts you to define the filter (Figure 4-17).



**Figure 4-17. Display Filters Window**

2. Enter the text string you want to filter in the Text field.
3. Specify the column where you want the filter to take effect.

Use the slider to select the column that displays the statistics that you want to filter.

In this case, Site Manager displays the statistics for the address mask in column 5. Thus, you use the slider to specify column 5.

4. Select either Display or No Display, depending on the desired action.

If you want the Statistics Manager to display only those statistics that match the filter, select Display. If you want the Statistics Manager to hide those statistics that match the filter, select No Display.

5. Click on OK to save the filter in memory, or click on Refresh to implement the filter immediately.
  - If you click on OK, the filter box disappears. There will be no immediate change to the statistics screen. However, the next time you refresh the statistics screen, it will display only the statistics specified by the filter.
  - If you click on Refresh, the Statistics Manager immediately refreshes the screen and displays only the statistics specified by the filter.
6. Click on OK to exit the Display Filters window.

**Display Filter Example:**

To filter out of the window shown in Figure 4-18 statistics for the circuit that has an address mask value of 255.0.0.0, configure the display filter shown in Figure 4-19.

The screenshot shows a window titled "IP Interface Information" with a menu bar containing "File", "View", "Options", "Search", and "Help". The main content area displays the following text:

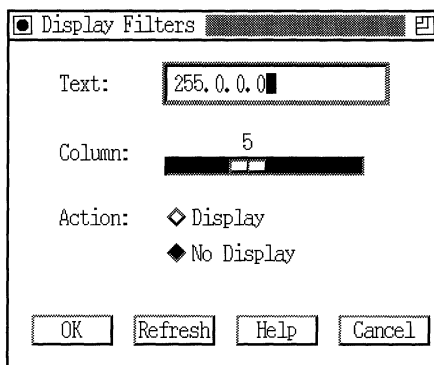
```

Screen Name: ip_main.dat
Description: IP Interface Information
Snmp Agent : 192.32.156.9
    
```

Below the text is a table with the following columns: Circuit Name, IP Address, State, MAC Address, and Address Mask. The table contains two rows of data:

Circuit Name	IP Address	State	MAC Address	Address Mask
E22	1.1.1.1	Down	-	255.0.0.0
E21	192.32.156.9	Up	0x0000A201B8D0	255.255.255.0

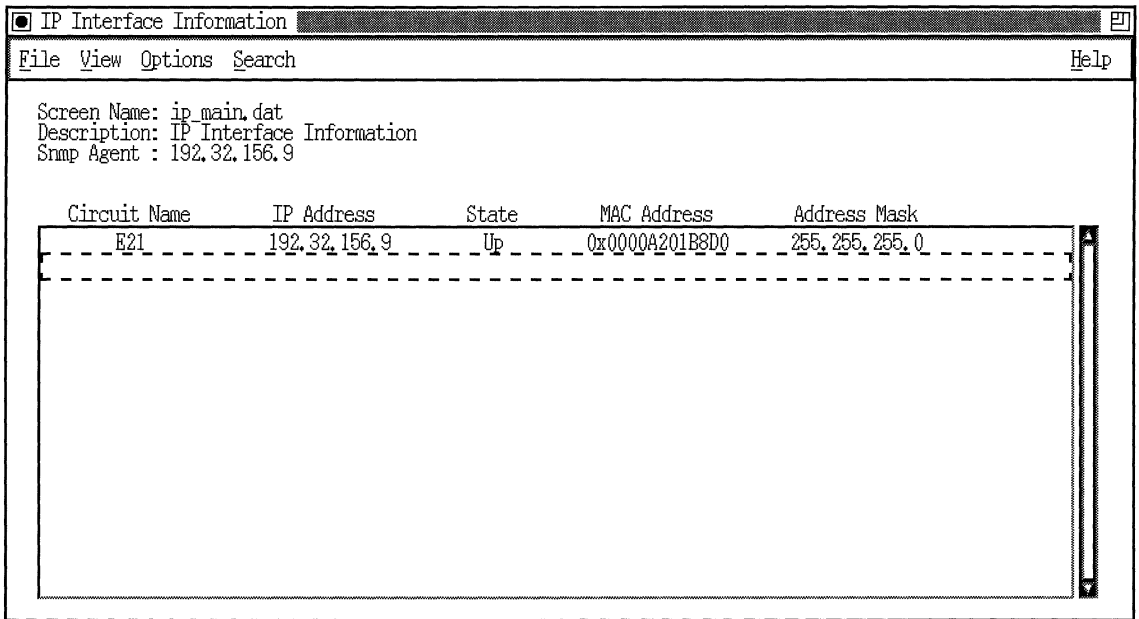
**Figure 4-18. Statistics Window Unfiltered**



**Figure 4-19. Sample Display Filters Window**

When you click on Refresh in the Display Filters window (Figure 4-19), the Statistics Manager filters out of the active statistics window the line with the IP address mask of 255.0.0.0 in column 5.

Figure 4-20 shows the result of applying the display filter to the active Statistics window.



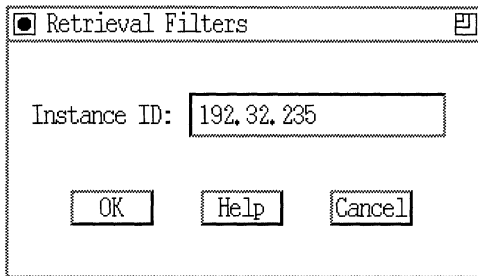
**Figure 4-20. Statistics Screen after Filter Implemented**

## Using Retrieval Filters

To create a retrieval filter, begin from a statistics screen, then

1. Select **Filters**→**Retrieval Filters**.

The Retrieval Filters window appears (Figure 4-21).

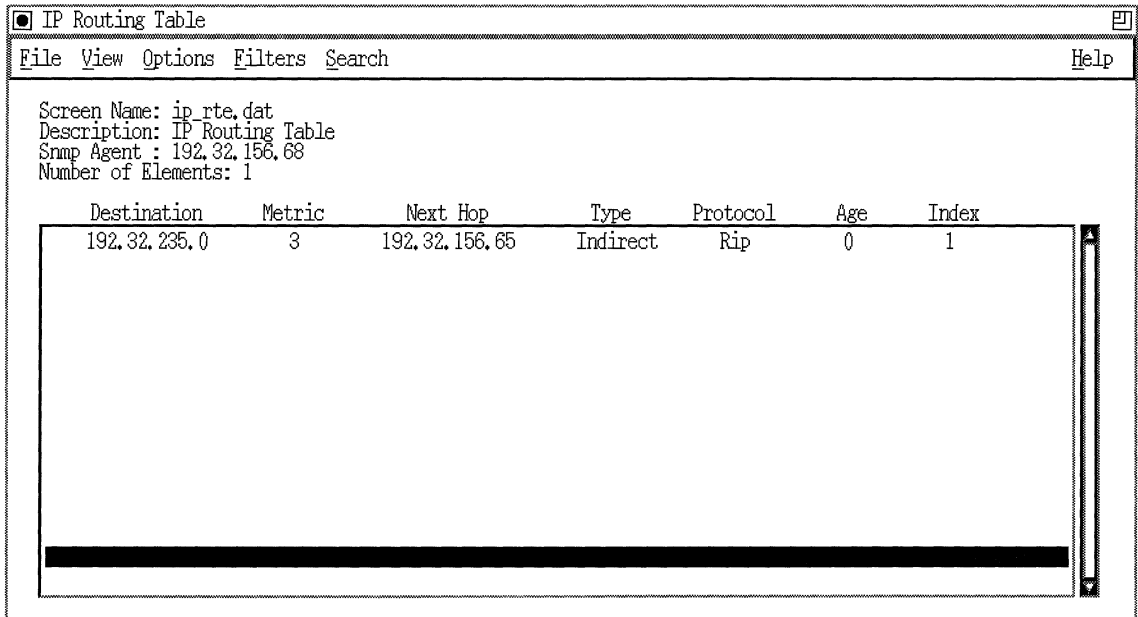


**Figure 4-21. Retrieval Filters Window**

2. Enter the Instance ID of the object(s) you want to view.  
Specifying a partial ID causes the Statistics Manager to poll and display all objects that begin with the same partial ID.
3. Click on OK to save the filter in memory associated with the current statistics screen.
4. Select View→Refresh Display from the statistics screen.

Figure 4-22 shows the result of this retrieval filter. The Statistics Manager retrieves only one MIB object; no other instances of the same object exist in the MIB associated with the currently connected router.





The screenshot shows a window titled "IP Routing Table" with a menu bar containing "File", "View", "Options", "Filters", "Search", and "Help". The window displays the following information:

Screen Name: ip\_rte.dat  
Description: IP Routing Table  
Snmp Agent : 192.32.156.68  
Number of Elements: 1

Destination	Metric	Next Hop	Type	Protocol	Age	Index
192.32.235.0	3	192.32.156.65	Indirect	Rip	0	1

Figure 4-22. Statistics Screen After Implementing a Retrieval Filter

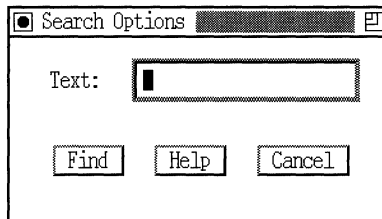
## Searching for Statistics Information

You can search for any text string that appears on a statistics screen.

To define the text string to search for, proceed as follows:

1. Select Search→Find.

The Statistics Manager displays a Search Options window that prompts you to define a text string (Figure 4-23).



**Figure 4-23. Search Options Window**

2. Enter the text you want to search for; then click on Find.

The Statistics Manager highlights the line where the next instance of the text string occurs. Continue clicking on Find in the Search Options window.

**Note:** The Search Options window is case-sensitive.

If you still want to search for the text string you defined, but would rather have the Search Options window disappear, proceed as follows:

1. Click on Cancel in the Search Options window.

The Search Options window disappears.

2. Select Search→Find Next.

The Statistics Manager highlights the line where the next instance of the text string occurs.

## Saving Statistics Information

The Statistics Manager allows you to save the information displayed on a statistics screen to an ASCII file on your Site Manager workstation.

To save the information shown on the statistics screen, proceed as follows:

1. Select **File**→**Save As** from the statistics screen. A file directory box appears, prompting you to select a place to store the data.
2. Select a directory in which to store the data.
3. Select a file in which to store the data. To do so, you can either select an existing file from the file list or type a new name for the file in the **Filename** field.
4. Click on **OK**. Site Manager stores the data in ASCII format.

You can use any text editor to view the data once you store it on your workstation.

## **Building Custom Statistics Screens**

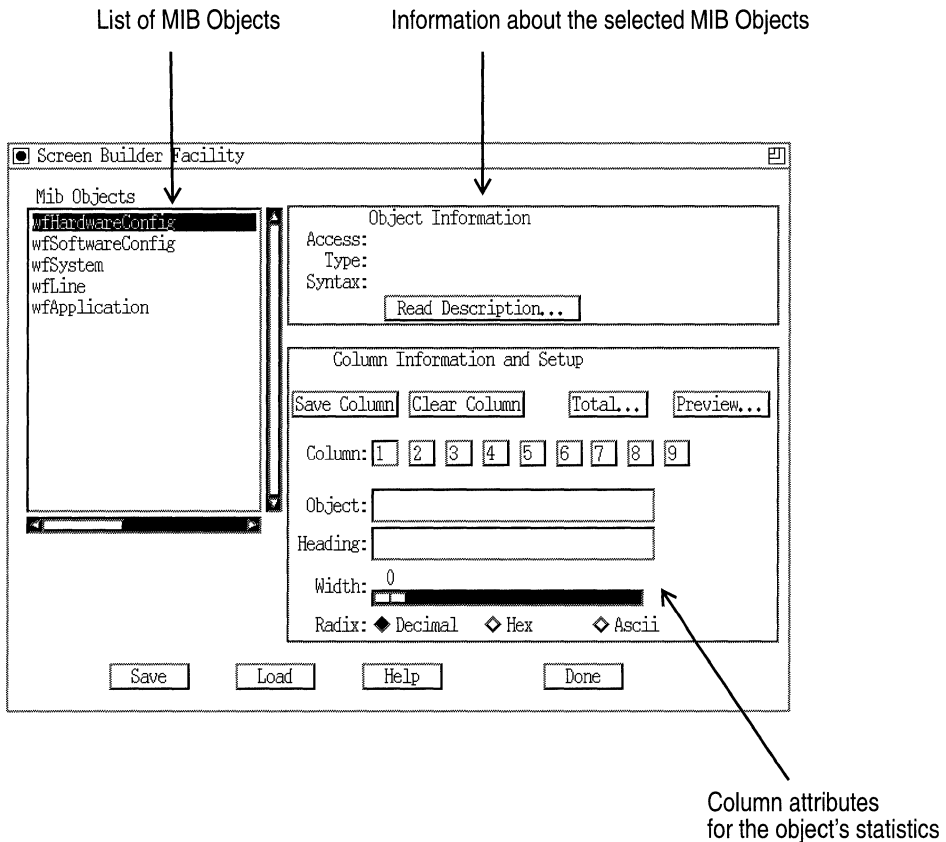
You can build custom statistics screens. You can select up to nine different objects from the Wellfleet MIB and define how the screen displays the statistics you select. After you save the custom statistics screen, it is added to the Screen Manager's user screen list.

### **Designing Statistics Screens**

To design a custom statistics screen, proceed from the Statistics Manager window as follows:

1. Select **Tools**→**Screen Builder**.

The Screen Builder Facility window appears (Figure 4-24).



**Figure 4-24. Screen Builder Facility Window**

The MIB Browser on the left side of the screen lets you scroll through the MIB and select MIB objects to add to the screen. (The section “Using the MIB Browser” explains how to maneuver through the MIB). The Column Information and Setup portion of the screen lets you specify how the statistics for the selected objects appear on the screen.

2. Specify the column you want to define in the screen design by clicking on the corresponding column number button.

For example, to define the first column on the statistics screen, click on the “1” button.

3. Scroll through the MIB tree and select the MIB object that you want to list in the column. The Object field in the Column Information and Setup portion of the screen displays the MIB object you select.
4. Select the Heading field and enter a name that describes the type of statistics that the Statistics Manager will collect and display in that column. For example, if you select the object *wfIPInterfaceAddr*, you could name the column “IP Address.”
5. Specify the column Width. Click on the sidebar and move it back and forth until the Screen Builder displays the appropriate column width.

The width displays in character units. The width you specify here must be greater than 0 and greater than or equal to the column heading width. Any data that exceeds the specified column width will cause the rest of the data on the same line to shift to the right.

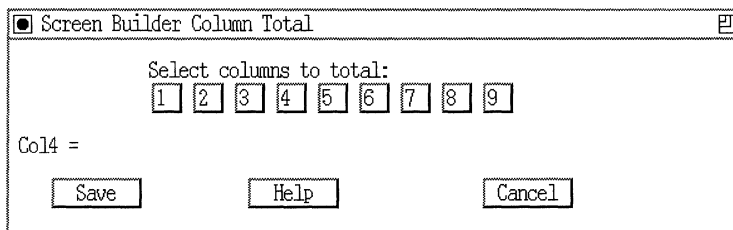
As a rule of thumb, allow at least the following widths:

IP addresses	18 units (15 for the address, plus 3 spaces)
MAC addresses	16 units (14 for the address, plus 2 spaces)
Circuit Names/ Numbers	18 units

6. Specify whether the Statistics Manager displays statistics in decimal, hexadecimal, or ASCII format by clicking on the corresponding button in the Radix field. (You may find the ASCII radix useful for displaying NetBIOS Names.)
7. Click on Save Column to save the column attribute information. The Screen Builder displays an asterisk in the column button for the column you just saved.
8. Repeat steps 1 to 7 to add other objects to the statistics screen.

9. To generate a sum of the values in two or more columns, follow these steps:
  - a. Click on the number of the column in which you want to display the sum.
  - b. Click on Total.

The Screen Builder Column Total window appears (Figure 4-25).

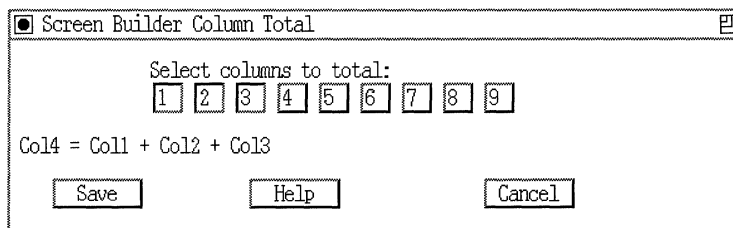


**Figure 4-25. Screen Builder Column Total Window**

- c. Click on each column that will contain values that you want to include in a total.

For example, suppose columns 1, 2, and 3 will contain information about different kinds of dropped packets. You can generate a total of all dropped packets by adding the values in the three columns.

Figure 4-26 shows that column 4 will display the total of the values in columns 1, 2, and 3.

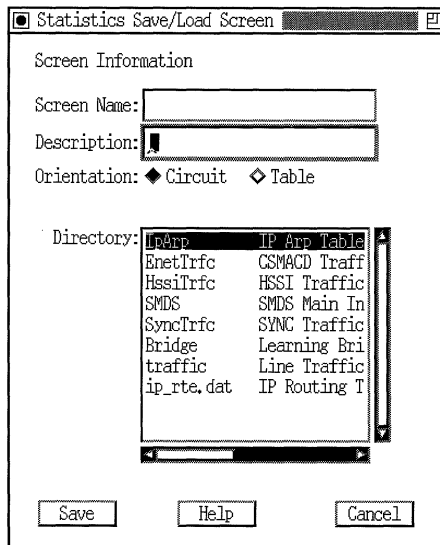


**Figure 4-26. Selecting Columns to Total**

- d. Click on Save. You then return to the Screen Builder Facility window.
  - e. Click on Save Column in the Screen Builder Facility window to save the totals column you just specified.
10. To preview the statistics screen you are building, click on the Preview button.

The statistics screen appears and displays the current column design. Note, however, that the Statistics Manager does not retrieve any statistics from the router.

11. Click on Save once you finish building the screen. The Statistics Save/Load Screen window appears (Figure 4-27). It lists all the custom statistics screen files that you save in the statistics screen directory.



**Figure 4-27. Statistics Save/Load Screen**

12. Complete the Statistics Save/Load Screen as follows:

- a. Enter a new name for the file in the Screen Name field. If you are saving the file to a PC, the name you enter must follow standard DOS format.
- b. Enter a description of the screen in the Description field. The maximum length of the screen description is 40 characters.
- c. Specify the screen mode by selecting either Circuit or Table. Choose Circuit if you want the Statistics Manager to continually update the screen with new statistics. Choose Table if you want the Statistics Manager to gather and display current statistics only once, when you launch the screen.
- d. Click on Save to save the statistics screen to a file.

Depending on whether you are running Site Manager on a UNIX or DOS computer, the Statistics Manager saves all custom screens to one of the custom screen directories listed:

Platform	Custom Screen Directory
UNIX	$\$(HOME)/.wfscrns$
DOS	$\backslash wf \backslash wfscrns$

## Displaying Custom Statistics Screens

To view a statistics screen you created, complete the following steps:

1. Add the screen to the current screen list. See “Defining the Current Screen List” for instructions.
2. Launch the screen. See “Displaying Statistics Screens” for instructions.

You can also view the text version of the statistics screen file using any text editor.



## Editing Custom Statistics Screens

You can load a statistics screen that you previously built and edit the screen. This is a two-step procedure.

**Note:** The default screens are write-protected, so you cannot edit them. To customize a default screen, simply use the operating system to copy it to the custom screen directory on your Site Manager workstation under a new name. Then load and edit it as described in this section.

### Retrieving a Statistics Screen File

Before you can edit a statistics screen file, you must load (retrieve) it from your Site Manager workstation.

To retrieve a statistics screen file, begin at the Statistics Manager screen and proceed as follows:

1. Select **Tools**→**Screen Builder**. The Screen Builder window appears.
2. Click on **Load**. The Statistics Save/Load Screen appears.
3. Highlight the statistics screen file you want to edit. Once you select a statistics screen file, the Screen Information fields reflect the screen name and type of data it collects.
4. Click on **Load** to load the screen's column attributes into the Screen Builder.

The Column Information and Setup portion of the Screen Builder window now reflects the statistics screen you retrieved, beginning with the first column defined.

## Editing a Statistics Screen File

After you retrieve the statistics screen, use the Screen Builder to edit the screen.

To edit the screen columns, follow these steps:

1. Select the number box corresponding to the column you want to edit.

When you select the column number, the Object, Heading, Width, and Radix fields are filled in with the current column information. If the column is currently undefined, these fields remain blank.

To remove all of the current column information, click on the Clear Column button.

2. Select and edit any of the column attributes you want to change as follows:
  - If you want the column to contain statistics about a different object, highlight a new object from the MIB Browser.
  - To change the column size, use the sliderbar to increase or decrease the current size.
  - To change the column heading, type a new heading.
  - To display the integer in a different format, change the Radix setting.

The section “Designing Statistics Screens” describes how to set each of the column’s attributes.

3. Click on Save Column to implement your changes.
4. Repeat this procedure to edit additional columns.

**Note:** To display the statistics screen and see the results of your edits, click on Preview.

5. Click on Save to save your changes to the screen. The Statistics Save/Load Screen appears. You can either save this modified window to an existing file or save it under a new name as follows:
  - To save the screen to an existing file, select the file from the list by highlighting it. Then click on Save. Click on OK to allow the Statistics Manager to overwrite the file.
  - To save the screen under a new name, enter the name of the file in the Screen Name field. Describe the file in the Description field, and specify whether the screen mode is Circuit or Table. Then click on Save.

If you save the statistics window under a new name, you must do the following to view this screen:

1. Add the window to the current screen list. See “Defining the Current Screen List” for instructions.
2. Launch the screen. See “Displaying Statistics Screens” for instructions.

## For More Information

For information about MIB standards, see the following references:

*Structure and Identification of Management Information for TCP/IP-based Internets* (SMI; RFC 1155).

*Information Processing Systems - Open Systems Interconnection Specification of Abstract Syntax Notation One* (ISO 8824).

---

# Chapter 5

## Using the Router Files Manager

For general information about using the Router Files Manager, see “Managing Router Files” in Chapter 1. For specific information about using buttons, windows, and other Site Manager features, refer to *Using Site Manager Software*.

Use the Router Files Manager to do the following:

- Display the contents of a router’s volume
- Connect to a router
- Name files
- Copy files
- Delete files
- Transfer files
- Back up files
- Modify a *config* file in remote configuration mode
- Compact file space on a memory card or flash SIMM
- Format a memory card or flash SIMM
- Partition media on Wellfleet routers

## Displaying the Contents of a Volume

To display files stored on a volume inside the router, begin at the Wellfleet Site Manager window and select Tools→Router Files Manager. The Router Files Manager window appears, showing the files in the active volume (Figure 5-1).

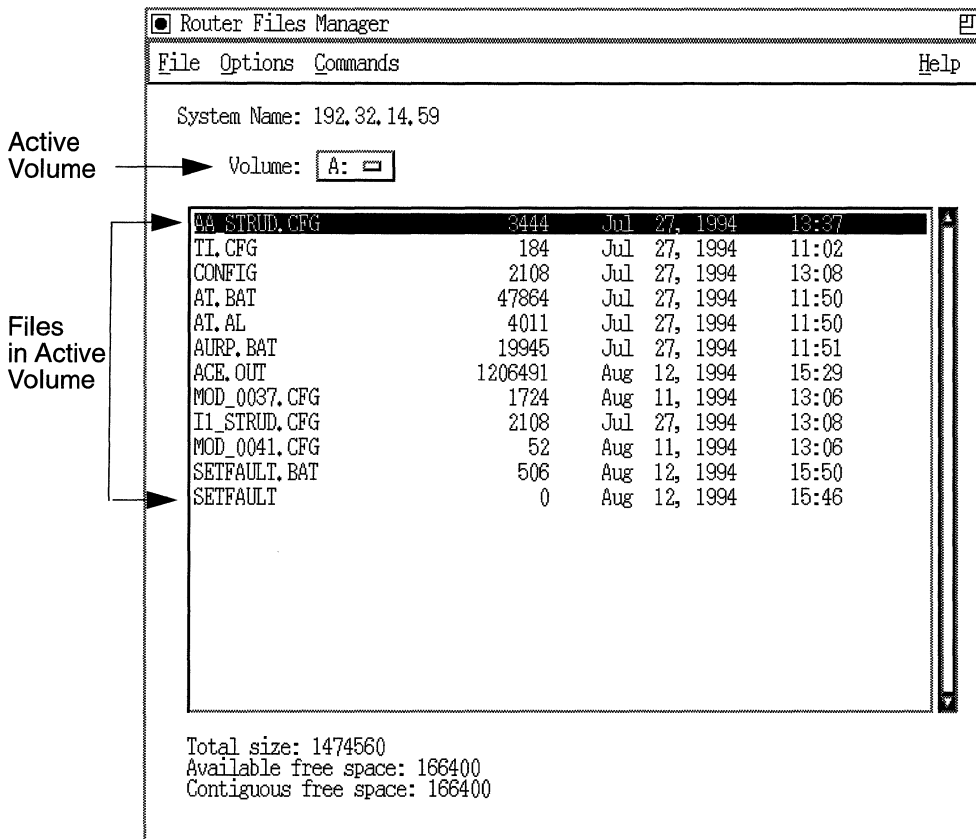


Figure 5-1. Router Files Manager Window

## Active Volumes

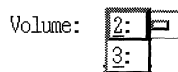
In the Router Files Manager window, the active volume is represented by a number or letter, depending on the type of media the router uses.

Media	Active Volume	Description
Memory Card or Memory Module	1 through 14*	If the router uses a memory card or a memory module, the active volume can be from 1 through 14, depending on the router platform.
Diskette	A	If the router uses a diskette, the active volume shown is A.

\*This number comes from the number of the slot hosting the first available memory card. Additional memory cards in the router are optional; they provide redundancy and additional storage.

In addition, if the router is an Access Node (AN) or Access Stack Node (ASN), and the media is partitioned, the active volume is represented by a number (for the slot) and a letter (for the volume). For example, 1a refers to volume a (the primary volume) on slot 1, and 1b refers to volume b (the secondary volume) on the same media in slot 1. For more information, see “Partitioning Media on Wellfleet Routers” later in this chapter.

To change the volume displayed, select the Volume box. The Volume box lists all available volumes on the router, as shown below. Select the volume you want.



## Available and Contiguous Free Space

The fields at the bottom of the Router Files Manager window show the amount of free space in a selected volume. The fields are as follows:

Total size	Total number of bytes (used and unused) on the volume
Available free space	Number of unused bytes on the volume
Contiguous free space	Number of unused bytes in the largest block available on the volume

## Default Filenames

Table 5-1 lists the default router filenames.

**Table 5-1. Default Router Filenames**

Filename	Description	Notes
<i>ace.out</i>	Bootable image for the FN, LN, ALN, AFN with diskette, and CN	The system automatically references this binary file for booting instructions, unless you specify another bootable image. You cannot read or change this file. It must have the correct filename for the system to boot successfully after a cold-start. The Administration→Boot Router option does, however, let you specify another software image.
<i>afn.exe</i>	Bootable image for the AFN with flash file system	
<i>an.exe</i>	Bootable image for the AN	
<i>asn.exe</i>	Bootable image for the ASN	
<i>bn.exe</i>	Bootable image for the BLN, BCN, and BNX	
<i>asndiag.exe</i>	Copy of the diagnostics image for the ASN	

*continued on the next page*



**Table 5-1. Default Router Filenames** *(continued)*

Filename	Description	Notes
<i>config</i>	Default configuration file	The system references this binary file for configuration data when booting. (However, you can specify another configuration file with the Boot Router option.) You can change the configuration by copying an alternate configuration file to <i>config</i> . Also, you can store alternate or future configurations. This file must have the <i>config</i> filename for the system to configure automatically after booting. We recommend that you back up the <i>config</i> file before overwriting it.
<i>debug.al</i>	ASCII file containing aliases	Aliases are commands that abbreviate long or multiple commands. They are used to debug common network problems.
<i>frediag.exe</i>	Copy of the diagnostics image resident on the diagnostics PROM for the BCN and BLN	You cannot read or change this file.
<i>freboot.exe</i>	Copy of the bootstrap image resident on the bootstrap PROM for the BCN and BLN	You cannot read or change this file.

*continued on the next page*

**Table 5-1. Default Router Filenames** *(continued)*

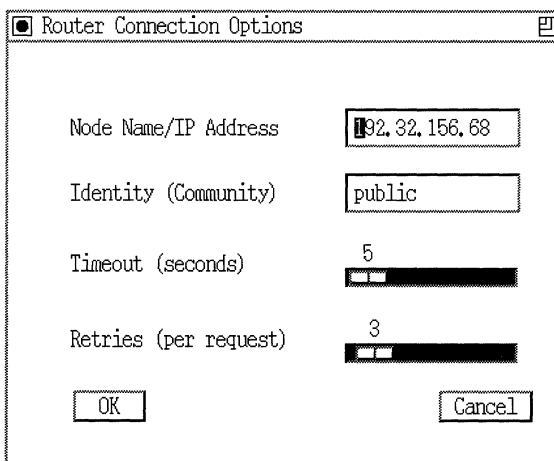
Filename	Description	Notes
<i>install.bat</i>	Script containing TI commands	You use the Wellfleet Technician Interface commands during the initial startup.
<i>ti.cfg</i>	Configuration file containing the MIB variables associated with the default TI console operating parameters	This file contains the minimal configuration necessary to operate the router. You boot with this file when updating a PROM. You may also want to boot with this file when copying a volume to provide full use of all system buffers. This file is stored in binary format.

## Connecting to a Router

To connect to a router using the Router Files Manager

1. Select Options→Router Connection from the Router Files Manager window.

The Router Connection Options window appears (Figure 5-2).



**Figure 5-2. Router Connection Options Window**

2. Enter an IP address in the Node Name/IP Address field, then click on OK.

The Router Files Manager connects you to the specified router. The IP address of that router appears in the Router Files Manager window.

## Naming a File

Before you go on to the next section, you need to know the rules for naming files.

- ❑ Filenames must start with an alphabetical character. The remaining characters must be alphanumeric and may also include the underscore (`_`) character.
- ❑ Filenames can consist of 1 to 8 characters. Note that configuration filenames can consist of 1 to 15 characters (including a period). However, we recommend that you limit filenames to 8 characters to ensure that all operating systems that we support can recognize the names.
- ❑ Filename extensions are optional and must be preceded by a filename and a dot. They can be from 1 to 3 characters.

Also, we recommend that you use the following conventions when you name files so that you can distinguish files by type.

- ❑ Use the `.exe` filename extension for software images for FRE processor modules and `.out` for ACE processor modules. (See Table 5-1, earlier.)
- ❑ Use the `.cfg` filename extension for alternate configuration files. (The default configuration file is `config`.)
- ❑ Use the `.al` filename extension for alias files.
- ❑ Use the `.log` filename extension for log files.

## Copying a File

You can use the Router Files Manager to copy a file on the router; you can copy the file to a different volume or to the same volume. To copy a file, you do the following:

1. Examine the existing filenames.
2. Verify the existence of adequate free space on the destination volume.
3. Create the copy.

The following sections describe each of these steps.

### Examining the Router Destination Volume

The router automatically overwrites any file that has the same filename as the file you are creating.

To avoid overwriting an existing file, display a list of the volume's contents and determine the filenames that are already in use. For information on how to do this, see "Displaying the Contents of a Volume" earlier in this chapter.

If you are unfamiliar with the file-naming rules and conventions, refer to the earlier section "Naming a File" before you proceed.

### Verifying Adequate Free Space

You must make sure that the router volume has enough space available for the copy. Depending on the Router Software Version you are using, your software might automatically check the available space for you.

To determine your Router Software Version, select Help→Site Manager Version in the Router Files Manager window.

Routers that run 7.80 (or later) software automatically verify the existence of adequate free space on the destination volume specified in a file copy operation.

For routers that use a software version lower than 7.80, you must

- ❑ Determine from the Router Files Manager window the size of the file you want to copy.
- ❑ Determine from the Router Files Manager window the amount of free space available to receive the file copy on the destination volume.
  - For a router diskette destination volume, use the number of bytes displayed for *Available free space*.
  - For a router memory card or flash SIMM (Single Inline Memory Module) destination volume, use the number of bytes displayed for *Contiguous free space*.



**Warning** If the destination volume has an insufficient amount of available free space (or contiguous free space, in the case of a memory card or flash SIMM volume), the router copies only part of your source file.

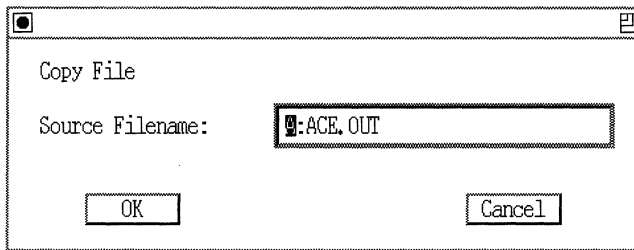
## Creating the Copy

Copy a file as follows:

1. In the Router Files Manager window, select the file you want to copy.

If you select a file that you decide not to copy, click on the file again to deselect it.

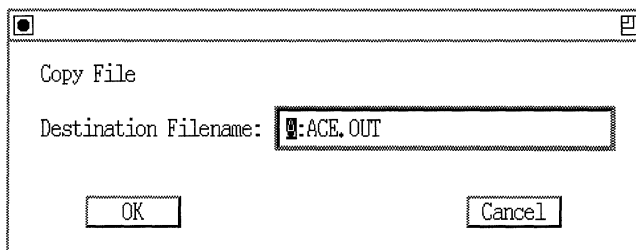
2. Select **Commands**→**Copy**. The Router Files Manager displays the source filename in a window (Figure 5-3).



**Figure 5-3. Copy File Window for Source Filename**

3. Click on OK.

A window prompts you for the destination filename (Figure 5-4).



**Figure 5-4. Copy File Window for Destination Filename**

4. Using the following format, overwrite the entry in the Destination Filename field with the volume and filename you want to give this file.

*<volume>:<filename>*

**Note:** If you are copying a file from diskette to memory card, enter the destination filename in lowercase letters only.

5. Click on OK. A confirmation window appears.
6. Click on OK.

The router copies the source file to the filename and volume you specified.



**Warning** Copying a file to a memory card “volume” that has an insufficient amount of contiguous free space results in a corrupted copy of the original source file. You must delete the corrupted file.

Before you again attempt to copy the same or any other source file(s) to the same volume, you must compact the volume. See “Compacting File Space on a Memory Card or Flash SIMM” later in this chapter.

## Deleting a File

You can delete one or more files at a time from a volume.



**Warning** You cannot recover a file after it is deleted.

To delete one or more files, follow these steps:

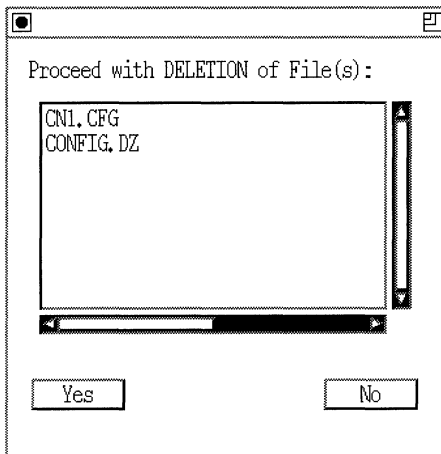
1. In the Router Files Manager window, select each file that you want to delete.

To select multiple files, just click on each file you want.

If you select a file that you decide not to delete, click on the file again to deselect it.

2. Select **Commands**→**Delete**.

A window prompts you to confirm your delete request (Figure 5-5).



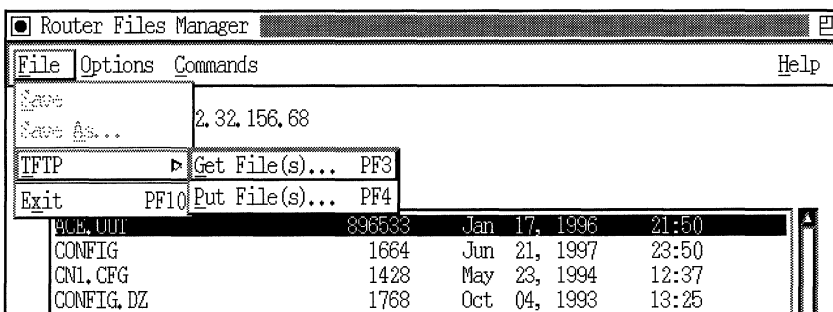
**Figure 5-5. Deleting Router Files**

3. Click on Yes.

The router deletes the files you specified from the volume displayed.

## Transferring a File

The Router Files Manager allows you to transfer files between any router and Site Manager workstation by selecting **File**→**TFTP** (Figure 5-6).



**Figure 5-6. Selecting the TFTP Option**



This option invokes the TFTP (Trivial File Transfer Protocol) software to execute file transfers.

**Note:** To transfer files to or from a router that uses a diskette-based file system, you must set the TFTP Retry Time Out parameter to 10 seconds. If you do not make this adjustment, duplicate transfer sessions may occur. This, in turn, may result in zero length or locked files on the diskette. (For more information on how to set the TFTP Retry Time Out parameter, refer to *Customizing IP Services*.)

You can choose TFTP→Put File(s) to transfer one or more files to several routers at the same time. For example, you might want to transfer a new *boot.exe* file to three different routers. Rather than performing the transfer three times (once for each router), you can transfer the file to all three routers at once.

To transfer files to multiple routers simultaneously, you must use the Router Files Manager to set up those routers. The next section describes how to do this.

If you want to transfer files to only one router, the Router Files Manager uses the Node Name/IP Address that you specified in the Router Connection Options window to determine the router to which you put files. For more information, see the section “Putting a File,” later in this chapter.

You can choose TFTP→Get File(s) to get one or more files from a router. Unlike the Put File(s) option, which lets you transfer files to several routers at the same time, you can get files from only one router at a time. Again, the Router Files Manager uses the Node Name/IP Address from the Router Connection Options window to determine the router from which you get files. For more information, see the section “Getting a File” later in this chapter.

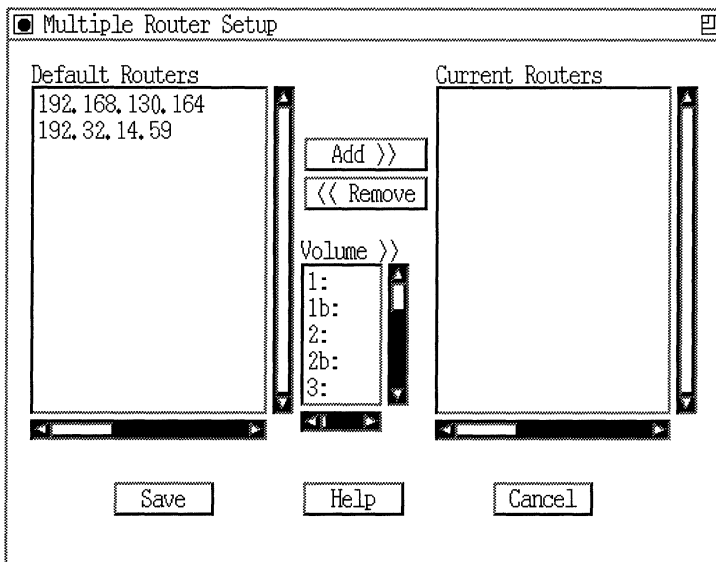
**Note:** We recommend that you ping the router before you transfer a file, if you are running IP in host-only mode and you have

configured the router with the same IP address on multiple physical interfaces.

## Setting Up Multiple Routers

To set up several routers so that you can put the same files on those routers at one time, follow these steps:

1. Select Options→Router Connection and complete the Router Connection Options window for each router to which you want to transfer the files.
2. Select Options→ Multiple Router Setup. The Multiple Router Setup window appears (Figure 5-7).

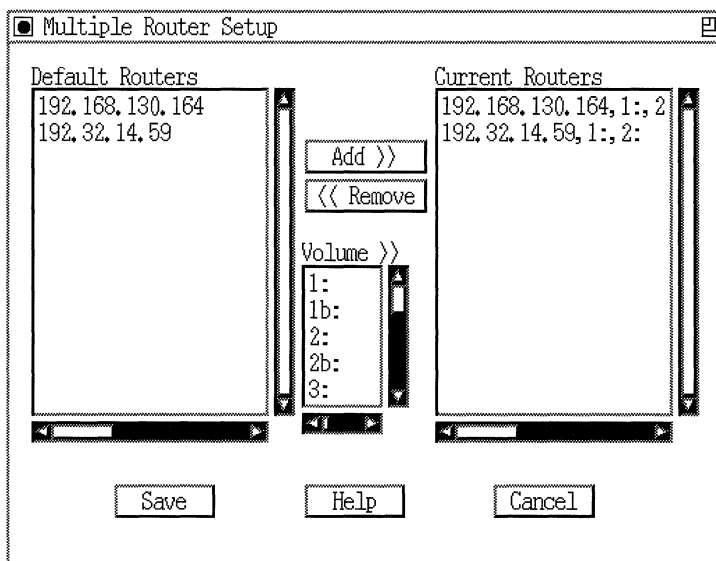


**Figure 5-7. Multiple Router Setup Window**

The Default Routers window lists the routers to which you are currently connected. The Current Routers window lists the routers whose files you want to manage simultaneously. The Volume window lists all of the volume identifiers for Wellfleet routers.

3. To transfer files to the same volume(s) on several different routers, follow these steps:
  - a. In the Default Routers list, click on each router to which you want to transfer the same files at the same time.
  - b. In the Volume list, click on each volume where you want to put files.
  - c. Click on Add.

The selected routers and volumes appear in the Current Routers list (Figure 5-8).



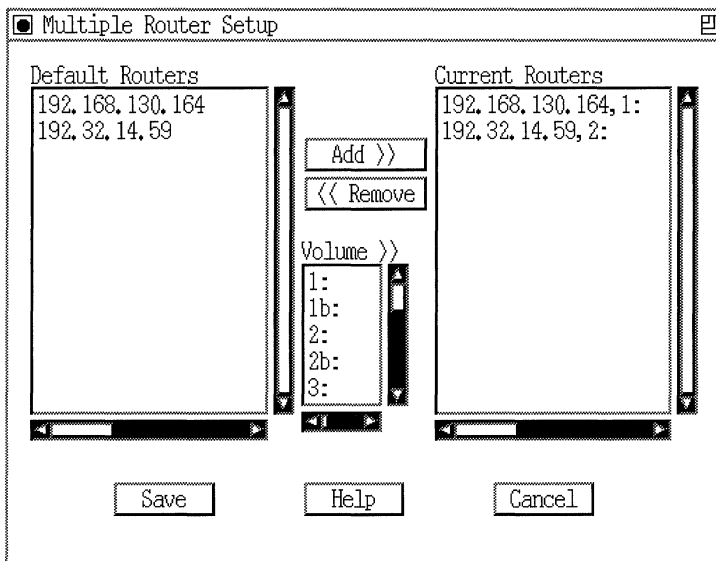
**Figure 5-8. Adding Routers to the Current Routers List**

Using the multiple router setup in Figure 5-8, you can transfer the same files to volumes 1 and 2 on the routers in the Current Routers list.

To transfer files to different volume(s) on several different routers, follow these steps:

- a. In the Default Routers list, click on the router to which you want to transfer files.
- b. In the Volume list, click on the volume(s) where you want to put files on the router you just selected.
- c. Click on Add.
- d. Repeat Steps a through c for each router to which you want to transfer the same files.

The selected routers and volumes appear in the Current Routers list (Figure 5-9).



**Figure 5-9. Adding Routers to the Current Routers List**

Using the multiple router setup in Figure 5-9, you can transfer the same files to volume 1 on the first router in the Current Routers list, and to volume 2 on the second router in the list.

If you inadvertently add a router and volume to the Current Routers list, you can remove it from that list. To do so, select the router (in the Current Routers list) and click on Remove.

4. Click on Save.

You can now proceed to “Putting a File” for information on putting files on the routers.

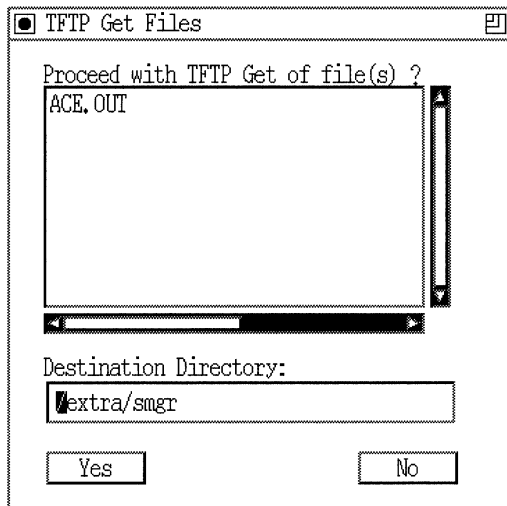
## Getting a File

The Get File option allows you to transfer one or more files from the router to the Site Manager workstation.

To transfer files from the router to the Site Manager workstation, begin at the Router Files Manager window and proceed as follows:

1. Select the Options→Router Connection option from the Router File Manager window.
2. Enter the IP address of the router that has the files you want to transfer, then click on OK.
3. Select the router volume from which you need to transfer a file. The Router Files Manager lists the files on that volume.
4. Select the files you want to transfer from the router to the Site Manager workstation.
5. Select File→TFTP→Get File(s).

The TFTP Get Files window appears (Figure 5-10).



**Figure 5-10. TFTP Get File Window**

In this example, you are transferring one file from the router to the Site Manager workstation.

6. In the Destination Directory field, enter the name of the directory on your Site Manager workstation where you want to store the file.
7. Click on Yes to proceed.

The Router Files Manager transfers the files to the Site Manager workstation.

If a file with the same name already exists in the destination directory on the Site Manager workstation, the file you are “getting” replaces it.

## Putting a File

The Put File option lets you transfer files from the Site Manager workstation to one or more routers. To transfer a file from the Site Manager workstation to a router, you must do the following:

1. Choose the router(s) to which you want to transfer the files.

2. Examine the existing filenames on the router destination volume.
3. Verify the existence of adequate free space on the destination volume.
4. Transfer the files to the destination volume.

The following sections describe each of these steps.

## Choosing the Routers

To transfer files to more than one router at a time, follow the instructions in the earlier section, “Setting Up Multiple Routers,” to select the routers you want.

To transfer files to only one router, follow these steps from the Router Files Manager window:

1. Select the Options→Router Connection option from the Router File Manager window.
2. Enter the IP address of the router to which you want to transfer files, then click on OK.

**Note:** We recommend that you ping the router before you attempt to transfer a file if

- ❑ You are running IP in host-only mode on the destination router
- ❑ You have configured the destination router with the same IP address on multiple physical interfaces

## Examining the Router Destination Volume

The router automatically overwrites any file that has the same filename as the file you are transferring from your Site Manager workstation.

To avoid overwriting an existing file on the router destination volume, display a list of the volume's contents and determine the filenames that are already in use. For information on how to do this, see "Displaying the Contents of a Volume" earlier in this chapter.

If you are unfamiliar with the file-naming rules and conventions, refer to the earlier section, "Naming a File," before you proceed.

## Verifying Adequate Free Space on the Destination Volume

You must make sure that the router destination volume has enough space available for the files you transfer. Depending on the Router Software Version you are using, your software might automatically check the available space for you.

To determine your Router Software Version, select Help in the Router Files Manager window.

Routers that run 7.80 (or later) software automatically verify the existence of adequate free space on the destination volume specified in a TFTP Put operation.

For routers that use a software version lower than 7.80, you must

- Determine from the Router File Manager window the size of the file you want to transfer to the router via TFTP.
- Determine from the Router File Manager window the amount of free space available to receive file copy on the destination volume.
  - For a router diskette destination volume, use the number of bytes displayed for `Available free space`.
  - For a router memory card or flash SIMM destination volume, use the number of bytes displayed for `Contiguous free space`.



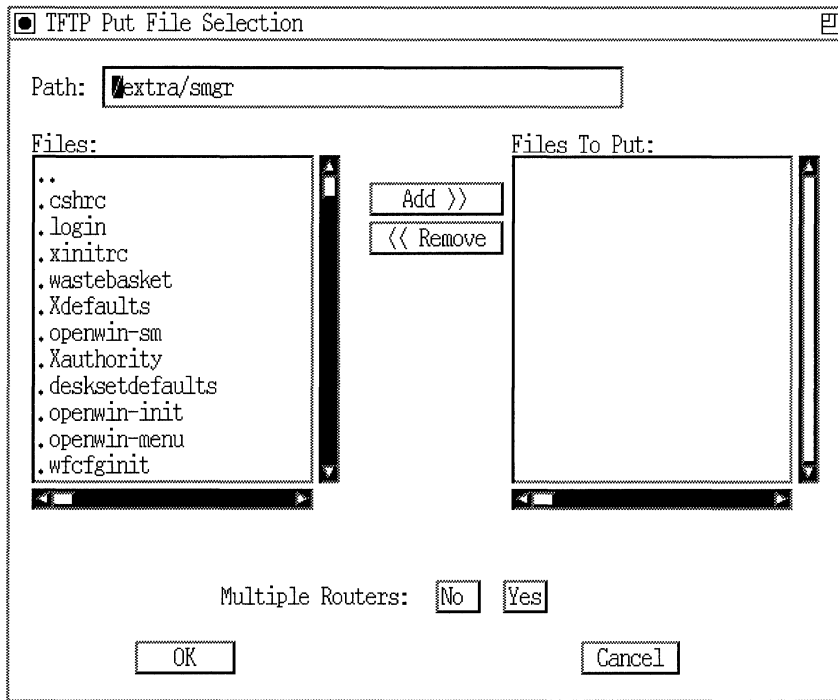
**Caution:** The destination volume may reside on a router that is running a version of the Series 7 software older than 7.80 (for example, 7.60). In this case, if the destination volume does not have enough free space (or contiguous free space, for a memory card volume), the router accepts only a partial (corrupted) copy of your source file.

If you inadvertently transfer a file to a memory card volume that cannot accommodate your entire source file, delete the corrupted file copy from the destination volume. (See “Deleting a File” earlier in this chapter.) Before you transfer the same or any other source file(s) to the same volume, compact the contents of that volume. (See “Compacting File Space on a Memory Card or Flash SIMM” later in this chapter.)

## Transferring Files to the Destination Volume

To transfer files from the Site Manager workstation to one or more routers, follow these steps from the Router Files Manager window:

1. Select File→TFTP→Put File(s). The TFTP Put File Selection window appears (Figure 5-11).



**Figure 5-11. TFTP Put File Selection Window**

2. In the Path box, enter the pathname of the directory on the Site Manager workstation that contains the files you want to transfer.  
The files in that directory appear in the Files window.
3. In the Files window, click on each file that you want to transfer to the router. Then click on Add. The selected files appear in the Files to Put window.  
If you inadvertently add files that you do not want to transfer to the router, select those files in the Files to Put window. Then click on Remove.
4. Repeat steps 2 and 3 to select files from other directories that you want to transfer to the router.

5. If you select multiple routers (see “Choosing the Routers” earlier), and you want to transfer the files to all of the routers you selected, click on Yes in the Multiple Routers field.

If you select only one router, or if you do not want to transfer the files to all of the routers you set up in the Multiple Router Setup window, click on No in the Multiple Routers field. In this case, if you previously set up multiple routers, the Router Files Manager transfers the selected files only to the router to which you are currently connected.

6. Click on OK.

During the file transfer operation, the Router Files Manager displays the address of the router that is receiving the files. When the transfer (to each of the routers) is complete, the TFTP Put File Selection window closes and you return to the Router Files Manager window.

## Backing Up Router Software Files to a Host Computer

We recommend that you use TFTP to back up the contents of each memory card or flash SIMM to a host computer on your network. After you back up all files, you can remove the files *freboot.exe* and *frediag.exe*. These files are not required on the router’s memory card, flash SIMM, or diskette and are distributed only as backups for the EEPROMs.

## Modifying *config* Files in Remote Configuration Mode

Use this procedure when you use the Configuration Manager remote mode to modify a *config* file.

1. Compact the contents of the memory card or flash SIMM if your router is equipped with one. (See the next section, “Compacting File Space on a Memory Card or Flash SIMM.”)
2. Copy the *config* file to a new file named *temp*. (See “Copying a File” earlier in this chapter.)

3. Modify *temp*, using the Configuration Manager remote mode. (Refer to the appropriate Bay Networks manual for customizing the type of router software you use.)
4. Save *temp*. When you save in remote mode, Site Manager automatically copies the file to the router.
5. To test your modifications, boot the router with the file *temp*. (Refer to “Booting a Router” in Chapter 7.)
6. Check the MIB version in the Site Manager main window. If the version is lower than 7.80, verify that
  - Adequate free space exists on the router’s diskette to copy *temp* to another file
  - Adequate contiguous free space exists on the router’s memory card or flash SIMM to copy *temp* to another file

**Note:** Routers that run 7.80 (or later) software automatically verify the existence of adequate free space on the destination volume specified in a file copy operation.

7. Copy the file *temp* to *config*.
8. Boot the router with *config*.
9. Delete *temp*.

## Compacting File Space on a Memory Card or Flash SIMM

**Note:** References to memory cards in this section also apply to flash SIMMs (Single Inline Memory Modules).

When you delete a file on a memory card, the file becomes inaccessible, but the data remains on the memory card.

Eventually all space is used. The Compact option copies the active files from the memory card to the router's memory, erases the memory card, and copies the files back to the memory card.

This procedure gives you more file space, provided that you have more available free space than contiguous free space (For more information, refer to "Available and Contiguous Free Space" earlier in this chapter).

**Caution:** We recommend that you back up the files by copying them to a second memory card before you use the Compact option.

To compact the files on a memory card, begin at the Router Files Manager window and proceed as follows:

1. Select the volume that contains the memory card you want to format.
2. Select Commands→Compact.  
A confirmation window appears.
3. Click on OK.

While the operation is in progress, a display of the percentage of the operation that has been completed appears next the Volume field in the Router Files Manager window. The router is unavailable for any other file system requests until it completes the compact procedure.

**Note:** Upon completion of the compacting operation, the Router Files Manager automatically displays the list of files stored in the

memory card. If you issue a file system request before the router finishes compacting all files on the designated volume, the message `Last command failed` appears. (The router did not successfully complete the command.)



**Warning** During the compacting operation, if the slot that contains the memory card resets, runs diagnostics, or loses power, the memory card loses all its data and can become corrupted.

## Formatting a Memory Card or Flash SIMM

**Note:** References to memory cards in this section also apply to flash SIMMs (Single Inline Memory Modules).

The Format option allows you to format and initialize a memory card. Use the Format option to format new memory cards, if you did not obtain them from Bay Networks.



**Warning** You cannot recover files from a memory card after you use the Format option. We recommend that you copy them to a second memory card before you use the Format option.

To format a volume, begin at the Router Files Manager window and proceed as follows:

1. Select the volume that contains the memory card you want to format.
2. Select **Commands**→**Format**.  
A confirmation window appears.
3. Click on **OK**. The router formats and initializes the memory card.
4. Display a list of the volume's contents when the format operation is done.

The format process is complete, if the Router Files Manager does not display a list of files.

## Partitioning Media on Wellfleet Routers

Site Manager lets you partition the nonvolatile file system (NVFS) on Wellfleet Access Nodes (ANs) or Access Stack Nodes (ASNs). These routers use a single flash file system; that is, the routers have only one medium where the file system resides. The NVFS for the AN resides on a Single Inline Memory Module (SIMM). The ASN uses a flash memory card. (You can stack ASNs and use more than one flash memory card in the stack to achieve file system redundancy. In this case, partitioning would not be necessary.) If the single flash file system fails, the router has no backup file system from which to boot.

Partitioning the file system divides it into two independent volumes of equal size. You can store default boot images and configuration files on each volume for redundancy. Then, if you are unable to boot the router from the primary file system, Site Manager automatically attempts to boot the router from the secondary (or backup) file system.

For example, suppose the NVFS for your Access Node resides on a 4-MB SIMM. Partitioning the file system creates two 2-MB volumes. The volumes function independently, and you reference them with unique slot and volume identifiers. You could then copy the files from the primary volume to the secondary volume.

**Note:** You can partition file systems on 4-MB media only.

## Creating a Partition

To partition the NVFS on an AN or ASN, follow these steps:

1. In the Router Files Manager window, select the volume you want to partition. Make sure the value for `Contiguous free space` is no more than half of the volume's total size.

To create volumes of equal size, the existing file system cannot be more than half of the total media size. If the file system is too large, you might want to do one or more of the following so that you will be able to create a partition:

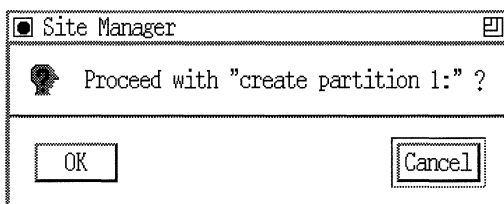
- Format the media, as described in the previous section
  - Delete some files, as described in “Deleting a File” earlier in this chapter
  - Compact the files, as described in “Compacting File Space on a Memory Card or Flash SIMM” earlier in this chapter
2. If you want to partition the file system on an ASN, make sure that the flash memory card is not write-protected. (By default, we ship memory cards unprotected.)

See *Installing and Maintaining ASN Routers* for information on setting the Read/Write switch on the flash memory card.



3. Select Commands→Create Partition

A window appears prompting you to confirm your decision to partition the media (Figure 5-12).



**Figure 5-12. Create Partition Confirmation Window**

4. Click on OK in the confirmation window.

Site Manager displays the following message beside the volume box in the Router Files Manager window:

```
CREATING media partition. Please wait...
```

When the process is complete, the following message appears:

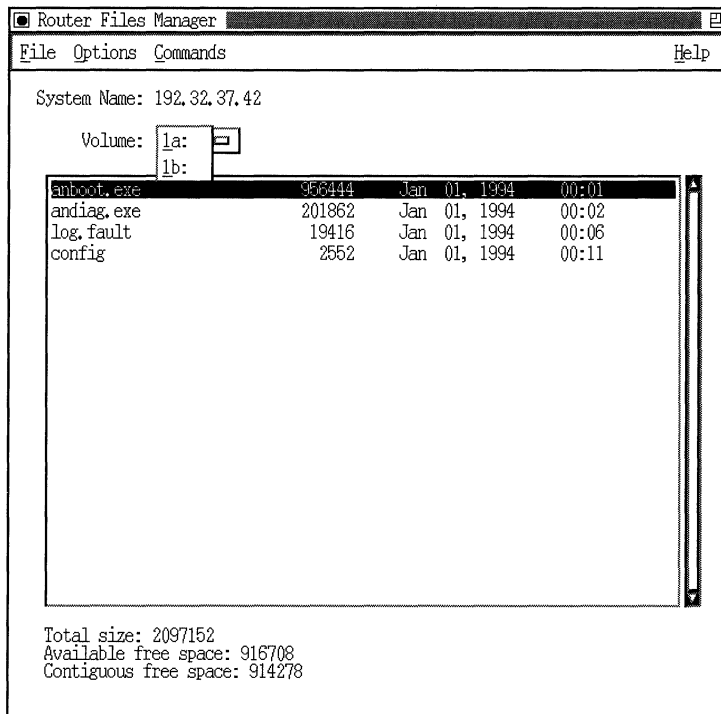
```
Media partition created. Issuing DIRECTORY command.
```

The partitions function as independent flash media. Site Manager uses the following format to identify the partitions:

*<slot><volume>*:

where *slot* refers to the number of the processor board that contains the partitioned media, and *volume* is *a* for the primary volume and *b* for the secondary volume.

In the AN, the slot is always 1. In an ASN, the slot can be from 1 to 4, depending on the setting of the Slot ID selector. (See *Installing and Maintaining ASN Routers* for information on setting the slot ID.) For example, suppose you partition an AN's file system. Site Manager refers to the primary volume as 1a and the secondary as 1b (Figure 5-13).



**Figure 5-13. Volume Identifiers for Partitioned Media**

To manage the files on a partitioned volume, you can use any of the commands that you would normally use to manage the files on an unpartitioned volume. For example, you can compact the files on one volume without affecting the files on the other.

You can use Command→Copy to copy the router files to the new volume. See “Copying a File” earlier in this chapter.

**Note:** In partitioning the volume, the router creates a special partition file in the secondary volume. (You will not see the file in the secondary volume’s list of files.) The partition file takes up 98 bytes of space in the secondary volume only.

## Deleting a Partition

If you partitioned the NVFS on your AN or ASN, you can remove the partition to revert to a single flash file system. You might want to do this, for example, if the router software image is larger than half of the total media size.

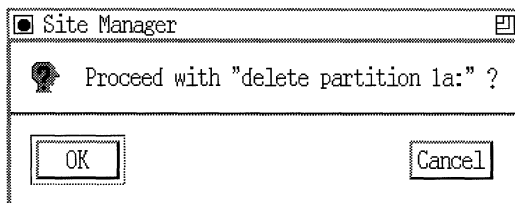


**Warning** Deleting a partition deletes all files from the secondary volume. Files on the primary volume remain intact, and the primary volume then represents the entire size of the medium.

To delete a partition, follow these steps:

1. In the Router Files Manager, click on the volume box and switch to the primary volume.
2. Select **Commands**→**Delete Partition**.

A window appears prompting you to confirm your decision to delete the partition (5-14).



**Figure 5-14. Delete Partition Confirmation Window**

3. Click on **OK** in the confirmation window.

Site Manager displays the following message beside the volume box in the Router Files Manager window:

```
DELETING media partition. Please wait...
```

When the process is complete, the following message appears:

```
Media partition deleted. Issuing DIRECTORY command.
```



---

# Chapter 6

## Using the Report Generator and Audit Trail Feature

For general information about tracking router configuration file changes, see “Monitoring Changes to Router Configuration Files” in Chapter 1. For specific information about using buttons, windows, and other Site Manager features, refer to *Using Site Manager Software*.

You can monitor changes to router configuration files by doing the following:

- Generating configuration file reports
- Maintaining an audit trail log

## Generating Configuration File Reports

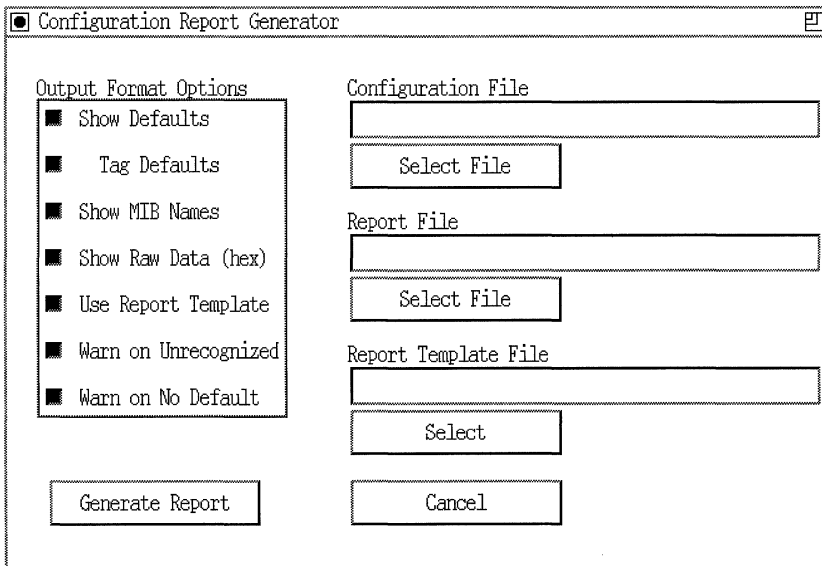
You can generate reports from a router's configuration file from the following:

- Site Manager
- The UNIX command line
- Windows on a PC

The following sections describe each method.

### Generating Reports from Site Manager

To generate a configuration file report from Site Manager, select **Tools**→**Report Generator** from the Site Manager main window. The Configuration Report Generator window appears. Figure 6-1 shows a sample window.



**Figure 6-1. Configuration Report Generator Window**

To complete the Configuration Report Generator Window, follow these steps:

1. Select the Output Format Options that you want to use in the report. To select an option, simply click in its box. Table 6-1 describes each option.

**Table 6-1. Output Format Options**

Option	Description
Show Defaults	Includes the MIB default value for any configurable attribute for which you did not specify a value in the configuration file.
Tag Defaults	Includes the label “[default]” beside any attribute that uses the MIB default value.  If you click on Tag Defaults while Show Defaults is not selected, Site Manager automatically selects Show Defaults as well.
Show MIB Names	Includes MIB attribute identifier names in addition to the ASCII translation of those names.
Show Raw Data (hex)	Includes the raw hex configuration data along with the ASCII translation of that data.  You might want to show the raw data if you intend to use the Technician Interface to enter configuration data. In the Technician Interface, you must enter the data in raw format.

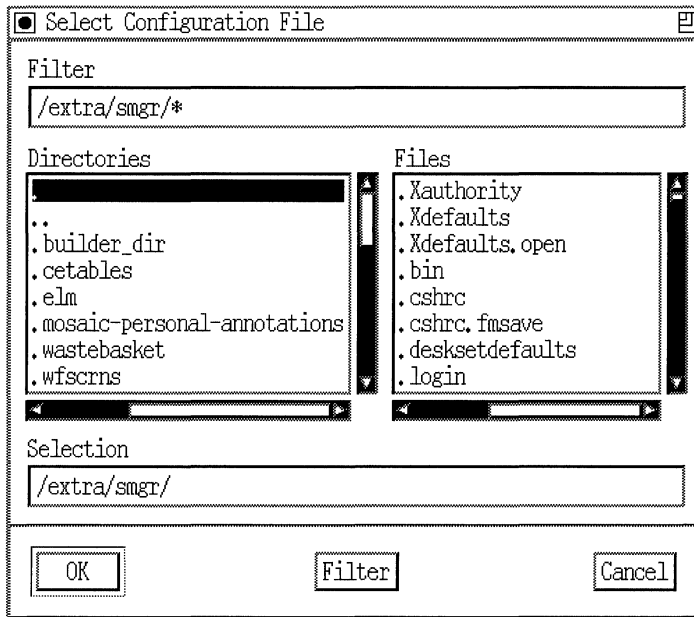
*continued on the next page*



**Table 6-1. Output Format Options** *(continued)*

Option	Description
Use Report Template	<p>Indicates that you want to use a report template other than the default. The default is a version-specific template based on the version of the configuration file. For example, the report generator uses a 7.80 template file to generate a report of a 7.80 configuration file. You might want to use a different report template, for example, a 7.60 template, to generate a report of a 7.80 configuration file.</p> <p>If you select this option, the Report Template File field appears in the window (as Figure 6-1 shows). You must enter a filename in the Report Template File field, as described later.</p>
Warn on Unrecognized	<p>Includes the warning “Unrecognized Attribute” for any attribute that is in the configuration file but is not present in the MIB.</p>
Warn on No default	<p>Includes the warning “NO VALUE, NO DEFAULT” for any attribute for which you did not specify a value in the configuration file and that does not have a MIB default value.</p>

2. Click on the Select File button beneath the Configuration File field. The Select Configuration File Window appears (Figure 6-2).



**Figure 6-2. Select Configuration File Window**

Complete the Select Configuration File window as follows:

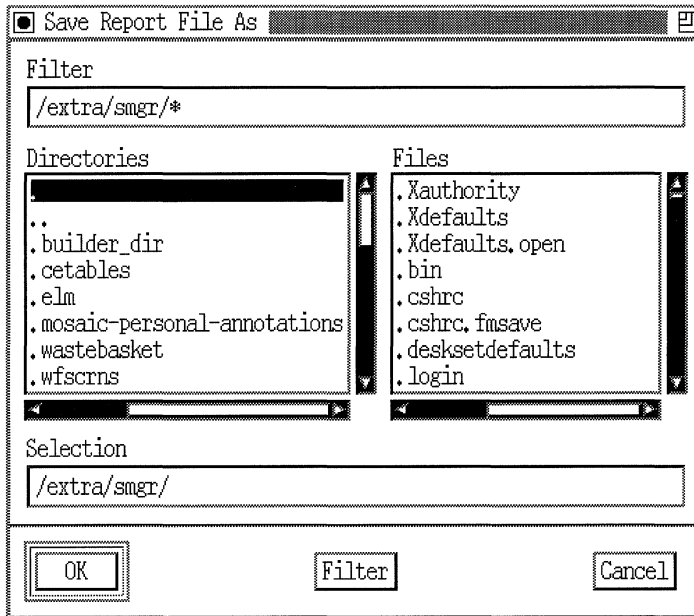
- a. In the Directories window, select the directory path that contains the configuration file from which you want to generate a report.
- b. In the Files window, select the configuration file.  
The path and filename appear in the Selection window.
- c. Click on OK.

You return to the Configuration Report Generator window.

3. Click on the Select File button beneath the Report File field.

**Note:** You can skip this step if you want the Report Generator to send the output to `<stdout>`.

The Save Report File As window appears (Figure 6-3).



**Figure 6-3. Save Report File As Window**

Complete the Save Report File As window as follows:

- a. In the Directories window, select the directory path where you want to store the configuration file report.

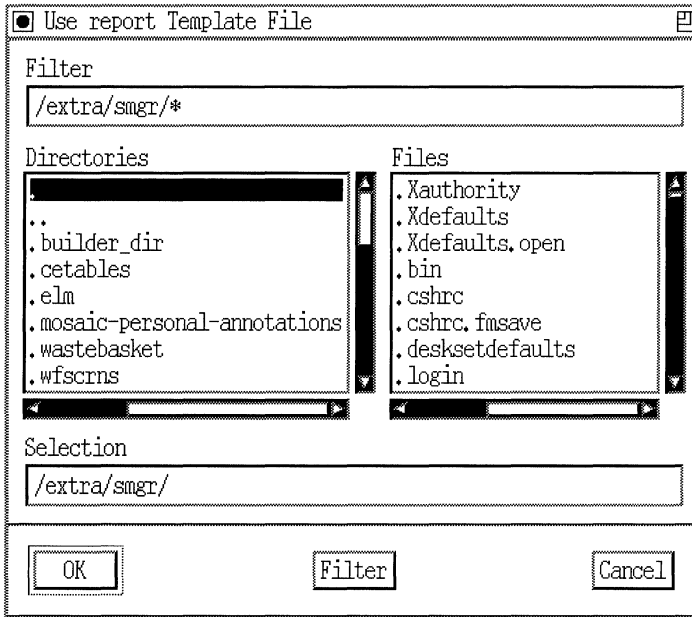
The path appears in the Selection window.

- b. Enter a filename for the report after the path in the Selection window.
- c. Click on OK.

You return to the Configuration Report Generator window.

4. If you select Use Report Template in the list of Output Format Options, the Report Template File field appears in the Configuration Report Generator window. Click on the Select button beneath the Report Template File field.

The Report Template File window appears (Figure 6-4).



**Figure 6-4. Report Template File Window**

Complete the Report Template File window as follows:

- a. In the Directories window, select the directory path that contains the template file you want to use.
- b. In the Files window, select the template file you want.

On UNIX workstations, template files are in */usr/wf/lib*. On PCs, the template files are in *c:\wf\lib*. The format of the template filename is

*<version>.rpt*

For example, the template file for the version 7.80 configuration file is *7\_80.rpt*.

The path and filename appear in the Selection window.

c. Click on OK.

You return to the Configuration Report Generator window.

5. Click on Generate Report.

Site Manager generates the configuration file report and saves the report under the filename you selected. You can then open the report in a text editor.

Figure 6-5 shows part of a report.

```
Console
-----
Report produced by smcfrprt Version (2.00)

date: Wed Aug  3 10:25:46 1994
configuration file: 8.00.cfg
Router Software/MIB Version (8.00)

Hardware Configuration Group (wfHwBase)

    Backplane Id (wfHwBpIdOpt) = Backbone Link Node (BLN) (0x00004100)

wfHwEntry Table

wfHwEntry Entry
  wfHwSlot(i0) = 4 (0x00000004)
  Module Type (wfHwModIdOpt) = DSDE1 (0x00000070)

wfHwEntry Entry
  wfHwSlot(i0) = 5 (0x00000005)
  Module Type (wfHwModIdOpt) = SYNC1 (0x00000010)

wfProtocols Group

  wfIPROTOLoad = 3087007744 (0xb8000000)
  wfDECNETLoad = NO VAUE, NO DEFAULT
  wfATLoad = NO VAUE, NO DEFAULT
  wfXNSLoad = NO VAUE, NO DEFAULT
  wfFIPXLoad = NO VAUE, NO DEFAULT
  wfOSILoad = NO VAUE, NO DEFAULT
  wfX25DTELoad = NO VAUE, NO DEFAULT
  wfX25DCELoad = NO VAUE, NO DEFAULT
  wfVINESLoad = NO VAUE, NO DEFAULT
  wfFRLoad = NO VAUE, NO DEFAULT
  wfRARPLoad = NO VAUE, NO DEFAULT
  wfATMLoad = 402653184 (0x18000000)
  wfDLSLoad = NO VAUE, NO DEFAULT
  wfLNLMLoad = NO VAUE, NO DEFAULT
  wfTelnetLoad = NO VAUE, NO DEFAULT
  wfTFTPLoad = 3087007744 (0xb8000000)
  wfSNMPLoad = 3087007744 (0xb8000000)
  wfTCPLoad = NO VAUE, NO DEFAULT
  wfBGPLoad = NO VAUE, NO DEFAULT
  wfEGPLoad = NO VAUE, NO DEFAULT
  wfOSPFLoad = 2684354560 (0xa0000000)
  wfWPROXYLoad = 402653184 (0x18000000)
  wfLLC2Load = NO VAUE, NO DEFAULT
  wfSMDSLoad = NO VAUE, NO DEFAULT
  wfPPPLoad = NO VAUE, NO DEFAULT
  wfPktCaptureLoad = NO VAUE, NO DEFAULT
  wfFRSWCNGCLoad = NO VAUE, NO DEFAULT
  wfSWPROXYLoad = NO VAUE, NO DEFAULT

--More--
```

Figure 6-5. Sample Configuration File Report

## Generating Configuration File Reports from UNIX

You can generate a configuration file report from the UNIX command line. The format of the UNIX command you use is as follows:

```
smcgrpt [-d] [-t] [-h] [-m] [-W <warning level>] [-r <report template>]
[-c] <configuration file> [[-o] <report file>]
```

where

- d** Includes the MIB default value for any configurable attribute for which you did not specify a value in the configuration file.
- t** Produces the same result as **-d**, except that default values are tagged “[Default].”
- h** Includes raw hexadecimal data in addition to the ASCII translation of that data.
- m** Includes the MIB attribute identifier names in addition to the ASCII translation of those names.
- W <warning level>**

Sets the warning level to indicate types of warnings to include in the report:

- 0 = no warning; this is the default warning level.
- 1 = warn on unrecognized attributes
- 2 = warn on unrecognized records
- 3 = combination of levels 1 and 2
- 4 = warn on unset attributes with no default
- 7 = combination of 3 and 4

**-r** *<report template>*

Specifies the report template file to use. By default, the Report Generator uses a version-specific template based on the version of the configuration file. Template files are in */usr/wf/lib*. The format of the template filename is

*<version>.rpt*

For example, the template file for the version 7.80 configuration file is *7\_80.rpt*.

**-c** *<configuration file>*

Specifies the name of the configuration file from which you want to generate a report.

**-o** *<report file>*

Specifies the pathname of the report file. If you omit this argument, the Report Generator sends the output to *<stdout>*.

## Generating Configuration File Reports from Windows

You can generate a configuration file report from Windows on a PC. To do so, follow these steps:

1. Bring up Windows on your PC.
2. Select File→Run.

The Run window appears.

3. In the Command Line field of the Run window, enter the **smcfrpt** command in the following format:

```
smcfrpt [-d] [-t] [-h] [-m] [-W <warning level>]  
[-r <report template>] [-c] <configuration file> [-o] <report file>  
where
```



- d** Includes the MIB default value for any configurable attribute for which you did not specify a value in the configuration file.
- t** Produces the same result as **/d**, except that default values are tagged “[Default].”
- h** Includes raw hexadecimal data in addition to the ASCII translation of that data.
- m** Includes the MIB attribute identifier names in addition to the ASCII translation of those names.

**-W** *<warning level>*

Sets the warning level to indicate types of warnings to include in the report:

0 = no warning; this is the default warning level.

1 = warn on unrecognized attributes

2 = warn on unrecognized records

3 = combination of levels 1 and 2

4 = warn on unset attributes with no default

7 = combination of 3 and 4

**-r** *<report template>*

Specifies the report template file to use. By default, the Report Generator uses a version-specific template based on the version of the configuration file. Template files are in *c:\wf\lib*. The format of the template filename is

*<version>.rpt*

For example, the template file for the version 7.80 configuration file is *7\_80.rpt*.

**-c** <configuration file>

Specifies the name of the configuration file from which you want to generate a report. If the path to the configuration file is not in your PATH statement, be sure to enter the full pathname.

**-o** <report file>

Specifies the pathname of the report file.

4. Click on OK in the Run window.

## Maintaining an Audit Trail Log

To use the audit trail feature, you must edit the default audit trail configuration file that comes with Site Manager. You edit the file to

- Specify an audit trail community; that is, the routers for which you want to create audit trail log files.
- Specify whether you want auditing on or off. By default, the audit trail feature is off.

The following section describes how to edit the audit trail configuration file.

## Editing the Audit Trail Configuration File

Site Manager provides a default audit trail configuration file, *audit.cfg*. The file resides in */usr/wf* on UNIX workstations, and in *c:\wf* on PCs. You must edit the file to specify the following for each router you want to audit:

- The IP address of the router
- The pathname of the audit trail log file
- The *email* addresses of all users that the audit trail feature should notify if the router's configuration file changes
- Whether the audit trail feature is on or off

To edit the audit trail configuration file, follow these steps:

1. To edit the audit trail configuration file on a UNIX workstation, copy the *audit.cfg* file to a directory where you have write permission.
2. Open *audit.cfg* in a standard text editor.

Figure 6-6 shows the default file.

```
#ROUTER=192.32.156.66
#AUDIT=ON
#FILE=/usr/wf/routerA.adt
#EMAIL=jdoe@wellfleet.com,jsmith@wellfleet.com
```

**Figure 6-6. Default Audit Trail Configuration File**

3. Copy the four default lines in the file and insert them at the end of the file.
4. Delete the pound sign at the beginning of the ROUTER= line. After the equal sign, overwrite the default value with the IP address of the router you want to audit.

For example, you might type

**ROUTER=192.32.156.3**

5. Delete the pound sign at the beginning of the FILE= line. After the equal sign, overwrite the default value with the path and filename for the audit trail log file for the router.

On UNIX workstations, the path for your audit trail log file should point to a directory in your UNIX environment where you have write permission. On PCs, the path is *c:\wf*. The filename should be the router's name (not its IP address) followed by the *.adt* extension.

For example, you might type

**FILE=/usr1/jb/southcape.adt**

6. Delete the pound sign at the beginning of the `EMAIL=` line. After the equal sign, overwrite the default value with the *email* addresses of users you want to notify of configuration changes. Use a comma to separate each *email* address.

For example, you might type

```
EMAIL=pgrant,llantz,odiaz
```

If you do not want to use mail notification, delete the pound sign at the beginning of the `EMAIL=` line and delete the default *email* addresses.

**Note:** The mail notification feature is not available on PCs.

7. Delete the pound sign at the beginning of the `AUDIT=` line. To enable audit trail logging, leave the default value, `ON`. To disable audit trail logging, type **off** after the equal sign.
8. Repeat steps 2 through 6 for each router that you want to audit.
9. Save your changes and exit the file.

You must specify the new pathname for the `AUDIT_PATH` environment variable. For UNIX platforms, this variable should point to the directory where you have placed the modified audit trail configuration file. For example:

```
AUDIT_PATH==/usr1/jake/audit.cfg
```

For the PC, the variable should point to the directory `c:\wf\audit.cfg`. For example:

```
set audit_path=c:\wf\audit.cfg
```

## Viewing an Audit Trail Log File

Once Site Manager creates an audit trail log file and appends information to it, you can open it in any standard text editor. You can also print the file. Figure 6-7 shows a sample audit trail log file.

```
Wed Jul 6 04:57:13 1994
 192.32.156.71 wfSerialPortTable.11=2 ksnw remote.
Wed Jul 6 04:57:13 1994
 192.32.156.71 wfSerialPortTable.11=15 ksnw remote.
Wed Jul 6 04:58:37 1994
 192.32.156.71 wfSoftwareConfig.20=4 ksnw remote.
Wed Jul 6 04:58:37 1994
 192.32.156.71 wfSoftwareConfig.30=5 ksnw remote.
Wed Jul 6 04:58:37 1994
 192.32.156.71 wfSoftwareConfig.30=1 ksnw remote.
Wed Jul 6 04:58:37 1994
 192.32.156.71 wfCSMACDTable.16.2=6 ksnw remote.
Wed Jul 6 04:58:37 1994
 192.32.156.71 wfLineMappingTable.1106102=4 ksnw remote.
Wed Jul 6 04:58:37 1994
 192.32.156.71 wfLineMappingTable.1106102=3 ksnw remote.
Wed Jul 6 04:58:37 1994
 192.32.156.71 wfCSMACDTable.16.2=38 ksnw remote.
Wed Jul 6 04:58:37 1994
 192.32.156.71 wfCircuitNameTable.12=3 ksnw remote.
Wed Jul 6 04:58:37 1994
 192.32.156.71 wfCircuitNameTable.12=4 ksnw remote.
Wed Jul 6 04:58:37 1994
 192.32.156.71 wfCircuitNameTable.12=5 ksnw remote.
Wed Jul 6 04:58:37 1994
 192.32.156.71 wfCircuitNameTable.12=6 ksnw remote.
Wed Jul 6 04:58:37 1994
 192.32.156.71 wfCircuitNameTable.12=7 ksnw remote.
Wed Jul 6 04:58:37 1994
```

**Figure 6-7. Sample Audit Trail Log File**

---

# Chapter 7

## Performing Administrative Functions

For general information about using the Site Manager Administration menu, see “Performing Administrative Functions,” in Chapter 1. For specific information about using buttons, windows, and other Site Manager features, refer to *Using Site Manager Software*.

Use the Administration menu to do the following:

- ❑ Display the Site Manager software release version and router software release version
- ❑ Boot a router
- ❑ Clear the event log
- ❑ Set a router’s date and time
- ❑ Ping a remote device
- ❑ Reallocate memory partitions for a processor module

## Displaying Software Versions

To display the Site Manager version, begin at the Wellfleet Site Manager window or any tools window. Select Help→Site Manager Version. The Version window displays the Wellfleet Site Manager software version. The Description and MIB Version fields in the Wellfleet Site Manager window display the router software version (Figure 7-1).

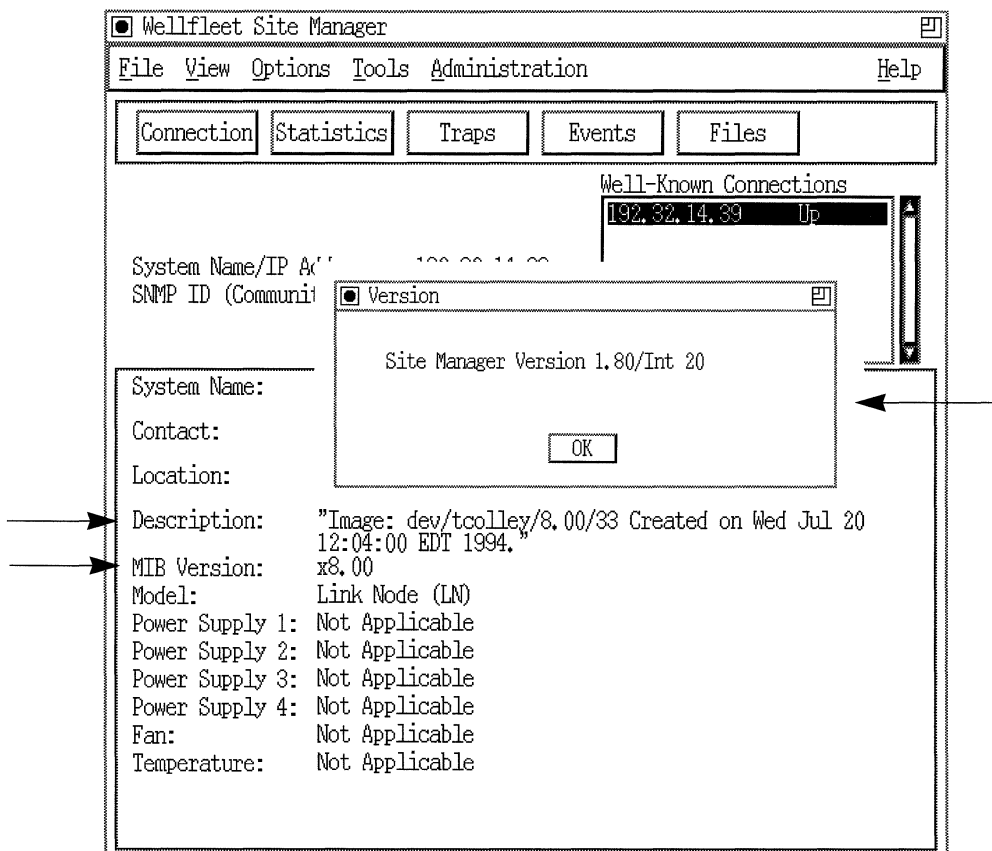


Figure 7-1. Displaying Version Information

Ensure that the version of Site Manager is compatible with the version of the router software (for example: 1.70 and 7.70, or 1.60 and 7.60).

## Router Booting Procedures

Booting a router warm-starts every processor module in the router. Pressing the Reset button on the front panel of the router performs the same procedure.

**Note:** You can use Site Manager to warm-start a router only. To cold-start a router to initiate diagnostic tests, you must physically power off and then power on the router, or use the **diags** command from the Technician Interface (TI). Refer to *Using Technician Interface Software* for more information.

You must boot a router to use a new configuration file or router software image.

### FN/LN/CN Router Boot Prerequisite

The PCMCIA/Floppy switch on the Flash System Controller board of an FN, LN, or CN determines where the router looks for the image (*ace.out*) and configuration file when it is booting. The PCMCIA (Personal Computer Memory Card International Association) position is for memory card boot access, and the Floppy position is for diskette boot access.

You can use Site Manager and the Technician Interface to access both the memory card and diskette files, regardless of the position of this switch. But you cannot override the switch setting when booting. For example, you cannot boot from a diskette if the switch is set in the PCMCIA position.

When you use the Site Manager to boot the router, or specify an image and configuration file in a Technician Interface **boot** command, the



software verifies the file's existence before allowing the boot to take place.

If the PCMCIA/Floppy switch is in the PCMCIA setting, and you boot the router, the following occurs:

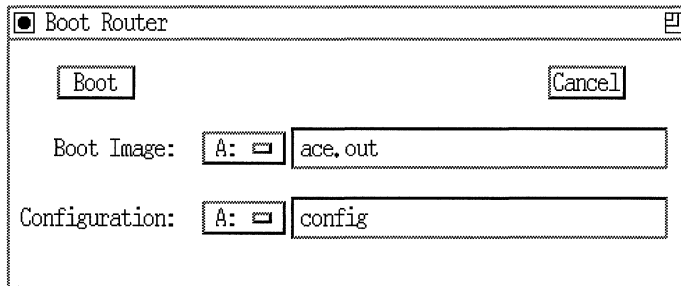
1. The router boots from *1:ace.out* if it is available. If not, it boots from *2:ace.out* if it is available. If both are unavailable, a boot error occurs.
2. The router configures from *1:config* if it is available. If not, it configures from *2:config* if it is available. If both are unavailable, a configuration error occurs.

## Booting a Router

You can boot a Wellfleet router as follows:

1. From the Wellfleet Site Manager window, select Administration→Boot Router.

The Boot Router window shows default filenames for the router software image and the configuration file (Figure 7-2).



**Figure 7-2. Boot Router Window**

You can enter alternative filenames in this window. The Boot Router window also shows two default router volumes for the

router software image and configuration file. You can select alternative volumes as well.

2. To boot from a router software image other than the one displayed, enter an image filename in the Boot Image field.
3. Select the rectangle next to the Boot Image volume. A pop-up window shows the available router volumes.
4. Select the volume where the image specified in step 2 is located. The pop-up window closes and the new volume is displayed.
5. To boot from an alternative configuration file, enter a configuration filename in the Configuration field.
6. Select the rectangle next to the Configuration volume shown. A pop-up window shows the available router volumes.
7. Select the volume where the configuration file specified in step 5 is located. The pop-up window closes and the new volume appears.
8. Click on Boot. A confirmation window appears.
9. Click on OK. Wait a few minutes to give the router time to reboot.
10. To determine if the router booted correctly, select View→Refresh Display from the Wellfleet Site Manager window.

If the router booted correctly, system information appears in the Wellfleet Site Manager window.

The same defaults appear in the Boot Router window after every boot. Depending on the router, the following may appear:

- the name of the router's boot image (The section "Default Filenames" in Chapter 5 lists the names of the boot images for the different Wellfleet routers.)
- config* for all routers
- Volume number for routers using a memory card or Single Inline Memory Module (SIMM)
- Volume indicated by the letter A for routers using a diskette

## Booting a Processor Module

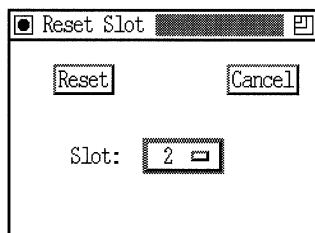
Booting a processor module by using the Reset Slot option warm-starts a single processor module in the router.

The reset option allows you to reboot a processor module with the boot image and configuration file the router is currently using.

You may want to reset a slot to troubleshoot a problem you are having with a router. To reset a slot, follow these directions:

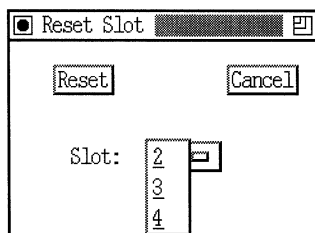
1. From the Wellfleet Site Manager window, select **Administration**→**Reset Slot**.

The Reset Slot window appears (Figure 7-3), showing the router's default slot.



**Figure 7-3. Reset Slot Window**

2. Click the rectangle adjacent to the slot number. A pop-up window shows the available slots (Figure 7-4).



**Figure 7-4. Selecting a Slot**

3. Select the slot where you want to boot a processor module. The pop-up window closes and the slot number you selected appears.
4. Click on Reset. A confirmation window appears.
5. Click on OK.

When you boot a processor module (reset a slot), the following occurs:

- ❑ The operating router software running on the processor module forwards a boot request to the other processor modules.
- ❑ The first processor module to respond to the boot request forwards the boot image resident in its memory.
- ❑ The resetting processor module receives and executes the boot image. At this instant, the router disrupts connectivity to the associated slot and the services provided in that slot. The other processor modules resynchronize their routing tables after the slot fails to receive packets.
- ❑ The resetting processor module completes the boot process and requests a configuration. The first available processor module forwards the configuration resident in its memory.
- ❑ The resetting processor module loads the configuration image and initiates the services provided by the slot, thus re-establishing connectivity. The resetting processor module alerts the other processor modules that it can receive packets.
- ❑ The other processor modules resynchronize their routing tables accordingly.

## Clearing the Event Log

To clear a router's current event log, follow these steps:

1. Select **Administration**→**Clear Log**.

A confirmation window appears.

2. Click on **OK** to delete all the event messages currently stored in the router's memory.

New event messages automatically start filling the event log again.

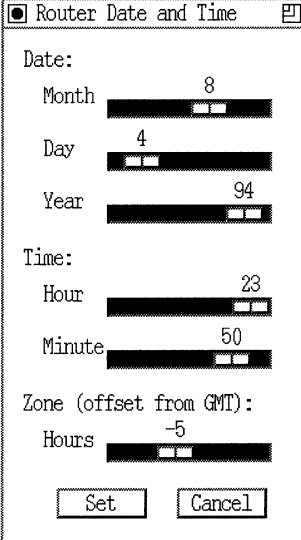
## Setting a Router's Date and Time

You can use the Router Date and Time command to update the router's date, time, and time zone.

To set the time and date recorded on the router, follow these steps:

1. From the Wellfleet Site Manager window, select **Administration**→**Router Date and Time**.

The Router Date and Time window appears (Figure 7-5).



The image shows a window titled "Router Date and Time" with a close button in the top right corner. The window is divided into three sections: "Date:", "Time:", and "Zone (offset from GMT):". Each section contains a label and a slider control with a numerical value displayed to its right. The "Date:" section has "Month" set to 8, "Day" set to 4, and "Year" set to 94. The "Time:" section has "Hour" set to 23 and "Minute" set to 50. The "Zone (offset from GMT):" section has "Hours" set to -5. At the bottom of the window are two buttons: "Set" and "Cancel".

Field	Value
Month	8
Day	4
Year	94
Hour	23
Minute	50
Zone (offset from GMT) Hours	-5

**Figure 7-5. Router Date and Time Window**

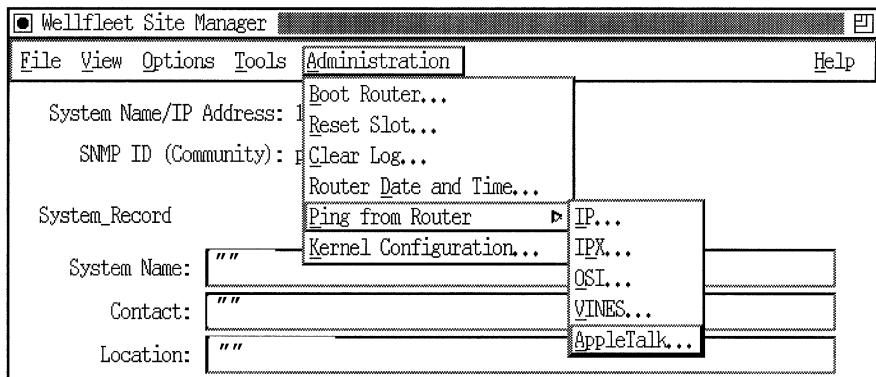
2. Use the slider in each field to specify the correct information. Then click on Set.

The Zone field lets you specify the number of hours your time zone is ahead of or behind Greenwich Mean Time (GMT). Move the slider to the left to select a value behind (-) GMT. Move the slider to the right to select a value ahead of GMT. For example, Eastern Standard Time Zone is 5 hours behind GMT, so you would select -5.

## Pinging a Remote Device

The Ping from Router option lets you test the reachability of a remote device using one of five protocols: IP, IPX, OSI, VINES, and AppleTalk.

You ping from the router by selecting Administration→Ping from Router and then one of the protocols listed in the menu (Figure 7-6).



**Figure 7-6. Selecting Ping from Router Option**

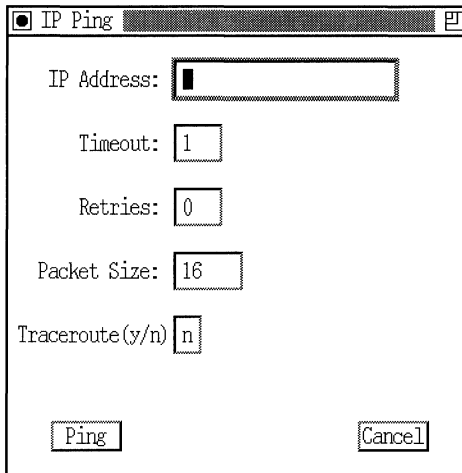
The following sections describe the five ping options.

### IP Ping

When you ping a remote device using the Internet Protocol, the ping program residing on the router sends an Internet Control Message Protocol (ICMP) echo request to the remote address you specified in the IP Ping window. The remote device responds to the router's request if it is reachable. A message window pops up, showing the response or the result of the request.

To send an ICMP echo request to a remote device running IP, proceed as follows:

1. Select Administration→Ping from Router→IP. The IP Ping window appears (Figure 7-7).



**Figure 7-7. IP Ping Window**

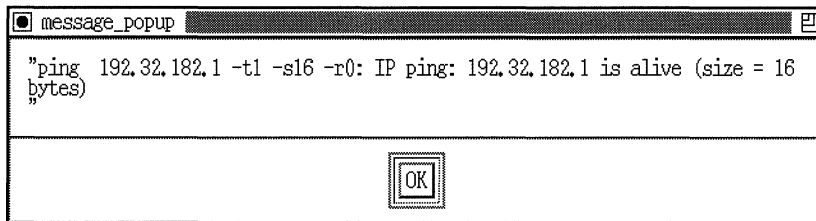
2. In the IP Address field, enter the IP address of the remote device, in dotted decimal notation.
3. In the Timeout field, enter the number of seconds after which you want each ping to time out. The default Timeout is 1 second.  
If the router receives a response to a ping after the ping has timed out, it does not send an “alive” message to Site Manager.
4. In the Retries field, enter the number of successive times the router should repeat the ping. The default for Retries is 0.  
The router does not wait for the timeout before it sends the next ping.
5. In the Packet Size field, enter the number of bytes of data to send with each ping. The default Packet Size is 16.
6. In the Traceroute field, specify **y** (yes), if you want the router to generate a path report that shows the intervening hop addresses to the destination. The default for Traceroute is **n** (no).
7. Click on Ping.



## IP Ping Responses

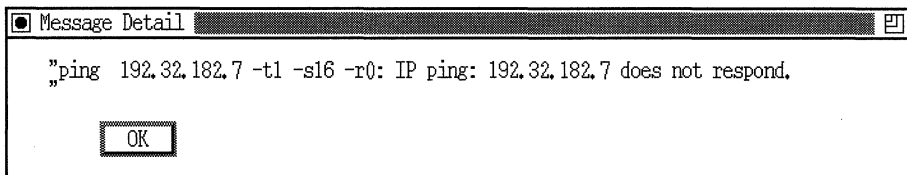
Site Manager displays one of the following messages when you select ping. (If you enter a value other than 0 for Retries, Site Manager displays one of the following messages for the default ping, plus one for each additional ping.)

- An “alive” message appears if the router received an ICMP echo response from the target device within the timeout allowed. The message also provides the size of the test packet. Figure 7-8 shows a sample message.



**Figure 7-8. Ping Is Alive Window**

- A “does not respond” message appears if the media access control (MAC) address of the target device is resolved, but the router did not receive an ICMP echo response from the target device within the timeout allowed. Figure 7-9 shows a sample message.



**Figure 7-9. Ping Does Not Respond Window**

- An “ICMP host unreachable from <y.y.y>” message appears if the router whose address is y.y.y cannot forward the ping request any

further along the path to the target device. IP updates its IP routing or ARP table accordingly. A sample message follows:

```
ping: ICMP host unreachable from 192.32.243.1
```

- ❑ A target address “is unreachable” message appears if the router previously issued an “ICMP host unreachable from <y.y.y>” message. Within 40 seconds, the router receives a subsequent ICMP echo request addressed to the same target device. The ARP times out or the address is not resolved. A sample message follows:

```
ping: 192.32.1.151 is unreachable
```

## IPX Ping

When you issue an Internet Packet Exchange Protocol (IPX) ping, the router sends an IPX configuration request packet to the remote IPX address that you specify. If the remote device is listening on socket number 456h for an IPX configuration request packet, it responds if it can be reached, and Site Manager displays a message indicating that the device “is alive” or “does not respond.”

IPX configuration request packets are typically used to get configuration information from other devices on a NetWare<sup>®</sup> network. However, the router only uses these packets to test the reachability of a remote device that listens for and responds to IPX configuration request packets.

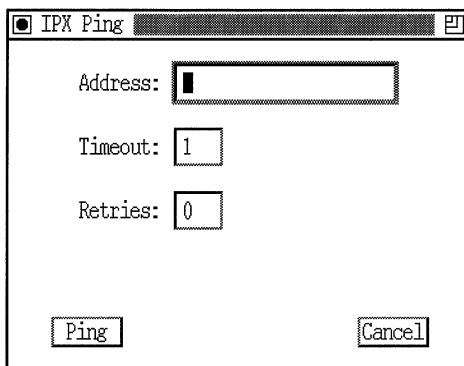
The IPX router will not send or acknowledge IPX configuration request packets addressed to

- ❑ Network 0x00000000 (local network destination) or network 0xFFFFFFFF
- ❑ Host 0x000000000000 or host 0xFFFFFFFFFFFFFFF (broadcast host destination)

The IPX router will only respond to request packets sent directly to one of its interface addresses. If you send a request packet from a router to an IPX interface on that same router, the router does not send the request packet out onto the line. Instead, the router sends the packet internally to the specified interface, which then responds internally.

To send an IPX configuration request packet, proceed as follows:

1. Select Administration→Ping from Router→IPX. The IPX Ping window appears (Figure 7-10).



**Figure 7-10. IPX Ping Window**

2. In the Address field, enter the IPX address of the remote device, in hexadecimal or decimal notation.

An IPX address consists of a 4-byte network address and a 6-byte host address, separated by a period (for example, 0x0000AB12.0x000000CD1234 [leading zero padding is not required]). 0x indicates that the address is in hexadecimal notation.

An IPX address in decimal notation consists of a 4-byte network address and a 6-byte host address, where each byte is a number between 0 and 255, inclusive, and each byte is separated from the next byte by a period (for example, 0.1.23.47.0.0.0.1.2.55).

**Note:** If you issue an IPX ping to an entity on a Token Ring network, you must enter the host portion of the IPX address in byte-swapped (noncanonical) form.

3. In the Timeout field, enter the number of seconds after which each ping times out. The default Timeout is 1 second.

If the router receives a response to a ping after it times out, it does not send an “alive” message to Site Manager.

4. In the Retries field, enter the number of successive times the router should repeat the ping. The default for Retries is 0.

The router does not wait for the timeout before sending the next ping.

5. Click on Ping.

## IPX Ping Responses

Site Manager displays one of the following messages when you issue an IPX ping. (If you enter a value other than 0 for Retries, Site Manager displays one of the following messages for the default ping, plus one for each additional ping.)

- ❑ A target address “is unreachable” message appears if the router cannot find the specified network address in its table of IPX networks. A sample message follows:  

```
IPX ping:  0xAB12.CD1234 is unreachable
```
- ❑ An “alive” message appears if the router receives an IPX reply packet from the target device within the timeout allowed. A sample message follows:  

```
IPX ping:  0xAB12.CD1234 is alive
```
- ❑ A “does not respond” message appears if the IPX address of the target device is resolved, but the router does not receive an IPX reply packet from the target device within the timeout allowed. A sample message follows:  

```
IPX ping:  0xAB12.CD1234 does not respond
```
- ❑ An “invalid parameter specified” message appears if the network or host address is all 0s, all Fs, or not a valid IPX address. A sample message follows:  

```
IPX ping:  invalid parameter specified
```

- ❑ A “resource error” message appears if the router cannot allocate a buffer for the request because no buffers are available. A sample message follows:

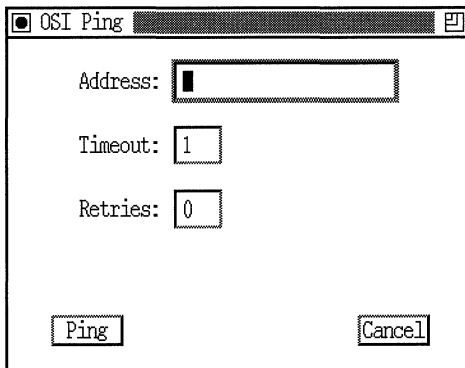
IPX ping: resource error

## OSI Ping

When you issue an OSI ping, the router sends a Connectionless Network Protocol (CLNP) echo request to the remote network service access point (NSAP) address you specify. The remote device responds if it can be reached, and Site Manager displays the response or the result of the request.

To send a CLNP echo request, proceed as follows:

1. Select Administration→Ping from Router→OSI. The OSI Ping window appears (Figure 7-11).



**Figure 7-11. OSI Ping Window**

2. In the Address field, enter the NSAP address of the remote device, in hexadecimal notation.
3. In the Timeout field, enter the number of seconds the router should wait for a response from the remote device. The default Timeout is 1.

4. In the Retries field, enter the number of successive times the router should repeat the ping. The router does not wait for the timeout before it sends the next ping after a response to a previous ping is received. The default for Retries is 0.
5. Click on Ping.

## OSI Ping Responses

Site Manager displays one of the following messages when you issue an OSI ping. (If you enter a value other than 0 for Retries, Site Manager displays one of the following messages for the default ping plus one for each additional ping.)

- ❑ An “alive” message appears if the router receives a CLNP echo response from the target device within the timeout allowed. A sample message follows:  

```
OSI ping: 49000400000a12121200 is alive
```
- ❑ A target address “is unreachable” message appears if the local router cannot find the specified address in its routing table. A sample message follows:  

```
OSI ping: 49000400000a12121200 is unreachable
```
- ❑ A “does not respond” message appears if the NSAP address of the target device is resolved, but the router does not receive a CLNP echo response from the target device within the timeout allowed. A sample message follows:  

```
OSI ping: 49000400000a12121200 does not respond
```
- ❑ An “NSAP address is too short” message appears if the NSAP address is too short. The minimum allowed NSAP address length is 20 hexadecimal characters (10 bytes). A sample message follows:  

```
OSI ping: NSAP address is too short
```
- ❑ An “OSI service is not running” message appears if the OSI service is not enabled on the router. A sample message follows:  

```
OSI ping: OSI service is not running
```

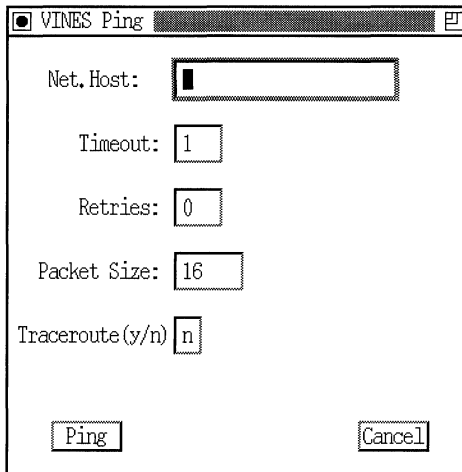
- ❑ A “resource error” message appears if the router cannot allocate a buffer for the request because no buffers are available. A sample message follows:  
OSI ping: resource error
- ❑ A “system error” message appears if the Technician Interface has failed. A sample message follows:  
OSI ping: system error
- ❑ A “<y.y.y.y.y.y.y.y.y.y.y.y.y.y.y.y> is a bad NSAP address” message appears if the NSAP address is more than 20 hexadecimal characters or nonhexadecimal characters.  
y.y.y.y.y.y.y.y.y.y.y.y.y.y.y.y is the address of the CLNP host.  
A sample message follows.  
OSI ping: 123456Z is a bad NSAP address

## VINES Ping

When you issue a VINES ping to a remote VINES device, the router responds if the device can be reached, and Site Manager displays the response or the result of the request.

To send a VINES request to determine the network connectivity of a VINES host, proceed as follows:

1. Select Administration→Ping from Router→VINES. The VINES Ping window appears (Figure 7-12).



**Figure 7-12. VINES Ping Window**

2. In the Network Host field, enter the network and host address of the remote device you want to ping. The Network ID is the 32-bit serial number of the server node that identifies the logical grouping of nodes on a VINES network. The Host address is the 16-bit subnetwork number, which identifies the node within the server node's logical grouping.

**Note:** You can enter the network and host addresses in decimal or hexadecimal format. If you use hexadecimal format, precede each address with the 0x prefix.

3. In the Timeout field, enter the number of seconds after which each ping times out. The default Timeout is 1 second.

If the router receives a response to a ping after it has timed out, it does not send an "alive" message to Site Manager.

4. In the Retries field, enter the number of successive times the router should repeat the ping. The default for Retries is 0.

The router does not wait for the timeout before it sends the next ping.



5. In the Packet Size field, enter the number of bytes of data to send with each ping. The default is 16.
6. In the Traceroute field, specify **y** (yes) if you want the router to generate a path report that displays the intervening hop addresses to the destination. The default is **n** (no).
7. Click on Ping.

## VINES Ping Responses

Site Manager displays one of the following messages when you issue a VINES ping (if you enter a value for Retries, Site Manager displays one of the following messages for the default ping, plus one for each additional ping):

- ❑ An “alive” message appears if the router receives a response from the target device within the timeout allowed. The message also indicates the size of the test packet. A sample message follows:  
VINES ping: 2705682.8003 is alive (size = 16 bytes)
- ❑ A “does not respond” message appears if the address of the target device is resolved, but the system did not receive a response from the target device within the timeout allowed. A sample message follows:  
VINES ping: 2705682.8003 does not respond
- ❑ A target address “is unreachable” message appears if the router cannot find the specified address in its routing table. A sample message follows:  
VINES ping: 2705682.8003 is unreachable
- ❑ A “resource error” message appears if the router cannot allocate a buffer for the request because no buffers are available. A sample message follows:  
VINES ping: resource error

- ❑ An “invalid parameter specified” message appears if you specify an invalid parameter when you issue a VINES ping. A sample message follows:

```
VINES ping: invalid parameter specified
```

- ❑ A “VINES service is not running” message appears if the VINES service is not enabled on the router. A sample message follows:

```
VINES ping: VINES service is not running
```

## AppleTalk Ping

When you issue an AppleTalk ping to a remote AppleTalk device, the router responds if the device can be reached, and Site Manager displays the response or the result of the request.

To send an AppleTalk request to determine the network connectivity of an Appletalk host, proceed as follows:

1. Select Administration→Ping from Router→AppleTalk. The AppleTalk Ping window appears (Figure 7-12).

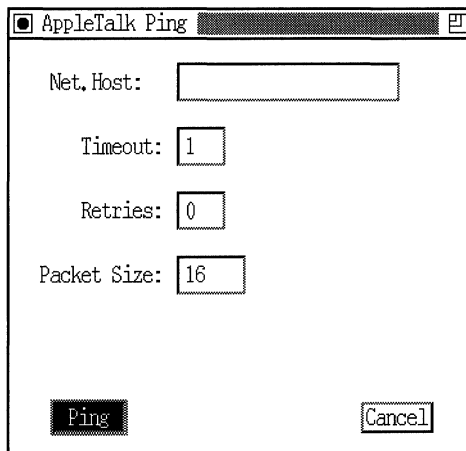


Figure 7-13. AppleTalk Ping Window

2. In the Net.Host field, enter the network address and node ID of the remote device you want to ping. The range of valid values for an AppleTalk network address is from 1 to 65279 (decimal). The range of valid values for an AppleTalk node ID is from 1 to 254 (decimal).

**Note:** You can enter the network address and node ID in decimal or hexadecimal format. (If you use hexadecimal format, precede each address or node ID with the 0x prefix.)

3. In the Timeout field, enter the number of seconds after which each ping times out. The default Timeout is 1 second.

If the router receives a response to a ping after it has timed out, it does not send an “alive” message to Site Manager.

4. In the Retries field, enter the number of successive times the router should repeat the ping. The default for Retries is 0.

The router does not wait for the timeout before it sends the next ping.

5. In the Packet Size field, enter the number of bytes of data to send with each ping. The default is 16 bytes, and the maximum is 585 bytes.
6. Click on Ping.

## AppleTalk Ping Responses

Site Manager displays one of the following messages when you issue an AppleTalk ping (if you enter a value for Retries, Site Manager displays one of the following messages for the default ping, plus one for each additional ping):

- An “alive” message appears if the router receives a response from the target device within the timeout allowed. The message also indicates the size of the test packet. A sample message follows:  
`AppleTalk ping: 2553.217 is alive (size = 16 bytes)`

- ❑ A “does not respond” message appears if the address of the target device is resolved, but the system did not receive a response from the target device within the timeout allowed. A sample message follows:

AppleTalk ping: 2553.217 does not respond

- ❑ A target address “is unreachable” message appears if the router cannot find the specified address in its routing table. A sample message follows:

AppleTalk ping: 2553.217 is unreachable

- ❑ A “resource error” message appears if the router cannot allocate a buffer for the request because no buffers are available. A sample message follows:

AppleTalk ping: resource error

- ❑ An “invalid parameter specified” message appears if you specify an invalid parameter when you issue an AppleTalk ping. A sample message follows:

AppleTalk ping: invalid parameter specified

- ❑ An “AppleTalk service is not running” message appears if the AppleTalk service is not enabled on the router. A sample message follows:

AppleTalk ping: Appletalk service is not running

## Reallocating Memory Partitions for a Processor Module

Using the Site Manager's Kernel Configuration tool, you can reallocate memory for the following routers and processor modules:

AFN	The AFN router contains a single processor module.
AN	The AN router contains a single processor module.
ASN	The ASN router contains a single processor module.
ACE32 (8 MB or greater)	The ACE32 processor module is used in VME-based routers—CN, LN, FN, and ALN.
FRE2	The FRE2 processor module is used in the BLN, BLN-2, and BCN routers.

### Partitioning Overview

Processor modules in a router use three types of memory:

- ❑ Global memory
- ❑ Local memory
- ❑ Nonvolatile RAM (NVRAM)

Global and local memory are separate partitions of a single, contiguous, memory address space. The RAM chips associated with this address space exist physically on each processor module.

The NVRAM for each processor module stores the memory partitioning configuration associated with that module. You cannot partition NVRAM.

---

Note carefully the differences in how NVRAM supports processor modules in PPX- and VME-bus Wellfleet routers:

FRE2 (PPX- based routers)	NVRAM is present on each FRE2 processor module inside the router.	If you move a FRE2 module to another slot in the router, the memory partitioning configuration moves with the FRE2 module to the new slot.
ACE32 (VME- based routers)	For routers using ACE32 processor modules, NVRAM is only present on the SYSCON processor module.	If you move an ACE32 module to another slot in the router, the memory partitioning configuration does <i>not</i> move with the ACE32 module to the new slot. The partitioning remains in effect at the original slot location.

You can specify the amount of local and global memory (that is, the size of the local and global memory partitions) used by a given processor module. Increasing the size of the Global Memory partition automatically decreases the size of the Local Memory partition. The router software ensures that the sum of local and global memory always equals the total amount of memory available on a given processor.

Site Manager does not allow you to configure more than 4 MB of global memory to an ACE32 processor if an ACE25 module resides in the same router. You overcome this constraint in a router with an ACE32 processor by upgrading any ACE25 processors in the same router to ACE32 processors.

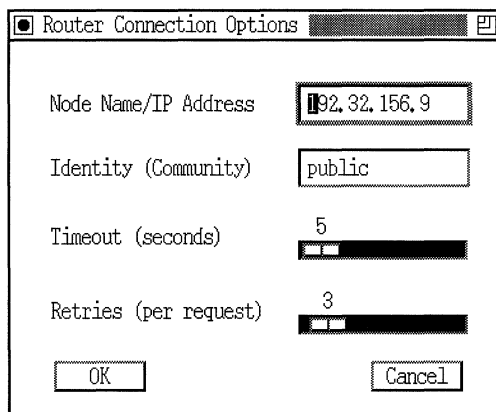
## Repartitioning Global and Local Memory

**Caution:** You should change memory partitioning only at the recommendation of, or under the direction of, your local Bay Networks Help Desk. Under normal router and network operating conditions, you should have no need to modify the default memory partitions established for a processor module. You reallocate processor memory partitions in rare instances, and only for the purpose of network troubleshooting.

Use the following procedure to

- Establish a connection to a router
  - Repartition global and local memory on a processor module
1. From the Wellfleet Site Manager window, select Options→Router Connection.

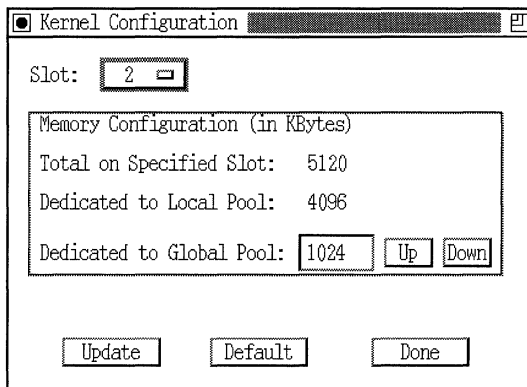
The Router Connection Options window appears (Figure 7-14).



**Figure 7-14. Specifying Router Connection Options**

2. Enter the IP address of a router that requires processor memory repartitioning, and set the Timeout and Retry options. Then click on OK.
3. From the Wellfleet Site Manager window, select Administration→Kernel Configuration.

The Kernel Configuration window appears (Figure 7-15).



**Figure 7-15. Kernel Configuration Window**

**Note:** If the router you are configuring is not an AN, AFN, or ASN, or if the router does not contain an ACE32 or a FRE2 processor module, a window appears with the following message:

No valid modules were found.

The message also means that the processor modules found in the currently connected router are not user-configurable. Such is the case when the Kernel Configuration routine immediately finds only ACE25 or FRE module(s) in the currently connected router.



The Site Manager Kernel Configuration window displays the following information:

<b>Total memory for the specified slot</b>	<b>Total memory displayed depends on the type of processor module.</b>
Memory dedicated to the local pool	Local pool refers to the memory used to manage the router. For example, it contains the statistics, event log, bootable image, and configuration file, along with the routes that IP has learned.
Memory dedicated to the global pool	Global pool refers to the memory dedicated for message buffers.

4. Select the slot of the processor module that requires memory repartitioning.

To do so, click on and hold the Slot button to display all the slots in the router. Then drag the pointer to the desired slot number and release the mouse button.

5. Enter an amount in the Dedicated to Global Pool field.

To add more memory to the global pool, click on the Up button until the desired amount of memory appears, or type a value in the Dedicated to Global Pool field. As you increase the amount of global memory, you decrease the amount of local memory proportionally.

To add more memory to the local pool, click on the Down button until the desired amount of memory appears or type a value in the field.

6. To restart the slot with the new values, click on Update. A confirmation window prompts

Restart slot?

(To reset the memory allocation to the factory-default values, click on Default rather than Update. A message then prompts you to confirm your decision to reset the values.)

7. Click on OK to restart the processor module located in that slot.

Site Manager stores the new configuration in NVRAM and restarts the module (ACE32 or FRE2) or router (AN, AFN, or ASN). This store-and-restart process takes about 10 seconds to complete.

8. Repeat steps 2 through 7 to reallocate memory partitioning on a different processor module, if applicable.

Repeat steps 1 through 7 to reallocate memory partitioning on a processor module in a different router.

9. When you finish, click on Done in the Kernel Configuration window. (The Wellfleet Site Manager window reappears.)



---

# Chapter 8

## Using the Ping MIB

For general information about the Ping management information base (MIB), refer to “Tracking Network Availability and Response Time” in Chapter 1. For specific information about using buttons, windows and other Site Manager features, refer to *Using Site Manager Software*.

To use the Ping MIB to track network availability and response time, you

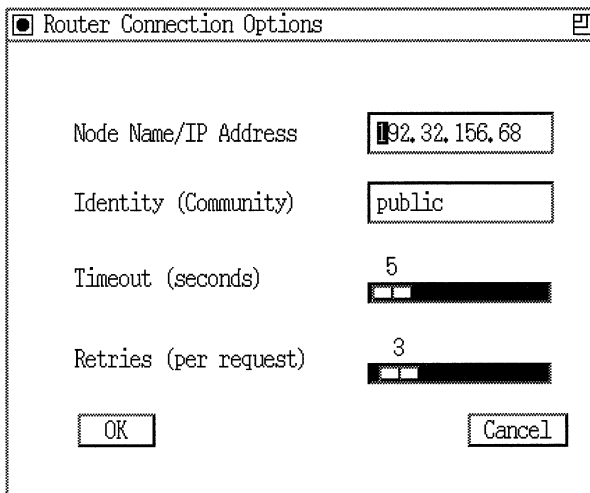
- Configure IP ping requests
- Review IP ping statistics

## Configuring IP Ping Requests

To configure the ping requests for which you want to store the results in the Ping MIB, follow the steps in this section.

**Note:** For Site Manager Release 2.10, the Ping MIB supports IP ping requests only.

1. From the Wellfleet Site Manager main window, select **Options**→**Router Connection**. The Router Connection Options window appears (Figure 8-1).



**Figure 8-1. Router Connection Options Window**

2. In the Node Name/IP Address field, type the IP address of the router you want to configure. Then click on OK.
3. Select **Tools**→**Configuration Manager**, and then select the configuration mode you want (Local File, Remote File, or Dynamic).  
If you choose Local File, the File Selection window appears (Figure 8-2). If you choose Remote File, the Edit Remote Configuration File

window appears, and if you choose Dynamic, the Configuration Manager window appears. This chapter assumes you chose the Local File configuration mode. See *Configuring Wellfleet Routers* for information on using the Remote File and Dynamic configuration modes.

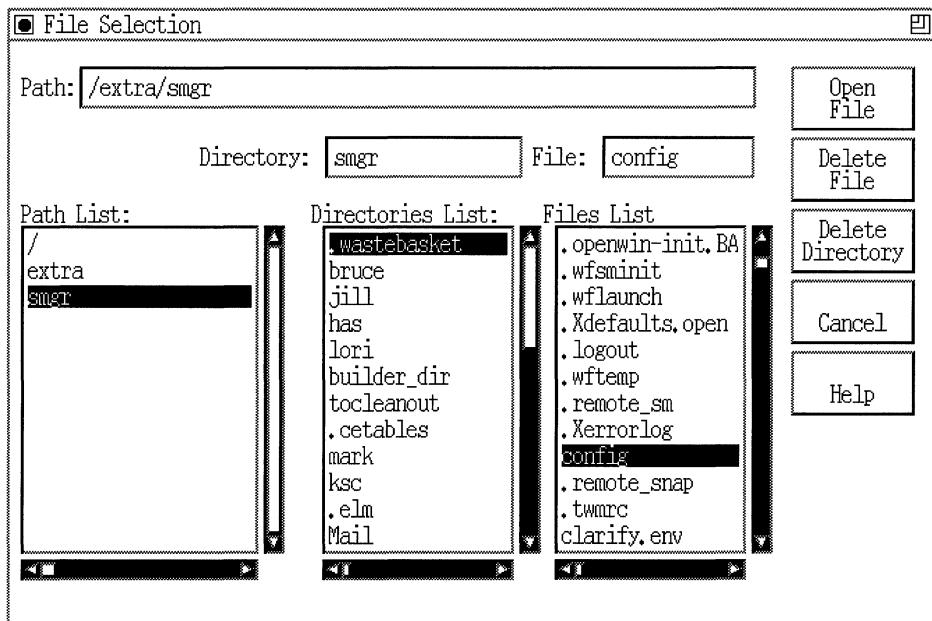
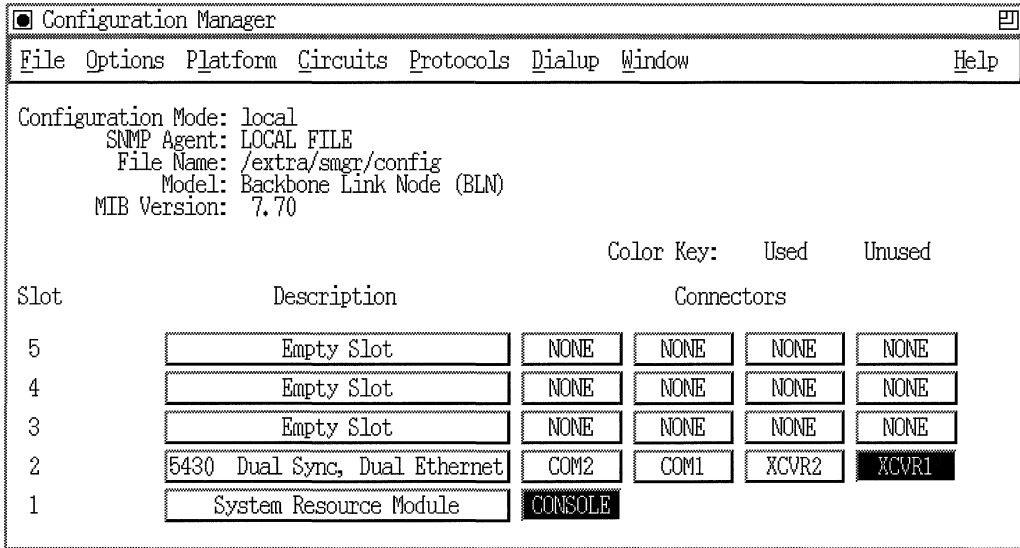


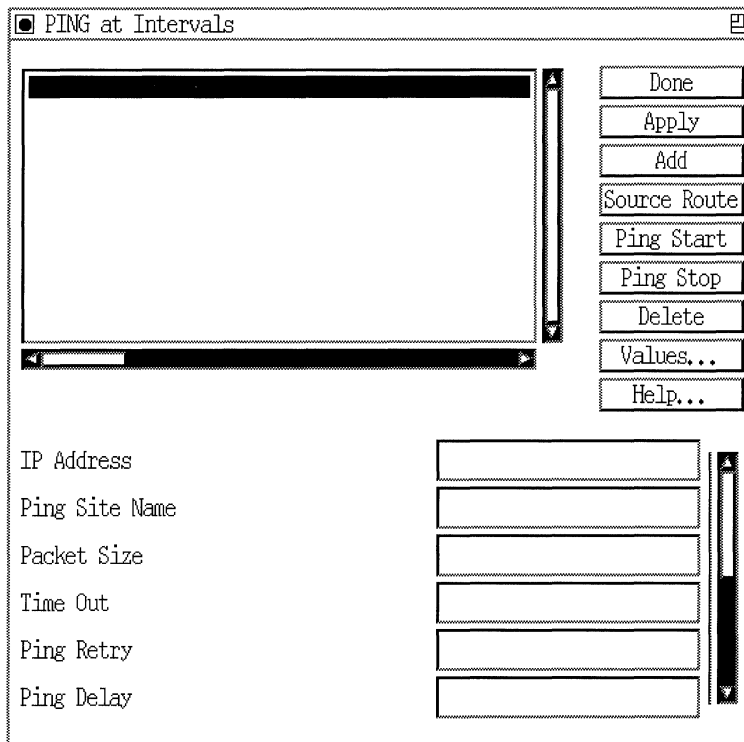
Figure 8-2. File Selection Window

4. Specify the name of the router's configuration file. Then click on Open File to open the file in the Wellfleet Configuration Manager window (Figure 8-3).



**Figure 8-3. Configuration Manager Window**

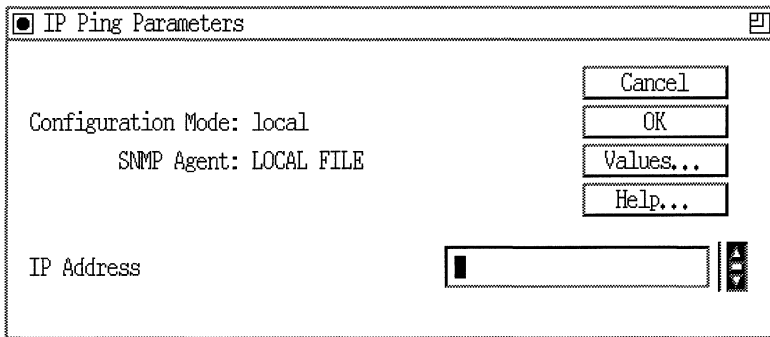
- From the Wellfleet Configuration Manager window, select Platform→Ping at Intervals→IP. The Ping at Intervals window appears (Figure 8-4).



**Figure 8-4. Ping at Intervals Window**

6. Click on the Add button. The IP Ping Parameters window appears (Figure 8-5).





**Figure 8-5. IP Ping Parameters Window**

7. Enter the IP address that you want to ping. Then click on OK.  
You then return to the Ping at Intervals window.
8. In the display area in the window, click on the IP address for which you want to configure the ping request.
9. Enter values for the parameters in the Ping at Intervals window, as described in the next section.
10. Click on Apply.
11. Click on Ping Start to begin pinging the IP address at the interval you specified.  
Site Manager stores the results of the ping requests in the Ping MIB tables.
12. Repeat steps 8 through 11 to configure (and start) ping requests for additional IP addresses.

To stop pinging an address, select the address in the Ping at Intervals window and click on Ping Stop.

## Specifying Values for Ping at Intervals Parameters

Use the information in this section to specify values for the parameters in the Ping at Intervals window. For each parameter, this section provides the following information:

- Default setting
- All valid parameter options
- Function or purpose of the parameter
- Instructions for setting the parameter value
- The Management Information Base (MIB) object ID

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

**Parameter:** **IP Address**

Default: None

Range: Any valid IP address

Function: Specifies the IP address of the device you want to ping.

Instructions: To change the IP address that appears in this field, type the new address in place of the existing one.

MIB Object ID: 1.3.6.1.4.1.18.3.3.2.13.1.1.4

**Parameter: Ping Site Name**

Default: None

Range: Any name you want to correspond to the device from which you are pinging

Function: Serves as descriptive information for your use.

Instructions: Optionally, enter a name for your ping site.

MIB Object ID: 1.3.6.1.4.1.18.3.3.2.13.1.1.17

**Parameter: Packet Size**

Default: 16

Range: 1 to 4850

Function: Specifies the size of the Internet Control Message Protocol (ICMP) packet in bytes.

Instructions: Enter the number of bytes of data that you want to send with each ping.

MIB Object ID: 1.3.6.1.4.1.18.3.3.2.13.1.1.5

**Parameter: Time Out**

Default: 5 seconds

Range: 1 to 65535

Function: Sets the length of time (in seconds) after which an unsuccessful ping expires.

Instructions: Enter a value from 1 through 65535 seconds.

MIB Object ID: 1.3.6.1.4.1.18.3.3.2.13.1.1.6

**Parameter: Ping Retry**

Default: 1

Range: 1 to 65535

**Function:** Specifies the number of successive times to repeat a ping.

**Instructions:** Enter a value from 1 through 65535

**MIB Object ID:** 1.3.6.1.4.1.18.3.3.2.13.1.1.7

**Parameter: Ping Delay**

**Default:** 250 milliseconds

**Range:** 1 to 65535

**Function:** Specifies the amount of time (in milliseconds) to wait between sending ICMP echo packets.

**Instructions:** Enter a value from 1 through 65535

**MIB Object ID:** 1.3.6.1.4.1.18.3.3.2.13.1.1.9

**Parameter: Timer**

**Default:** 0

**Range:** Any integer

**Function:** Specifies the number of minutes that will pass before the ping occurs again.

**Instructions:** Enter a value (in minutes) or enter 0 if you want to initiate the ping request only once.

**MIB Object ID:** 1.3.6.1.4.1.18.3.3.2.13.1.1.11

**Parameter: Trace Route**

**Default:** PING\_NOTRACE

**Range:** PING\_NOTRACE/PING\_TRACE

**Function:** Lets you turn on the Trace Routes features to show the intermediate IP addresses (hops) the ICMP echo packet went through to reach the destination address.

Instructions: Select PING\_TRACE to turn on the Trace Routes feature; otherwise, leave the default, PING\_NOTRACE.

MIB Object ID: 1.3.6.1.4.1.18.3.3.2.13.1.1.8

**Parameter: Source Route**

Default: PING\_NOSOURCEROUTE

Range: PING\_NOSOURCEROUTE/  
PING\_STRICTSOURCEROUTE/  
PING\_LOOSESOURCEROUTE

Function: Lets you override the routing table and specify the alternate addresses you want the ping to go through.

Instructions: Choose the default PING\_NOSOURCEROUTE to use the routing table.

Choose PING\_STRICTSOURCEROUTE if you want to specify all the IP addresses that the ping *must* go through to reach the destination address. You must know all of the addresses for strict source routing to work. With strict source routing, if the ping cannot get from one of the specified addresses to another, the ping will terminate.

Choose PING\_LOOSESOURCEROUTE if you want to specify the addresses that the ping *should* go through to reach the destination address; however, the ping might pass through intermediate hops between the addresses you specify.

If you choose strict or loose source routing, click on the Source Route button to specify the routes. See “Specifying Source Routes,” later in this chapter.

MIB Object ID: 1.3.6.1.4.1.18.3.3.2.13.1.1.12

---

**Parameter: Ping Source Address**

Default: 0.0.0.0

Range: Any valid IP address

Function: Specifies the IP address of the source of the ping request.

Instructions: Optionally, enter the IP address you want to use as the source address of the ping request.

MIB Object ID: 1.3.6.1.4.1.18.3.3.2.13.1.1.13

**Parameter: Ping Type of Service**

Default: 1 (Normal)

Range: 1 through 8, where  
1=normal, routine service  
2=priority  
3=immediate  
4=flash  
5=flash override  
6=critic ecp  
7=internetnetwork control  
8=network control

Function: Specifies the quality of service (service precedence) for handling the ICMP packet.

Instructions: Select 1 for normal service, or enter a value from 2 through 8 to specify a different type of service. Refer to an IP programmer's manual for information on the different types of services.

MIB Object ID: 1.3.6.1.4.1.18.3.3.2.13.1.1.14

**Parameter: Num Hist Buckets Requested**

Default: 1

Range: 1 through 60

Function: If the ping is on a timer (see the Timer parameter), this parameter specifies the number of entries that you want to store in the Ping History table. In other words, you can save information about each ping request sent on the expiration of a timer. (If the ping is not on a timer, the ping generates only one entry in the history table.)

Instructions: Enter a number from 1 though 60 to specify the number of instances of the ping you want to save information about in the Ping History table.

MIB Object ID: 1.3.6.1.4.1.18.3.3.2.13.1.1.15

## Deleting Ping Requests

To remove the results of a ping request from the Ping MIB, follow these steps:

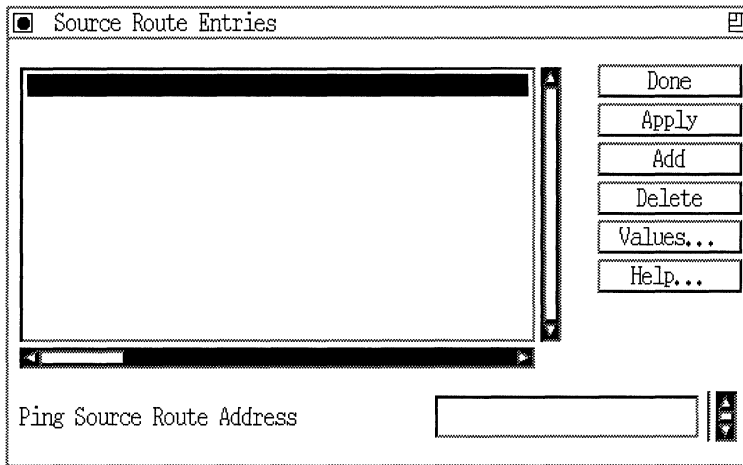
1. In the display area at the top of the Ping at Intervals window, select the ping request you want to delete.
2. Click on Delete.
3. Click on Apply or Done.

Site Manager removes all entries for the selected request from the appropriate tables.

## Specifying Source Routes

If you chose in the Ping at Intervals window to use strict or loose source routing (see the description of the Source Route parameter in the previous section), you must specify the routes that you want to use.

To do so, click on the Source Route button in the Ping at Intervals window. The Source Route Entries window appears (Figure 8-6).

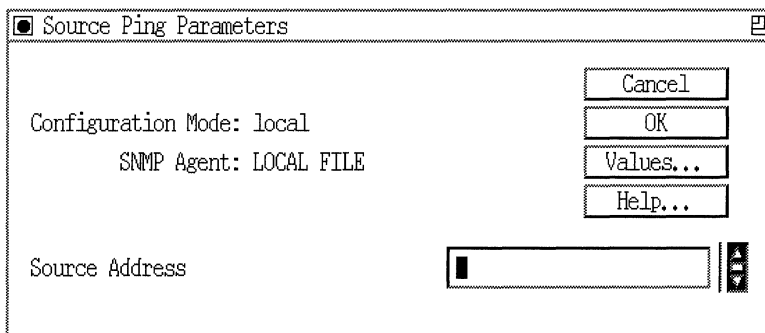


**Figure 8-6. Source Route Entries Window**

Proceed as follows:

1. Click on the Add button.

The Source Ping Parameters window appears (Figure 8-7).



**Figure 8-7. Source Ping Parameters Window**



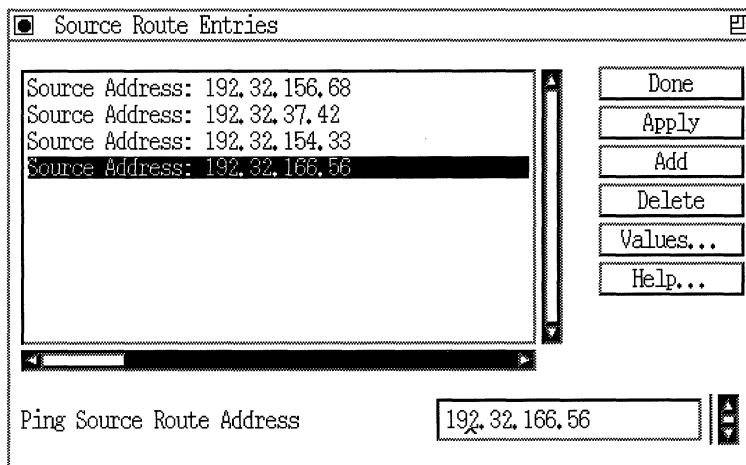
2. In the Source Address field, enter the IP address of the device you want the ping to go through to reach its destination. Then click on OK.

You return to the Source Route Entries window. The IP address you just entered appears in the display area.

3. To enter additional source route addresses, repeat steps 1 and 2.

You can enter as many as eight source route addresses. Figure 8-8 shows the Source Route Entries window with four completed entries.

Be sure to enter the source route addresses in the order that you want the packet to traverse them (from source to destination).



**Figure 8-8. Completed Source Route Entries**

4. Click on Done. You then return to the Ping at Intervals window.

## Changing or Deleting Source Route Addresses

To change an IP address that appears in the Source Route Entries display window, follow these steps:

1. Click on the address you want to change.  
The address appears in the Ping Source Route Address field.
2. Type the new address in place of the old one.
3. Click on **Apply** (to save your changes and remain in the window) or click on **Done** (to save your changes and return to the Ping at Intervals window).

To delete an address from the list of source route addresses, follow these steps:

1. Click on the address in the display area of the Source Route Entries window.
2. Click on **Delete**.
3. Click on **Apply** (to save your changes and remain in the window) or click on **Done** (to save your changes and return to the Ping at Intervals window).

Site Manager removes the entry from the Source Route Entries window and from the Ping MIB tables.

## Reviewing IP Ping Statistics

You can view the information in the Ping MIB using the Statistics Manager in Site Manager. The Statistics Manager provides four default screens that contain information from the Ping MIB. Table 8-1 describes the four screens.

**Table 8-1. Default Ping MIB Statistics Screens**

Screen Name	Contents
<i>pingmain.dat</i>	Information from the main Ping MIB table
<i>pinghist.dat</i>	Information from the Ping history table
<i>pingsrc.dat</i>	Information from the Ping source route table
<i>pingtrc.dat</i>	Information from the Ping trace route table

Refer to Chapter 4 for information on viewing statistics screens.

## Removing Entries from the Ping MIB

You should periodically clear entries from the Ping MIB to prevent the entries from using up too much of your router's memory resources.

To remove entries from the ping tables (main, history, source route, and trace route), follow these steps:

1. In the Ping at Intervals display window, select the IP address of the device whose ping information you want to remove from the ping tables.
2. Click on Delete.

---

# Appendix A

## Using UNIX Commands to Start Site Manager

This appendix provides instructions for directly accessing Site Manager tools. You can use the commands from this appendix only if you use a UNIX computer to run Site Manager.

These commands are optional and are recommended only for experienced Site Manager users.

Table A-1 lists commands you can enter to start Site Manager tools from a UNIX command line. Table A-2 lists options you can enter when you use these commands.

You can add options to the startup commands listed in Table A-1 to override Site Manager default settings. Table A-2 lists the options, the startup commands with which they can be used, their function, the default setting, and an example of how you enter the option.

**Note:** To start the Image Builder tool, type **builder** at the command line. You cannot use the command options listed in Table A-2 with the **builder** command.

To start a Site Manager tool from the UNIX command line, follow these directions:

1. Start the X Window System on your UNIX workstation, if it is not already running.

- 
2. At a command line, enter one of the commands listed in Table A-1 and any number of command options you want from Table A-2.

Append the command with a space and an ampersand (&), so that you can continue to enter commands in the command line window while the tool is running.

For example, you can enter the following command to start the Configuration Manager with a connection to IP address 192.32.4.2 and an SNMP timeout of 10 seconds:

**wfcfg -a 192.32.4.2 -t10 &**

The tool's window appears, displaying the IP address and the community name of the router you specified.

**Table A-1. Site Manager Startup Commands**

<b>Command</b>	<b>Function</b>
<b>wfsm</b>	Starts Site Manager, which establishes a connection with the router.
<b>wfcfg</b>	Starts the Configuration Manager, which establishes a connection with the router.
<b>wflog</b>	Starts the Events Manager.
<b>wftraps</b>	Starts the Trap Monitor.
<b>wfrfs</b>	Starts the Router Files Manager, which establishes a connection with the router. ( <b>Note:</b> You must specify the SNMP agent's IP address using the <b>-a &lt;SNMP Agent IP Address&gt;</b> startup option.)
<b>wfstats</b>	Starts the Statistics Manager, which establishes a connection with the router. ( <b>Note:</b> You must specify the SNMP agent's IP address using the <b>-a &lt;SNMP Agent IP Address&gt;</b> startup option.)
<b>wflaunch</b>	Displays an individual statistics window. ( <b>Note:</b> You must specify the SNMP agent's IP address using the <b>-a &lt;SNMP Agent IP Address&gt;</b> startup option.)

Table A-2. Site Manager Startup Command Options

Start-Up Option	Startup Commands	Function	Default Setting	Sample Use of Option
<b>-c</b> <SNMP Community>	All	Specifies the SNMP community string.	public	<b>wfsm -c Sitemgr</b>
<b>-a</b> <SNMP Agent IP Address>	All	Specifies the SNMP agent's IP address.	none	<b>wfstats -a 192.32.4.2</b>
<b>-m</b> <SNMP MIB Definitions File>	All	Specifies the MIB definitions file in the path <i>/usr/wf/lib</i> .	WFMIB.defs	<b>wfcfg -m mymib.defs</b>
<b>-r</b> <SNMP retry count>	All	Specifies the number of SNMP retries.	3	<b>wfrfs -r 5</b>
<b>-t</b> <SNMP Timeout>	All	Specifies the number of seconds for the SNMP timeout.	5	<b>wflog -t 10</b>
<b>-s</b> <SNMP Destination Port>	All	Specifies the UDP port for the SNMP destination. The default setting causes the application to retrieve the SNMP destination port from <i>/etc/services</i> .	0	<b>wftraps -s 1161</b>

*continued on the next page*

Table A-2. Site Manager Startup Command Options (continued)

Start-Up Option	Startup Commands	Function	Default Setting	Sample Use of Option
<b>-e</b> <SNMP Trap Port>	<b>wfsm wftraps</b>	Specifies the UDP port on which the Trap Monitor should listen for SNMP traps. The default setting causes the application to retrieve the SNMP trap port from <i>/etc/services</i> .	0	<b>wftraps -e 1161</b>
<b>-v</b> <Config Volume>	<b>wfsm wfcfg</b>	Specifies the volume for remote configuration file access.	2	<b>wfsm -v 3</b>
<b>-f</b> </path /> <file>	<b>wfcfg wflaunch</b>	Specifies the configuration or statistics screen filename.	2	<b>wfcfg -f /wf/ file.cfg</b>
<b>-o</b> <Config Mode>	<b>wfcfg</b>	Specifies the configuration mode: local, remote, or dynamic.	local	<b>wfcfg -o remote</b>
<b>-p</b>	<b>wflaunch</b>	Displays an individual statistics window in preview mode (without displaying data).	10	<b>wflaunch - p 1</b>

---

# Appendix B

## Configuring a Router with a New Link Module

When you install (in a Wellfleet router) a replacement link module or net module that is a different type than you removed, you must edit the router's configuration file to reflect this change.

**Note:** Only the Wellfleet ASN router uses net modules.

This appendix describes how to edit a router's configuration file to include the new link module or net module information. This appendix covers the following topics:

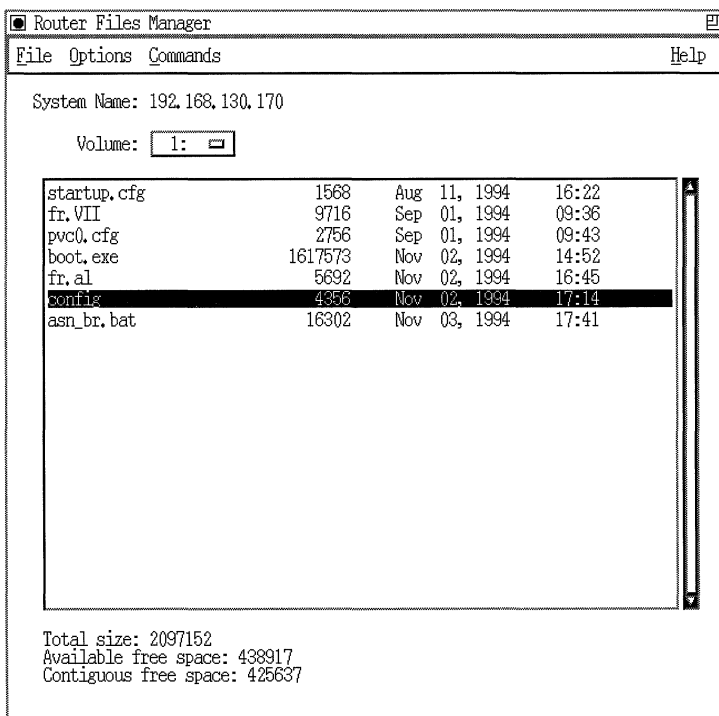
- ❑ Copying the router's configuration file
- ❑ Transferring the configuration file to a local directory
- ❑ Editing the configuration file
- ❑ Transferring the edited configuration file to the router
- ❑ Rebooting the router with the edited configuration file
- ❑ Deleting the old configuration file from the router
- ❑ Renaming the edited configuration file to the default



## Copying the Configuration File

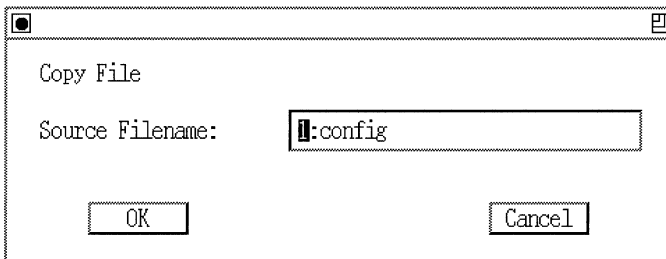
To work with a router's configuration file, you should first create a copy of the file to transfer to your workstation. To copy the file, follow these steps:

1. Connect to the router by selecting Options→Router Connection from the Wellfleet Site Manager window.
2. Enter the router's IP address and click on OK.
3. From the Wellfleet Site Manager window, select Tools→Router Files Manager. The Router Files Manager window appears (Figure B-1).



**Figure B-1. Router Files Manager Window**

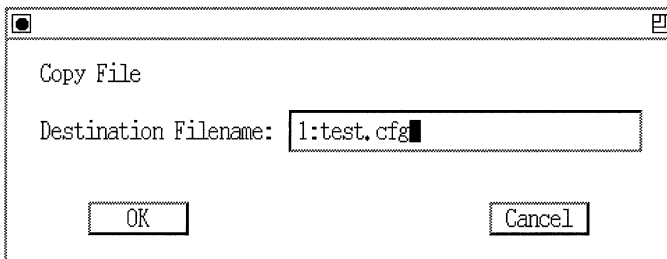
4. Select the router volume where the configuration file resides.
5. Select the configuration file from the list that appears in the Router Files Manager window (Figure B-1).
6. Select **Commands**→**Copy**. The Router Files Manager displays the source filename in a window (Figure B-2).



**Figure B-2. Copy File Window Source Filename**

7. Click on OK.

A window prompts you for the destination filename (Figure B-3).



**Figure B-3. Copy File Window/Destination Filename**

8. Enter a new filename for the copy, such as *test.cfg*.
9. Click on OK. A confirmation window appears.
10. Click on OK.

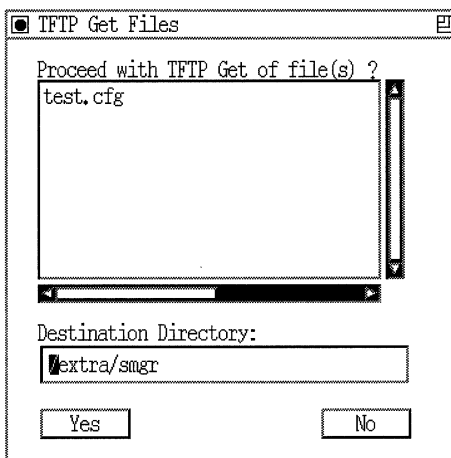
The router copies the source file to the filename and volume you specified.

## Transferring the Configuration File to a Local Directory

To transfer the copy of the configuration file from the router to your Site Manager workstation, follow these steps from the Router Files Manager window:

1. Select the router volume where you stored the copy of the router's configuration file.
2. Select the file; that is, the copy of the configuration file.
3. Select File→TFTP→Get File(s).

A window appears prompting you to confirm your decision to get the configuration file (Figure B-4).



**Figure B-4. TFTP Get File Window**

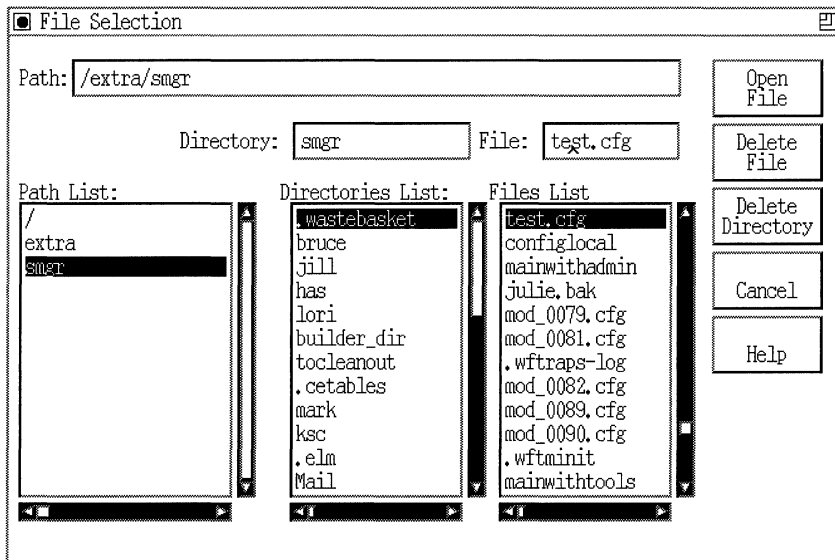
4. In the Destination Directory field, enter the directory where you want to store the file on your Site Manager workstation.
5. Click on Yes to proceed.

The configuration file now resides in a local directory on your Site Manager workstation.

## Editing the Configuration File

Use the Configuration Manager tool to edit the configuration file you retrieved from the router.

1. Select **Tools**→**Configuration Manager**→**Local File**. The File Selection window appears (Figure B-5).



**Figure B-5. File Selection Window**

2. Open the configuration file you transferred to the Site Manager workstation.

You can select the file and the directory path to the file by clicking on the Path List, Directories List, and Files List. The Path List shows the path from the root directory to the current directory. Select from the Path List to move up a directory level.

The Directories List shows the directories available from the current directory. Select from the Directories List to move down a directory level. The Files List shows files available from the current directory.

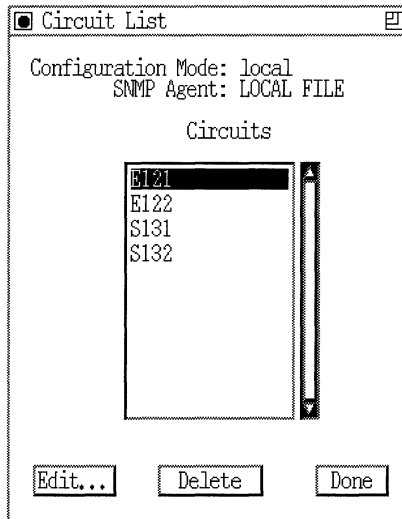
Your current selections appear in the Path, Directory, and File boxes at the top of the window. You can edit this information directly by clicking on the appropriate box and entering a path, directory, or file.

Once you specify the file, click on Open File. The Wellfleet Configuration Manager window appears. Figure B-6 shows the Configuration Manager window for an ASN.

File Options Platform Circuits Protocols Dialup Window Help						
Configuration Mode: local						
SNMP Agent: LOCAL FILE						
File Name: /extra/smgr/test.cfg						
Model: Access Stack Node (ASN)						
MIB Version: 8,10						
					Color Key: Used Unused	
Slot	Module	Description	Connectors			
4	4	Empty Module	NONE	NONE	NONE	NONE
	3	Empty Module	NONE	NONE	NONE	NONE
	2	Empty Module	NONE	NONE	NONE	NONE
	1	Empty Module	NONE	NONE	NONE	NONE
3	4	Empty Module	NONE	NONE	NONE	NONE
	3	Empty Module	NONE	NONE	NONE	NONE
	2	Empty Module	NONE	NONE	NONE	NONE
	1	Empty Module	NONE	NONE	NONE	NONE
2	4	Empty Module	NONE	NONE	NONE	NONE
	3	Empty Module	NONE	NONE	NONE	NONE
	2	Empty Module	NONE	NONE	NONE	NONE
	1	Empty Module	NONE	NONE	NONE	NONE
1	4	Empty Module	NONE	NONE	NONE	NONE
	3	34001 Dual Sync	COM2	COM1	NONE	NONE
	2	34000 Dual Ethernet	NCVR2	NCVR1	NONE	NONE
	1	Empty Module	NONE	NONE	NONE	NONE

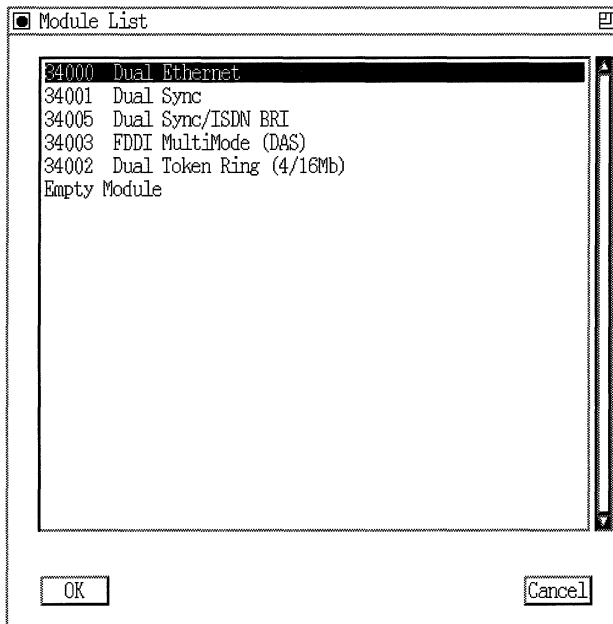
Figure B-6. Wellfleet Configuration Manager Window

3. Select Circuits→Delete Circuit from the Configuration Manager window. The Circuit List window appears (Figure B-7).



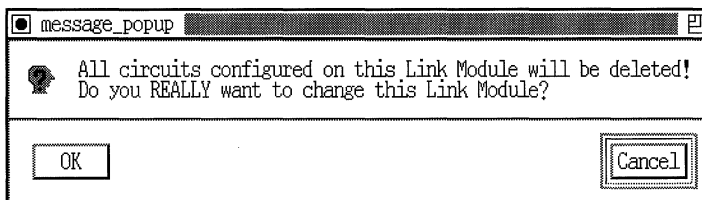
**Figure B-7. Circuit List Window**

4. Select each circuit on the slot (and module for ASNs) in which you swapped the link module or net module. Then click on Delete. A confirmation window appears.
5. Click on Delete again.
6. Click on Done in the Circuit List window when you are done deleting circuits from this list.
7. In the Wellfleet Configuration Manager window, click on the link module or net module you swapped. The Module List window appears (Figure B-8).



**Figure B-8. Module List Window**

8. Select the link module or net module you inserted into the router and click on OK. A confirmation window appears (Figure B-9).



**Figure B-9. Confirming a Circuit Delete Request**

9. Click on OK in the confirmation window.

10. Select File→Save to save your changes. A confirmation window appears (Figure B-10).



**Figure B-10. File Save Confirmation Window**

11. Click on OK in the confirmation window.

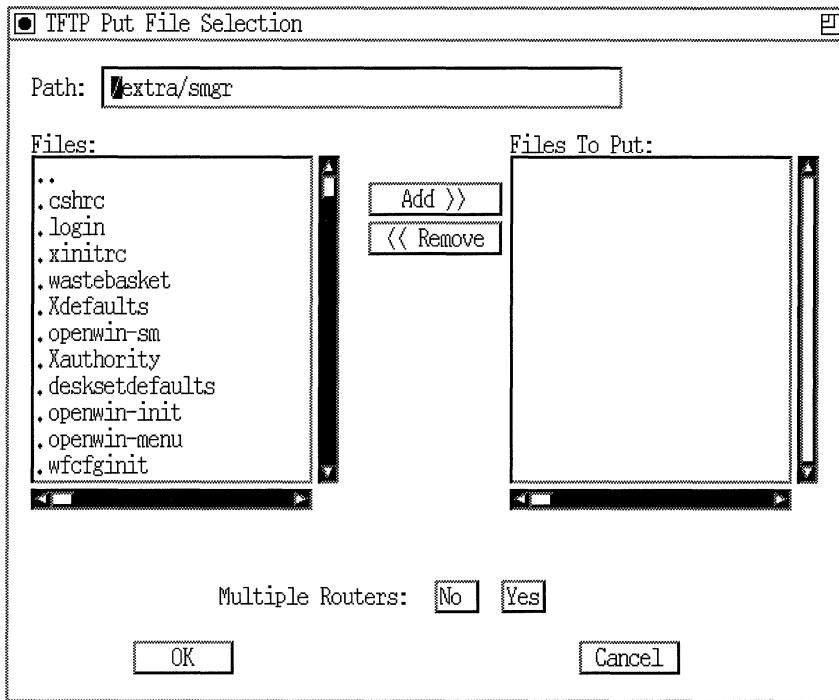
## Transferring the Edited Configuration File to the Router

Use the Router Files Manager to transfer the configuration file back to the router.

1. Select Tools→Router Files Manager to redisplay the Router Files Manager window.
2. Select a router volume.
3. Select File→TFTP→Put File(s).

The TFTP Put File Selection window appears (Figure B-11).





**Figure B-11. TFTP Put File Selection Window**

4. In the Path box, enter the pathname of the directory on the Site Manager workstation that contains the configuration file.  
The files in that directory appear in the Files window.
5. In the Files window, click on the copy of the configuration file you just edited. Then click on Add. The file appears in the Files to Put window.
6. Click on No in the Multiple Routers field.
7. Click on OK.

When the transfer is complete, the TFTP Put File Selection window closes and you return to the Router Files Manager window.

## Rebooting the Router with the Edited Configuration File

Use the Administration menu to reboot the router.

1. From the Wellfleet Site Manager window, select Administration→Boot Router. The Boot Router window appears.
2. Specify the correct volume and boot image.
3. Select the correct router volume and the new configuration file. Then click on Boot. A confirmation window appears.
4. Click on OK in the confirmation window and wait a few minutes.
5. Select View→Refresh Display from the Wellfleet Site Manager window to verify that the router booted correctly.

If the router booted correctly, the new system information appears in the Wellfleet Site Manager window.

If the router did not boot correctly, system information does not appear. In this case, make sure that you followed the procedures described in this chapter.

**Note:** If you have any questions, call your local Bay Networks Help Desk.

## Deleting the Old Configuration File from the Router

Use the Router Files Manager to delete the old configuration file from the router.

1. Select Tools→Router Files Manager.
2. Select the old configuration file from the available volumes.
3. Select Commands→Delete. A confirmation window appears.
4. Click on OK in the confirmation window.

**Note:** If the router uses a memory card, use the Commands→Compact option to compact the memory card.

## Renaming the Edited Configuration File to the Default

By default, the file named *config* is the configuration file used to boot the router. Use the Router Files Manager to change the name of your edited configuration file to the default filename and delete the old file.

1. Select Tools→Router Files Manager.
2. Select the edited configuration file from the list of files in the Router Files Manager window.
3. Select Commands→Copy so that you can copy the new configuration file to a file named *config* on the router.  
A window displays the source filename you selected.
4. Click on OK in the window.  
A window prompts you for the name of the copy.
5. Enter *config* in the window, and then click on OK.  
A confirmation window appears.
6. Click on OK in the confirmation window.
7. Select the edited configuration file.
8. Select Commands→Delete to delete your edited configuration file from the router.  
A confirmation window appears.
9. Click on Yes in the confirmation window.

Your edited configuration file has effectively been renamed to the default filename *config*.

---

# Index

## A

access information about MIB objects, 4-8  
ace.out, 5-5, 7-5  
ACE32, 7-24, 7-25, 7-29  
address  
    filters, 2-20  
        default setting, 2-20  
    MAC, 4-32  
    mask, 4-24  
Administration menu, 1-18, 7-1  
AFN, 5-5, 7-24, 7-29  
afn.exe, 5-5  
agent  
    SNMP  
        configuring, 2-3 to 2-7  
        enabling, 2-14  
        IP address, A-2, A-3  
aliases in debug.al file, 5-6  
ALL trap category, 2-10  
ALN, 5-5, 7-24  
ampersand in UNIX commands, A-2  
AN, 5-5, 7-24, 7-29  
    partitioning media on, 5-3, 5-28 to 5-33  
an.exe, 5-5  
AppleTalk Ping option, 7-21  
ARP, 7-13

## ASCII file

    saving event messages to an, 1-10, 3-10  
    saving statistics to an, 4-29  
    saving trap messages to an, 2-22

## ASN, 5-5, 7-24, 7-29, B-1

    partitioning media on, 5-3, 5-28 to 5-33

## asn.exe, 5-5

## asndiag.exe, 5-5

## audit trail logging, 6-13 to 6-15

## automatic overwrite, 5-9, 5-21

## available free space, 5-4, 5-26

## B

## backing up router files, 5-24, 5-26

## backplane ID, 4-6

## BCN, 7-24

## binary format

    default configuration file, 5-6

    event logs in, 1-10, 3-3, 3-11

    ti.cfg file, 5-7

## BLN, 7-24

## BLN-2, 7-24

## BN, 5-5

## bn.exe, 5-5

## BNX, 5-5

## bnx.exe, 5-5

---

## boot

- command, 5-5
- FN/LN/CN, 7-3
- image, 5-5, 5-6, 7-5, 7-28
- processor module, 7-6
- PROM, 5-6
- router, 7-3, 7-4
- slot, 7-6
- verification, 7-5

builder command, A-1

## C

categories of traps, 2-10

### circuit

- deleting, B-6
- mode
  - statistics screens, 1-13, 4-17, 4-35
- name table, 4-6

### clearing

- counter objects, 4-18
- event log, 3-12, 7-8
- Events Manager window, 3-10
- trap history file, 2-21

CLNP echo request, 7-16

CN, 5-5, 7-24

### code

- entity, 1-8, 2-13
- event, 1-8, 2-13

cold-starting a router, 7-3

### columns

- setting up in statistics screens, 4-32

### commands

- Site Manager startup, A-2

### communities

- SNMP, 2-4

compacting memory, 5-26, B-11

config file, 7-5, B-12

### configuration

- file, 5-6, 5-8
  - audit trail, 6-13
  - copying, B-12
  - deleting, B-11
  - editing, B-5
  - generating report of, 6-2 to 6-13
  - logging changes to, 6-13 to 6-15
  - opening, B-5
  - renaming, B-11
- remote, 5-24
- saving, 2-6

### Configuration Manager

- setting up SNMP on a router, 2-3
- tool, 1-5, A-2
- window, B-6

### configuring

- IP Ping requests for Ping MIB, 8-2 to 8-12
- kernel, 7-24, 7-27
- traps
  - by category, 2-8
  - by entity, 2-11
  - by event type, 2-12

### connection

- router, 2-2, 3-2, 4-3

console in wfSystem MIB object group, 4-6

contiguous free space, 5-4, 5-26

conventions for filenames, 5-8

### copying

- configuration file, B-12
- router files, 5-9 to 5-11, B-2 to B-3

counters, zeroing, 4-18

current screen list, 1-13, 4-12, 4-14

custom screen directories, 1-14, 4-35

customizing statistics screens, 1-13, 4-30 to 4-35

- 
- D**
- date
    - router, 7-8
  - debug messages, 2-11
  - debug.al, 5-6
  - debugging network, 1-13, 5-6
  - decimal format
    - displaying statistics in, 4-32
  - Dedicated to Global Pool field, 7-28
  - default
    - address filter, 2-20
    - button, 7-28
    - configuration file, 5-6, 5-8
    - router software image, 7-4
    - slot, 7-6
    - statistics screens, 1-13, 4-12, 4-14, 4-36
  - deleting
    - circuit, B-6
    - configuration file, B-11
    - IP Ping requests from Ping MIB, 8-12
    - media partition, 5-32
    - router files, 5-12
  - diagnostics
    - command, 7-3
    - image, 5-6
    - PROM, 5-6
    - tests, 7-3
  - diskette
    - router software on, 5-3
  - display
    - Site Manager
      - refreshing, 7-5
    - statistics
      - refreshing, 4-24
  - Display Filters window, 4-23
  - displaying
    - Site Manager software version, 7-2
    - statistics, 4-15
      - custom screens, 4-35
      - volume contents, 5-2
  - dynamic mode
    - performing, 1-2
- E**
- editing
    - audit trail configuration file, 6-13
    - configuration files, B-5
    - SNMP global parameters, 2-15
    - statistics files, 4-37
  - enabling
    - SNMP agent, 2-14
  - entity
    - code, 1-8, 2-13
    - specifying an, 2-11
  - erasing memory cards, 5-26
  - event
    - code, 1-8, 2-13
    - log, 1-4, 7-28
      - clearing, 3-12
      - current, 3-3
      - displaying, 3-3
      - local, 3-6
      - remote, 3-5
    - message
      - record, 3-8
      - saving, 3-10
      - searching for, 3-9
  - Events Manager
    - tool, 1-10, 3-1, A-2
    - window, 1-9, 3-4
      - clearing, 3-10
      - refreshing, 3-10
  - exiting Site Manager, 2-7
-

---

## F

fault messages, 2-11

FDDI tables, 4-6

file

- backup, 5-24, 5-26

- configuration, 5-6, 5-8

  - audit trail, 6-13

  - copying, B-12

  - deleting, B-11

  - editing, B-5

  - generating report of, 6-2 to 6-13

  - opening, B-5

  - renaming, B-11

- copying, 5-9 to 5-11, B-2 to B-3

- deleting, 5-12

- extensions, 4-14, 5-8

- naming conventions, 5-8

- partition, 5-31

- remote configuration modifications, 5-24

- retrieving, 5-18

- statistics, 1-14

  - retrieving, 4-36

- transfer, 5-13

- trap history, 1-4, 2-16

  - clearing, 2-21

filter

- address, 2-20

- by display string, 4-23

- creating, 4-21

- Quick Get retrieval, 4-8

- statistics display, 4-21

- statistics retrieval, 4-22, 4-26

- traps, 2-18 to 2-21

  - by IP address, 2-19

  - by severity, 2-19

Filtering Parameters window, 3-8

Find Text Pattern window, 3-9

FN, 5-5, 7-24

formatting memory cards, 5-27

FRE2, 7-24, 7-25, 7-29

freboot.exe, 5-6

frediag.exe, 5-6

free space, 5-4

## G

generating configuration file report, 6-2 to 6-13

- format options, 6-3

- from UNIX, 6-10

- from Windows, 6-11

- specifying a template, 6-7

GENERIC trap category, 2-10

Get File option, B-4

Get Remote Log File window, 3-5

getting files, 5-18

global memory, 7-28

Greenwich Mean Time, 7-9

## H

Help menu, 7-2

hexadecimal format

- displaying statistics in, 4-32

- entering network and host addresses in, 7-19, 7-22

host

- address, 7-19

- ID, 7-19

- mode

  - running IP in, 5-14, 5-20

---

## I

ICMP echo request, 7-10

### ID

- network, 7-19
- Site Manager workstation, 2-3

### image

- boot, 5-5, 5-6, 7-5, 7-28
- diagnostics, 5-6
- router default, 7-4

information messages, 2-11, 2-19

instances of MIB objects

- retrieving, 4-7

interface drivers, 4-6

### IP

address filters, 2-19

#### Ping

- configuring requests for Ping MIB, 8-2 to 8-12
- deleting requests from Ping MIB, 8-12
- option, 7-10
- specifying source routes, 8-12 to 8-14
- statistics, 8-16
- window, 7-10

routes, 7-28

routing statistics, 4-14

IP address parameter, 8-7

### IPX

address, 7-14

#### Ping

- option, 7-13
- window, 7-14

## K

kernel configuration, 7-24, 7-27

## L

Launch Facility tool, 4-15

line state and traffic, 4-6

### link module

- replacement, B-1
- selecting in Module List window, B-7
- viewing with Configuration Manager, B-6

LN, 5-5, 7-24

Load Local Log File window, 3-6

Load Screen window, 4-34

local memory, 7-28

### log

- audit trail, 6-13 to 6-15
- events, 1-4
  - clearing, 3-12
  - current, 3-3
  - displaying, 3-3
  - local, 3-6
  - remote, 3-5
  - searching for, 3-9

loose source routing, 8-10

## M

MAC address, 4-32, 7-12

### manager

- adding, 2-5
- SNMP, 2-5

### media

- partitioning, 5-3, 5-28 to 5-33



- 
- memory
    - card
      - compacting, 5-26, B-11
      - erasing, 5-26
      - formatting, 5-27
      - router software on, 5-3
    - global, 7-28
    - local, 7-28
    - module
      - router software on, 5-3
    - partitioning, 7-24
  - MIB
    - browser, 4-3, 4-5, 4-6, 4-7, 4-31
    - description, 1-12
    - object groups, 4-6
    - Objects window, 4-4
    - Ping, 1-18, 8-1
      - configuring IP Ping requests, 8-2 to 8-12
      - deleting IP Ping requests, 8-12
      - specifying IP Ping source routes, 8-12 to 8-14
      - viewing IP Ping statistics, 8-16
    - standards, 4-38
    - variables, 5-7
    - Version field, 7-2
    - viewing, 1-11
    - Wellfleet, 1-11, 4-3, 4-5
  - modifying configuration files, 5-24
  - Module List window, B-8
  - monitoring traps, 2-16
  - multiple routers
    - setting up, 5-15
- N**
- net module
    - replacement, B-1
    - selecting in Module List window, B-7
  - NetWare network, 7-13
  - network
    - ID, 7-19
    - management applications, 2-6
    - NetWare, 7-13
    - Token Ring, 7-14
  - NONE trap category, 2-10
  - NSAP address, 7-16, 7-17, 7-18
  - Num Hist Buckets Requested parameter, 8-12
  - NVRAM, 7-24, 7-29
- O**
- object
    - groups, 4-5, 4-6
    - MIB, 4-4
    - type, 4-8
  - opening configuration file, B-5
  - OSI
    - Ping, 7-16
  - overwrite, 5-9, 5-21
- P**
- packet information, 4-6
  - Packet Size parameter, 8-8
  - parameters
    - editing SNMP global, 2-15
    - see also* individual names
  - partitioning media, 5-28 to 5-33
  - partitioning memory, 7-24
-

---

## Ping

- IP, 7-10
  - IPX, 7-13, 7-14
  - MIB, 1-18, 8-1
    - configuring IP Ping requests, 8-2 to 8-12
    - deleting IP Ping requests, 8-12
    - specifying IP Ping source routes, 8-12 to 8-14
    - viewing IP Ping statistics, 8-16
  - OSI, 7-16
  - remote devices, 7-10
  - router, 5-20
  - VINES, 7-18, 7-19, 7-21
- Ping Delay parameter, 8-8, 8-9
- Ping Retry parameter, 8-8
- Ping Site Name parameter, 8-8
- Ping Source Address parameter, 8-11
- Ping Type of Service parameter, 8-11
- polling
  - rate, 1-13, 4-18
  - router, 1-11, 4-17
- ports, A-4
- power supply
  - router, 4-6
- previewing statistics screens, 4-34
- processor module
  - booting, 7-6
  - partitioning memory, 7-24
- PROM, 5-6, 5-7
  - boot, 5-6
  - diagnostic, 5-6
- protocol state information, 4-6
- Put File option, B-9
- putting files on multiple routers, 5-15

## Q

### Quick Get

- Facility window, 4-4, 4-8
  - retrieval filter, 4-8
  - tool, 1-12, 4-3
- quitting Site Manager, 2-7

## R

- Radix field, 4-32
- reallocating memory, 7-24
- real-time display of trap messages, 2-16
- refreshing
  - Events Manager window, 3-10
  - Site Manager window, 7-5
  - statistics, 4-17, 4-24
- remote configuration mode, 5-24
- remote mode
  - description of, 1-2
- renaming configuration file, B-11
- replacement link module or net module, B-1
- report
  - generating from configuration file, 6-2 to 6-13
    - format options, 6-3
    - from UNIX, 6-10
    - from Windows, 6-11
    - specifying a template, 6-7
- reset
  - button, 7-3
  - slot, 7-6
- retrieval filter
  - Quick Get, 4-8
  - statistics, 4-22, 4-26
  - window, 4-27
- Retrieve Request option, 4-12

- 
- retrieving
    - a file, 5-18
    - statistics files, 4-36
  - router
    - backplane ID, 4-6
    - boot procedures, 7-3
    - circuit name table, 4-6
    - cold-starting, 7-3
    - connection, 2-2, 3-2, 4-3
    - date and time, 7-8
    - default software image, 7-4
    - Ping, 5-20, 7-10
    - polling, 4-17
    - power supply, 4-6
    - serial number, 4-6
    - software version, 7-2
    - system record, 4-6
    - temperature, 4-6
    - warm-starting, 7-3
  - Router Date and Time window, 7-8
  - Router Files Manager
    - tool, A-2
    - window, B-2
  - routes, IP, 7-28
  - routing tables, 4-6, 7-7
- S**
- Save Log window, 3-11
  - saving
    - configuration, 2-6
    - event messages, 3-10
    - trap messages, 2-22
  - Screen
    - Builder Facility window, 4-31
    - Builder tool, 1-13, 4-36, 4-37
    - Launch Facility tool, 1-13, 4-15
    - Manager tool, 1-13, 4-13
  - screens
    - default statistics, 4-14
    - designing, 4-30
  - Search Options window, 4-29
  - searching the event log, 3-9
  - Selected Trap Types window, 2-19
  - serial number
    - router, 4-6
  - Set Address Filters option, 2-18
  - severity
    - filtering events by, 3-7
    - messages, 2-19
  - Site Manager
    - Administration menu, 1-18
    - exiting, 2-7
    - restarting from command line, 2-8
    - startup commands, A-2
    - workstation ID, 2-3
  - slot
    - default, 7-6
    - filtering events by, 3-7
    - reset, 7-6
  - SNMP
    - acronym, 1-3
    - adding a Manager, 2-5
    - agent, 1-5, 1-8
      - configuring, 2-3 to 2-7
      - enabling, 2-14
      - IP address, A-2, A-3
      - specifying an entity, 2-11
    - Community List window, 2-4
    - editing global parameters, 2-15
    - Manager List window, 2-5
    - polling, 1-11
    - trap port, 2-6, A-4
  - socket number 456h, 7-13
  - software versions
    - displaying, 7-2
  - Source Route parameter, 8-9, 8-10
-

---

source routes  
specifying for IP Ping requests, 8-12 to 8-14

SPECIFIC trap category, 2-10

start-up commands, A-1, A-2

statistics

- custom-built screens, 1-13, 4-30
- database of screens, 1-13
- default screens, 1-13, 4-12, 4-14, 4-36
- description, 1-11
- designing screens, 4-30
- display filter, 4-21
- displaying, 4-15
- files, 1-14, 4-35
  - editing, 4-37
  - retrieving, 4-36
- filter, 4-21
- generating totals of, 4-33
- IP Ping, 8-16
- IP routing, 4-14
- refreshing screen, 4-17
- retrieval filters, 4-22, 4-26
- updating, 4-17

Statistics Manager

- Quick Set, 1-12
- tool, 1-11, 4-15, A-2
- Tools menu, 1-11
- window, 4-2

strict source routing, 8-10

suggestions

- backing up configuration files, 5-6
- compacting files, 5-26
- customizing statistics screens, 4-32
- diagnosing network problems, 3-8
- filenaming, 5-8
- looking up event messages, 1-10
- managing statistics screens, 4-13
- putting files, 5-9, 5-21
- starting Site Manager from a UNIX command line, A-1

- transferring files, 5-20
- viewing event messages, 1-7

syntax for MIB objects, 4-8

SYSCON, 7-25

system record  
router, 4-6

## T

table mode screens, 1-13, 4-35

Technician Interface, 5-7  
diags command, 7-3

temperature  
router, 4-6

templates for configuration file reports, 6-4

test

- diagnostics, 7-3
- Ping, 5-20, 7-10
- VINES Ping, 7-18, 7-19, 7-21

TFTP, 5-14

ti.cfg, 5-7

time

- router, 7-8

Time Out parameter, 8-8

Timer parameter, 8-9

Toggle button in Filtering Parameters  
window, 3-7

Token Ring network, 7-14

tools

- Events Manager, 1-10, 3-1, A-2
- Launch Facility, 1-13, 4-15
- Screen Builder, 1-13, 4-36, 4-37
- Screen Manager, 1-13, 4-13
- Statistics Manager, 1-11, 4-15, A-2
- Trap Monitor, 2-1

totals

- generating from statistics, 4-33

---

trace messages, 2-11  
Trace Route parameter, 8-9  
transferring  
    configuration file, B-4, B-9  
    files, 5-13  
trap history file, 1-4, 2-16  
    clearing, 2-21  
Trap Monitor tool, 1-5, 2-1, 2-18, A-2  
traps  
    adding, 2-13  
    categories of, 2-10  
    clearing from Trap Monitor window, 2-21  
    configuring  
        by category, 2-8  
        by entity, 2-11  
        by event type, 2-12  
    exceptions lists, 2-12, 2-14  
    filtering, 2-18 to 2-21  
        by IP address, 2-19  
        by severity, 2-19  
    monitoring, 2-16  
    port, 2-6, 2-7, A-4  
    saving, 2-22  
    types, 2-7, 2-18, 2-19  
    viewing, 1-6, 2-16  
troubleshooting, 7-6  
type  
    MIB object, 4-8

## U

UDP, A-4  
    port for traps, 2-6  
UNIX, A-1  
    command line, A-1

## V

Version window, 7-2

viewing trap messages, 2-16  
VINES  
    Ping, 7-18, 7-19, 7-21  
VME, 7-24  
volume  
    displaying contents, 5-2  
    number, 7-5  
    partitioning, 5-3, 5-28 to 5-33

## W

warm-starting a router, 7-3  
warning messages, 2-11, 2-19  
Wellfleet  
    MIB, 1-11, 4-3, 4-5  
wfApplication, 4-5, 4-6, 4-7  
wfHardwareConfig, 4-5, 4-6  
wfLine, 4-5  
wfLines, 4-6  
wfSoftwareConfig, 4-5, 4-6  
wfSystem, 4-5, 4-6  
workstation ID, 2-3

## X

X Window System, A-1

## Z

zeroing counter objects, 4-18





# Bay Networks

The Merged Company of SynOptics and Wellfleet

8 Federal Street  
Billerica, MA 01821



Printed in U.S.A. on Recycled Paper